Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Εργαστήριο Ασφάλειας Συστημάτων

Διπλωματική Εργασία

Συγκριτική ανάλυση της κατάστασης Κυβερνοασφάλειας των χωρών – μελών της ΕΕ

Αποστόλου Μάριος

Μάιος 2014

Επιβλέπων Καθηγητής

Σωκράτης Κάτσικας, Καθηγητής

Πανεπιστήμιο Πειραιώς

Εξεταστική Επιτροπή

Σωκράτης Κάτσικας, Καθηγητής

Πανεπιστήμιο Πειραιώς

Κωνσταντίνος Λαμπρινουδάκης, Αναπληρωτής Καθηγητής

Πανεπιστήμιο Πειραιώς

Χρήστος Ξενάκης, Επίκουρος Καθηγητής

Πανεπιστήμιο Πειραιώς

Πίνακας περιεχομένων

Ακρωνύμια

A

AARNIEC Agenția de Administrare a Rețelei Naționale de Informatică pentru Educație și Cercetare

ABW Agencja Bezpieczeństwa Wewnętrznego

AGPD Agencia Española de Protección de Datos

AIPSI Associazione Italiana Professionisti della Sicurezza Informatica

AKOS Agencija za komunikacijska omrežja in storitve Republike Slovenije

ANACOM Autoridade Nacional de Comunicações

ANETIE Associação Nacional das Empresas das Tecnologias de Informação e Electrónica

ANISP Asociatia Nationala a ISP

ANITEC Associazione Nazionale Industrie Informatica, Telecomunicazioni ed Elettronica di Consumo

ANSPDCP Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal

ANSSI Agence nationale de la sécurité des systèmes d'information

APRITEL Associação dos Operadores de Telecomunicações

ARCEP Autorité de Régulation des Communications Électroniques et des Postes

ARNES Akademska in raziskovalna mreža Slovenije

ATIC Asociatia pentru Tehnologia Informatiei si Comunicatii din Romania

AZOP Agencija za zaštitu osobnih podataka

B

BENELUX Belgium Netherlands Luxembourg

BFV Bundesamt für Verfassungsschutz

BIS Department for Business, Innovation & Skills

BKA Bundeskanzleramt

BMI Bundesministerium für Inneres

BMWi Bundesministeriums für Wirtschaft und Energie

BNetzA Bundesnetzagentur

BND Bundesnachrichtendienst

BSI Bundesamt für Sicherheit in der Informationstechnik

C

CASES Cyberworld Awareness & Security Enhancement Services

CCDoE Cooperative Cyber Defence Centre of Excellence

CCN Centro Nacional Criptológico

CDCOC Chief Directorate Combating Organized Crime

CEZNET Czech Republic's National Research and Education Network

CEENet Central and Eastern European Networking Association

CERT Computer Emergency Readiness Team

CESGCommunications-Electronics Security Group

CFCS Center of Cyber Security

CFSSI Centre de formation à la sécurité des systèmes d'information

CICREST Commission Interministérielle de Coordination des Réseaux et des Services de Télécommunications

CIIP Critical Information Infrastructure Protection

CIP Critical Infrastructure Protection

CIRL Computer Incident Response Center Luxembourg

CIWIN Critical Infrastructure Warning Information Network

CLUSIB Club de la Sécurité de l'Information Belge

CLUSIF Club de la Sécurité de l'Information Français

CLUSIL Club de la Sécurité de l'Information Luxembourg.

CNAIPIC Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche

CNCCS National Advisory Council on Cyber-Security

CNDPD Comissão Nacional de Protecção de Dados

CNI Centro Nacional de Inteligência

CNIL Commission nationale de l'informatique et des libertés

CNP Cuerpo Nacional de Policía

CNPD Commission nationale pour la protection des données

CNPIC National Centre for Critical Infrastructure Protection

CONATEL Comité national des Télécommunications

CONATIC Comité national de l'infrastructure critique

COSIC Computer Security and Industrial Cryptography

CPNI Centre for the Protection of National Infrastructure

CSIRT Computer Security Incident Response Team

CTIE Centre des technologies de l'information de l'Etat

D

DCENR Department of Communications, Energy and Natural Resources

DHS Department of Homeland Security

DIICOT Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism

DKSI State Commission on Information Security

DPA Data Protecton Authority

DSI Data State Inspectorate

E

EA ECNIS Executive Agency Electronic Communication Networks and Information Systems

EFSI Estonian Forensic Science Institute

EGC European Government CERTs

EITS Estonian Information Technology Society

ENISA European Union Agency for Network and Information Security

EPCIP European Programme for Critical Infrastructure Protection

F

FCCU Federal Computer Crime Unit)

FDN Fundacja dzieci Niczyje

FEBELFIN Fédération Financiere belge

FEDICT Federal Public Service Information and Communication Technology

FEDIL Business Federation Luxembourg

FICORA Finnish communications regulatory authority

FIRST Forum of Incident Response and Security Teams

FMV Swedish Defence Materiel Administration

FPSJ Federal Public Service Justice

FRA National Defence Radio Establishment

FSWS Foundation for Social Welfare Services

G

GARR Gruppo per l'Armonizzazione delle Reti della Ricerca

GBFI Garda Bureau of Fraud Investigation

GCC Greek Cybercrime Center

GCHQ Government Communications Headquarters

GDT Grupo de Delitos Telemáticos

GIODO Generalnego Inspektora Ochrony Danych Osobowych

GNS Gabinete Nacional de Segurança.

H

HCPN Haut-commissariat à la Protection nationale

HITB Hat In The BoX

I

IAIK Institute for Applied Information Processing and Communications

ICO Information Commissioner's Office

IDPC Information and Data Protection Commissioner

IISP Institute of Information Security Professionals

IMPACT International Multilateral Partnership Against Cyber Threats

INTECO National Communications Technology Institute

INSCC National Communications Research Institute

ISCOM Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

ISITS International School of IT Security

ISP Internet service provider

ISPAI Internet Service Providers Association of Ireland

ISSA Information Systems Security Association

ITAS IT Asociácia Slovenska

ITL Association of Information Technology and Telecommunications

ITU International Telecommunication Union

IVSZ Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége

L

LACS Laboratory of Algorithmics, Cryptology and Security

LIA Latvijas Interneta Asociācija

LIKTA Latvijas Informācijas un komunikācijas tehnoloģijas asociācija

LVM Liikenne- ja viestintäministeriö

M

MAC Ministerstwo Administracji i Cyfryzacji

MAI Direcţia Generală pentru Comunicaţii şi Tehnologia Informaţiei

MAPN Ministerul Apărării Naţionale

MCA Malta Communications Authority

MCSI Ministerul pentru Societatea Informaţională

MEAC Ministry of Economic Affairs and Communications

MITA Malta Information Technology Agency

MTA Academia Tehnică Militară

MTE Magyarországi Tartalomszolgáltatók Egyesülete

MSB Myndigheten för samhällsskydd och beredskap

MUST Military Intelligence and Security Service

N

NAIH Nemzeti Adatvédelmi és Információszabadság Hatóság

NATO North Atlantic Treaty Organization

NASK Naukowej i Akademickiej Sieci Komputerowej

NBI National Bureau of Investigation

NBF Nemzeti Biztonsági Felügyelet

NBU Národný bezpečnostný úrad

NCAZ Nationales Cyber-Abwehrzentrum

NCCU National Cyber Crime Unit

NCDMB NATO Cyber Defense Management Board

NCIRC NATO Computer Incident Response Center

NCKB Národní centrum kybernetické bezpečnosti

NCSC Nationaal Cyber Security Centrum

NESA National Emergency Supply Agency

NFA National Fraud Authority

NICS Network Information and Computer Security

NIIF Nemzeti Információs Infrastruktúra Fejlesztési Intézet

NORDEFCO Nordic Defense Cooperation

O

OCLCTIC L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication

OCSI Organismo di Certificazione della Sicurezza Informatica

OCSIA Office of Cyber Security & Information Assurance

OSAC Overseas Security Advisory Council

OSCS Österreichische Strategie für Sicherheit Cyber

P

PET Politiets Efterretningstjeneste

PJ Polícia Judiciária

PKI Public Key Infrastructure

PTS Post and Telecom Agency

R

RCB Rządowego Centrum Bezpieczeństwa

RESTENA Réseau Téléinformatique de l'Education Nationale et de la Recherche.

RIA Estonian Information System's Authority

RISO Department of State Information Systems

RRT Respublikos ryšių reguliavimo tarnyba

S

SAM Satiksmes ministrijas

SAMFI Cooperation Group for Information Security

SÄPO Swedish Security Service

SASIB Slovak Association for Information Security

SCSEC Swedish Certification Body for IT Security

SIC Safer Internet Center

SICS Swedish Institute of Computer Science

SICSA Scottish Informatics and Computer Science Alliance

SMILE Security Made In Luxembourg

SRI Serviciul Român de Informaţii

STS Serviciul de Telecomunicatii Speciale

T

TI Trusted Introducer

U

UCL University of London

UKE Urząd Komunikacji Elektronicznej)

UM1 Université Montpellier I

UMIC Agência para a Sociedade do Conhecimento

UOOU Úřad pro ochranu osobních údajů

UTT University of Technology of Troyes

UVNS Ureda Vijeća za nacionalnu sigurnost

UVTP Urada Vlade RS za varovanje tajnih podatkov

V

VAHTI Government Information Security Management Board

W

WARP Warning Advice and Reporting Point

Z

ZSIS Zavod za sigurnost informacijskih sustava

Α

ΑΔΑΕ Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών

ΑΠΔΠΧ Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΑΠΘ Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Γ

ΓΓΕΤ Γενική Γραμματεία Έρευνας και Τεχνολογίας

ΓΕΕΦ Γενικό Επιτελείο Εθνικής Φρουράς

ΓΕΠΔΠΧ Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

ΓΕΡΗΕΤ Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων

ΓΚΗΕ Γραφείου Καταπολέμησης Ηλεκτρονικού Εγκλήματος

Δ

ΔΙΚΥΒ/ΓΕΕΘΑ Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας

Ε

ΕΔΕΤ Ελληνικό Δίκτυο Έρευνας & Τεχνολογίας

ΕΕΤΤ Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων

ΕΚΑ Εθνικός Κανονισμού Ασφάλειας

ΕΥΠ Εθνική Υπηρεσία Πληροφοριών

ΙΤΕ Ίδρυμα Τεχνολογίας και Έρευνας

Κ

ΚΕΑΔ Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο

ΚΕΜΕΑ Κέντρο Μελετών Ασφαλείας

ΚΥΠ Κεντρική Υπηρεσία Πληροφοριών

Σ

ΣΕΠΕ Σύνδεσμος Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδας

Τ

ΤΗΕ Τμήμα Ηλεκτρονικών Επικοινωνιών

ΤΠΕ Τεχνολογίες Πληροφορικής και Επικοινωνιών

ΤΥΠ Τμήμα Υπηρεσιών Πληροφορικής

Υ

ΥΣΕ Υπουργείο Συγκοινωνιών και Έργων

Περίληψη

Σκοπός της εργασίας είναι να μελετηθεί ο τομέας της ασφάλειας του κυβερνοχώρου στην Ε.Ε. προκειμένου να εξαχθούν χρήσιμα συμπεράσματα για τα κράτη μέλη αλλά και περαιτέρω να διαμορφωθούν συγκεκριμένες προτάσεις για τη βελτίωση της Ελλάδας στο συγκεκριμένο τομέα. Αυτό θα επιτευχθεί μέσω της συγκριτικής ανάλυσης δηλαδή της έρευνας όλων των ενεργειών που έχουν πραγματοποιηθεί από τα κράτη - μέλη και της σύγκρισής τους σύμφωνα με συγκεκριμένα κριτήρια. Μέσω της συγκριτικής ανάλυσης θα τονισθούν τόσο τα θετικά σημεία και οι βέλτιστες πρακτικές που χρησιμοποιούνται όσο και τα προβλήματα και τα κενά που υπάρχουν.

Πιο αναλυτικά, στο πρώτο κεφάλαιο μελετώνται οι οδηγοί και οι προτάσεις διεθνών οργανισμών σχετικά με τα μέτρα και τους στόχους κυβερνοασφάλειας που θα πρέπει να έχουν θέσει τα κράτη, με σκοπό την εξαγωγή κριτηρίων για τη δημιουργία ενός πλαισίου σύγκρισης. Στη συνέχεια, με βάση τα κριτήρια που έχουν θεσπιστεί εξετάζεται κάθε χώρα της Ε.Ε. προκειμένου να εντοπιστούν οι δράσεις που συμβάλουν στη βελτίωση του επιπέδου της κυβερνοασφάλειας αλλά και να τονισθούν ενδεχόμενα προβλήματα ή παραλείψεις. Ακολούθως, έχοντας περιγράψει τον τρόπο που κάθε χώρα προσεγγίζει το θέμα, αναδεικνύονται οι χώρες με τις βέλτιστες πρακτικές καθώς και αυτές που υπολείπονται σημαντικά. Τέλος, προτείνονται συγκεκριμένες λύσεις για τη βελτίωση της κατάστασης στην Ελλάδα.

Abstract

The purpose of this paper is to study the field of cybersecurity in the Europian Union in order to draw useful conclusions for each member state and further to develop specific recommendations for Greece improvement in this field. This will be achieved through comparative analysis of research of all actions executed in this area by the member-states and also by comparing them according to specific criteria. Comparative analysis will highlight not only the strengths and best practices but also the problems and the gaps.

More specifically, in the first chapter it is studied international organization's guides and recommendations for actions and targets of cybersecurity that should be set by each country in order to form criteria for a comparison framework. Then, based on the established criteria every EU country will be examined for identifing actions that improve the level of cybersecurity and also to highlight potential problems or omissions. Then, having described how each country approaches the issue it's being highlighted the countries with the best practices and those that fall short. Finally, concrete solutions are being proposed for improving the situation in Greece.

Εισαγωγή

Στις μέρες μας η λειτουργία και η ανάπτυξη των κρατών αλλά και των Διεθνών οργανισμών βασίζεται στη χρήση των Τεχνολογιών Πληροφορικής και Επικοινωνιών (ΤΠΕ). Επίσης κάθε μέρα, εκατομμύρια άνθρωποι βασίζονται στις υπηρεσίες και τις πληροφορίες που συνθέτουν το λεγόμενο κυβερνοχώρο δηλαδή όλες τις μορφές των δικτυωμένων ψηφιακών δραστηριοτήτων. Η καθημερινή ζωή, τα θεμελιώδη δικαιώματα, οι κοινωνικές αλληλεπιδράσεις και οι οικονομίες εξαρτώνται επίσης από τις ΤΠΕ. Η πληροφορία έχει γίνει ένα από τα πιο επιθυμητά αγαθά, ενώ οι σχεδόν απεριόριστες δυνατότητες επικοινωνίας, που δημιουργήθηκαν με τις τελευταίες τεχνολογικές εξελίξεις έχουν αλλάξει οριστικά την καθημερινότητα.

Καθώς η εξάρτηση των κρατών στον κυβερνοχώρο μεγαλώνει, λαμβάνοντας υπόψη το γεγονός ότι οι εφαρμογές και οι λύσεις των ΤΠΕ σχετίζονται άμεσα με την κοινωνικοοικονομική ανάπτυξη, η ασφάλεια του κυβερνοχώρου γίνεται όλο και πιο σημαντική. Οι κυβερνοαπειλές, έχουν επίσης αλλάξει τον τρόπο που οι άνθρωποι θεωρούν την ασφάλεια. Το φαινόμενο της προοδευτικής ψηφιοποίησης κρίσιμων στοιχείων που ευθύνονται για τη λειτουργία των πιο σημαντικών τομέων των σύγχρονων κρατών ευνοεί την εμφάνιση νέων απειλών. Συστήματα ΤΠΕ χρησιμοποιούνται για τη σωστή λειτουργία ζωτικής σημασίας υποδομών, συμπεριλαμβανομένων, μεταξύ άλλων, συστημάτων που σχετίζονται με την ενέργεια, τις υποδομές ύδρευσης και φυσικού αερίου. Οι συνέπειες μιας κυβερνοεπίθεσης με στόχο κρίσιμα περιουσιακά στοιχεία μπορεί να είναι πολύ μεγάλες λόγω των οικονομικών απώλειών, την αποδιοργάνωση και την παράλυση των κρατών. Όλα τα ανωτέρω οδηγούν σε μια κατάσταση όπου οι κυβερνοεπιθέσεις μπορεί να γίνουν ένα ιδιαίτερα επιθυμητό μέσο για κυβερνοτρομοκρατία. Άλλοι κίνδυνοι που σχετίζονται με τον κυβερνοχώρο είναι το έγκλημα στον κυβερνοχώρο, ή/και ο κυβερνοπόλεμος.

Στη Ε.Ε. ισχύουν οι ίδιοι κανόνες, αρχές και αξίες με τη μη διαδικτυακή ζωή, δηλαδή η προστασία των θεμελιωδών δικαιωμάτων, της δημοκρατίας και του κράτους δικαίου. Ο κυβερνοχώρος πρέπει να προστατεύεται από περιστατικά, κακόβουλες δραστηριότητες και καταχρήσεις ενώ οι κυβερνήσεις έχουν σημαντικό ρόλο στη διασφάλιση της ελευθερίας και της προστασίας του ώστε να διατηρηθεί η αξιοπιστία και η διαλειτουργικότητα. Η οικονομία της ΕΕ ήδη επηρεάζεται από τις

δραστηριότητες του κυβερνοεγκλήματος. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν όλο και πιο εξελιγμένες μεθόδους για κλοπή κρίσιμων δεδομένων ενώ η αύξηση της οικονομικής κατασκοπείας και των κρατικά επιχορηγούμενων δραστηριοτήτων στον κυβερνοχώρο αποτελεί μια νέα κατηγορία απειλών για τις κυβερνήσεις και τις επιχειρήσεις της ΕΕ. Επίσης δεδομένου του παγκόσμιου χαρακτήρα του διαδικτύου και του ότι τα δίκτυα και τα πληροφοριακά συστήματα διασυνδέονται, πολλά περιστατικά ασφάλειας υπερβαίνουν τα εθνικά σύνορα και υπονομεύουν τη λειτουργία του συνόλου στη Ε.Ε.

Λόγω αυτών των παραγόντων οι κυβερνήσεις έχουν αρχίσει να αναπτύσσουν την ασφάλεια στον κυβερνοχώρο εισάγοντας τους δικούς τους κανονισμούς, στρατηγικές και μέτρα προστασίας. Ωστόσο σε ευρωπαϊκό και διεθνές επίπεδο, δεν υπάρχει εναρμόνιση του ορισμού της Κυβερνοασφάλειας καθώς η κατανόηση της ασφάλειας αλλά και άλλων βασικών όρων ποικίλλει από χώρα σε χώρα με συνέπεια τις διαφορετικές προσεγγίσεις. Αυτό έχει ως αποτέλεσμα όχι μόνο την αυξημένη δυσκολία για διεθνή συνεργασία αλλά και τη δυσκολία παρατήρησης του επιπέδου προστασίας του κυβερνοχώρου κάθε χώρας. Για το λόγο αυτό διεθνείς οργανισμοί έχουν δημοσιεύσει εγχειρίδια με σκοπό τη δημιουργία κοινών πολιτικών και πρακτικών ασφάλειας. Επίσης η Ε.Ε. μέσω της Στρατηγικής Ασφάλειας του Κυβερνοχώρου της, που δημοσιεύτηκε το 2013, περιγράφει το όραμά της αποσαφηνίζοντας τους ρόλους και τις ευθύνες και καθορίζοντας τις ενέργειες που απαιτούνται για ισχυρή και αποτελεσματική προστασία των δικαιωμάτων των πολιτών στο διαδικτυακό περιβάλλον. Στην συνέχεια της εργασίας μελετώνται οι οδηγοί και οι προτάσεις των διεθνών οργανισμών σχετικά με τα μέτρα και τους στόχους κυβερνοασφάλειας που θα πρέπει να έχουν θέσει τα κράτη, με σκοπό να δημιουργηθεί ένα πλαίσιο σύγκρισης των χωρών-μελών της Ε.Ε. στον τομέα της κυβερνοασφάλειας βάση του οποίου θα εξαχθούν χρήσιμα συμπεράσματα για τα κράτη μέλη και επίσης θα διαμορφωθούν συγκεκριμένες προτάσεις με σκοπό να συνεισφέρουν στη βελτίωση της Ελλάδας στο συγκεκριμένο τομέα.

Κεφάλαιο 1ο

Ανάπτυξη Πλαισίου Μελέτης Κυβερνοασφάλειας

Για τη μελέτη της κατάστασης της Κυβερνοασφάλειας κάθε χώρας απαιτείται η ύπαρξη ενός πλαισίου με συγκεκριμένα κριτήρια βάση των οποίων θα γίνει η αξιολόγηση. Ωστόσο δεν υπάρχει ένα διεθνώς αναγνωρισμένο και αποδεκτό σύστημα μελέτης του επιπέδου Κυβερνοασφάλειας των χώρων. Δημιουργείτε λοιπόν η ανάγκη ανάπτυξης του. Η μεθοδολογία που θα ακολουθηθεί γι' αυτό τον σκοπό είναι η μελέτη των πρακτικών που προτείνονται από διεθνείς οργανισμούς όπως είναι Ο Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύων ENISA, το Κέντρο Αριστείας Κυβερνοασφάλειας (CCDoE)του NATO και η Ε.Ε. Συγκεκριμένα μελετώντας τον Οδηγό Στρατηγικής Κυβερνοασφάλειας του ENISA, το εγχειρίδιο- πλαισίου Κυβερνοασφάλειας του NATO CCDoE και την Στρατηγική Κυβερνοασφάλειας της Ε.Ε., αρχικά θα εντοπιστούν οι προτεινόμενες δράσεις και οι βέλτιστες πρακτικές. Στη συνέχεια θα γίνει προσπάθεια αναγνώρισης των κοινών προτάσεων των τριών οργανισμών καθώς και εξέταση ομαδοποίησης ορισμένων εξ' αυτών με σκοπό την τελική εξαγωγή των κριτηρίων τα οποία θα αποτελούν το πλαίσιο, βάση του οποίου θα μπορεί να μελετηθεί η κατάσταση Κυβερνοασφάλειας κάθε χώρας.

1.1 Οδηγός Στρατηγικής Κυβερνοασφάλειας ENISA [1]

Ο ENISA έχει αναπτύξει αυτό τον οδηγό με στόχο να εντοπίσει τα πιο κοινά και επαναλαμβανόμενα στοιχεία και τις πρακτικές των εθνικών στρατηγικών ασφάλειας του κυβερνοχώρου, στις χώρες της ΕΕ και των τρίτων χωρών. Ο ENISA έχει μελετήσει τις υπάρχοντες στρατηγικές, προκειμένου να προσδιοριστεί η καταλληλόλητα των προτεινόμενων μέτρων για τη βελτίωση της ασφάλειας και της ανθεκτικότητας. Με βάση αυτή την ανάλυση έχει αναπτύξει έναν οδηγό που απευθύνεται σε φορείς χάραξης πολιτικής των κρατών μελών που ενδιαφέρονται για τη διαχείριση των σχετικών διαδικασιών ασφάλειας στον κυβερνοχώρο εντός της χώρας τους. Στο πλαίσιο αυτό έχει προσδιορίσει μια δέσμη συγκεκριμένων δράσεων. Μελετώντας τον οδηγό διακρίθηκαν οι εξής δράσεις:

1.1.1 Θέσπιση του οράματος, του πεδίου εφαρμογής, των στόχων και των προτεραιοτήτων

Ο στόχος μιας στρατηγικής για την ασφάλεια στον κυβερνοχώρο είναι να αυξηθεί η παγκόσμια ανθεκτικότητα και η ασφάλεια των εθνικών περιουσιακών στοιχείων των ΤΠΕ, που υποστηρίζουν κρίσιμες λειτουργίες του κράτους ή της κοινωνίας στο σύνολό της. Η θέσπιση ξεκάθαρων επιμέρους στόχων και προτεραιοτήτων, είναι επομένως υψίστης σημασίας για την επίτευξη αυτού του στόχου. Τα κύρια θέματα που πρέπει να εξεταστούν σε αυτό το βήμα είναι:

1. Ο καθορισμός του οράματος και το πεδίου εφαρμογής σε ένα συγκεκριμένο χρονικό διάστημα (συνήθως 5-10 χρόνια).
2. Ο καθορισμός των υπηρεσιών.
3. Η εκτέλεση μιας ολοκληρωμένης εθνικής αξιολόγησης κινδύνου για τον προσδιορισμό των στόχων και του πεδίου εφαρμογής της στρατηγικής.
4. Η ιεράρχηση των στόχων όσον αφορά τον αντίκτυπο στην κοινωνία, την οικονομία και τους πολίτες.
5. Η καταγραφή της υφιστάμενης κατάστασης.
6. Ο καθορισμός συγκεκριμένων δραστηριοτήτων που θα ανταποκρίνονται στους στόχους της στρατηγικής.

1.1.2 Μελέτη των υφιστάμενων πολιτικών, κανονισμών και δυνατότητων

Πριν από τον ορισμό του στόχου της στρατηγικής Κυβερνοασφάλειας, είναι σημαντικό να γίνει ένας απολογισμός της κατάστασης σε εθνικό επίπεδο. Στο τέλος αυτής της δραστηριότητας θα πρέπει να προσδιορίζονται τα σημαντικά κενά. Η μελέτη θα πρέπει να περιλαμβάνει:

• Την καταγραφή των υφιστάμενων πολιτικών που αναπτύχθηκαν κατά τη διάρκεια των ετών στον τομέα της ασφάλειας στον κυβερνοχώρο (δηλαδή ηλεκτρονικών επικοινωνιών, προστασία των δεδομένων, ασφάλεια των πληροφοριών).

• Τον προσδιορισμό όλων των ρυθμιστικών μέτρων που εφαρμόζονται σε διάφορους τομείς (π.χ. υποχρεωτική αναφορά συμβάντων στον τομέα των ηλεκτρονικών επικοινωνιών).

• Την καταγραφή υπάρχουσων δυνατότητων για την αντιμετώπιση των προκλήσεων Κυβερνοασφάλειας (π.χ. εθνικές ή κυβερνητικές CERT).

• Τον εντοπισμό των υφιστάμενων δεσμευτικών ρυθμιστικών μηχανισμών.

• Την ανάλυση των ρόλων και των αρμοδιοτήτων των υφιστάμενων δημόσιων οργανισμών που ασχολούνται με την ασφάλεια του κυβερνοχώρου ώστε να εντοπιστούν οι αλληλεπικαλύψεις και τα κενά.

1.1.3 Ανάπτυξη μια σαφούς δομής διακυβέρνησης

Προκειμένου να αξιολογηθεί η δομή διακυβέρνησης, οι υπεύθυνοι χάραξης πολιτικής θα πρέπει να οργανώσουν εθνικές ασκήσεις στον κυβερνοχώρο για να δοκιμάσουν το επίπεδο της διοίκησης και ελέγχου και τις επικοινωνίες της υφιστάμενης δομής διακυβέρνησης.

1.1.4 Αναγνώριση και συμμετοχή των ενδιαφερομένων

Για την επιτυχή υλοποίηση της στρατηγικής είναι ζωτικής σημασίας ένας μεγάλος αριθμός εμπλεκόμενων φορέων. Θα πρέπει να ληφθεί υπόψη ο αριθμός των φορέων τόσο στον ιδιωτικό όσο και στον δημόσιο τομέα. Επίσης θα πρέπει να υπολογιστεί ο αριθμός των μελών που δραστηριοποιούνται στην ασφάλεια στον κυβερνοχώρο σε εθνικό επίπεδο.

1.1.5 Καθιέρωση συνεργασίας δημόσιου-ιδιωτικού τομέα

Μια συνεργασία δημόσιου-ιδιωτικού τομέα, καθιερώνει ένα κοινό πεδίο δράσης και στόχων και καθορίζει τους ρόλους και τη μεθοδολογία εργασίας για την επίτευξή τους.

1.1.6 Ανταπόκριση σε συμβάντα

Οι Εθνικές / κυβερνητικές ομάδες CERT διαδραματίζουν βασικό ρόλο στο συντονισμό των αρμόδιων φορέων στη διαχείριση περιστατικών ασφάλειας. Επιπλέον, φέρουν την ευθύνη για τη συνεργασία με τις εθνικές / κυβερνητικές ομάδες άλλων χωρών. Για να εκτελούν σωστά τα καθήκοντά τους, είναι σημαντικό η εθνική στρατηγική Κυβερνοασφάλειας να ενδυναμώνει τις CERT με επαρκείς δυνατότητες.

1.1.7 Καταπολέμηση του εγκλήματος στον κυβερνοχώρο

Η επιτυχής καταπολέμηση του εγκλήματος στον κυβερνοχώρο απαιτεί τη συνεργασία πολλών φορέων και κοινοτήτων. Από την άποψη αυτή, είναι σημαντικό για την αντιμετώπιση και την καταπολέμηση της αύξησης της εγκληματικότητας στον κυβερνοχώρο να υπάρχει κατάλληλη προετοιμασία και συντονισμένη αντίδραση. Τυπικά θέματα που πρέπει να εξεταστούν περιλαμβάνουν τα εξής :

• Προσαρμογή της απαιτούμενης νομοθεσίας και επικύρωση των υφιστάμενων διεθνών συνθηκών.

• Δημιουργία ειδικευμένων εθνικών μονάδων καταπολέμησης του εγκλήματος στον κυβερνοχώρο.

• Εξασφάλιση της συνεχούς και εξειδικευμένης κατάρτισης για την αστυνομία και το προσωπικό δικαστικών αρχών(π.χ. στην ψηφιακή εγκληματολογία).

• Ανάπτυξη των γνώσεων σχετικά με τις αναδυόμενες απειλές που συνδέονται με το έγκλημα στον κυβερνοχώρο μέσω ανταλλαγής πληροφοριών σε εθνικό και σε διεθνές επίπεδο.

• Δημιουργία εναρμονισμένου σύνολου κανόνων για την τήρηση αρχείων.

• Καθιέρωση φόρουμ για την προώθηση της συνεργασίας μεταξύ των διαφόρων φορέων (π.χ. ομάδες CERT).

• Ενθάρρυνση της βιομηχανίας που ειδικεύεται στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

• Ανάπτυξη συνεργασιών με κορυφαίους ακαδημαϊκούς φορείς και φορείς έρευνας στις νέες ψηφιακές εγκληματολογικές τεχνικές.

• Ανάπτυξη συνεργασίας μεταξύ των φορέων του δημόσιου και του ιδιωτικού τομέα για το γρήγορο εντοπισμό εγκλημάτων στον κυβερνοχώρο.

1.1.8 Ευαισθητοποίηση των χρηστών

Η ευαισθητοποίηση σχετικά με τις απειλές στον κυβερνοχώρο, τα τρωτά σημεία και τις επιπτώσεις τους στην κοινωνία έχει γίνει ζωτικής σημασίας. Μέσω της ευαισθητοποίησης, μεμονωμένοι και εταιρικοί χρήστες μπορούν να μάθουν πώς να συμπεριφέρονται στον διαδικτυακό κόσμο και να προστατεύσουν τον εαυτό τους από τους τυπικούς κινδύνους. Δράσεις ευαισθητοποίησης πρέπει να λαμβάνουν χώρα σε συνεχή βάση και να χρησιμοποιούν μια ποικιλία μεθόδων για την επίτευξη ευρύτερων δράσεων ευαισθητοποίησης. Οι δραστηριότητές μπορεί να είναι διάφορες εκδηλώσεις ή παράγοντες όπως για παράδειγμα ενημερώσεις για τις πρόσφατες παραβιάσεις ασφάλειας, απειλές και περιστατικά, νέους κινδύνους, ενημερώσεις της πολιτικής ή / και της στρατηγικής ασφάλειας, νέοι κανονισμοί, πολιτικές κτλ.

1.1.9 Ενίσχυση της κατάρτισης και εκπαιδευτικά προγράμματα

Η ασφάλεια στον κυβερνοχώρο δεν είναι συνήθως ένα ξεχωριστό ακαδημαϊκό θέμα, αλλά μέρος του προγράμματος σπουδών της επιστήμης των υπολογιστών. Η ασφάλεια στον κυβερνοχώρο είναι επίσης ένα συνεχώς μεταβαλλόμενο θέμα που απαιτεί συνεχή κατάρτιση και εκπαίδευση. Οι στόχοι ενός προγράμματος κατάρτισης και εκπαίδευσης θα πρέπει να είναι:

• Ενίσχυση των επιχειρησιακών δυνατοτήτων του υπάρχοντος εργατικού δυναμικού της ασφάλειας των πληροφοριών.

• Ενθάρρυνση των μαθητών να συμμετάσχουν και στη συνέχεια να προετοιμαστούν για να εισέλθουν στον τομέα της ασφάλειας στον κυβερνοχώρο.

• Εθνική πληροφόρηση και εκπαίδευση σε θέματα ασφάλειας και εκπαιδευτικά προγράμματα.

• Προσθήκη μαθημάτων ασφάλειας πληροφοριών σε πανεπιστημιακά προγράμματα σπουδών - όχι μόνο για αυτά που σχετίζονται με την επιστήμη των υπολογιστών, αλλά και σε οποιαδήποτε άλλη επαγγελματική ειδικότητα προσαρμοσμένη στις ανάγκες του εν λόγω επαγγέλματος.

1.1.10 Οργάνωση ασκήσεων για την ασφάλεια στον κυβερνοχώρο

Οι ασκήσεις επιτρέπουν στις αρμόδιες αρχές να δοκιμάσουν υφιστάμενα σχέδια έκτακτης ανάγκης, στοχεύουν σε συγκεκριμένες αδυναμίες, συμβάλλουν στην ενίσχυση της συνεργασίας μεταξύ των διαφόρων φορέων, στον εντοπισμό των αλληλεξαρτήσεων, στις βελτιώσεις στο σχεδιασμό και στη δημιουργία μιας κουλτούρας συνεργατικής προσπάθειας. Οι ασκήσεις στον κυβερνοχώρο είναι σημαντικά εργαλεία για την αξιολόγηση της ετοιμότητας της κοινότητας των φυσικών καταστροφών, των τεχνολογικών αποτυχιών και των επιθέσεων στον κυβερνοχώρο.

1.1.11 Διεθνής συνεργασία

Οι απειλές για την ασφάλεια στον κυβερνοχώρο και τα τρωτά σημεία έχουν διεθνή χαρακτήρα. Η συνεργασία και η ανταλλαγή πληροφοριών με εταίρους στο εξωτερικό είναι σημαντική για την καλύτερη κατανόηση και ανταπόκριση σε ένα διαρκώς μεταβαλλόμενο περιβάλλον απειλών. Τα κυριότερα θέματα που πρέπει να εξεταστούν είναι:

• Η προώθηση της διεθνούς συνεργασίας μέσω της ανταλλαγής πληροφοριών (για παράδειγμα συγκριτική αξιολόγηση, τεχνολογικές γνώσεις και βασικές εκτιμήσεις απειλής).

• Συμμετοχή σε διμερείς, πολυμερείς ή διεθνείς συνθήκες και συμβάσεις (π.χ. Διεθνή Κώδικα Δεοντολογίας για την Ασφάλεια Πληροφοριών, Σύμβαση για το έγκλημα στον κυβερνοχώρο) που σχετίζονται με την ασφάλεια των πληροφοριών.

• Συμβολή στις διεθνείς προσπάθειες για τη σύνταξη των τυποποιημένων διαδικασιών λειτουργίας που πρέπει να χρησιμοποιούνται για την ανταλλαγή πληροφοριών και την ανταπόκριση σε μεγάλες κρίσεις.

• Ενθάρρυνση της συμμετοχής σε περιφερειακές, ευρωπαϊκές και διεθνείς ασκήσεις ως μέσο για τη στήριξη της συνεργασίας με τους στρατηγικούς εταίρους.

1.2 Εγχειρίδιο - πλαίσιο Κυβερνοασφάλειας NATO CCDoE [2]

Το εγχειρίδιο απευθύνεται σε ενδιαφερόμενα μέρη στα κράτη μέλη του ΝΑΤΟ ή χώρες-εταίρους του ΝΑΤΟ, συμπεριλαμβανομένων των ηγετών, νομοθετών, των ρυθμιστικών αρχών και των παρόχων υπηρεσιών διαδικτύου με σκοπό να χρησιμεύσει ως οδηγός για να αναπτύξουν και να βελτιώσουν τις εθνικές πολιτικές, νομοθετικές και κανονιστικές διατάξεις και άλλες πτυχές που σχετίζονται με την εθνική ασφάλεια στον κυβερνοχώρο. Το εγχειρίδιο πραγματεύεται ποικίλες πτυχές και δυνατότητες που πρέπει να εξεταστούν κατά τη διάρκεια της εκπόνησης μιας εθνικής στρατηγικής για την ασφάλεια στον κυβερνοχώρο, παρουσιάζει διαφορετικές δυνατότητες προσεγγίσεων, και προβάλλει τις καλές πρακτικές στο πλαίσιο της εθνικής ασφάλειας στον κυβερνοχώρο. Από τη μελέτη του οδηγού αναγνωρίσθηκαν οι εξής προτεινόμενες δράσεις:

1.2.1 Στρατιωτικές Επιχειρήσεις Κυβερνοασφάλειας

Οι λειτουργίες ασφαλείας στον κυβερνοχώρο εντός του στρατιωτικού τομέα διαφέρουν από χώρα σε χώρα. Γενικά, η δράση αυτή μπορεί να περιλαμβάνει ένα πολύ ευρύ φάσμα επιμέρους δράσεων και όχι το σύνολο εκείνων που θα εφαρμόζονται σε κάθε χώρα. Πρώτα, περιλαμβάνει την «άμυνα στον κυβερνοχώρο» - την προστασία των συστημάτων ΤΠΕ, συνήθως με μια CERT / CSIRT (Computer Emergency Response Team / Computer Security Response Team). Δεύτερον, μπορεί να περιλαμβάνει επιλογές για τις πράξεις στρατηγικής στον κυβερνοχώρο. Τρίτον, μπορεί να περιλαμβάνει ειδικές ικανότητες μάχης στον κυβερνοχώρο - δηλαδή αυτές που είναι ικανές να αναπτυχθούν μέσα σε ένα επιχειρησιακό και τακτικό περιβάλλον. Τέλος, μπορεί να περιλαμβάνει προσπάθειες εκσυγχρονισμού των πιο παραδοσιακών στρατιωτικών δυνατοτήτων.

1.2.2 Καταπολέμηση του εγκλήματος στον κυβερνοχώρο

Η καταπολέμηση του εγκλήματος στον κυβερνοχώρο περιλαμβάνει ένα ευρύ σύνολο οργανισμών. Το υπουργείο δικαιοσύνης πρέπει να συμμετάσχει σε εθνικό και διεθνές επίπεδο στην ανάπτυξη και τη συντήρηση της νομοθεσίας για την ασφάλεια στον κυβερνοχώρο. Ομοίως, ένα υπουργείο πρέπει να διαχειρίζεται τις ειδικευμένες αστυνομικές δυνάμεις. Η Πρόληψη της εγκληματικότητας στον κυβερνοχώρο είναι επίσης ένα πολυεπίπεδο θέμα. Είναι ένα οργανωτικό ζήτημα που αφορά όλες τις δημόσιες υπηρεσίες και οργανισμούς. Στο επιχειρησιακό / τακτικό επίπεδο, μια

λειτουργική μονάδα της αστυνομίας είναι απαραίτητη για τη διερεύνηση του εγκλήματος στον κυβερνοχώρο, την επιτήρηση και την δίωξη των εγκληματιών του κυβερνοχώρου. Πρέπει επίσης να υπάρχουν διασυνδέσεις και ανταλλαγές πληροφοριών με ξένες αστυνομικές δυνάμεις, είτε βάσει διμερούς συνεργασίας, είτε μέσω των μονάδων καταπολέμησης του εγκλήματος στον κυβερνοχώρο των διεθνών αστυνομιών οργανισμών όπως η Europol και η Interpol. Για να είναι αποτελεσματική, η οργάνωση της αστυνομίας μπορεί να συνδεθεί με την εθνική ομάδα CERT και άλλες τέτοιες ομάδες.

1.2.3 Διακυβέρνηση του Διαδικτύου και Διπλωματία του κυβερνοχώρου

Διπλωματία του κυβερνοχώρου είναι η χρήση των διπλωματικών διεργασιών ενός κράτους στον τομέα της παγκόσμιας ασφάλειας στον κυβερνοχώρο. Συγκεκριμένα, αναφέρεται σε πολυμερή ή διμερή δραστηριότητα που αποσκοπεί στη διαχείριση των σχέσεων των κρατών στον κυβερνοχώρο. Η διπλωματία στο κυβερνοχώρο μοιάζει με τις παραδοσιακές μορφές διπλωματίας, όπως ο έλεγχος των όπλων και η καταπολέμηση των απειλών.

1.2.4 Διαχείριση Κρίσεων Κυβερνοασφάλειας και Προστασία Κρίσιμων Υποδομών

Είναι απαραίτητη μια εθνική ομάδα αντιμετώπισης έκτακτων περιστατικών Κυβερνοασφάλειας (CERT / CSIRT). Σοβαρά επεισόδια στον κυβερνοχώρο μπορεί να οδηγήσουν σε σημαντικές διαταραχές και διάλυση της κοινωνίας. Περιστατικά, για παράδειγμα, κρίσιμων τομέων των υποδομών (όπως η ενέργεια και οι τηλεπικοινωνίες), μπορεί να έχουν σοβαρές επιπτώσεις σε εθνικό επίπεδο, αν καταστραφούν κρίσιμες λειτουργίες του κυβερνοχώρου. Επίσης είναι απαραίτητη η ανάπτυξη ή η υιοθέτηση προτύπων ασφάλειας των πληροφοριών τόσο στον δημόσιο όσο και στον ιδιωτικό τομέα.

1.2.5 Συντονισμός

Οι δράσεις συντονισμού σε θέματα ασφάλειας στον κυβερνοχώρο θεωρείται επίσης ότι συμβάλλουν στην εθνική διακυβέρνηση για την ασφάλεια στον κυβερνοχώρο.

1.2.6 Ανταλλαγή πληροφοριών και προστασία των δεδομένων

Αρκετές δραστηριότητες έχουν ως επίκεντρο την ανταλλαγή πληροφοριών και την προστασία των δεδομένων. Η ανταλλαγή πληροφοριών και προστασίας των δεδομένων έχει κύριο στόχο της την πρόληψη, την αντιμετώπιση και την αποκατάσταση. Ανταλλαγές πληροφοριών θα πρέπει να υπάρχουν μεταξύ οργανισμών, όπως ομάδες

διαχείρισης εθνικών κρίσεων και από οργανισμούς έρευνας. Η προστασία των δεδομένων πρέπει να εξετάζεται σε επίπεδο πολιτικών και κατά τη θέσπιση νέων νόμων και λειτουργιών του κυβερνοχώρου.

1.2.7 Έρευνα, Ανάπτυξη και Εκπαίδευση

Η ασφάλεια στον κυβερνοχώρο σε εθνικό επίπεδο θα αποτύχει όταν υπάρχει ένα ακατάλληλο επίπεδο ευαισθητοποίησης και εκπαίδευσης. Απαιτείται η συμμετοχή της εκπαίδευσης ή / και της επιστήμης για την ανάπτυξη στρατηγικών / επιχειρησιακών προγραμμάτων για την ευαισθητοποίηση σε θέματα ασφαλείας στον κυβερνοχώρο και την εκπαίδευση. Τα προγράμματα πρέπει να καλύπτουν ένα ευρύ φάσμα ενδιαφερόμενων. Μερικά από αυτά τα προγράμματα, ωστόσο, μπορεί να οργανωθούν από τον ιδιωτικό τομέα (π.χ. μια anti-phishing τηλεοπτική εκστρατεία εκ μέρους χρηματοπιστωτικών ιδρυμάτων). Εκτός από το γενικό πληθυσμό, μια εκπαιδευτική δομή για την ασφάλεια στον κυβερνοχώρο είναι απαραίτητη για να εξασφαλιστεί ότι ένας επαρκής αριθμός εμπειρογνωμόνων σε θέματα ασφάλειας στον κυβερνοχώρο θα είναι διαθέσιμος για την υποστήριξη όλων των δραστηριοτήτων. Εξίσου σημαντική όσο και η βασική εκπαίδευση είναι η ευαισθητοποίηση μεταξύ των βασικών φορέων λήψης αποφάσεων τόσο σε κρατικούς όσο και μη κρατικούς οργανισμούς. Η μεταξύ τους συνεργασία θα πραγματοποιηθεί μόνο όταν οι εν λόγω φορείς λήψης αποφάσεων έχουν πλήρη επίγνωση των θεμάτων κυβερνοασφάλειας.

1.3 Στρατηγική Κυβερνοασφάλειας της Ε.Ε. [3]

Το Φεβρουάριο του 2013 η εκπρόσωπος της Ε.Ε. σε θέματα εξωτερικής πολιτικής και ασφάλειας Κάθριν Άστον παρουσίασε την Ευρωπαϊκή Στρατηγική Κυβερνοασφάλειας. Η Στρατηγική καθορίζει μια σειρά προτεραιοτήτων για τη βελτίωση των συστημάτων πληροφορικής, τη μείωση του εγκλήματος στον κυβερνοχώρο, καθώς και τη δημιουργία μιας διεθνούς πολιτικής κυβερνοχώρου για την Ευρωπαϊκή Ένωση. Το όραμα της Ε.Ε. που παρουσιάζεται στην παρούσα στρατηγική διαρθρώνεται σε πέντε στρατηγικές προτεραιότητες:

• Επίτευξη ανθεκτικότητας στον κυβερνοχώρο.

• Δραστική μείωση της εγκληματικότητας στον κυβερνοχώρο.

• Ανάπτυξη της πολιτικής κυβερνοάμυνας και των ικανοτήτων που σχετίζονται με την Κοινή Πολιτική Ασφάλειας και Άμυνας.

• Ανάπτυξη των βιομηχανικών και τεχνολογικών πόρων για την ασφάλεια στον κυβερνοχώρο.

• Καθιέρωση μιας συνεκτικής διεθνούς πολιτικής κυβερνοχώρου για την Ευρωπαϊκή Ένωση και προώθηση των αξιών της.

1.3.1 Επίτευξη ανθεκτικότητας στον κυβερνοχώρο

Για την προώθηση της ανθεκτικότητας του κυβερνοχώρου στην ΕΕ, τόσο οι δημόσιες αρχές όσο και ο ιδιωτικός τομέας πρέπει να αναπτύξουν τις δυνατότητές τους και να συνεργάζονται αποτελεσματικά.

Η στρατηγική θα πρέπει να συνοδεύεται από **νομοθετική πρόταση** η οποία θα ορίζει :

• Τη θέσπιση κοινών ελάχιστων απαιτήσεων για την ασφάλεια δικτύων και πληροφοριών σε εθνικό επίπεδο, η οποία θα υποχρεώνει τα κράτη-μέλη να ορίζουν τις αρμόδιες εθνικές αρχές, να δημιουργήσουν μια λειτουργική ομάδα CERT και να υιοθετήσουν μια εθνική στρατηγική και ένα εθνικό σχέδιο συνεργασίας.

• Τη σύσταση μηχανισμών συντονισμένης πρόληψης, ανίχνευσης και αντίδρασης, επιτρέποντας την ανταλλαγή πληροφοριών και την αμοιβαία συνδρομή μεταξύ των εθνικών αρμόδιων αρχών.

• Τη βελτίωση της ετοιμότητας και την εμπλοκή του ιδιωτικού τομέα. Δεδομένου ότι η μεγάλη πλειοψηφία των συστημάτων δικτύων και πληροφοριών είναι ιδιωτικής ιδιοκτησίας και λειτουργίας, η συμμετοχή του ιδιωτικού τομέα για την ενίσχυση της ασφάλειας στον κυβερνοχώρο είναι ζωτικής σημασίας.

• Τέλος, οι ασκήσεις για συμβάντα στον κυβερνοχώρο σε επίπεδο ΕΕ είναι απαραίτητες για την προσομοίωση της συνεργασίας μεταξύ των κρατών μελών και του ιδιωτικού τομέα.

Ευαισθητοποίηση

Η ασφάλεια του κυβερνοχώρου είναι μια κοινή ευθύνη. Οι τελικοί χρήστες διαδραματίζουν καίριο ρόλο στη διασφάλιση της ασφάλειας των δικτύων και των συστημάτων πληροφοριών. Θα πρέπει να έχουν επίγνωση των κινδύνων που αντιμετωπίζουν και να κάνουν τα πρώτα βήματα για να προφυλαχθούν από αυτούς.

1.3.2 Δραστική μείωση της εγκληματικότητας στον κυβερνοχώρο

Θα πρέπει να υπάρχουν τα σωστά επιχειρηματικά εργαλεία και δυνατότητες για την αντιμετώπισή της εγκληματικότητας. Οι δυνάμεις επιβολής του νόμου πρέπει να υιοθετήσουν μια συντονισμένη και συλλογική προσέγγιση ώστε να ανταποκριθούν σε αυτή την αυξανόμενη απειλή.

Ισχυρή και αποτελεσματική νομοθεσία

Η ΕΕ και τα κράτη μέλη χρειάζονται ισχυρή και αποτελεσματική νομοθεσία για την αντιμετώπιση της εγκληματικότητας στον κυβερνοχώρο. Η ΕΕ έχει ήδη θεσπίσει νομοθεσία για το έγκλημα στον κυβερνοχώρο, συμπεριλαμβανομένης της οδηγίας για την καταπολέμηση της σεξουαλικής εκμετάλλευσης των παιδιών στο διαδίκτυο και της παιδικής πορνογραφίας.

Ενισχυμένη επιχειρησιακή ικανότητα για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο

Η εξέλιξη των τεχνικών του εγκλήματος στον κυβερνοχώρο έχει αυξηθεί ραγδαία. Οι υπηρεσίες επιβολής του νόμου δεν μπορούν να καταπολεμήσουν το έγκλημα στον κυβερνοχώρο με ξεπερασμένα επιχειρησιακά εργαλεία. Επί του παρόντος, δεν διαθέτουν όλα τα κράτη μέλη της ΕΕ την επιχειρησιακή ικανότητα που χρειάζονται για να ανταποκριθούν αποτελεσματικά στο έγκλημα στον κυβερνοχώρο. Όλα τα κράτη μέλη χρειάζονται αποτελεσματικές εθνικές μονάδες κατά της εγκληματικότητας στον κυβερνοχώρο.

Βελτίωση του συντονισμού σε επίπεδο ΕΕ

Η ΕΕ μπορεί να συμπληρώσει το έργο των κρατών μελών, διευκολύνοντας μια συντονισμένη και συνεργατική προσέγγιση, μεταξύ των αρχών επιβολής του νόμου, των δικαστικών αρχών των δημόσιων και ιδιωτικών φορέων τόσο εντός της ΕΕ όσο και εκτός αυτής.

1.3.3 Ανάπτυξη της πολιτικής κυβερνοάμυνας και δυνατότητες που σχετίζονται με το πλαίσιο της Κοινής Πολιτικής Ασφάλειας και Άμυνας

Για να αποφευχθούν οι αλληλοεπικαλύψεις, η ΕΕ θα διερευνήσει τις δυνατότητες για το πώς η ΕΕ και το ΝΑΤΟ μπορούν να συμπληρώσουν τις προσπάθειές τους για να βελτιώσουν την ανθεκτικότητα των κρίσιμων κυβερνητικών και άλλων πληροφοριακών υποδομών από τις οποίες εξαρτώνται τα μέλη και των δύο οργανισμών.

1.3.4 Ανάπτυξη βιομηχανικών και τεχνολογικών πόρων για την ασφάλεια στον κυβερνοχώρο

Προώθηση των επενδύσεων Έρευνας και Ανάπτυξης

Η Έρευνα και η Ανάπτυξη μπορούν να υποστηρίξουν μια ισχυρή βιομηχανική πολιτική, την προώθηση ενός αξιόπιστου ευρωπαϊκού κλάδου ΤΠΕ, την ενίσχυση της εσωτερικής αγοράς και την μείωση της ευρωπαϊκής εξάρτησης από ξένες τεχνολογίες. Η Έρευνα και η Ανάπτυξη θα πρέπει να καλύψουν τα κενά της τεχνολογίας στον τομέα της

ασφάλειας των ΤΠΕ, λαμβάνοντας υπόψη τη συνεχή εξέλιξη των αναγκών των χρηστών.

1.3.5 Καθιέρωση μιας συνεκτικής διεθνούς πολιτικής στον κυβερνοχώρο για την Ευρωπαϊκή Ένωση και την προώθηση των βασικών αξιών της ΕΕ

Η Επιτροπή, ο Ύπατος Εκπρόσωπος και τα κράτη μέλη πρέπει να εντάξουν μια συνεκτική διεθνή πολιτική κυβερνοχώρου της ΕΕ, που θα στοχεύει στην αυξημένη εμπλοκή και στη σύσφιγξη των σχέσεων με βασικούς διεθνείς εταίρους και οργανισμούς, καθώς και με την κοινωνία των πολιτών και τον ιδιωτικό τομέα.

1.4 Εξαγωγή κριτηρίων για τη δημιουργία του πλαισίου Κυβερνοασφάλειας

Όπως είδαμε για τον ENISA πρώτη προτεραιότητα είναι η θέσπιση ενός οράματος που θα θέτει τους στόχους και της προτεραιότητες. Αυτό θα πρέπει να γίνει λαμβάνοντας υπόψη τις ήδη υπάρχουσες πολιτικές. Κύριος στόχος και προτεραιότητα του εγχειριδίου του ΝΑΤΟ είναι η υποστήριξη των μελών του στη δημιουργία μιας στρατηγικής. Αντίστοιχα για την Ε.Ε. η ανάπτυξη της πολιτικής κυβερνοάμυνας και των ικανοτήτων που σχετίζονται με την Κοινή Πολιτική Ασφάλειας και Άμυνας είναι ιδιαίτερα σημαντική. Λαμβάνοντας αυτά υπόψη μπορούμε να πούμε ότι το πρώτο κριτήριο που θα πρέπει να πληρούν οι χώρες είναι η ύπαρξη μιας **Εθνικής Στρατηγικής Κυβερνοασφάλειας** η οποία θα θέτει τους στόχους και τις δράσεις που θα πρέπει να υλοποιήσει κάθε χώρα, θα ορίζει τους αρμόδιους φορείς και τη μεταξύ τους συνεργασία καθώς και τα μέτρα τα οποία θα πρέπει να ληφθούν.

Για την επίτευξη καλύτερου επιπέδου της Κυβερνοασφάλειας σημαντική είναι επίσης για τον ENISA η δραστική μείωση της εγκληματικότητας. Ένα από τα μέσα για να επιτευχθεί αυτός ο στόχος θεωρείται πως είναι η ύπαρξη ισχυρής και αποτελεσματικής νομοθεσίας. Στο στόχο αυτό επικεντρώνεται και η στρατηγική της Ε.Ε. Η καταπολέμηση του κυβερνοεγκλήματος αναφέρεται επίσης στο εγχειρίδιο του ΝΑΤΟ το οποίο συντείνει στην ανάπτυξη και τη συντήρηση ικανής νομοθεσίας. Για το λόγο αυτό ένα δεύτερο κριτήριο αξιολόγησης το οποίο θα πρέπει να εξεταστεί είναι το **Νομοθετικό Πλαίσιο** της κάθε χώρας.

Σύμφωνα με τον ENISA αναγκαία είναι επίσης η ανάπτυξη μιας σαφούς δομής διακυβέρνησης του κυβερνοχώρου, η αναγνώριση των συμμετεχόντων φορέων, η καθιέρωση συνεργασίας μεταξύ δημόσιων και ιδιωτικών φορέων καθώς και η ύπαρξη φορέων που θα ανταποκρίνονται σε συμβάντα Κυβερνοασφάλειας και θα βοηθήσουν

στη μείωση του κυβερνοεγκλήματος. Σύμφωνα με το εγχειρίδιο του ΝΑΤΟ η ύπαρξη φορέων καταπολέμησης του κυβερνοεγκλήματος αλλά και προστασίας των κρίσιμων υποδομών και διαχείρισης κρίσεων κυβερνοασφάλειας είναι ένα από τα βασικά θέματα που θα πρέπει να απασχολήσουν μια χώρα. Σημαντικός είναι επίσης ο συντονισμός και η συνεργασίας μεταξύ των φορέων για την ανταλλαγή πληροφοριών και την προστασία των δεδομένων. Για την Ε.Ε. η επίτευξη ανθεκτικότητας στον κυβερνοχώρο απαιτεί τον ορισμό αρμόδιων εθνικών αρχών, σύσταση μηχανισμών συντονισμένης πρόληψης , ανίχνευσης και αντίδρασης και εμπλοκή του ιδιωτικού τομέα. Ομαδοποιώντας τις παραπάνω απαιτήσεις η εξέταση ύπαρξης αρμόδιων **Αρχών και Οργανισμών** καθώς και η μεταξύ τους συνεργασία μπορεί να καθοριστεί ως ένα ακόμα κριτήριο.

Το εγχειρίδιο του ΝΑΤΟ αναφέρει ότι η ασφάλεια στον κυβερνοχώρο σε εθνικό επίπεδο θα αποτύχει όταν υπάρχει ένα ακατάλληλο επίπεδο ευαισθητοποίησης και εκπαίδευσης. Η ευαισθητοποίηση των χρηστών και η ενίσχυση της κατάρτισης και τα εκπαιδευτικά προγράμματα περιλαμβάνονται επίσης στις προτεινόμενες δράσεις του ENISA καθώς και στους στόχους της Ε.Ε. Παράλληλα και από τους τρείς οργανισμούς προτείνεται η διεξαγωγή ασκήσεων Κυβερνοασφάλειας. Τα ανωτέρω μπορούμε να τα ομαδοποιήσουμε στην ύπαρξη **Δράσεων Ευαισθητοποίησης και Εκπαίδευσης** τόσο των εμπειρογνωμόνων αλλά και του ευρύτερου κοινού.

Τέλος για τον ENISA η συνεργασία και η ανταλλαγή πληροφοριών μεταξύ των κρατών είναι σημαντική για την καλύτερη κατανόηση και ανταπόκριση σε ένα διαρκώς μεταβαλλόμενο περιβάλλον απειλών. Το εγχειρίδιο του ΝΑΤΟ συγκεκριμένα αναφέρεται σε πολυμερή ή διμερή δραστηριότητα που θα αποσκοπεί στη διαχείριση των σχέσεων των κρατών στον κυβερνοχώρο. Τέλος η Ε.Ε. δίνει ιδιαίτερη σημασία στον συντονισμό τόσο μεταξύ των κρατών-μελών αλλά και με χώρες εκτός αυτής. Συνεπώς η **Διεθνής Συνεργασία** μπορεί να θεωρηθεί ως κριτήριο του πλαισίου μελέτης.

Κεφάλαιο 2ο

Αυστρία

2.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η αυστριακή Στρατηγική για την Κυβερνοασφάλεια / (Österreichische Strategie für Sicherheit Cyber / OSCS) [4] αποτελεί ένα ολοκληρωμένο σχέδιο για την προστασία του κυβερνοχώρου. Στοχεύει στην ενίσχυση της ασφάλειας και της αντοχής των αυστριακών υποδομών και υπηρεσιών στο κυβερνοχώρο καθώς και στην ανάπτυξη της ευαισθητοποίησης της αυστριακής κοινωνίας. Η Στρατηγική Κυβερνοασφάλειας της Αυστρίας έχει αναπτυχθεί με βάση την γενικότερη Στρατηγική Ασφάλειας και καθοδηγείται από τις αρχές του αυστριακού προγράμματος για την προστασία των κρίσιμων υποδομών. Στο πλαίσιο της στρατηγικής της, η Αυστρία επιδιώκει ως στρατηγικούς στόχους τη διαθεσιμότητα, την αξιοπιστία και την εμπιστευτικότητα της ανταλλαγής δεδομένων, τη διασφάλιση της ανθεκτικότητας των υποδομών του τομέα των ΤΠΕ έναντι των απειλών, την οικοδόμηση μιας κουλτούρας για την ασφάλεια στον κυβερνοχώρο με τη λήψη μιας σειράς μέτρων ευαισθητοποίησης, τη διαδραμάτιση ενεργού ρόλου στη διεθνή συνεργασία σε ευρωπαϊκό και παγκόσμιο επίπεδο και την εξασφάλιση και ανάπτυξη των διοικητικών υπηρεσιών ηλεκτρονικής διακυβέρνησης.

2.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας Ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων[5]

Ο αυστριακός νόμος περί προστασίας δεδομένων του 2000 (Datenschutzgesetz 2000 DSG 2000, BGBl I αριθ. 165/1999) τέθηκε σε ισχύ την 1η Ιανουαρίου 2000. Στο πλαίσιο της εφαρμογής της οδηγίας για την προστασία των δεδομένων 95/46/ΕΚ, η πράξη παρέχει ένα θεμελιώδες δικαίωμα στην προστασία της ιδιωτικής ζωής σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα που συνεπάγεται το δικαίωμα στην ενημέρωση, διόρθωση εσφαλμένων δεδομένων και διαγραφή παράνομης επεξεργασίας δεδομένων.

Νομοθεσία περί ηλεκτρονικού εμπορίου[5]

Ο αυστριακός νόμος για το ηλεκτρονικό εμπόριο (eCommerce Gesetz), τέθηκε σε ισχύ την 1η Ιανουαρίου 2002, και θέτει σε εφαρμογή την οδηγία 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο.

Νομοθεσία περί ηλεκτρονικών επικοινωνιών [5]

Ο νόμος για τις τηλεπικοινωνίες τέθηκε σε ισχύ στις 20 Αυγούστου 2003. Με τον τρόπο αυτό, το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες μεταφέρθηκε στο εθνικό δίκαιο.

Νομοθεσία περί ηλεκτρονικού εγκλήματος [6]

Ποινικός Κώδικας (StGB)

Παράγραφος 118: Παράνομη πρόσβαση σε σύστημα υπολογιστή.

Παράγραφος 119: Παράβαση του απορρήτου των τηλεπικοινωνιών.

Παράγραφος 119α: Υποκλοπή δεδομένων.

Παράγραφος 126β: Διακοπή της λειτουργικότητας των πληροφοριακών συστημάτων.

Παράγραφος 126γ: Κατάχρηση των προγραμμάτων ηλεκτρονικών υπολογιστών ή της πρόσβαση σε δεδομένα.

Παράγραφος 225α: Πλαστογραφία με χρήση Η/Υ.

Παράγραφος 248α: Απάτη με χρήση Η/Υ.

2.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς [7]

Η Επιτροπή Ασφάλειας Πληροφοριών της Εθνικής Αρχής Ασφάλειας (Bundeskanzleramt Informationssicherheitskommission) [8] είναι υπεύθυνη για την ασφάλεια των πληροφοριών όλων των ομοσπονδιακών υπουργείων. Αποτελεί το κύριο σημείο επαφής για τα εθνικά και διεθνή ζητήματα που αφορούν την ασφάλεια των πληροφοριών, εξασφαλίζει την παρουσία των ενοποιημένων εθνικών μέτρων ευρείας προστασίας και συντονίζει όλες τις δραστηριότητες στον τομέα των διαβαθμισμένων πληροφοριών σε σχέση με την Ομοσπονδιακή διοίκηση. Το Τμήμα Πολιτικής Ασφάλειας [9] της Ομοσπονδιακής Καγκελαρίας της Δημοκρατίας της Αυστρίας συντονίζει την ολοκληρωμένη πολιτική ασφάλειας και εθνικής άμυνας. Επίσης, συντονίζει, σε συνεργασία με το Υπουργείο Εσωτερικών, το Ευρωπαϊκό Πρόγραμμα για την Προστασία των Υποδομών Ζωτικής Σημασίας (EPCIP). Το Ομοσπονδιακό Υπουργείο Εσωτερικών / Bundesministerium für Inneres (BMI) [10] είναι αρμόδιο για

εσωτερικές υποθέσεις στην Αυστρία και οι αρμοδιότητες του περιλαμβάνουν δραστηριότητες που σχετίζονται με την παιδική πορνογραφία και εγκλήματα στο Διαδίκτυο. Η Αυστριακή Επιτροπή Προστασίας Δεδομένων (Datenschutzkommission) [11] είναι η Αυστριακή εποπτική αρχή για την προστασία των δεδομένων. Τέλος το A-SIT κέντρο για την ασφάλεια της πληροφορικής [12] είναι ένα σωματείο μη κερδοσκοπικού χαρακτήρα δημόσιας χρηματοδότησης. Ο σκοπός του είναι να ενεργεί ως ανεξάρτητος οργανισμός σε θέματα ασφάλειας, να συντονίζει τα προγράμματα ασφάλειας πληροφορικής και να ενεργεί ως ανεξάρτητο συμβουλευτικό όργανο.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13][14]

Η CERT.at [15] είναι η αυστριακή εθνική CERT. Είναι το πρωταρχικό σημείο επαφής για την ασφάλεια των ΤΠΕ σε εθνικό πλαίσιο και συντονίζει άλλες ομάδες CERT που λειτουργούν στην περιοχή της κρίσιμης ή επικοινωνιακής υποδομής. Επίσης παρέχει βασικές πληροφορίες -ασφάλειας (προειδοποιήσεις, συμβουλές). Η GovCERT [16] είναι η CERT της αυστριακής κυβέρνησης και συνεργάζεται με την CERT.at. Η R-IT CERT [17] είναι η ομάδα της Raiffeisen του μεγαλύτερου πάροχου πληροφορικής στην Αυστρία. Η ACOnet-CERT [18] είναι η αυστριακή CERT του Ακαδημαϊκού Δίκτυού Υπολογιστών και η WienCERT [19] είναι η ομάδα CERT του δήμου της Βιέννης.

Ιδιωτικοί φορείς

Όσον αφορά τον ιδιωτικό τομέα το Τμήμα πληροφορικής του Αυστριακού Ομοσπονδιακού Οικονομικού Επιμελητηρίου, [20] συντονίζει και εκπροσωπεί τα συμφέροντα της Αυστριακής επιχειρηματικής κοινότητας τόσο σε εθνικό όσο και σε διεθνές επίπεδο. Οι δραστηριότητες στον τομέα της ασφάλειας πληροφοριακών συστημάτων περιλαμβάνουν ζητήματα όπως η διατήρηση δεδομένων και η ευαισθητοποίηση των καταναλωτών. Οι Υπηρεσίες για τα μέλη περιλαμβάνουν ελέγχους ασφαλείας και το "IT Sicherheitshandbuch" έναν οδηγό ασφαλείας, ο οποίος αφορά τόσο τις επιχειρήσεις όσο και το προσωπικό τους.

Η IT-Security Experts [21] είναι μια ομάδα εμπειρογνωμόνων που παρέχουν λύσεις ασφάλειας με στόχο την ευαισθητοποίηση, την ανταλλαγή εμπειριών, καθώς και την παροχή κατάρτισης στις μικρές και μεσαίες επιχειρήσεις.

Το SBA Research GmbH (SBA) [22] είναι ένα ερευνητικό κέντρο για την Ασφάλεια Πληροφοριακών Συστημάτων το οποίο αποτελείται από 25 επιχειρήσεις, 4 αυστριακά πανεπιστήμια, και διεθνείς ερευνητικούς εταίρους.

Ακαδημαϊκοί φορείς

Το Ινστιτούτο Εφαρμοσμένης Επεξεργασίας Πληροφοριών και Επικοινωνιών (IAIK) [23] εστιάζει στην ασφάλεια των πληροφοριών. Το ινστιτούτο αποτελεί μέρος του Τμήματος Επιστήμης Υπολογιστών του Graz University of Technology. Επίσης Το Πανεπιστήμιο του Linz [24] έχει ερευνητική δραστηριότητα στον τομέα της ασφάλειας δικτύων και πληροφοριών.

Συνεργασία μεταξύ φορέων

Η Ομοσπονδιακή Καγκελαρία της Δημοκρατίας της Αυστρίας μέσω της Εθνικής Αρχής Ασφάλειας είναι υπεύθυνη για την πολιτική ασφαλείας της κυβέρνησης και στο πλαίσιο αυτό συνεργάζεται στενά με μια σειρά από υπουργεία και μια σειρά από άλλες δημόσιες αρχές. Συμμετέχει στην προετοιμασία των επιμέρους στρατηγικών για όλους τους τομείς που σχετίζονται με τη γενική πολιτική ασφάλειας της Αυστρίας, μία εκ των οποίων είναι η στρατηγική για την ασφάλεια των ΤΠΕ. Επίσης σε συνεργασία με την ομοσπονδιακή καγκελαρία, η CERT.at λειτουργεί την αυστριακή GovCERT. Η CERT.at λειτουργεί από τον Απρίλιο του 2008, ως εθνικό επιχειρησιακό κέντρο για την ανάλυση κρίσεων, και είναι σε θέση να δημιουργήσει μια «αίθουσα πολέμου» σε περίπτωση έκτακτης ανάγκης. Η CERT.AT και η GovCERT ερευνούν τις δυνατότητες για τη δημιουργία ενός δικτύου αισθητήρων για ένα σύστημα έγκαιρης προειδοποίησης. Η CERT.AT είναι το πρωταρχικό σημείο επαφής για την ασφάλεια των ΤΠΕ σε εθνικό πλαίσιο και συντονίζει άλλες ομάδες CERT που λειτουργούν στην περιοχή των κρίσιμων υποδομών. Σε περίπτωση σημαντικών ηλεκτρονικών επιθέσεων κατά της αυστριακής υποδομής, η CERT.at είναι υπεύθυνη να συντονίσει τις αντιδράσεις των φορέων. Η CERT.AT συνεργάζεται επίσης με άλλους οργανισμούς στον τομέα της ασφάλειας των υπολογιστών ανταλλάσσοντας πληροφορίες σχετικά με συμβάντα ασφάλειας και τρωτά σημεία λειτουργώντας σύμφωνα με τους περιορισμούς που επιβάλλονται από το αυστριακό δίκαιο. Όλα τα συμβάντα θα πρέπει να αναφέρονται στο GovCERT το οποίο αναλύει τις απειλές με διαφορετικούς τρόπους.

2.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Κύριος φορέα ενημέρωσης και ευαισθητοποίησης είναι η Πύλη ασφάλειας των ΤΠΕ (onlinesicherheit.) [7] η οποία είναι μια διυπουργική πρωτοβουλία. Η πύλη απευθύνεται σε διαφορετικές κοινωνικές και επιχειρηματικές ομάδες της Αυστρίας (παιδιά & νέους, γονείς, καθηγητές, πολίτες άνω των 60, επιχειρήσεις, υπαλλήλους, δημόσιους οργανισμούς κ.α.) και περιέχει ευρύ φάσμα πληροφόρησης. Σε συνεργασία με το

Υπουργείο Παιδείας, διοργανώνει εργαστήρια στα σχολεία. Ορισμένα σχολεία υλοποιούν ακόμη και δικά τους σχέδια εκπαίδευσης καθώς η Ασφάλεια στο Διαδίκτυο είναι ένα ζωτικό μέρος των σπουδών της ανώτερης δευτεροβάθμιας εκπαίδευσης (γενικής και επαγγελματικής εκπαίδευσης) [25].

Επιπλέον, το A-SIT έχει εκδώσει ένα Εγχειρίδιο Ασφάλειας Πληροφοριών [26], το οποίο αποτελεί βασικό εργαλείο για την ευαισθητοποίηση και χρησιμοποιείται σε διάφορους τομείς για την εγκαθίδρυση ολοκληρωμένων διαδικασιών ασφάλειας των ΤΠΕ. Επίσης το Αυστριακό Ομοσπονδιακό Οικονομικό Επιμελητήριο, τμήμα πληροφορικής διοργανώνει κάθε χρόνο το " IT security road show "[27] ένα γεγονός που λαμβάνει χώρα σε όλες τις μεγάλες πόλεις με σκοπό την προώθηση νέων λύσεων ασφάλειας πληροφορικής και την προώθηση της ευαισθητοποίησης. Τέλος, το 2012 διοργανώθηκε στην Αυστρία μια εθνική άσκηση κυβερνοάμυνας με την ονομασία Cyber Planspiel [28][29].

2.5 Διεθνής Συνεργασία

Η Αυστρία, μέσω του A-SIT εκπροσωπεί τη χώρα στον οργανισμό ENISA και συμμετέχει στην άσκηση Cyber Europe που διοργανώνεται από τον ίδιο οργανισμό προσομοιώνοντας μια μαζική επίθεση κατά των ευρωπαϊκών σημείων διασύνδεσης στο Διαδίκτυο, με σκοπό την παράλυση του δίκτυού και την απενεργοποίηση των ηλεκτρονικών επικοινωνιών. Επιπλέον ο A-SIT ανταλλάσσει πληροφορίες και εμπειρία σε τακτική βάση με το BSI της Γερμανίας και το ISB της Ελβετίας βάση διμερών συμφωνιών συνεργασίας [30]. Η Αυστρία συμμετείχε επίσης στις διεθνείς ασκήσεις: - Cyberstorm 2010 ως παρατηρητής - Cybex 2011 ως σχεδιαστής και ως παίκτης - Cyber Atlantic 2011 ως σχεδιαστής και ως παίκτης - LÜKEX 2011 ως παρατηρητής [29]. Η GovCERT.AT είναι ενεργό μέλος των ευρωπαϊκών κυβερνητικών ομάδων CERT (EGC) [31] μιας άτυπης ομάδα κυβερνητικών CSIRTs με σκοπό την αποτελεσματική συνεργασία σε θέματα αντιμετώπισης περιστατικών μεταξύ των μελών της. Οι R-IT CERT, ACOnet-CERT, CERT.AT είναι μέλη του διεθνούς φόρουμ των ομάδων CERT FIRST[32][14] . Τέλος η Αυστρία είναι μέλος της διεθνούς συμμαχίας υπο την αιγίδα του Ο.Η.Ε. για την καταπολέμηση του κυβερνοεγκλήματος (IMPACT) [33].

Κεφάλαιο 3ο

Βέλγιο

3.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Το Υπουργικό Συμβούλιο συνέθεσε στις 30 Σεπτεμβρίου 2005 την πλατφόρμα του Βελγίου για την των Ασφάλεια Δικτύων και Πληροφοριών με την ονομασία Belnis. Η Belnis έχοντας αρμοδιότητες και ευθύνες για την ασφάλεια των πληροφοριακών συστημάτων δημιούργησε τη λευκή βίβλο «Προς μια εθνική πολιτική στον τομέα της ασφάλειας πληροφοριών» [34] που οδήγησε σε μια σειρά από ενέργειες που έγιναν από την κυβέρνηση εκείνη την εποχή, όπως η εγκατάσταση ενός νέου εθνικού CERT, του CERT.BE. Το 2012 ολοκλήρωσε το προσχέδιο για τη Βελγική Στρατηγική Κυβερνοασφάλειας το οποίο αναμένεται να εγκρίθηκε από την βελγική κυβέρνηση το 2014 [35]. Σύμφωνα με το προσχέδιο, το Βέλγιο ορίζει τρείς στρατηγικούς στόχους: τη Δημιουργία ενός ασφαλούς και αξιόπιστου κυβερνοχώρου, τη βέλτιστη ασφάλεια και προστασία των κρίσιμων υποδομών και των κυβερνητικών συστημάτων στον κυβερνοχώρο και την ανάπτυξη εθνικών δυνατότητων ασφάλειας στον κυβερνοχώρο.

3.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [36]

Ο Νόμος περί ιδιωτικότητας του Δεκεμβρίου 1992 έχει ως στόχο να προστατεύσει τους πολίτες από την καταχρηστική επεξεργασία των προσωπικών δεδομένων. Ο νόμος ορίζει τα δικαιώματα και τις υποχρεώσεις τόσο του υποκειμένου των δεδομένων όσο και του επεξεργαστή. Επιπλέον, παρέχει τη νομική βάση για τη λειτουργία της Επιτροπής για την Προστασία των Προσωπικών Δεδομένων ως ανεξάρτητου οργάνου

Νομοθεσία ηλεκτρονικού εμπορίου [36]

Δύο νόμοι για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας εγκρίθηκαν στις 11 Μαρτίου 2003. Και τα δύο κείμενα ορίζουν τις

βασικές έννοιες που διέπουν το ηλεκτρονικό εμπόριο και μεταφέρουν την οδηγία της ΕΕ για το ηλεκτρονικό εμπόριο - 2000/31/ΕΚ) στο βελγικό δίκαιο.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [36]

Ο νόμος για τις ηλεκτρονικές επικοινωνίες εκδόθηκε στις 13 Ιουνίου 2005 και είχε ως στόχο να μεταφέρει το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες στο βελγικό δίκαιο.

Νομοθεσία Κυβερνοεγκλήματος

Ποινικός Κώδικας [37]

Το βελγικό Κοινοβούλιο το Νοέμβριο του 2000 εξέδωσε νέα άρθρα του ποινικού κώδικα για εγκλήματα πληροφορικής, με ισχύ από την 13η Φεβρουαρίου 2001:

Άρθρο 210 Αλλαγή ή διαγραφή ηλεκτρονικών δεδομένων.

Άρθρο 550 Πρόκληση ζημιάς σε υπολογιστή ή αποθηκεμένα δεδομένα, μη εξουσιοδοτημένη πρόσβαση σε σύστημα υπολογιστή.

Άρθρο 314 Παρακολούθηση των ιδιωτικών επικοινωνιών και δεδομένων.

3.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Η B-CCENTRE [38][39] είναι η κύρια πλατφόρμα στο Βέλγιο και στοχεύει στη συνεργασία και τον συντονισμό σε θέματα Κυβερνοασφάλειας, συνδυάζοντας την εμπειρία των ακαδημαϊκών ερευνητικών ομάδων, των εταίρων της βιομηχανίας και των δημόσιων οργανισμών (επιβολής του νόμου, δικαστές και φορείς χάραξης πολιτικής).

Η Βελγική Ομοσπονδιακή Μονάδα Εγκλήματος Υπολογιστών (Federal Computer Crime Unit) (FCCU) [40] είναι υπεύθυνη για την καταπολέμηση της εγκληματικότητας στον κυβερνοχώρο με στόχο την προστασία όλων των πολιτών. Η Fedict (Federal Public Service Information and Communication Technology) [41] ως ομοσπονδιακή δημόσια υπηρεσία, καθορίζει και εφαρμόζει την ομοσπονδιακή στρατηγική ηλεκτρονικής διακυβέρνησης. Η FPS Justice [42] είναι διαδικτυακή πύλη της κυβέρνησης του Βελγίου για το έγκλημα στον κυβερνοχώρο. Η Βελγική Αρχή Προστασίας Δεδομένων [43] έχει ως βασική αποστολή να εξασφαλίσει την εφαρμογή του νόμου όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Τέλος η υπηρεσία πληροφοριών και ασφάλειας του Βελγίου [44], βοηθά τις βελγικές εταιρείες για την προστασία από επιθέσεις στον κυβερνοχώρο.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CERT.be [45] είναι το πρωταρχικό σημείο επαφής του Βελγίου για την αντιμετώπιση απειλών για την ασφάλεια του διαδικτύου και τα τρωτά σημεία που επηρεάζουν τα συμφέροντα του Βελγίου. Η ομάδα CERT.be είναι διαπιστευμένη από τον TF - CSIRT και έχει ωριμάσει στο ρόλο της ως εθνικού CSIRT. Το 2011 έλαβε 2609 αναφορές συμβάντων, αντιμετώπισε 1494 περιστατικά και διεξήγαγε 1161 έρευνες. Την ίδια χρονιά δημοσίευσε 2058 προειδοποιήσεις και 3 συστάσεις για επαγγελματίες και 16 συμβουλές και 8 συστάσεις προς τους πολίτες. Δημοσιεύει επίσης ένα εβδομαδιαίο ενημερωτικό δελτίο[46]. Άλλες ομάδες είναι η ομάδα GSC-NDC-OC που είναι υπεύθυνη για τις υποδομές δικτύων που λειτουργούν από τη Γενική Γραμματεία του Συμβουλίου της Ευρωπαϊκής Ένωσης και η Belgacom CSIRT του τηλεπικοινωνιακού παρόχου Belgacom.

Ιδιωτικοί φορείς

Η BELTUG [47] είναι η μεγαλύτερη βελγική ένωση διαχειριστών των ΤΠΕ, με εξειδίκευση στην εταιρικά δίκτυα, τις κινητές επικοινωνίες, και τα υπολογιστικά νέφη η οποία αναλαμβάνει κρίσιμα ζητήματα σχετικά με την ασφάλεια σε εθνικό και διεθνές επίπεδο. Επίσης η βελγική ομάδα ασφαλείας υπολογιστών CLUSIB/BELCLIV[48] έχει στόχο να αναλάβει κάθε πρωτοβουλία που αποσκοπεί στην ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και δικτύων. Ο LSEC [49] είναι ένας μη κερδοσκοπικός οργανισμός, που βρίσκεται στο Βέλγιο, και δραστηριοποιείται στον τομέα της ασφάλειας των πληροφοριών, στην ευαισθητοποίηση και την εκπαίδευση πάνω από 10 χρόνια. Η βελγική ομοσπονδία για τον κλάδο της τεχνολογίας Agoria [50] υποστηρίζει 1.700 εταιρείες-μέλη της στην καταπολέμηση του εγκλήματος στον κυβερνοχώρο, μέσω τακτικών συναντήσεων. Οι πληροφορίες που παρέχονται απευθύνονται κυρίως σε Διευθύνοντες Συμβούλους που επιθυμούν να ενσωματώσουν τις πτυχές της ασφάλειας του κυβερνοχώρου στην επιχειρηματική στρατηγική τους. Η Βελγική Ομοσπονδία του χρηματοπιστωτικού τομέα Febelfin [51], υποστηρίζει τα μέλη της στην καταπολέμηση του ηλεκτρονικού εγκλήματος μέσω της ανταλλαγής πληροφοριών και της συνεργασίας με όλους τους εμπλεκόμενους ενδιαφερόμενους. Διατηρεί μια ειδική ιστοσελίδα (www.safeinternetbanking.be) και έχει δρομολογήσει αρκετές εκστρατείες ευαισθητοποίησης σε θέματα ασφάλειας. Τέλος το Διεθνές Εμπορικό Επιμελητήριο ICC Belgium [52] διεξάγει συζητήσεις σχετικά με θέματα του εγκλήματος στον κυβερνοχώρο και την ανάπτυξη κατευθυντήριων γραμμών. Μέσω του τμήματος καταπολέμησης του εγκλήματος αντιμετωπίζει όλες τις μορφές

εγκληματικότητας που επηρεάζουν τις επιχειρήσεις, συμπεριλαμβανομένης της εγκληματικότητας στον κυβερνοχώρο.

Ακαδημαϊκοί φορείς

Στον ακαδημαϊκό τομέα η ερευνητική ομάδα Ασφάλειας Υπολογιστών και Βιομηχανικής Κρυπτογραφίας ESAT-COSIC [53], είναι μια ερευνητική ομάδα του Τμήματος Ηλεκτρολόγων Μηχανικών του Πανεπιστημίου Leuven. Η έρευνα επικεντρώνεται στο σχεδιασμό, την αξιολόγηση και την εφαρμογή κρυπτογραφικών αλγορίθμων και πρωτοκόλλων, για την ανάπτυξη των αρχιτεκτονικών ασφάλειας για τα συστήματα πληροφοριών και επικοινωνιών. Επίσης το Πανεπιστήμιο του Leuven συνεργάζεται σε διάφορα ερευνητικά θέματα που αφορούν την ασφάλεια των υπολογιστών με το Διεπιστημονικό Κέντρο για τον Νόμο και ΤΠΕ, και άλλα ερευνητικά κέντρα στα πλαίσια συνεργασίας μέσω του Βελγικού Κέντρου Αριστείας για το Κυβερνοέγκλημα [39].

Συνεργασία μεταξύ φορέων

Το B-CCENTRE είναι η κύρια πλατφόρμα συνεργασία στο Βέλγιο. Το κέντρο μαζί με εμπειρογνώμονες στον τομέα από οργανισμούς του δημόσιου της ακαδημαϊκής κοινότητας και των εταίρων της βιομηχανίας (όπως οι Microsoft, CSC, η Cisco, η Atos Origin και η βελγική ομοσπονδία του χρηματοπιστωτικού τομέα - Febelfin) συμμετέχουν στην αντιμετώπιση της εγκληματικότητας στον κυβερνοχώρο, και αναπτύσσουν πρωτοβουλίες ευαισθητοποίησης για τους Βέλγους πολίτες [39].

3.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Κύρια δράση για την αύξηση της ευαισθητοποίησης του βελγικού πληθυσμού είναι το πρόγραμμα "saferinternet". Ως κέντρο ευαισθητοποίησης αναπτύσσει εργαλεία σχετικά με την ασφαλή και υπεύθυνη χρήση του Διαδικτύου και ενημερώνει τους γονείς, τους εκπαιδευτικούς και τα παιδιά σχετικά με την χρήση του Διαδικτύου και των νέων τεχνολογιών. Οι δραστηριότητες αυτές χρηματοδοτούνται από την Ευρωπαϊκή Επιτροπή στο πλαίσιο του προγράμματος Safer Internet. Η Safeonweb είναι μια πρωτοβουλία του CERT.be για να ενημερώνει και να παρέχει συμβουλές στους Βέλγους πολίτες για την ασφάλεια στον κυβερνοχώρο και σημαντικές ψηφιακές απειλές. Επίσης η πρωτοβουλία του Belgian Information Security Support ιδρύθηκε για να στηρίξει την ανάπτυξη και την προώθηση μιας κοινωνίας που προσπαθεί να βελτιώσει το επίπεδο της Ασφάλειας Πληροφοριών στο Βέλγιο[38]. Η FCCU

διαχειρίζεται την ηλεκτρονική υπηρεσία www.ecops.be όπου οι χρήστες του διαδικτύου μπορούν να αναφέρουν τα αδικήματα που διαπράττονται μέσω του διαδικτύου έτσι ώστε η αστυνομία να ελέγξει και να αξιολογήσει τις παράνομες online δραστηριότητες [54]. Το 2012 διοργανώθηκε στο Βέλγιο η εθνική άσκηση κυβερνοασφάλειας με την ονομασία BelgoCybex [55].

3.5 Διεθνής Συνεργασία

Το Βέλγιο συνεργάζεται με τον ENISA μέσω του FCCU. Επίσης συμμετέχει στην άσκηση Cyber Europe [55][56] καθώς και στην άσκηση κυβερνοάμυνας Cyber Coalition [55][57] του NATO. Όσον αφορά τη συνεργασία των CERT η εθνική/κυβερνητική ομάδα CERT.be είναι ένα ενεργό και αναγνωρισμένο μέλος της TF-CSIRT και του διεθνούς φόρουμ FIRST[32][46]. Τα μέλη της ομάδας είναι παρόντα στις συνεδριάσεις και συμβάλουν με διαλέξεις και παρουσιάσεις. Το 2011 η ομάδα CERT.be φιλοξένησε επίσης τη πρώτη σύσκεψη εργασίας AbuseHelper στις Βρυξέλλες. Ο στόχος ήταν να φέρει σε επαφή CSIRTs και να ενθαρρύνει την καλύτερη ανταλλαγή γνώσεων και πληροφοριών σχετικά με τα τρέχοντα περιστατικά. Από τότε και άλλες ευρωπαϊκές CSIRTs οργάνωσαν επίσης παρόμοιες συσκέψεις. Το B-CENTRE συνεργάζεται επίσης με άλλα εθνικά κέντρα αριστείας για το κυβερνοέγκλημα και εκπροσωπεί το Βέλγιο σε κύρια θεσμικά όργανα όπως η Ευρωπαϊκή Επιτροπή, το Συμβούλιο της Ευρώπης, η Europol, και ο ENISA [39]. Τέλος το Βέλγιο συνεργάζεται στενά με τις υπόλοιπες χώρες της BENELUX βάση συμφωνίας που υπέγραψαν τον Απρίλιο του 2011 [58].

Κεφάλαιο 4ο

Βουλγαρία

4.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Από τη Βουλγαρία απουσιάζει μια Εθνική Στρατηγική Κυβερνοασφάλειας. Η μόνη σχετική αναφορά προέρχεται από την «Εθνική Στρατηγική της Βουλγαρίας για την Αντιμετώπιση του Εγκλήματος» [59] η οποία αναγνωρίζει το έγκλημα στον κυβερνοχώρο ως ένα ζήτημα με μια εντατική ανάπτυξη. Ως εκ τούτου, το υπουργικό συμβούλιο της Βουλγαρίας έχει εξετάσει τη σύνταξη των σχετικών εγγράφων για εγκληματικές πράξεις σε δίκτυα και συστήματα ηλεκτρονικών υπολογιστών (αναζήτηση και κατάσχεση ηλεκτρονικών υπολογιστών, σύνταξη τροποποιήσεων του Κώδικα Ποινικής Δικονομίας και των σχετικών διατάξεων, φορείς πληροφοριών, δεδομένων, κλπ.).

4.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [60]

Ο νόμος για την προστασία των προσωπικών δεδομένων εγκρίθηκε τον Δεκέμβριο του 2001, τροποποιήθηκε τον Ιούλιο του 2007, και έχει διαμορφωθεί σχετικά με την οδηγία 95/46/ΕΚ της ΕΕ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Η εφαρμογή του νόμου εποπτεύεται από την Επιτροπή για την Προστασία Προσωπικών Δεδομένων μια ανεξάρτητη αρχή που δημιουργήθηκε το 2003. Τα μέλη αυτής της Επιτροπής διορίζονται από το Κοινοβούλιο.

Νομοθεσία ηλεκτρονικού εμπορίου [60]

Ο νόμος για το ηλεκτρονικό εμπόριο ψηφίστηκε στη Βουλή το 2006, προκειμένου να εφαρμόσει την οδηγία της ΕΕ για το ηλεκτρονικό εμπόριο (2000/31/EC5). Ρυθμίζει τις υποχρεώσεις των παρόχων υπηρεσιών και εισάγει έναν ορισμό του SPAM καθώς και την ανάπτυξη ενός ειδικού μητρώου των πολιτών που δεν επιθυμούν να λαμβάνουν τέτοια μηνύματα.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [60]

Τον Δεκέμβριο του 2010, το Συμβούλιο Υπουργών ενέκρινε το ψήφισμα αριθ. 972 και ενέκρινε την Πολιτική για τις Ηλεκτρονικές Επικοινωνίες της Δημοκρατίας της Βουλγαρίας. Ο στόχος της πολιτικής είναι να παρέχει εύκολη πρόσβαση του πληθυσμού και των επιχειρήσεων σε σύγχρονες, αποτελεσματικές, ποιοτικές και ασφαλείς υπηρεσίες ηλεκτρονικών επικοινωνιών.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [61]

Ποινικός Κώδικας

Η Βουλή της Βουλγαρίας ενέκρινε στις 13 Σεπ 2002, τροποποιήσεις στον Ποινικό Κώδικα συμπεριλαμβάνοντας ένα νέο κεφάλαιο για το κυβερνοέγκλημα. Στο κεφάλαιο περιγράφονται αδικήματα που συνιστούν τις παρακάτω κατηγορίες εγκλημάτων.

Άρθρο 319α Παράνομη πρόσβαση.

Άρθρο 319β Παράνομη υποκλοπή, απάτη με Η/Υ.

Άρθρο 319γ Παρεμβολή σε δεδομένα.

Άρθρο 319δ Κακή χρήση ηλεκτρονικών συσκευών.

Άρθρο 319ε Πλαστογραφία με Η/Υ.

4.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Κύριος φορέας είναι ο Εκτελεστικός Οργανισμός Δικτύων Ηλεκτρονικών Επικοινωνιών και Πληροφοριακών Συστημάτων (ΕΑ ECNIS) [62] οι δραστηριότητες του οποίου επικεντρώνονται σε τρεις βασικούς τομείς:

- Την κατασκευή, τη συντήρηση, την ανάπτυξη, τη λειτουργία και τη διαχείριση ενός δικτύου ηλεκτρονικών επικοινωνιών της δημόσιας διοίκησης, της εθνικής ασφάλειας και των ενόπλων δυνάμεων, το οποίο αποτελεί μέρος ενός ολοκληρωμένου συστήματος επικοινωνίας και ανταλλαγής πληροφοριών της χώρας.
- Την ανάπτυξη και διαχείριση των κέντρων δεδομένων, αυτοματοποιημένων συστημάτων πληροφοριών και πυλών πρόσβασης για την ηλεκτρονική διακυβέρνηση.
- Την ανάπτυξη και συντήρηση ενός Κέντρου για την αντιμετώπιση περιστατικών σε σχέση με την ασφάλεια των πληροφοριών (CERT).

Ο Κρατικός οργανισμός για τις διαβαθμισμένες πληροφορίες, (DKSI) [63] είναι μια κρατική επιτροπή για την ασφάλεια των πληροφοριών η οποία οργανώνει, ελέγχει και

είναι υπεύθυνη για την εκπλήρωση των υποχρεώσεων σχετικά με την προστασία των διαβαθμισμένων πληροφοριών, που προκύπτουν από τις διεθνείς συνθήκες στις οποίες η Βουλγαρία είναι συμβαλλόμενο μέρος. Η Επιτροπή Προστασίας Προσωπικών δεδομένων είναι υπεύθυνη για την επίβλεψη της επεξεργασίας των προσωπικών δεδομένων.ν Τέλος, η Μονάδα για την Καταπολέμηση του Οργανωμένου Εγκλήματος, Τμήμα Εγκλημάτων Υπολογιστών (GDBOP) [64] είναι υπεύθυνη για την καταπολέμηση και τη διερεύνηση των κυβερνοεγκλημάτων.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CERT Bulgaria [65][66]είναι η εθνική CERT της Βουλγαρίας. Αποστολή της είναι η εφαρμογή προληπτικών μέτρων για τη μείωση των κινδύνων των περιστατικών ασφάλειας καθώς και η αντιμετώπισή τους. Οι στόχοι της ομάδας περιλαμβάνουν προστασία των πληροφοριών και των τεχνολογικών περιουσιακών στοιχείων, μείωση των επιπτώσεων των περιστατικών ασφάλειας στην κοινωνία της πληροφορίας, διάδοση τεχνικών πληροφοριών σχετικά με συμβάντα ασφάλειας των υπολογιστών, διεξαγωγή μελετών που σχετίζονται με τις νέες τεχνολογίες ασφάλειας δικτύων και πληροφοριών και οργάνωση της εκπαίδευσης και της ευαισθητοποίησης.

Ακαδημαϊκοί φορείς

Στην ακαδημαϊκή κοινότητα σημαντικό έργο προφέρει η National Laboratory of Computer Virology [68] η οποία είναι μια επιστημονική οργάνωση, που ειδικεύεται στον τομέα των ιών και της ασφάλειας του υπολογιστή. Επίσης το Πανεπιστήμιο της Σόφιας St. Kliment Ohridski, Τμήμα Μαθηματικών και Πληροφορικής [69] συνεργάζεται με εταιρείες πληροφορικής στην οργάνωση διαφόρων εκδηλώσεων και εκπαιδεύσεων στον τομέα της ασφάλειας πληροφορικής. Το Τεχνικό Πανεπιστήμιο της Σόφιας [70] παρέχει προπτυχιακά και μεταπτυχιακά προγράμματα, τα οποία περιλαμβάνουν μαθήματα στον τομέα της ασφάλειας πληροφορικής. Το Τεχνικό Πανεπιστήμιο της Βάρνας [71] μέσω του τμήματος Επιστήμης και Μηχανικών Υπολογιστών προσφέρει μαθήματα στον τομέα της ασφάλειας της πληροφορικής. Η σχολή συνεργάζεται με τις εταιρείες Cisco Systems και Microsoft. Τέλος η Ακαδημία του Υπουργείου Εσωτερικών[72] παρέχει εκπαίδευση επαγγελματιών για την Εθνική Αστυνομία και τα άλλα γραφεία εθνικής ασφάλειας.

Συνεργασία μεταξύ φορέων

Το Βουλγαρικό Κέντρο Αριστείας για το Κυβερνοέγκλημα [73] είναι ένα πρόγραμμα υπό υλοποίηση και αποσκοπεί στη δημιουργία ενός αποτελεσματικού δημόσιου-

ιδιωτικού κέντρου συνεργασίας των αρχών επιβολής του νόμου, ιδιωτικού τομέα, και της ακαδημαϊκής κοινότητας.

4.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Η εθνική CERT της Βουλγαρίας δημοσιεύει σε τακτική βάση εκθέσεις των πρόσφατων αδυναμιών, καθώς και προειδοποιήσεις για τις επιθέσεις στον κυβερνοχώρο. Η βουλγαρική Γενική Διεύθυνση για την Καταπολέμηση του Οργανωμένου Εγκλήματος (CDCOC) διατηρεί μια ιστοσελίδα [64][74] με σκοπό να παρέχει χρήσιμες πληροφορίες για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο, το phishing, τη σεξουαλική εκμετάλλευση των παιδιών, τα εγκλήματα κατά της πνευματικής ιδιοκτησίας και τα παράνομα τυχερά παιχνίδια. Η πλατφόρμα διατηρεί επίσης στατιστικά στοιχεία για τα σήματα που κατέθεσε σχετικά με τις παραβιάσεις στο διαδίκτυο. Η Επιτροπή για την Προστασία Προσωπικών Δεδομένων σε τακτά χρονικά διαστήματα διοργανώνει εκστρατείες πληροφόρησης σε σχέση με τις δραστηριότητές της στο πλαίσιο του νόμου για την προστασία των προσωπικών δεδομένων. Κατά την τελευταία μεγάλη καμπάνια δημιουργήθηκαν ειδικές ιστοσελίδες με χρήσιμες πληροφορίες και εκτυπώθηκαν ενημερωτικά φυλλάδια, που περιέχουν χρήσιμες συμβουλές για γονείς και παιδιά για τη χρήση των δικτύων και των υπηρεσιών του διαδικτύου.[74] Η βουλγαρική ιστοσελίδα για το παράνομο και επιβλαβές περιεχόμενο στο διαδίκτυο [75][76] στο πλαίσιο του προγράμματος SAFE-NET BG που υποστηρίζεται από την Ευρωπαϊκή Επιτροπή έχει ως στόχο να δημιουργήσει ένα ασφαλέστερο διαδίκτυο στη Βουλγαρία. Μέσω της ιστοσελίδας της επιτρέπει στους χρήστες του διαδικτύου να αναφέρουν περιπτώσεις παράνομου και επιβλαβούς περιεχομένου που διαδίδεται μέσω του Διαδικτύου. Στη Βουλγαρία γιορτάζεται επίσης κάθε χρόνο η Διεθνής Ημέρα για το Ασφαλέστερο Διαδίκτυο [76]. Επιπλέον το Νοέμβριο του 2013 έλαβε χώρα στο ξενοδοχείο Hilton στη Σόφια, της Βουλγαρίας ένα περιφερειακό τριήμερο φόρουμ για την ασφάλεια στον κυβερνοχώρο και το ηλεκτρονικό έγκλημα.[77] Το φόρουμ διοργανώθηκε από το Γνωμοδοτικό Συμβούλιο Ασφαλείας (OSAC), μαζί με τη βουλγαρική Κρατική Υπηρεσία Εθνικής Ασφαλείας με την οικονομική υποστήριξη των Η.Π.Α. Περισσότεροι από 270 συμμετέχοντες από αμερικανικές και διεθνείς εταιρείες και επιχειρήσεις, υπάλληλοι επιβολής του νόμου από περισσότερες από 15 χώρες, δικαστές, εισαγγελείς και άλλοι επαγγελματίες από τον δημόσιο και τον ιδιωτικό τομέα συζήτησαν για τις βέλτιστες πρακτικές σε μια

ποικιλία από θέματα που σχετίζονται με την ασφάλεια στον κυβερνοχώρο. Τέλος, στη Βουλγαρία έχουν διοργανωθεί δύο εθνικές ασκήσεις κυβερνοάμυνας. η PHOENIX το 2010 και η CYBER WINTER το 2011 [28].

4.5 Διεθνής Συνεργασία

Το Υπουργείο Μεταφορών, Τεχνολογίας των Πληροφοριών και Επικοινωνιών της Βουλγαρίας μέσω του ΕΑ ECNIS αποδίδει μεγάλη σημασία στη διεθνή συνεργασία και διατηρεί επαφές με την Ευρωπαϊκή Ένωση, μέσω του ENISA, με το NATO με το οποίο έχει υπογράψει ένα μνημόνιο συμφωνίας για την κυβερνοασφάλεια, και με την ITU [33]. Η Βουλγαρία λαμβάνει επίσης μέρος στην πανευρωπαϊκή άσκηση για την προστασία των κρίσιμων υποδομών πληροφοριών Cyber Europe [76] και ως μέλος του NATO συμμετέχει στην άσκηση κυβερνοάμυνας Cyber Coalition [57]. Σημαντική είναι επίσης η συνεργασία με τις Ηνωμένες Πολιτείες [78] καθώς το Υπουργείο Εσωτερικής Ασφάλειας των ΗΠΑ συνεργάζεται με τους Βούλγαρους εταίρους για την ανταλλαγή πληροφοριών, την επιβολή του νόμου και την ασφάλεια στον κυβερνοχώρο στο πλαίσιο συμφωνίας που υπεγράφη με Βούλγαρους αξιωματούχους στις 10 Οκτωβρίου 2010. Η Βουλγαρία είναι επίσης μέλος της Ένωσης Δικτύωσης Κεντρικής και Ανατολικής Ευρώπης (CEENet)[79], Η CEENet αποτελείται από 23 εθνικά δίκτυα έρευνας και εκπαίδευσης από τις εξής χώρες: Αλβανία, Αρμενία, Αυστρία, Αζερμπαϊτζάν, Βουλγαρία, Κροατία, Δημοκρατία της Τσεχίας, Εσθονία, Γεωργία, Ελλάδα, Ουγγαρία, Λετονία, Λιθουανία, ΠΓΔΜ, Μολδαβία, Πολωνία, Ρουμανία, Ρωσία, Σερβία, Μαυροβούνιο, Σλοβενία, Σλοβακία, Τουρκία και το Ουζμπεκιστάν. Η κύρια αποστολή της είναι να συντονίζει τις διεθνείς πτυχές των ακαδημαϊκών, ερευνητικών και εκπαιδευτικών δικτύων στην Κεντρική και Ανατολική Ευρώπη και σε γειτονικές χώρες. Ο συντονισμός πρόσφατα επεκτάθηκε στην περιοχή της ασφάλειας των δικτύων υπολογιστών. Η ανταλλαγή πληροφοριών μεταξύ των χωρών αυτών αποτελεί βασικό στοιχείο για την επίτευξη ενός αποδεκτού επίπεδου της ασφάλειας των ΤΠΕ σε ολόκληρη την περιοχή. Η κοινότητα CEENet σχεδιάζει να δημιουργήσει ένα δίκτυο συνεργασίας μεταξύ των ομάδων CERT [80]. Τέλος η CERT Bulgaria είναι ένα από τα διαπιστευμένα μέλη του Trusted Introducer [66].

Κεφάλαιο 5ο

Γαλλία

5.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Γαλλία προέβη τα τελευταία χρόνια σε ενδελεχή επανεξέταση των πολιτικών άμυνας και εθνικής ασφάλειας. Στη λεγόμενη γαλλική Λευκή Βίβλο για την Άμυνα και την Εθνική ασφάλεια που δημοσιεύθηκε το 2008 [81] καθορίστηκαν οι προτεραιότητες συμπεριλαμβάνοντας τις επιθέσεις στον κυβερνοχώρο ως μία από τις κύριες απειλές για την εθνική επικράτεια. Το 2013 δημοσιεύθηκε νέα Λευκή βίβλος [82] όπου επισημαίνεται η ολοένα αυξανόμενη σημασία των συστημάτων πληροφορικής στη ζωή των κοινωνιών η οποία αυξάνει τις απαιτήσεις για την άμυνα και την ασφάλεια των πληροφοριακών συστημάτων, τόσο για να διατηρηθεί η εθνική κυριαρχία όσο και για την υπεράσπιση της οικονομίας και της απασχόλησης. Η ικανότητα προστασίας από επιθέσεις στον κυβερνοχώρο, ανίχνευσης και εντοπισμού των δραστών έχει καθοριστεί ως ένα από τα σημαντικότερα στοιχεία της εθνικής κυριαρχίας.

Τον Ιούλιο του 2009, η γαλλική κυβέρνηση έκανε ένα πρώτο βήμα σε αυτή την πολιτική με τη δημιουργία του Anssi, του Γαλλικού Οργανισμού Ασφάλειας Δικτύων και Πληροφοριών, ο οποίος ενεργεί ως εθνική αρχή για την ασφάλεια στον κυβερνοχώρο. Η Γαλλία εξέδωσε Εθνική Στρατηγική για την Άμυνα και την Ασφάλεια των Πληροφοριακών Συστημάτων, τον Φεβρουάριο του 2012 [83]. Η στρατηγική έχει τέσσερις κύριους στόχους: να είναι η Γαλλία μια παγκόσμια δύναμη στην κυβερνοάμυνα, διατηρώντας παράλληλα την αυτονομία της, να εγγυηθεί την ελευθερία της λήψης αποφάσεων με την προστασία των πληροφοριών εθνικής κυριαρχίας, να ενισχυθεί η ασφάλεια των υποδομών ζωτικής σημασίας και να επιτευχθεί η ασφάλεια στην κυβερνοχώρο. Προκειμένου να επιτευχθούν οι στόχοι αυτοί, έχουν επιλεγεί επτά άξονες:

1. Καλύτερη πρόβλεψη και ανάλυση του περιβάλλοντος, προκειμένου να λαμβάνονται οι κατάλληλες αποφάσεις.
2. Εντοπισμός των επιθέσεων και αντιμετώπισή τους, προειδοποίηση των πιθανών θυμάτων και παροχή βοήθειας.

3. Αύξηση των επιστημονικών, τεχνικών και βιομηχανικών ικανοτήτων, στην κατεύθυνση της διατήρησης της απαραίτητης αυτονομίας.
4. Προστασία των πληροφοριακών συστημάτων του κράτους και των φορέων εκμετάλλευσης των υποδομών ζωτικής σημασίας, για την καλύτερη εθνική ανθεκτικότητα.
5. Προσαρμογή των νόμων ώστε να λαμβάνονται υπόψη οι εξελίξεις της τεχνολογίας.
6. Ανάπτυξη διεθνών συνεργασιών στους τομείς της ασφάλειας των πληροφοριακών συστημάτων, της καταπολέμησης του εγκλήματος στον κυβερνοχώρο, και της κυβερνοάμυνας.
7. Επικοινωνία και ενημέρωση, έτσι ώστε να μπορούν οι Γάλλοι πολίτες να κατανοούν καλύτερα τα ζητήματα που συνδέονται με την ασφάλεια των συστημάτων πληροφορικής.

5.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας/Προστασία Προσωπικών Δεδομένων [84]

Η Γαλλία ενέκρινε τον νόμο για την Πληροφορική και την Ελευθερία (*Loi Informatique et Libertés*) στις 6 Ιανουαρίου 1978 και ήταν μία από τις πρώτες Ευρωπαϊκές χώρες που είχαν νομοθεσία για την προστασία των δεδομένων. Ο νόμος παρέχει ένα νομικό πλαίσιο για τη χρήση των αναγνωριστικών σε βάσεις δεδομένων και την επεξεργασία των δεδομένων προσωπικού χαρακτήρα από οργανισμούς του δημόσιου και του ιδιωτικού τομέα. Ο νόμος προέβλεπε τη δημιουργία μιας Εθνικής Επιτροπής για την Πληροφορική και την Ελευθερία (CNIL). Η CNIL έχει επίσης συμβουλευτικό ρόλο στο σχεδιασμό των διοικητικών συστημάτων δεδομένων. Ο νόμος για την Πληροφορική και την Ελευθερία τροποποιήθηκε με τον νόμο 2004-801 της 6ης Αυγούστου 2004 για την εφαρμογή της οδηγίας προστασίας προσωπικών δεδομένων της ΕΕ (95/46/ΕΚ).

Νομοθεσία ηλεκτρονικού εμπορίου[84]

Ο νόμος για την εμπιστοσύνη στην ψηφιακή οικονομία εφαρμόζει την οδηγία της ΕΕ για το ηλεκτρονικό εμπόριο (2000/31/ΕΚ) και θεσπίζει το νομικό πλαίσιο για την ανάπτυξη των υπηρεσιών ηλεκτρονικού εμπορίου στη Γαλλία. Μεταξύ άλλων, ο νόμος αυτός καθορίζει την αρχή για τη λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου για διαφήμιση και ρυθμίζει την ευθύνη των παρόχων υπηρεσιών πιστοποίησης που εκδίδουν αναγνωρισμένα ψηφιακά πιστοποιητικά.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [84]

Ο κώδικας ταχυδρομικών και ηλεκτρονικών επικοινωνιών ορίζει τους κανόνες που σχετίζονται με τις ηλεκτρονικές επικοινωνίες. Μεταξύ άλλων η παράγραφος L.35-1 καλύπτει την κινητή τηλεφωνία και την πρόσβαση στο Internet και η L.45 καθορίζει την οργάνωση που διαχειρίζεται τα Γαλλικά Domain Names.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Η Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο έγινε στις 10 Ιανουαρίου 2006. Ο Ποινικός Κώδικας περιγράφει τα σχετικά αδικήματα: [85]

Άρθρο 323-1 Παράνομη προσπέλαση, παρεμβολή σε δεδομένα, παρεμβολή σε σύστημα.

Άρθρο 226-15 Παράνομη υποκλοπή.

Άρθρο 323-3-1 Κακή χρήση ηλεκτρονικών συσκευών, απάτη με Η/Υ.

Άρθρο 323-4 Πλαστογραφία με Η/Υ.

5.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Ο Γαλλικός Οργανισμός Ασφάλειας Δικτύων και Πληροφοριακών συστημάτων (Anssi) [86] είναι υπεύθυνος να αντιμετωπίζει «αμέσως» περιπτώσεις επιθέσεων σε υπολογιστές των υποδομών του κράτους. Οι βασικές αποστολές του οργανισμού είναι:

- Εντοπισμός και έγκαιρη αντίδραση στις επιθέσεις στον κυβερνοχώρο, χάρη στη δημιουργία ενός ισχυρού επιχειρησιακού κέντρου άμυνας, που λειτουργεί όλο το εικοσιτετράωρο και είναι υπεύθυνο για τη συνεχή επιτήρηση των ευαίσθητων κυβερνητικών δικτύων, καθώς και για την εφαρμογή των κατάλληλων μηχανισμών άμυνας.
- Αποτροπή των απειλών με την υποστήριξη της ανάπτυξης αξιόπιστων προϊόντων και υπηρεσιών για φορείς του δημοσίου και οικονομικούς παράγοντες.
- Παροχή αξιόπιστων συμβουλών και υποστήριξης σε κυβερνητικούς φορείς και επιχειρήσεις Υποδομών Ζωτικής Σημασίας

Στον οργανισμό, υπάρχει μια υπηρεσία που είναι επιφορτισμένη με την κατάρτιση δημοσίων υπαλλήλων στον τομέα της ασφάλειας των πληροφοριακών συστημάτων που ονομάζεται CFSSI. Ο οργανισμός περιέχει επίσης ένα φορέα πιστοποίησης της Κεντρικής Διεύθυνσης Ασφάλειας Πληροφοριακών Συστημάτων[87].

Η Γαλλική Αρχή Προστασίας Προσωπικών Δεδομένων (CNIL) [88] έχει τη συνολική ευθύνη ώστε να εξασφαλιστεί ότι η ανάπτυξη της πληροφορικής παραμένει στην υπηρεσία των πολιτών και δεν παραβιάζει τα ανθρώπινα δικαιώματα, την προστασία της ιδιωτικής ζωής ή τα προσωπικά δεδομένα ή τις δημόσιες ελευθερίες.

Η Ρυθμιστική Αρχή Ηλεκτρονικών Επικοινωνιών και Ταχυδρομικών Υπηρεσιών (ARCEP) [89] είναι αρμόδια για την εφαρμογή του νομικού πλαισίου που προκύπτει από τη μεταφορά των ευρωπαϊκών οδηγιών για τις ηλεκτρονικές επικοινωνίες.

Το Κεντρικό Γραφείο για την Καταπολέμηση Εγκλήματος της Πληροφορικής και των Επικοινωνιών (OCLCTIC) [90] ανήκει στην Γαλλική αστυνομία και έχει σκοπό να διευκολύνει και να συντονίζει τις δραστηριότητες της αστυνομίας κατά του κυβερνοεγκλήματος σε εθνικό επίπεδο. Τα καθήκοντα του OCLCTIC περιλαμβάνουν τη διεξαγωγή ερευνών και την παροχή βοήθειας στην αστυνομία, τη Γενική Διεύθυνση Ανταγωνισμού, Κατανάλωσης και Καταπολέμησης της Απάτης. Επίσης στηρίζει την τοπική και περιφερειακή αστυνομία σε θέματα πληροφορικής, συλλογής δεδομένων, και άλλες ανάγκες του εγκλήματος πληροφορικής.

Ομάδες Αντιμετώπισης Περιστατικών Ασφαλείας

Στη Γαλλία λειτουργεί ένα πλήθος από ομάδες CERT ανάλογα με τον τομέα στον οποίο δραστηριοποιούνται [13] όπως φαίνεται στον πίνακα 5.1. Επίσημη κυβερνητική ομάδα είναι η CERT-FR η οποία λειτουργεί εντός του Anssi και είναι υπεύθυνη για την ενίσχυση των διοικητικών οργάνων, για την εφαρμογή μέτρων προστασίας και την αντιμετώπιση επεισοδίων και επιθέσεων.

Χρηματοπιστωτικός τομέας	**Εμπορικών Οργανώσεων**
CERT-Societe Generale http://cert.societegenerale.com/ FIRST: member **CSIRT BNP Paribas** **CSIRT La Poste**	**CERT-LC** : http://www.solucom.fr/index.php/Nos-savoir-faire/Risk-management-securite-de-l-information/CERT-Solucom **Orange-CERT-CC** FIRST member

Εθνικά / κυβερνητικά / Στρατιωτικά **CERT-FR** http://www.certa.ssi.gouv.fr FIRST member	**Έρευνας και Εκπαίδευσης** **CERT-Renater** http://www.renater.fr/ FIRST member
Παρόχων υπηρεσιών **CERT-DVT** : http://www.cert-devoteam.com **Cert-IST** : http://www.cert-ist.com/ FIRST member **CERT-LEXSI** : http://www.lexsi.com/ FIRST member **CERT-XMCO** http://www.xmco.fr/index-en.html	

Πίνακας 5.1: CERT Γαλλίας

Ιδιωτικοί φορείς

Το GITEP TiCS [91] είναι ένα επαγγελματικό σωματείο που δημιουργήθηκε με σκοπό να εκπροσωπεί τον κλάδο των ΤΠΕ τόσο στη Γαλλία όσο και στην Ευρωπαϊκή Ένωση. Η Bertin Technologies [92] είναι Γαλλική εταιρεία που δραστηριοποιείται στους τομείς της κυβερνοασφάλειας και της ψηφιακής εγκληματολογίας.

Ακαδημαϊκοί φορείς

Το Τεχνολογικό Πανεπιστήμιο της Troyes (UTT) και το Πανεπιστήμιο του Μονπελιέ (UM1) έχουν αναλάβει τη δημιουργία του Γαλλικού Κέντρου Αριστείας για το κυβερνοέγκλημα (French 2Centre) [93]. Επίσης το Renater [94] είναι ένα εθνικό δίκτυο έρευνας, που ιδρύθηκε για να συγκεντρώσει την τηλεπικοινωνιακή υποδομή για το σκοπό της έρευνας και της εκπαίδευσης. Στις αρμοδιότητές του είναι η λειτουργία της CERT-Renater.

Συνεργασία μεταξύ φορέων [95]

Ο αρμόδιος υπουργός για τις ηλεκτρονικές επικοινωνίες προεδρεύει της Διυπουργικής Επιτροπής Συντονισμού των Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών για την άμυνα και τη δημόσια ασφάλεια (CICREST) [96][97]. Η Επιτροπή καταρτίζει και προτείνει κανόνες που πρέπει να εφαρμόζονται λαμβάνοντας υπόψη αφενός τη λειτουργία των δικτύων και των υπηρεσιών και αφ' εταίρου τις ανάγκες της εθνικής άμυνας και της δημόσιας ασφάλειας. Η σύνθεση και η λειτουργία της επιτροπής καθορίζεται με απόφαση του Πρωθυπουργού.

Στο πλαίσιο της ενίσχυσης των αρμοδιοτήτων του Υπουργείου Άμυνας στον κυβερνοχώρο, δημιουργήθηκε το 2011 η θέση του Γενικού Διευθυντή Κυβερνοάμυνας, με την ευθύνη για το συντονισμό των δραστηριοτήτων του Υπουργείου στον κυβερνοχώρο που ενεργεί ως κύρια διεπαφή μεταξύ των φορέων σε περίπτωση κρίσης στον κυβερνοχώρο.

Με το διάταγμα του 2006 για την Προστασία Κρίσιμων Υποδομών, κάθε φορέας ή πάροχος πρέπει να υποβάλει ένα γενικό σχέδιο για την ασφάλεια. Αυτό χρησιμοποιείται για να ελεγχθεί αν ο πάροχος είναι συμβατός με τις εθνικές κατευθυντήριες οδηγίες ασφαλείας. Το γαλλικό Υπουργείο Οικονομίας, Βιομηχανίας και Απασχόλησης εξακριβώνει αν το σχέδιο έχει εφαρμοστεί σωστά και ικανοποιητικά.

5.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Ο Anssi προσφέρει μια διαδικτυακή πύλη που παρέχει πληροφορίες και συμβουλές για τους πολίτες, τους επαγγελματίες και μικρομεσαίες επιχειρήσεις. Οι πληροφορίες περιλαμβάνουν ένα γλωσσάριο της ορολογίας ασφάλειας των υπολογιστών, κατευθυντήριες γραμμές για τη σωστή ρύθμιση του λογισμικού, τεχνικές πληροφορίες σχετικά με την ασφάλεια των πληροφοριών, on-line εκπαιδευτικά προγράμματα, λύσεις για την προστασία των υπολογιστών, και ειδοποιήσεις για απειλές [98]. Στη Γαλλία έχει συσταθεί επίσης μια εθνική πλατφόρμα έγκαιρης προειδοποίησης η οποία υποστηρίζεται από την αστυνομία και στην οποία μπορούν να σταλούν αναφορές για παράνομο περιεχόμενο ή συμπεριφορά κατά τη χρήση του Διαδικτύου [99]. Η Signal Spam [100] είναι μια ένωση γαλλικών οργανώσεων ενάντια στο spam. Η ένωση καλεί τους πολίτες και τους επαγγελματίες να συμμετάσχουν στον anti-spam αγώνα με την υιοθέτηση των βέλτιστων πρακτικών. Μια σειρά συστάσεων είναι διαθέσιμες on-line και σχετίζονται με την εμπιστευτικότητα, το φιλτράρισμα και την ασφάλεια. Επίσης αξίζει να αναφερθεί η ένωση CLUSIF[101], που διοργανώνει κάθε χρόνο αρκετά

συνέδρια για την ασφάλεια στην πληροφορική. Ο OSSIR είναι ένα σύλλογος μη κερδοσκοπικού χαρακτήρα από το 1996, και απευθύνεται σε χρήστες που ενδιαφέρονται για την ασφάλεια των πληροφοριακών συστημάτων και δικτύων. Κάθε χρόνο ο σύλλογος διοργανώνει την «Ημέρα της Ασφάλειας των Πληροφοριακών Συστημάτων» (JSSI) [102]. Η Ευρωπαϊκή Επιτροπή υποστηρίζει το Internet Sans Crainte ως πρόγραμμα ευαισθητοποίησης στη Γαλλία. Το Internet Sans Crainte είναι το γαλλικό τμήμα του ευρωπαϊκού δικτύου ευαισθητοποίησης, του Προγράμματος Safer Internet. Επίσης η γαλλική Υπηρεσία παρόχων διαδικτύου με βοήθεια χρηματοδότησης από την ΕΕ έχει δημιουργήσει μια τηλεφωνική γραμμή βοήθειας για την ασφάλεια του διαδικτύου [103][104]. Τέλος στη Γαλλία διεξάγεται η εθνική άσκηση κυβερνοάμυνας PIRANET [105][106].

5.5 Διεθνής Συνεργασία

Στο γαλλογερμανικό Συμβούλιο των Υπουργών, που πραγματοποιήθηκε τον Φεβρουάριο του 2010 η Γαλλία και η Γερμανία συμφώνησαν να συνεργαστούν για την ενίσχυση των μέτρων προστασίας κατά των επιθέσεων στον κυβερνοχώρο. Σ' αυτό το πλαίσιο οι υπεύθυνες γερμανικές και γαλλικές αρχές δηλαδή το BSI και η Anssi συνεργάζονται έχοντας αναπτύξει εταιρική σχέση [107]. Ο Anssi συμμετέχει επίσης στην άσκηση Cyber Storm [108][109], που οργανώνεται από το αμερικανικό Υπουργείο Εσωτερικής Ασφάλειας (DHS), στην οποία συμμετέχουν αρκετές χώρες και ιδιωτικές εταιρείες. Επιπλέον. η Γαλλία, συμμετέχει στην άσκηση Cyber Europe που διοργανώνεται από τον ENISA [28][109] και στην άσκηση κυβερνοάμυνας Cyber Coalition, του NATO [57][109]. Ο Anssi εκπροσωπεί τη Γαλλία, μαζί με το γαλλικό Υπουργείο Άμυνας. Η CERT-FR είναι ενεργό μέλος του EGC [31] και του FIRST [110]. Τέλος το Γαλλικό Κέντρο Αριστείας Κυβερνοεγκλήματος με την ολοκλήρωσή του θα είναι μέλος του 2Centre Network. Το 2Centre είναι ένα ευρωπαϊκό πρόγραμμα που χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή με στόχο να δημιουργηθεί ένα δίκτυο Κέντρων Αριστείας για την εκπαίδευση, την έρευνα και την εκπαίδευση για το έγκλημα στον κυβερνοχώρο στην Ευρώπη [93].

Κεφάλαιο 6ο

Γερμανία

6.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Εθνική Στρατηγική της Γερμανίας για την Προστασία Κρίσιμων Υποδομών (CIP στρατηγική) δημοσιεύτηκε τον Ιούνιο του 2009 [111] από το Ομοσπονδιακό Υπουργείο Εσωτερικών - Bundesministerium des Innern (BMI) και συνοψίζει τους στόχους, καθώς και την πολιτική - στρατηγική προσέγγιση, για την προστασία των υποδομών στον τομέα των ΤΠΕ. Για την υλοποίηση της στρατηγικής είναι διαθέσιμο ένα εκτεταμένο σύνολο μέσων όπως: Προγράμματα, σχέδια (Εθνικό Σχέδιο για την προστασία υποδομών πληροφοριών και των σχετικών σχεδίων για την προστασία των υποδομών πληροφορικής) πρότυπα, και κανονισμοί (π.χ. Πρότυπα Ασφάλειας Πληροφοριών). Στη Γερμανία, κυριαρχεί η αντίληψη ότι η προστασία των κρίσιμων υποδομών είναι ένα έργο που πρέπει να πραγματοποιείται από κοινού από την κυβέρνηση, τις εταιρείες, αλλά και από την κοινωνία των πολιτών. Οι κατευθυντήριες αρχές είναι οι σχέσεις εμπιστοσύνης στη συνεργασία μεταξύ του κράτους και των επιχειρήσεων σε όλα τα επίπεδα και η ύπαρξη των κατάλληλων και ανάλογων μέτρων για τη χρήση των πόρων που θα αυξήσουν το επίπεδο προστασίας.

Όπως αναφέρεται στη στρατηγική CIP, η Γερμανία αναγνωρίζει ότι για να είναι επιτυχής η κοινή δράση, θα πρέπει να υπάρχουν κατευθυντήριες γραμμές στρατηγικής οι οποίες περιγράφουν τη βασική φιλοσοφία, τη δράση και τις πρακτικές σε όλα τα θέματα ουσιαστικής σημασίας για την πολιτική ασφάλειας όσον αφορά την προστασία των κρίσιμων υποδομών. Για το λόγο αυτό στις αρχές του 2011, η Γερμανία δημοσίευσε τη νέα Ομοσπονδιακή Στρατηγική Κυβερνοασφάλειας [112]. Με τη νέα στρατηγική για την ασφάλεια στον κυβερνοχώρο, η Γερμανική Ομοσπονδιακή κυβέρνηση θα υιοθετήσει μέτρα για τις τρέχουσες απειλές με βάση τις δομές που δημιουργήθηκαν από το πρόγραμμα CIP και το σχέδιο για την ομοσπονδιακή διοίκηση. Η ομοσπονδιακή κυβέρνηση θα επικεντρωθεί ειδικά σε δέκα στρατηγικούς τομείς :

1. Προστασία των κρίσιμων υποδομών πληροφοριών. Είναι βασική προτεραιότητα της ασφάλειας στον κυβερνοχώρο και επεκτείνει τη συνεργασία που καθιερώνεται από το σχέδιο CIP

2. Ασφάλεια των συστημάτων πληροφορικής. Θα οργανώνονται κοινές πρωτοβουλίες με τη συμμετοχή ομάδων πολιτών έτσι ώστε να συγκεντρώνονται πληροφορίες και συμβουλές. Επίσης θα ενισχυθεί η διαθεσιμότητα εργαλείων για την ασφάλεια.

3. Ενίσχυση της ασφάλειας των συστημάτων ΤΠΕ στη δημόσια διοίκηση. Θα δημιουργηθεί μια κοινή, ενιαία και ασφαλή υποδομή δικτύου στην ομοσπονδιακή διοίκηση. Επίσης, η επιχειρησιακή συνεργασία των ομόσπονδων κρατών θα πρέπει να ενταθεί περαιτέρω με τη δημιουργία ενός συμβουλίου πληροφορικής.

4. Εθνικό Κέντρο αντιμετώπισης περιστατικών κυβερνοχώρου. Θα βελτιστοποιήσει την επιχειρησιακή συνεργασία μεταξύ όλων των κρατικών αρχών και θα συμβάλει στον συντονισμό των μέτρων προστασίας και αντιμετώπισης των περιστατικών ασφάλειας.

5. Εθνικό Συμβούλιο Κυβερνοασφάλειας. Προτίθεται να συντονίσει τα μέτρα πρόληψης και τις διεπιστημονικές προσεγγίσεις μεταξύ του δημόσιου και του ιδιωτικού τομέα . Θα συντονίζει τη διαχείριση και τη διασύνδεση στον τομέα της πληροφορικής σε ομοσπονδιακό επίπεδο, μεταξύ των διαφόρων υπουργείων και των ομοσπονδιακών υπηρεσιών.

6. Αποτελεσματικός έλεγχος της εγκληματικότητας στον κυβερνοχώρο. Περιλαμβάνει τη δημιουργία κοινών οργάνων με τον ιδιωτικό τομέα και τη συμμετοχή των αρμόδιων αρχών επιβολής του νόμου. Θα πρέπει να γίνει μια μεγάλη προσπάθεια για την επίτευξη παγκόσμιας εναρμόνισης του ποινικού δικαίου με βάση το Συμβούλιο της Ευρώπης και τη Σύμβαση για το έγκλημα στον κυβερνοχώρο.

7. Αποτελεσματικός συντονισμός των ενεργειών για την εξασφάλιση του κυβερνοχώρου στην Ευρώπη και σε όλο τον κόσμο. Η εξωτερική πολιτική της Γερμανίας στον κυβερνοχώρο θα πρέπει να διαμορφωθεί έτσι ώστε τα γερμανικά συμφέροντα και ιδέες σχετικά με την ασφάλεια στον κυβερνοχώρο να είναι συντονισμένα και να προωθηθούν σε διεθνείς οργανισμούς.

8. Χρήση αξιόπιστης τεχνολογίας πληροφορικής. Η Γερμανία θα συνεχίσει και θα εντείνει την έρευνα σχετικά με την ασφάλεια πληροφορικής και την προστασία των κρίσιμων υποδομών. Θα ενισχύσει την τεχνολογική κυριαρχία και την οικονομική της ικανότητα σε όλο το φάσμα των βασικών στρατηγικών ικανοτήτων πληροφορικής.

9. Ανάπτυξη προσωπικού στις ομοσπονδιακές αρχές. Αφορά την εκτίμηση του κατά πόσον απαιτείται επιπλέον προσωπικό και κατάρτιση στις αρχές προς το συμφέρον της ασφάλειας στον κυβερνοχώρο, καθώς και εντατικοποίηση της ανταλλαγής προσωπικού μεταξύ των ομοσπονδιακών αρχών.

10. Εργαλεία για να ανταποκριθεί η Γερμανία στις επιθέσεις στον κυβερνοχώρο. Ένα συντονισμένο και ολοκληρωμένο σύνολο εργαλείων θα πρέπει να δημιουργηθεί σε συνεργασία με τις αρμόδιες κρατικές αρχές.

6.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων[113]

Η Γερμανία έχει έναν από τους πιο αυστηρούς νόμους προστασίας δεδομένων στην Ευρωπαϊκή Ένωση. Η πρώτη νομοθεσία για την προστασία δεδομένων στον κόσμο ψηφίστηκε στο γερμανικό κρατίδιο της Έσσης το 1970. Το 1977 ακολούθησε ένας ομοσπονδιακός νόμος περί προστασίας των δεδομένων. Αντικαταστάθηκε το 1990, τροποποιήθηκε το 1994 και το 1997. Μια πρόσθετη αναθεώρηση πραγματοποιήθηκε τον Αύγουστο του 2002 για την ευθυγράμμιση της γερμανικής νομοθεσίας με την οδηγία για την προστασία των δεδομένων της ΕΕ (95/46/ΕΚ).

Νομοθεσία Ηλεκτρονικού Εμπόριού[113]

Ο νόμος για το ηλεκτρονικό εμπόριο της 14ης Δεκεμβρίου 2001 εφαρμόζει την οδηγία για το ηλεκτρονικό εμπόριο στην ΕΕ (2000/31/ΕΚ) στο γερμανικό δίκαιο.

Νομοθεσία ηλεκτρονικών επικοινωνών[113]

Ο νόμος για τη ρύθμιση των υπηρεσιών ηλεκτρονικού ταχυδρομείου και τροποποιήσεις άλλων νομοθετικών πράξεων εγκρίθηκε από το Ομοσπονδιακό Υπουργικό Συμβούλιο στις 13 Οκτωβρίου 2010 και τέθηκε σε ισχύ στις 3 Μαΐου 2011. Οι πάροχοι ηλεκτρονικού ταχυδρομείου πρέπει να πληρούν υψηλές απαιτήσεις για την ασφάλεια, τις λειτουργίες, τη διαλειτουργικότητα και την προστασία των δεδομένων.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Ο Γερμανικός Ποινικός Κώδικας(stGB) [114] περιγράφει τα αδικήματα σχετικά με το έγκλημα στον κυβερνοχώρο.

Άρθρο 202a: Κατασκοπεία δεδομένων.

Άρθρο 303a: Αλλοίωση δεδομένων.

Άρθρο 303b: Δολιοφθορά Υπολογιστή.

Άρθρο 263a: Ηλεκτρονική Απάτη.

Άρθρο 269: Παραποίηση Νομικών Δεδομένων.

Άρθρο 270: Παραπλάνηση σε έννομες σχέσεις μέσω της επεξεργασίας δεδομένων.

Νόμος για την ενίσχυση της ασφάλειας της Πληροφορικής (2009) [115]

Στις 14 Αυγούστου 2009, η βουλή ψήφησε τον νόμο για την ενίσχυση της ασφάλειας Πληροφορικής. Ο νόμος προβλέπει τις λεπτομέρειες σχετικά με τα κύρια καθήκοντα της Ομοσπονδιακής Υπηρεσίας για την Ασφάλεια Πληροφοριών(BSI). Ορίζει ότι η BSI είναι το κεντρικό γραφείο αναφοράς για τη συνεργασία μεταξύ των ομοσπονδιακών αρχών σε θέματα που σχετίζονται με την ασφάλεια της τεχνολογίας των πληροφοριών (προστασία από κακόβουλο λογισμικό, απειλές των ομοσπονδιακών επικοινωνιών, την καταστροφή των δεδομένων προσωπικού χαρακτήρα, καθώς και προειδοποιήσεις για αδυναμίες της ασφάλειας). Επιπλέον, ορίζει τη BSI ως εθνική αρχή πιστοποίησης της ομοσπονδιακής κυβέρνησης για την ασφάλεια πληροφορικής και ενεργεί ως αρμόδιο όργανο για την έκδοση κανονιστικών πράξεων.

6.3 Αρχές και Οργανισμοί

Η Συνολική ευθύνη ανήκει στο Ομοσπονδιακό Υπουργείο Εσωτερικών (BMI) [116], μαζί με οργανισμούς, όπως η BSI [117] και η Αστυνομική Υπηρεσία (BKA) [118]. Η ανάπτυξη στρατηγικής και η εφαρμογή της συντονίζεται με άλλα ομοσπονδιακά υπουργεία, ειδικά το Ομοσπονδιακό Υπουργείο Οικονομικών και Τεχνολογίας (BMWi) [119], το Ομοσπονδιακό Υπουργείο Δικαιοσύνης, το Ομοσπονδιακό Υπουργείο Εξωτερικών, το Ομοσπονδιακό Υπουργείο Άμυνας, και άλλους σχετικούς οργανισμούς, όπως η Ομοσπονδιακή Υπηρεσία Δικτύων (BNetzA)[120] .

Δημόσιοι φορείς

Το BMI είναι η αρμόδια κυβερνητική υπηρεσία για τη διασφάλιση της εσωτερικής ασφάλειας της Γερμανίας. Η υπηρεσία αυτή ασχολείται και συντονίζει θέματα, όπως η φυσική προστασία στο πλαίσιο της πολιτικής προστασίας και η πρόληψη απειλών στο πλαίσιο της επιβολής του νόμου. Επίσης είναι αρμόδιο για θέματα πληροφορικής που σχετίζονται με την προστασία κρίσιμων υποδομών. Η BSI ασχολείται με όλους τους τομείς που σχετίζονται με την ασφάλεια στον κυβερνοχώρο και λαμβάνει προληπτικά μέτρα, αναλύοντας τις αδυναμίες και αναπτύσσοντας προστατευτικά μέτρα, συμπεριλαμβανομένων της ασφάλειας των εφαρμογών και των υποδομών ζωτικής σημασίας, της ασφάλειας των δικτύων, της τεχνολογίας κρυπτογράφησης και τις νέες τεχνολογίες (π.χ. τη χρήση βιομετρικών στοιχείων, RFID). Η BSI ερευνά τους κινδύνους ασφάλειας που συνδέονται με τη χρήση της πληροφορικής και αναπτύσσει προληπτικά μέτρα. Επίσης παρέχει πληροφορίες σχετικά με τους κινδύνους και τις απειλές και αναπτύσσει τις κατάλληλες λύσεις. Το έργο αυτό περιλαμβάνει τον έλεγχο

και την αξιολόγηση των συστημάτων πληροφορικής, συμπεριλαμβανομένης της ανάπτυξής τους, σε συνεργασία με τη βιομηχανία. Τέλος εντός της υπηρεσίας λειτουργεί από το 2011 το κέντρο κυβερνοάμυνας (NCAZ). Η BKA, είναι αρμόδια σε πρώτο βαθμό για τη δίωξη των εγκλημάτων κατά της εσωτερικής ή εξωτερικής ασφάλειας της Γερμανίας και για τη δίωξη εγκλημάτων που αφορούν βλάβη ή καταστροφή των υποδομών ζωτικής σημασίας, που θα μπορούσαν να οδηγήσουν σε μια σοβαρή απειλή για τη ζωή, την υγεία ή τη λειτουργία της κοινωνίας. Περαιτέρω, η BKA είναι η κεντρική υπηρεσία για τη διερεύνηση εγκλημάτων που αφορούν την πληροφορική και τις επικοινωνίες. Το BMWi μέσω της BNetzaA είναι υπεύθυνο για την εξασφάλιση της διαθεσιμότητας επαρκούς τηλεπικοινωνιακής υποδομής και υπηρεσιών.

Η Επίτροπος Προστασίας Προσωπικών Δεδομένων και Ελευθερίας της Πληροφορίας έχει αναλάβει το καθήκον της επίβλεψης και της επιβολής του νόμου περί προστασίας των προσωπικών δεδομένων.

Ομάδες αντιμετώπισης περιστατικών ασφαλείας

Στη Γερμανία λειτουργεί ένα πλήθος από ομάδες CERT ανάλογα με τον τομέα στον οποίο δραστηριοποιούνται [13] όπως φαίνεται στον πίνακα 6.1. Η Εθνική CERT είναι η CERT-BUND [121]. Ιδρύθηκε το 2001, από τη BSI. Είναι ένα κεντρικό σημείο επαφής επιφορτισμένο με την προστασία και την ασφάλεια των δικτύων της ομοσπονδιακής δημόσιας διοίκησης. Τα κύρια καθήκοντα περιλαμβάνουν την προειδοποίηση και την ανταλλαγή πληροφοριών, τη συλλογή δεδομένων, ανάλυση, επεξεργασία, τεκμηρίωση και διάδοση των πληροφοριών, την ευαισθητοποίηση των ιθύνοντων της πληροφορικής, και τη συνεργασία με τις υπάρχουσες ομάδες CERT. Είναι μέλος του οργανισμού FIRST και λειτουργεί σε 24ωρη βάση.

Χρηματοπιστωτικός τομέας	**Τομέας Πωλητών ΤΠΕ**
ComCERT	**CERT BWI**
http://www.commerzbank.com/	http://ww.bwi-systeme.de
FIRST member	FIRST member
CSIRT-ECB	**SAP CERT**
csirt@ecb.europa.eu	FIRST member

dbCERT http://www.db.com FIRST member **S-CERT** http://www.s-cert.de/ FIRST member	
Εθνικά / κυβερνητικά / Στρατιωτικά **CERTBw** FIRST member **CERT NRW** **CERT-BUND** https://www.bsi.bund.de/IT-Krisenmanagement FIRST member **CERT-rlp** http://www.cert-rlp.de	**Εμπορικών Οργανώσεων** **BASF gCERT** cert@basf.com FIRST Member **BFK** http://www.bfk.de/en_index.html FIRST Member **CERT-VW** FIRST member **TK CERT** **XING** https://corporate.xing.com/english/company/security-at-xing/

Βιομηχανικός Τομέας
Siemens-CERT
http://www.siemens.com/cert
FIRST member
	Τηλεπικοινωνιακών παρόχων
	Deutsche Telekom-CERT
	http://www.telekom.com
	Vodafone-CERT
	http;//www.vodafone.com
	FIRST member

Παρόχων υπηρεσιών **dCERT** http://www.dcert.de/ FIRST: member **FTS-CERT** http://www.fujitsu.com/fts/ FIRST: Member	**Έρευνας και Εκπαίδευσης** **DFN-CERT** https://www.dfn-cert.de FIRST member **KIT-CERT** http://www.kit.edu/cert FIRST member **RUS-CERT**

GNS-CERT http://www.gnsec.net/ **PRE-CERT** http://www.pre-secure.de/ FIRST member **SECU-CERT** http://www.secunet.com FIRST member	http://cert.uni-stuttgart.de FIRST member

Πίνακας 6.1 Cert Γερμανίας

Ιδιωτικοί φορείς

Η BITKOM [122] είναι ο εκπρόσωπος των επιχειρήσεων πληροφορικής, και τηλεπικοινωνιών στη Γερμανία και αντιπροσωπεύει πάνω από 2.100 εταιρείες. Η BITKOM διοργανώνει ανταλλαγές μεταξύ εμπειρογνωμόνων και των στελεχών, προσφέροντας στα μέλη πλατφόρμες για συνεργασία και αλληλεπίδραση. Κεντρικά θέματα της πολιτικής ατζέντας της είναι η εκπαίδευση και η κατάρτιση των ειδικών της πληροφορικής και των τηλεπικοινωνιών σε θέματα πνευματικής ιδιοκτησίας, στην ασφάλεια και στην προστασία της ιδιωτικής ζωής, και σε νέες τεχνολογίες λογισμικού.
Η ECO [123] αντιπροσωπεύει και υποστηρίζει όλες τις επιχειρήσεις του Διαδικτύου. Με περίπου 700 οργανισμούς-μέλη, είναι η μεγαλύτερη ένωση του κλάδου στην Ευρώπη. Παρέχει στα μέλη της υποστήριξη σε θέματα νομιμότητας και ασφάλειας.
Η IT Security Made in Germany (ITSMIG) [124] είναι μια ένωση των γερμανικών εταιρειών ασφάλειας IT που έχει ως στόχο να προωθήσει λύσεις ασφάλειας πληροφορικής μεταξύ των γερμανικών προμηθευτών και συνεργατών σε χώρες του εξωτερικού.

Ακαδημαϊκοί φορείς

Στη Γερμανία υπάρχει μεγάλος αριθμός πανεπιστημίων που δραστηριοποιούνται στον τομέα της πληροφορικής και των επικοινωνιών. Από αυτά κυρίως ασχολούνται με θέματα ασφάλειας:
Το Ινστιτούτο για την Ασφάλεια στο Διαδίκτυο του Πανεπιστήμιο Εφαρμοσμένων Επιστημών του Gelsenkirchen [125] διεξάγει έρευνα και ανάπτυξη στον τομέα του Διαδικτύου, σε συστήματα έγκαιρης προειδοποίησης, στην ασφάλεια ηλεκτρονικού ταχυδρομείου, και στη διαχείριση ταυτοτήτων. Το International School of IT Security (ISITS) [126] είναι πολύ δραστήριο στην διοργάνωση συνεδριών ευαισθητοποίησης σε θέματα ασφάλειας. Επίσης το Πανεπιστήμιο της Καρλσρούης διεξάγει έρευνα μέσω

του Ινστιτούτου Κρυπτογραφίας και του Ινστιτούτου για την Ασφάλεια των συστημάτων [127]. Τέλος το Fraunhofer Institute for Secure Information Technology [128] προσφέρει συμβουλές σχετικά με την ανάπτυξη των εννοιών της ασφάλειας, και εκπονεί μελέτες τόσο για τον ιδιωτικό τομέα όσο και για την κυβέρνηση.

Συνεργασία μεταξύ φορέων [129]

Στη Γερμανία λειτουργεί από το 2011 το κέντρο κυβερνοάμυνας (NCAZ) από την BSI. Ο στόχος είναι να βελτιστοποιηθεί η λειτουργική συνεργασία μεταξύ των αρμόδιων κυβερνητικών υπηρεσιών. Αποτέλεσμα είναι η γρήγορη ανταλλαγή πληροφοριών, οι γρήγορες κριτικές και επακόλουθες συστάσεις για δράση. Οι συμμετέχοντες φορείς είναι η BSI, το Ομοσπονδιακό Γραφείο για την Προστασία του Συντάγματος (BFV), η Ομοσπονδιακή Υπηρεσία Πολιτικής Προστασίας (BBK) η BKA, και η Ομοσπονδιακή Υπηρεσία Πληροφοριών (BND). Όλοι οι οργανισμοί συνεργάζονται μεταξύ τους, εκπληρώνοντας παράλληλα πλήρως τις νομικές τους υποχρεώσεις. Το κέντρο είναι δικτυωμένο με τα κέντρα των υπόλοιπων αρχών. Για να εκτιμήσει η BSI μια επίθεση στον κυβερνοχώρο από τεχνική άποψη, η BND ασχολείται με το αν η επίθεση μπορεί να προέρχεται από μια ξένη υπηρεσία πληροφοριών και η BBK αξιολογεί τον αντίκτυπο των πιθανών επιθέσεων κατά των υποδομών. Οι υπόλοιπες αρχές συνεργαζόμενες προσθέτουν τις ιδέες τους σχετικά με τους φορείς της επίθεσης και τα εργαλεία επίθεσης, με αποτέλεσμα μέσα σε ένα πολύ σύντομο χρονικό διάστημα να δημιουργείται η συνολική εικόνα της κατάστασης.

Επίσης οι CERT- Bund, DFN Cert Services GmbH και Cert - Verbund έχουν μια συνεργατική σχέση και μεταξύ τους κάνουν τακτικές συσκέψεις [122]. Η CERT –Bund λειτουργεί ως κεντρικό σημείο επαφής για την επίλυση προβλημάτων σε ομοσπονδιακούς θεσμούς. Σε περιστατικά ασφάλειας η CERT-Bund παρέχει μια ομάδα ειδικών που ενημερώνει τους χρήστες αμέσως για τις απειλές και τα μέτρα που πρέπει να ληφθούν.

6.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Προκειμένου να αυξηθεί η ευαισθητοποίηση όσον αφορά τη σημασία της ασφάλειας στην πληροφορική, οι γερμανικές επιχειρήσεις κρίσιμων υποδομών έχουν ξεκινήσει συνεργασίες με τους οργανισμούς της δημόσιας διοίκησης, όπως η BSI, η Ομοσπονδιακή Αστυνομία, η Ομοσπονδιακή Υπηρεσία Δικτύων και άλλα αρμόδια

υπουργεία. Τον Σεπτέμβριο του 2010 η BSI κυκλοφόρησε ένα σχέδιο πλαισίου σε θέματα ασφάλειας που σχετίζονται με το cloud computing. Το σχέδιο καθορίζει τις ελάχιστες απαιτήσεις ασφαλείας για τους παρόχους υπηρεσιών cloud, και παρέχει μια βάση για τις συζητήσεις μεταξύ των παρόχων υπηρεσιών και των χρηστών. Η BSI für Bürger (BSI για το κοινό) [123] παρέχει σε συνεργασία με την BKA πληροφορίες σχετικά με θέματα ασφάλειας πληροφοριών για τους πολίτες, όπως το πώς να αποτρέψουν την παράνομη κυκλοφορία σε ιστοσελίδες και τους γενικούς κανόνες και νόμους γύρω από το Internet. Για την καλύτερη ενημέρωση του κοινού διαθέτει και τηλεφωνική γραμμή επικοινωνίας καθώς και ιστοσελίδα στο facebook. Επίσης, στην πλατφόρμα Bürger-CERT [124], το προσωπικό μικρών επιχειρήσεων μπορεί να λάβει πληροφορίες σχετικά με ιούς, worms, και άλλους κινδύνους για την ασφάλεια του υπολογιστή. Το BMI έχει εκδώσει ένα οδηγό διαχείρισης κινδύνων και κρίσεων για εταιρίες και κυβερνητικές αρχές, προκειμένου να τους βοηθήσει να προσδιορίσουν τους κινδύνους, να εφαρμόσουν προληπτικά μέτρα και να αντιμετωπίσουν τις κρίσεις αποτελεσματικά και αποδοτικά [125].Το 2005, μια σειρά από μεγάλες επιχειρήσεις, οργανισμούς, και επαγγελματικές οργανώσεις δημιούργησαν την πρωτοβουλία "Deutschland im Netz sicher" ώστε να συμβάλει ενεργά στην ενίσχυση της ασφάλειας των ΤΠΕ στη Γερμανία. Ως ένα ανεξάρτητο όργανο στοχεύει στην υποστήριξη των χρηστών και των μικρών επιχειρήσεων. Επίσης το Συμβουλευτικό Κέντρο Anti-Botnet είναι μια υπηρεσία της Γερμανικής Βιομηχανίας Internet το οποίο βοηθά στην αφαίρεση απειλών Botnet από τους υπολογιστές των χρηστών. Συνεργάζεται με τους παρόχους υπηρεσιών διαδικτύου, οι οποίοι πληροφορούν τους πελάτες που επηρεάζονται [126]. Επιπλέον το ομοσπονδιακό υπουργείο εκπαίδευσης και έρευνας (BMBF) παρείχε από το 2009 χρηματοδότηση περίπου € 66.000.000 για έργα στον τομέα της ασφάλειας της πληροφορικής και υποστηρίζει καινοτόμες διαδικασίες και τεχνολογίες για την προστασία των πληροφοριακών συστημάτων από επιθέσεις και μη εξουσιοδοτημένη πρόσβαση [127].

Στη Γερμανία διοργανώνεται σε ετήσια βάση το Διεθνές Συνέδριο IT Security Incident Management & IT ιforensics[128]. Επίσης έχουν διοργανωθεί οι εθνικές ασκήσεις κυβερνοάμυνας COM 10-1 (2010), CYBER DEFENCE (2011), LÜKEX (2011) [28][129].

6.5 Διεθνής Συνεργασία

Η Γερμανία ως πλήρες μέλος της Ε.Ε. και του ΝΑΤΟ συνεργάζεται με τους αρμόδιους φορείς σε θέματα που αφορούν την ασφάλεια των υπολογιστών όπως είναι ο Ευρωπαϊκός Οργανισμός Ασφάλειας Δικτύων και Πληροφοριών (ENISA), και η Αρχή Διαχείρισης Κυβερνοάμυνας του ΝΑΤΟ (CDMB). Επίσης είναι ιδρυτικό μέλος του CCDCoE [130]. Συμμετέχει στην πανευρωπαϊκή άσκηση Cyber-Europe [129] και στην άσκηση Cyber Atlantic μεταξύ Ε.Ε. και Η.Π.Α [28b]. Επίσης συμμετέχει στην ετήσια άσκηση Cyber Coalition που διοργανώνεται από το ΝΑΤΟ[57]. Στο πλαίσιο διμερούς συμφωνίας [107] η BSI και η Anssi της Γαλλίας συνεργάζονται έχοντας αναπτύξει εταιρική σχέση. Επίσης η BSI ανταλλάσσει πληροφορίες και εμπειρία σε τακτική βάση με το A-SIT της Αυστρίας βάση αντίστοιχων διμερών συμφωνιών συνεργασίας [30]. Επιπλέον, η BSI συμμετέχει στην άσκηση Cyber Storm που οργανώνεται από το αμερικανικό Υπουργείο Εσωτερικής Ασφάλειας (DHS), στην οποία συμμετέχουν αρκετές χώρες 13 και ιδιωτικές εταιρείες[108]. Όσον αφορά τη διεθνή συνεργασία των CERT η CERT-Bund είναι μέλος των ευρωπαϊκών κυβερνητικών CERT (EGC) [31]. Επίσης είναι μέλος του FISRT όπως επίσης και άλλες εικοσιμία CERT της χώρας [32].

Κεφάλαιο 7ο

Δανία

7.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Δανία είναι μια από τις χώρες που δεν έχει δημοσιεύσει Εθνική Στρατηγική Κυβερνοάμυνας. Το Δανικό στρατιωτικό δόγμα για το 2013-2017 [131]αναφέρεται στον κυβερνοχώρο ως ένα στρατιωτικό πεδίο μάχης, αλλά δεν παρέχει λεπτομέρειες σχετικά με συγκεκριμένες τεχνικές και επιχειρησιακές δυνατότητες της Δανίας στον κυβερνοχώρο και επικεντρώνεται κυρίως στην προστασία των στρατιωτικών συστημάτων πληροφορικής, από κυβερνοεπιθέσεις, χωρίς έμφαση στην ανάπτυξη μηχανισμών απάντησης. Η Υπηρεσία Πληροφοριών Άμυνας είναι υπεύθυνη για την εύρεση και την πρόληψη των απειλών στον κυβερνοχώρο και σχεδιάζει να δημιουργήσει τη μονάδα κυβερνοπολέμου. Η Δανική Επιτροπή Άμυνας πρότεινε τη θέσπιση επιχειρήσεων δικτύωσης ηλεκτρονικών υπολογιστών, προκειμένου να προωθήσει τις δυνατότητες του κυβερνοχώρου της Δανίας και την προστασία της τεχνολογίας της πληροφορικής των ενόπλων δυνάμεων.

7.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [132]

Ο νόμος τέθηκε σε ισχύ την 1η Ιουλίου 2000, προκειμένου να εφαρμοστεί η οδηγία 95/46/ΕΚ σχετικά με την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Ο νόμος που τροποποιήθηκε το 2007 και η εφαρμογή του επιβλέπεται από την Datatilsynet (Υπηρεσία Προστασίας Δεδομένων).

Νομοθεσία ηλεκτρονικού εμπορίου [132]

Ο νόμος για το ηλεκτρονικό εμπόριο (No 227) της 22ας Απριλίου 2002 εφαρμόζει την οδηγία 2000/31/ΕΚ, της 8ης Ιουνίου 2000 για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [132]

Ο εν λόγω νόμος τέθηκε σε ισχύ στις 25 Μαΐου 2011 και μεταφέρει το μεγαλύτερο μέρος του κανονιστικού πλαισίου της ΕΕ για τις ηλεκτρονικές επικοινωνίες στη Δανική νομοθεσία.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [37]

Ένα νομοσχέδιο για το έγκλημα στην πληροφορική παρουσιάστηκε στο δανικό κοινοβούλιο στις 5 Νοεμβρίου 2003. Το Κοινοβούλιο ενέκρινε το νομοσχέδιο στις 19 του Μάη 2004 προσθέτοντας στον ποινικό κώδικα τα εξής αδικήματα:

Άρθρο 193. Παρεμβολή σε δεδομένα, παρεμβολή σε σύστημα.

Άρθρο 263 Παράνομη προσπέλαση, Παράνομη υποκλοπή.

Άρθρο 279 Απάτη με Η/Υ, Κακή χρήση ηλεκτρονικών συσκευών.

Άρθρο 301 Πλαστογραφία με Η/Υ.

7.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Κέντρο για την ασφάλεια στον κυβερνοχώρο (CFCS) [133] αποτελεί μέρος της Στρατιωτικής Υπηρεσίας Πληροφοριών του Υπουργείου Άμυνας. Αποστολή του είναι η προστασία της Δανίας από τις απειλές στον κυβερνοχώρο. Είναι επίσης υπεύθυνο για την ασφάλεια των πληροφοριών και την ετοιμότητα στον τομέα των τηλεπικοινωνιών και είναι η αρχή εθνικής ασφάλειας πληροφορικής της Δανίας. Στο κέντρο λειτουργούν δύο υπηρεσίες προειδοποίησης: Το GovCERT για απειλές που στρέφονται κατά του κράτους και το MILCERT για άλλες στρατιωτικές υπηρεσίες. Ειδικότερα, οι δραστηριότητές του εστιάζονται σε τρεις τομείς :

- Στην προστασία από απειλές εναντίον των ΤΠΕ της Δανίας
- Στην εξασφάλιση μιας ισχυρής υποδομής στη Δανία
- Στην έγκαιρη προειδοποίηση και αντιμετώπιση των επιθέσεων στον κυβερνοχώρο, προκειμένου να ενισχυθεί η προστασία των συμφερόντων της Δανίας.

Η Υπηρεσία Πληροφοριών της Δανίας (PET) προκειμένου να βελτιώσει την απόδοση σε απειλές του κυβερνοχώρου και της ασφάλειας στον κυβερνοχώρο δημιούργησε ένα ειδικό τμήμα όσον αφορά τις απειλές στον κυβερνοχώρο που επηρεάζουν την εθνική ασφάλεια. Το Τμήμα έχει στενή συνεργασία με το CFCS. Προκειμένου να ενισχυθεί και ο συντονισμός με την αστυνομία προβλέπεται επίσης μια ειδική ομάδα εργασίας με εκπροσώπους της PET, της Εθνικής Αστυνομίας (Rigspolitiet), της τοπικής

αστυνομίας, του Γενικού Εισαγγελέα και των περιφερειακών εισαγγελέων [134]. Επίσης η εθνική αστυνομία και το γραφείο του εισαγγελέα αποφάσισαν τον Ιανουάριο του 2014 την ίδρυση ενός κέντρου για την καταπολέμηση, την ανάλυση και την πρόληψη του εγκλήματος στο κυβερνοχώρο [135]. Η Δανική Υπηρεσία Προστασίας Δεδομένων [136] είναι η κρατική αρχή που επιβλέπει τους νόμους προσωπικών δεδομένων. Δημιουργήθηκε μετά την εφαρμογή της κοινοτικής οδηγίας 95/46/ΕΚ, σχετικά με την προστασία των φυσικών προσώπων όσον αφορά τη διαδικασία των προσωπικών δεδομένων και την ελεύθερη κυκλοφορία. Ο οργανισμός ασκεί εποπτεία της επεξεργασίας των δεδομένων, ωστόσο, ο οργανισμός ασχολείται κατά κύριο λόγο σε συγκεκριμένες περιπτώσεις βάσει των ερευνών δημόσιων αρχών ή ιδιωτών ή υποθέσεις που συντάσσονται από την αρχή με δική της πρωτοβουλία.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η DK-CERT [137] ιδρύθηκε το 1991 από το Δανικό Κέντρο Εκπαίδευσης και Έρευνας (UNIC), μια εθνική οργάνωση που υπάγεται στο Υπουργείο Παιδείας της Δανίας. Η ομάδα εξυπηρετεί ένα ειδικό δίκτυο αφιερωμένο σε ερευνητικούς σκοπούς. Δημοσιεύει τακτικά άρθρα με προειδοποιήσεις, συμβουλές και ειδήσεις. Τα αντικείμενα αυτά περιλαμβάνουν, μεταξύ άλλων, πληροφορίες σχετικά με τα τρωτά σημεία στο λογισμικό και τα δίκτυα, καθώς και την πρόληψη των συμβάντων ασφαλείας. Ασκεί συμβουλευτικό ρόλο και δεν έχει την εξουσία να αναγκάσει άλλους να εκτελέσουν συγκεκριμένες πράξεις. Η CSIRT.DK [138] είναι η Ομάδα Αντιμετώπισης περιστατικών ασφαλείας που χειρίζεται υποθέσεις των επαγγελματικών πελατών του τηλεπικοινωνιακού παρόχου TDC. Η Danish GovCERT [139] θεσπίστηκε από την κυβέρνηση τον Μάιο του 2009 και καλύπτει ουσιαστικά τις κρατικές αρχές. Επιπλέον, οι περιφέρειες, οι δήμοι και ιδιωτικές εταιρείες που δραστηριοποιούνται σε κρίσιμες υποδομές μπορούν να ενταχθούν εθελοντικά. Η KMD IAC [140] είναι ένα τμήμα της ιδιωτικής εταιρείας πληροφορικής KMD. Αναπτύσσει και παρέχει λύσεις για τις τοπικές αρχές, το κράτος και ιδιωτικές εταιρίες. Η Secunia Research [141] είναι ιδιωτική εταιρεία πληροφορικής που παρέχει υπηρεσίες ασφάλειας.

Ιδιωτικοί φορείς

Η DI ITEK [142] είναι η δανική εμπορική ένωση των εταιριών πληροφορικής, τηλεπικοινωνιών και ηλεκτρονικών. Έχει ενεργό ρόλο στη συνεργασία ιδιωτικού και δημόσιου τομέα και προσφέρει πληροφόρηση στα μέλη της σε θέματα ασφάλειας της πληροφορικής

Ακαδημαϊκοί φορείς

Ο UNI-C DK [143] είναι ένας οργανισμός που υπάγεται στο Υπουργείο Παιδείας της Δανίας και προσφέρει μια ποικιλία υπηρεσιών πληροφορικής προς τις εκπαιδευτικές και ερευνητικές κοινότητες. Στις δραστηριότητές του συγκαταλέγεται και η λειτουργεία του DK-CERT. Το Πανεπιστήμιο Πληροφορικής της Κοπεγχάγης (ITU) [144] συμβάλλει μέσω ερευνητικών έργων στην ανάπτυξη της πληροφορικής και συμμετάσχει στη λειτουργεία του DK-CERT.

Συνεργασία μεταξύ φορέων [145]

Το Κέντρο για την ασφάλεια στον κυβερνοχώρο είναι η αρχή εθνικής ασφάλειας της πληροφορικής στη Δανίας. Βοηθά το Υπουργείο Άμυνας στο τομέα της ασφάλειας στον κυβερνοχώρο, στις διεθνείς εργασίες και ασκήσεις , ιδιαίτερα στην Ευρωπαϊκή Ένωση και το ΝΑΤΟ. Παράλληλα, στο κέντρο έχουν δημιουργηθεί τα κατάλληλα πλαίσια συνεργασίας με τους ιδιωτικούς φορείς κρίσιμων υποδομών ΤΠΕ καθώς και με τις δημόσιες αρχές που διαδραματίζουν σημαντικό ρόλο στην ασφάλεια στον κυβερνοχώρο στη Δανία. Συγκεκριμένα έχουν δημιουργηθεί δύο φόρουμ για την ασφάλεια των κρίσιμων υποδομών ΤΠΕ. Το πρώτο ως επαφή με τους εκπροσώπους των αρμοδίων υπουργείων και κυβερνητικών αρχών των κρίσιμων υποδομών ΤΠΕ με σκοπό την διασφάλιση του κυβερνοχώρου. Το δεύτερο ως επαφή δημόσιων και ιδιωτικών ιδιοκτητών και παρόχων υποδομών ΤΠΕ.

7.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Το Safer Internet Dennmark [156] αποτελεί ένα Κόμβο Ευαισθητοποίησης και αποτελείται από το Συμβούλιο για τα παιδιά και τους νέους της Δανίας, από τον οργανισμό Save the Children και από τον οργανισμό Cyberhus. Το Συμβούλιο ενεργεί ως Κόμβος Επαγρύπνησης στη Δανία από το 2004 στο πλαίσιο του προγράμματος Safer Internet plus. Το έργο CIT AWARE [147] έχει συσταθεί για να εκτελέσει μια σε βάθος διερεύνηση του επιπέδου ευαισθητοποίησης των κρίσιμων ζητημάτων ασφάλειας των ΤΠΕ από τους Δανούς πολίτες, προκειμένου να εκθέσει περιοχές στις οποίες πρέπει να αυξηθούν οι προσπάθειες για να μπορούν οι πολίτες να κατανοούν τι συνιστά ασφαλή και τι μη ασφαλή χρήση των ΤΠΕ. Η DK-CERT μέσω της ιστοσελίδας της παρέχει συμβουλές για την καταπολέμηση του spam καθώς και για την ασφάλεια στον χώρο της πληροφορικής σε χρήστες και μικρές επιχειρήσεις. Στην Δανία διοργανώνεται η εθνική άσκηση Κυβερνοασφάλειας KRISESTYRINGSØVELSE [28]. Τέλος στη

Κοπεγχάγη διοργανώνεται κάθε χρόνο ένα διεθνές συνέδριο για την Κρυπτογραφία και Ασφάλεια υπολογιστών [148] που έχει ως στόχο να φέρει σε επαφή κορυφαίους ακαδημαϊκούς επιστήμονες, ερευνητές και επιστήμονες για να ανταλλάξουν και να μοιραστούν τις εμπειρίες τους και τα αποτελέσματα της έρευνας σχετικά με όλες τις πτυχές της Κρυπτογραφίας και Ασφάλειας Υπολογιστών. Παρέχει επίσης ένα φόρουμ για τους ερευνητές, τους επαγγελματίες και τους εκπαιδευτικούς να παρουσιάσουν και να συζητήσουν τις πιο πρόσφατες καινοτομίες, τις τάσεις και τις ανησυχίες, στον τομέα της Κρυπτογραφίας και Ασφάλειας Υπολογιστών.

7.5 Διεθνής Συνεργασία

Στις 9 Φεβρουαρίου 2009 η έκτακτη συνεδρίαση των υπουργών Εξωτερικών των σκανδιναβικών χωρών πραγματοποιήθηκε στο Oslo με στόχο να παρουσιάσουν προτάσεις για τη συνεργασία μεταξύ των σκανδιναβικών χωρών. Μία από τις προτάσεις ήταν ένα σχέδιο για τη δημιουργία ενός δικτύου συνεργασίας μεταξύ των σκανδιναβικών χωρών το οποίο θα αποσκοπεί στην προστασία από επιθέσεις στον κυβερνοχώρο μέσω της ανταλλαγής εμπειριών και συντονισμού για την πρόληψη και την προστασία από επιθέσεις καθώς και την παροχή συμβουλών στις σκανδιναβικές χώρες που βρίσκονται σε πρώιμο στάδιο ανάπτυξης δυνατοτήτων κυβερνοασφάλειας [149]. Στις 3 Νοεμβρίου 2010 έγινε η ίδρυση του Δικτύου Ανταλλαγής Πληροφοριών CERT με την ονομασία NORDUnet. Οι χώρες της Βαλτικής έχουν επίσης προσκληθεί να συμμετάσχουν στο δίκτυο, το συντομότερο δυνατό.

Το Κέντρο για την ασφάλεια στον κυβερνοχώρο, είναι υπεύθυνο για τη διεθνή συνεργασία, ιδίως σε σχέση με την Ε.Ε. και συνεργάζεται με τον ENISA. Στα πλαίσια της συνεργασίας συμμετέχει στην άσκηση Cyber Europe [28]. Επιπλέον εκπροσωπεί τη χώρα στο NATO μαζί με το Δανικό Υπουργείο Άμυνας. και συμμετέχει στην άσκηση Cyber Coalition [57][150]. Όσον αφορά τις συνεργασίες των ομάδων CERT η GovCERT είναι ενεργό μέλος των ευρωπαϊκών κυβερνητικών ομάδων CERT (EGC) [31][151]. Επίσης οι πέντε από τις έξι ομάδες που λειτουργούν στην Δανία είναι μέλη του διεθνούς φόρουμ FIRST. Η DK-CERT εκπροσωπεί τη Δανία στο NORDUnet [152].

Κεφάλαιο 8ο

Ελλάδα

8.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Στην Ελλάδα μέχρι σήμερα δεν υπάρχει Εθνική Στρατηγική για την Κυβερνοασφάλεια. Οι μοναδικές επίσημες εθνικές στρατηγικές είναι η «Ψηφιακή Στρατηγική 2006-2013» [153] της οποίας βασικός στόχος είναι η χρήση των τεχνολογιών της Πληροφορικής για την επίτευξη υψηλότερης παραγωγικότητας στην οικονομία και για τη βελτίωση της ποιότητας ζωής των πολιτών και η στρατηγική για την ψηφιακή ανάπτυξη 2014-2020 [154]. Στην τελευταία αν και δεν υπάρχουν συγκεκριμένοι στόχοι και μέτρα σχετικά με την κυβερνοασφάλεια γίνεται ωστόσο αναφορά στην ανάγκη για αύξηση της εμπιστοσύνης και της ασφάλειας στο διαδίκτυο. Η Ελλάδα έχει ωστόσο ανακοινώσει πως θα υιοθετήσει Εθνική Στρατηγική Κυβερνοασφάλειας μέχρι το τέλος της προεδρίας της στην Ε.Ε. το πρώτο εξάμηνο του 2014 [155].

8.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [156]

Ο Νόμος 2472/1997 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, καθορίζει τους όρους υπό τους οποίους είναι νόμιμη η επεξεργασία δεδομένων προσωπικού χαρακτήρα και τις προϋποθέσεις που πρέπει να διενεργούνται έτσι ώστε να προστατεύονται τα θεμελιώδη δικαιώματα και οι ελευθερίες των φυσικών προσώπων και ιδίως η ιδιωτική τους ζωή. Συμπληρώθηκε με το Ν. 2774/1999 για την προστασία των προσωπικών δεδομένων στις τηλεπικοινωνίες, και από το νόμο 3115/2003 που ιδρύει την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).

Ο Νόμος 3471/2006 εκδόθηκε στις 28/06/2006, ως αναθεώρηση του νόμου 2472/1997, με σκοπό την ψήφιση των προϋποθέσεων όσον αφορά την επεξεργασία δεδομένων

προσωπικού χαρακτήρα και για την διασφάλιση του απορρήτου των τηλεπικοινωνιών. Ο Νόμος 3674/2008 καθορίζει τις υποχρεώσεις των φορέων παροχής υπηρεσιών όσον αφορά την ασφάλεια των τηλεφωνικών υπηρεσιών.

Νομοθεσία ηλεκτρονικού εμπορίου [156]

Το Προεδρικό Διάταγμα 131/2003 για το ηλεκτρονικό εμπόριο μεταφέρει την οδηγία 2000/31 του Ευρωπαϊκού Κοινοβουλίου σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά

Νομοθεσία ηλεκτρονικών επικοινωνιών [156]

Ο Νόμος 3431/2006 καθορίζει το γενικό πλαίσιο για την παροχή δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών στην Ελλάδα, ενώ ταυτόχρονα εφαρμόζει την πλήρη μεταφορά των κανονισμών της ΕΕ 2002/19/EC, 2002/20/EC, 2002/21/EC, 2002/22/EC και 2002/77/EC στο Εθνικό Δίκαιο.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Στον Ποινικό Κώδικα της Ελλάδας περιγράφονται αδικήματα που σχετίζονται με το έγκλημα στον Κυβερνοχώρο. [157]

Άρθρο 292Α Εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών.

Άρθρο 370 Παραβίαση του απορρήτου των επιστολών.

Άρθρο 370Α Παραβίαση του απορρήτου της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας.

Άρθρο 370Β, Άρθρο 370Γ Παραβίαση προγραμμάτων - στοιχείων ηλεκτρονικών υπολογιστών.

Άρθρο 386Α Απάτη με υπολογιστή.

8.3 Αρχές και Οργανισμοί

Δημόσιοι Φορείς

Το Υπουργείο Υποδομών, Μεταφορών και Δικτύων [158] είναι αρμόδιο για τη χάραξη πολιτικών για την ασφάλεια των δημόσιων δικτύων και των υπηρεσιών ηλεκτρονικών επικοινωνιών (Ν.3431/2006), από κοινού με συναρμόδια Υπουργεία. Το Υπουργείο Διοικητικής Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης [159] έχει ως αποστολή του να σχεδιάσει και να υλοποιήσει τον Οδικό Χάρτη εφαρμογής της ηλεκτρονικής διακυβέρνησης στη χώρα. Το Κέντρο Μελετών Ασφαλείας (ΚΕΜΕΑ) [160] είναι ερευνητικός και συμβουλευτικός φορέας του Υπουργείου Δημόσιας Τάξης & Προστασίας του Πολίτη στον τομέα της Ασφάλειας. Αποτελεί την Εθνική Αρχή της

Χώρας σε ό,τι αφορά την προστασία των κρίσιμων υποδομών, καθώς και το Εθνικό Σημείο Επαφής με τα αρμόδια όργανα της Ευρωπαϊκής Επιτροπής και τα Κράτη–Μέλη της Ευρωπαϊκής Ένωσης. Το ΚΕΜΕΑ είναι ένα από τα συμβαλλόμενα μέλη που έχουν δημιουργήσει το Ελληνικό Κέντρο για το Κυβερνοέγκλημα (GCC) [161]. Το Κέντρο αποτελεί μέρος μιας συντονισμένης ευρωπαϊκής προσπάθειας με σκοπό να βελτιωθεί η εκπαίδευση για την καταπολέμηση του αναπτυσσόμενου, εγκλήματος στον κυβερνοχώρο. Παράλληλα, αξιοποιώντας τόσο τη στενή συνεργασία με το ΚΕΜΕΑ, όσο και την ερευνητική εμπειρία των μελών του, το GCC σκοπεύει να καταστεί κέντρο αριστείας στον τομέα της έρευνας κατά του εγκλήματος στον κυβερνοχώρο. Το GCC συνδυάζει την τεχνογνωσία των εθνικών αρχών επιβολής του νόμου και του βιομηχανικού και ακαδημαϊκού κόσμου. Η Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ) [162] αποτελεί την Αρχή Ασφάλειας Πληροφοριών (INFOSEC) (Ν. 39/2008), είναι υπεύθυνη για την Εθνική CERT (Π.Δ. 325/2003) και αποτελεί την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Π.Δ. 325/2003). Η αποστολή της Αρχής είναι να ασχοληθεί με την πρόληψη, καθώς και την αντιμετώπιση, των ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης δεδομένων και συστημάτων πληροφορικής. Είναι ο αρμόδιος οργανισμός για την προστασία κυρίως του Δημόσιου Τομέα, μαζί με τις κρίσιμες εθνικές υποδομές [163].

Η Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας (ΔΙΚΥΒ/ΓΕΕΘΑ) [164] έχει επιτελικό ρόλο σε εθνικό επίπεδο. Το ΓΕΕΘΑ είναι αρμόδιο για την έκδοση του Εθνικού Κανονισμού Ασφάλειας (ΕΚΑ) (Π.Δ. 17/1974), σε συνεργασία με την Εθνική Υπηρεσία Πληροφοριών (ΕΥΠ). Ο ΕΚΑ έχει εφαρμογή σε όλη την ελληνική επικράτεια και τη δημόσια διοίκηση. Η Δίωξη Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας [165] υπάγεται στο Υπουργείο Δημόσιας Τάξης και Προστασίας του Πολίτη, και αποστολή της είναι η συμβολή στην πρόληψη, την έρευνα και την καταστολή εγκλημάτων ή αντικοινωνικών συμπεριφορών, που διαπράττονται μέσω του διαδικτύου ή άλλων μέσων ηλεκτρονικής επικοινωνίας. Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) [166] είναι αρμόδια για την τήρηση του απόρρητου και της ελεύθερης επικοινωνίας, για την πιστοποίηση προϊόντων ασφαλείας και για τον έλεγχο όλων των εμπλεκόμενων φορέων (Ν. 3115/2003) Η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ)[167] έχει αναλάβει τον έλεγχο των φορέων παροχής υπηρεσιών ηλεκτρονικής υπογραφής (Π.Δ.150/2001), καθώς και την αρμοδιότητα για την ακεραιότητα και διαθεσιμότητα

των δημόσιων δικτύων επικοινωνίας - και σε περιόδους έκτακτης ανάγκης. Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)[168] είναι αρμόδια για θέματα προστασίας προσωπικών δεδομένων και για τον έλεγχο όλων των εμπλεκόμενων φορέων (Ν. 2472/1997, Ν. 2774/1999).

Ομάδες αντιμετώπισης περιστατικών ασφαλείας[13]

Η NCERT-GR[169] είναι η Εθνική CERT και λειτουργεί στα πλαίσια της ΕΥΠ. Η αποστολή της είναι να μεριμνά για την πρόληψη και την αντιμετώπιση ηλεκτρονικών επιθέσεων κατά δικτύων επικοινωνιών, εγκαταστάσεων αποθήκευσης πληροφοριών και συστημάτων πληροφορικής. Επιπλέον είναι υπεύθυνη για τη συλλογή και την επεξεργασία ηλεκτρονικών δεδομένων και την ενημέρωση των αρμόδιων φορέων. Με το Νόμο 3649/2008 άρθρο 6 παράγρ.1, οι δημόσιες υπηρεσίες, τα νομικά πρόσωπα δημοσίου δικαίου και οι δημόσιες επιχειρήσεις υποχρεούνται να παρέχουν σε ειδικά εξουσιοδοτημένους υπαλλήλους της ΕΥΠ κάθε πληροφορία, στοιχείο ή συνδρομή για την εκπλήρωση της αποστολής της. Η FORTH CERT [170] είναι η Ομάδα του Ινστιτούτου Πληροφορικής του Ιδρύματος Έρευνας και Τεχνολογίας. και παρέχει υπηρεσίες σχετικά με συμβάντα ασφάλειας πληροφοριών. Οι κύριες υπηρεσίες περιλαμβάνουν προειδοποιήσεις, χειρισμό περιστατικών και συντονισμό δράσης. Η GRNET-CERT [171] παρέχει υπηρεσίες αντιμετώπισης περιστατικών ασφάλειας για το Ελληνικό Δίκτυο Έρευνας & Τεχνολογίας (ΕΔΕΤ) και σε όλα τα Ελληνικά Πανεπιστήμια, ερευνητικά ιδρύματα και εκπαιδευτικά δίκτυα στην Ελλάδα. Η AUTH-CERT [172] αντιμετωπίζει περιστατικά ασφάλειας που αφορούν τους χρήστες του δικτύου του Αριστοτέλειου Πανεπιστημίου.

Ιδιωτικοί φορείς

Ο Σύνδεσμος Επιχειρήσεων Πληροφορικής και Επικοινωνιών Ελλάδας (ΣΕΠΕ)[173] έχει ως μέλη του πάνω από 400 εταιρείες της χώρας στον τομέα της πληροφορικής και της βιομηχανίας τηλεπικοινωνιών. Κύριος στόχος του είναι η προώθηση των τεχνολογιών πληροφορικής και επικοινωνιών (ΤΠΕ). Ο ΣΕΠΕ εκπροσωπεί επίσης τα συμφέροντα των ελληνικών Επιχειρήσεων Πληροφορικής & Επικοινωνιών στην Ελληνική Κυβέρνηση, και την Ευρωπαϊκή Επιτροπή.

Ακαδημαϊκοί και ερευνητικοί φορείς

Το Εργαστήριο Πληροφοριακών & Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου [174] διεξάγει έρευνα σε τομείς όπως η ασφάλεια και η προστασία προσωπικών δεδομένων το ασφαλές ηλεκτρονικό εμπόριο, ανάπτυξη ασφαλών

πληροφοριακών συστημάτων και συμμετέχει σε αρκετά εθνικά και διεθνή προγράμματα ασφάλειας. Το Εργαστήριο Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών του Οικονομικού Πανεπιστημίου Αθηνών [175] διεξάγει επίσης έρευνα σε αρκετούς τομείς που σχετίζονται με την ασφάλεια των υπολογιστών. Το Εργαστήριο Ασφάλειας Συστημάτων του Τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς [176] διεξάγει έρευνα και εκπαιδευτικές δραστηριότητες σε διάφορους τομείς της ασφάλειας συστημάτων. Το Ίδρυμα Τεχνολογίας και Έρευνας (ΙΤΕ) [177] είναι ένα από τα μεγαλύτερα ερευνητικά κέντρα της χώρας και εποπτεύεται από τη Γενική Γραμματεία Έρευνας και Τεχνολογίας (ΓΓΕΤ). Οι ερευνητικές και τεχνολογικές κατευθύνσεις του ΙΤΕ επικεντρώνονται σε τομείς, όπως η πληροφορική και οι τηλεπικοινωνίες. Το Ι.Τ.Ε. είναι ο διαχειριστής του Ελληνικού Κέντρου για το Κυβερνοέγκλημα και διεξάγει έρευνα αιχμής στον τομέα της ασφάλειας στον κυβερνοχώρο, δημοσιεύοντας σε κορυφαία περιοδικά και συνέδρια καθώς και συμμετέχοντας σε έργα σχετικά με την ασφάλεια στον κυβερνοχώρο.

Συνεργασία φορέων

Στη Ελλάδα δεν υπάρχει κάποιο θεσμοθετημένο σχέδιο συνεργασίας μεταξύ των φορέων. Ο συντονισμός των εμπλεκόμενων για την αντιμετώπιση περιστατικών κυβερνοασφάλειας είναι ευθύνη της Εθνικής CERT στην οποία πρέπει να γίνεται η αναφορά των συμβάντων μέσω των στοιχείων επικοινωνίας που παρέχονται στην ιστοσελίδα της. Ωστόσο, η δημιουργία του Κέντρου Κυβερνοεγκλήματος της Ελλάδας είναι μια πρώτη προσπάθεια επίσημης και συντονισμένης συνεργασίας μεταξύ των φορέων. Προς το παρόν στο κέντρο συμμετέχουν το ΚΕΜΕΑ το ΙΤΕ και το Τμήμα Νομικής του ΑΠΘ.

8.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Στην Ελλάδα λαμβάνονται αρκετά μέτρα ευαισθητοποίησης και ενημέρωσης, τόσο από τις αρμόδιες αρχές, όσο και από ιδιωτικές επιχειρήσεις, ακαδημαϊκούς φορείς και ΜΚΟ. Ο δικτυακός τόπος της Ελληνικής Αρχής Προστασίας Δεδομένων περιέχει πληροφορίες για την ευαισθητοποίηση σχετικά με το spam. Οι Ελληνικοί πάροχοι καθώς και αρκετές τράπεζες διαθέτουν πληροφορίες στην ιστοσελίδα τους σχετικά με την ασφάλεια στο διαδίκτυο. Κύριος φορέας ενημέρωσης είναι το Ελληνικό Κέντρο Ασφαλούς Διαδικτύου (SIC)[178] που ιδρύθηκε το 2009 από τη συγχώνευση των υφιστάμενων κόμβων ευαισθητοποίησης Saferinternet.gr την τηλεφωνική γραμμή Safeline.gr και τη Γραμμή ΥποΣΤΗΡΙΖΩ. Από το 2009, οι τρεις οργανισμοί έχουν

στενή συνεργασία για την εκπλήρωση των στόχων του προγράμματος Safer Internet της Ευρωπαϊκής Επιτροπής. Το κέντρο υλοποιεί δραστηριότητες όπως διοργάνωση ενημερωτικών εκδηλώσεων για το κοινό, σεμινάρια προς εκπαιδευτικούς, προώθηση θεμάτων που σχετίζονται με την ασφάλεια στο Διαδίκτυο και στα ΜΜΕ, δημιουργία ψηφιακού και έντυπου ενημερωτικού υλικού, καθώς και τηλεοπτικές και ραδιοφωνικές καμπάνιες. Στο πλαίσιο αυτό, εξειδικευμένο προσωπικό έχει επισκεφθεί εκατοντάδες σχολεία σε όλη την Ελλάδα και έχει συντάξει διάφορα εγχειρίδια με στόχο την διαδικτυακή ασφάλεια των μαθητών, των εκπαιδευτικών, των γονέων και άλλων ευαίσθητων ομάδων. Η SafeLine συγκεντρώνει στατιστικά στοιχεία σε μηνιαία βάση για τις εκθέσεις που λαμβάνει. Οι εκθέσεις κατατάσσονται σε διάφορες κατηγορίες σύμφωνα με την επίσημη κατάταξη του INHOPE, την ευρωπαϊκή ένωση των παρόχων hotline. Τα στατιστικά στοιχεία εγγράφονται στο site INHOPE σε μηνιαία βάση, συμβάλλοντας έτσι στα διεθνή στατιστικά στοιχεία που συλλέγονται. Επιπλέον, οι αθροιστικές στατιστικές αναφορές δημοσιεύονται στην ιστοσελίδα της SafeLine. Η Ελληνική ανοικτή γραμμή επικοινωνίας συνεργάζεται στενά με τις αρχές επιβολής του νόμου, και ειδικότερα τη Μονάδα Δίωξης Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας. Η SafeLine προωθεί όλες τις αναφορές που αφορούν παράνομο περιεχόμενο στο εξειδικευμένο προσωπικό της αστυνομίας. Εκπρόσωποι της ελληνικής αστυνομίας συμμετέχουν επίσης στις συμβουλευτικές συνεδριάσεις του διοικητικού συμβουλίου της Ελληνικής hotline συμμετέχοντας σε συζητήσεις σχετικά με το πώς να αντιμετωπίσουν την παράνομη δραστηριότητα στο Διαδίκτυο. Μια πρόσφατη έρευνα έδειξε ότι περισσότερο από το 50% της ελληνικής κοινής γνώμης είναι ενήμεροι για την ύπαρξη και την αποστολή της SafeLine[179][180]. Η Δίωξη Ηλεκτρονικού Εγκλήματος στην ιστοσελίδα της παρέχει αρκετές πληροφορίες και συμβουλές για ασφαλή πλοήγηση στο διαδίκτυο. Επίσης έχει δημιουργήσει δική της σελίδα ευαισθητοποίησης που απευθύνεται κυρίως σε παιδιά και γονείς [181]. Επιπλέον στην Ελλάδα διοργανώνεται σε ετήσια βάση η άσκηση κυβερνοάμυνας «Πανόπτης» Η άσκηση διοργανώνεται και συντονίζεται από την Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ και σκοπός της είναι η εξάσκηση των εμπλεκομένων, η δοκιμή των υφισταμένων σχεδίων, δομών και διαδικασιών που αφορούν στην αντιμετώπιση μειζόνων συμβάντων στον Κυβερνοχώρο καθώς και η επαύξηση του επιπέδου συνεργασίας μεταξύ των εμπλεκομένων φορέων. Στην άσκηση συμμετέχουν φορείς του Δημοσίου, Πανεπιστημιακά Ιδρύματα, Κρατικές Υπηρεσίας Ασφαλείας καθώς και

οι ιδιωτικοί πάροχοι Διαδικτύου της χώρας οι οποίοι διαχειρίζονται το σύνολο του δικτύου της χώρας [182][183].

8.5 Διεθνής Συνεργασία

Η Ελλάδα ως πλήρες μέλος της Ε.Ε. και του NATO συνεργάζεται με τους αρμόδιους φορείς σε θέματα που αφορούν την ασφάλεια των υπολογιστών όπως είναι ο η Αρχή Διαχείρισης Κυβερνοάμυνας του NATO και ο ENISA ο οποίος έχει ως έδρα του την Ελλάδα. Στα πλαίσια αυτών των συνεργασιών διοργανώθηκε το 2013 στην Αθήνα το 2ο Διεθνές Συνέδριο του ENISA για τη Συνεργία στις Κυβερνοκρίσεις και στις Ασκήσεις[184] και το 2014 κατά τη διάρκεια της Ελληνικής Προεδρίας στην Ε.Ε. το συνέδριο σχετικά με την ασφάλεια και την προστασία του κυβερνοχώρου της Ε.Ε [185]. Επίσης η Ελλάδα συμμετέχει στην πανευρωπαϊκή άσκηση Cyber Europe που διοργανώνεται από τον ENISA[28]. Η ΔΙΚΥΒ/ΓΕΕΘΑ καθώς και άλλοι δημόσιοι φορείς συμμετέχουν επίσης σε Νατοϊκές ασκήσεις όπως η Cyber Coalition που διοργανώνεται από το 2011. Το 2010 συμμετείχε στην Cyber Defence Exercise (NCDEX 10)[186][187]. Ο σκοπός των ασκήσεων αυτών είναι η εκπαίδευση στις διαδικασίες λήψης αποφάσεων, σχετικά με τις τεχνικές διαδικασίες σε επιχειρησιακό επίπεδο και η ανάπτυξη της συνεργασίας μεταξύ των μελών του NATO σε θέματα άμυνας στον κυβερνοχώρο. Τέλος η Ομάδα CERT του Ιδρύματος Έρευνας και Τεχνολογίας είναι μέλος του FIRST [32] του διεθνούς φόρουμ συνεργασίας των ομάδων αντιμετώπισης έκτακτων περιστατικών Κυβερνοασφάλειας.

Κεφάλαιο 9ο

Εσθονία

9.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Εσθονία είναι μία από τις πιο ραγδαία αναπτυσσόμενες κοινωνίες της πληροφορίας στην Κεντρική και Ανατολική Ευρώπη. Κάθε χρόνο το Τμήμα Πληροφοριακών Συστημάτων της Εσθονίας (RISO)[188], δημοσιεύει μια έκθεση για τις εξελίξεις της δημόσιας διοίκησης. Η έκθεση αυτή περιέχει πληροφορίες όπως η στρατηγική και οι κανονισμοί ασφάλειας, αλλά καλύπτει και θέματα όπως της ασφάλειας στον κυβερνοχώρο και της ηλεκτρονικής ταυτότητας. Οι εκθέσεις είναι εθνικές εκδόσεις και είναι διαθέσιμες στον δικτυακό τόπο της RISO.

Στρατηγική Κυβερνοασφάλειας [189]

Η Επιτροπή Στρατηγικής Κυβερνοασφάλειας υπό την ηγεσία του Υπουργείου Άμυνας σε συνεργασία με το Υπουργείο Παιδείας και Έρευνας, το Υπουργείο Δικαιοσύνης, το Υπουργείο Οικονομικών Υποθέσεων και Επικοινωνιών, το Υπουργείο Εσωτερικών και το Υπουργείο Εξωτερικών έχουν υποβάλει τη «στρατηγική ασφάλειας για τον κυβερνοχώρο της Εσθονίας για την περίοδο 2008-2013». Η στρατηγική αυτή εγκρίθηκε από την κυβέρνηση τον Μάιο του 2008. Καθορίζει τις προτεραιότητες και τις δραστηριότητες που αποσκοπούν στη βελτίωση της ασφάλειας του κυβερνοχώρου χώρας. Η στρατηγική επικεντρώνεται στους ακόλουθους τομείς: Στις ευθύνες του κράτους και των ιδιωτικών οργανισμών, στις εκτιμήσεις ευπάθειας των κρίσιμων εθνικών υποδομές πληροφορικής, στο σύστημα αντίδρασης, στις εγχώριες και διεθνείς νομικές πράξεις, στη διεθνή συνεργασία, καθώς και στην κατάρτιση την ευαισθητοποίηση. Οι αρχές της τρέχουσας στρατηγικής είναι σύμφωνες με το Πλαίσιο Διαλειτουργικότητας Ασφάλειας Πληροφοριών, που εγκρίθηκε από το Υπουργείο Οικονομίας και Επικοινωνιών.

Στρατηγική της Κοινωνίας της Πληροφορίας 2013[190]

Το πλαίσιο αυτό καθορίζει τις αρχές, για την ασφάλεια των πληροφοριών, τις αρχές για την εκπαίδευση στην ασφάλεια των πληροφοριών, καθώς και τις δραστηριότητες που είναι απαραίτητες για την προστασία των υποδομών πληροφορικής. Το έγγραφο ήταν το πρώτο βήμα προς την καθιέρωση κοινών προτύπων για τις κρατικές υπηρεσίες και

τον ιδιωτικό τομέα με σκοπό την προστασία των υποδομών ζωτικής σημασίας της χώρας.

Πολιτική Ασφάλειας Πληροφοριών [191]

Το Εσθονικό Υπουργείο Οικονομικών και Επικοινωνιών (MEAC) έχει δημοσιεύσει μια πολιτική ασφάλειας των πληροφοριών σε εθνικό επίπεδο που καθορίζει και συντονίζει τις προσεχείς πρωτοβουλίες που σχετίζονται με την ηλεκτρονική προστασία. Ειδικοί στόχοι περιλαμβάνουν την εξάλειψη των κινδύνων, την υπεράσπιση των βασικών ανθρωπίνων δικαιωμάτων, την ασφάλεια των πληροφοριών, τη συμμετοχή σε διεθνείς πρωτοβουλίες που σχετίζονται με την ηλεκτρονική προστασία, καθώς και την ανταγωνιστικότητα της οικονομίας.

9.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας Ιδιωτικότητας / Προστασίας Προσωπικών Δεδομένων[192]

Ο νόμος τέθηκε σε ισχύ στις 19 Ιουλίου 1996 και τροποποιήθηκε το 2003, ώστε να γίνει πλήρως συμβατός με την οδηγία προστασίας δεδομένων της ΕΕ 95/46/ΕΚ, και τροποποιήθηκε εκ νέου τον Ιανουάριο του 2008. Ο νόμος προστατεύει τα θεμελιώδη δικαιώματα και τις ελευθερίες των προσώπων όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων, σύμφωνα με το δικαίωμα των ατόμων να λάβουν ελεύθερα τις πληροφορίες που διαδίδονται για δημόσια χρήση.

Νομοθεσία Ηλεκτρονικού εμπορίου[192]

Ο νόμος των υπηρεσιών της κοινωνίας της πληροφορίας ψηφίστηκε στις 14 Απριλίου 2004 και τέθηκε σε ισχύ την 1η Μαΐου 2004. Υλοποιεί την οδηγία της ΕΕ 2000/31/ΕΚ σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά. Καθορίζει τις απαιτήσεις για τους φορείς παροχής υπηρεσιών, καθώς και την οργάνωση της εποπτείας και την ευθύνη σε περίπτωση παραβίασης αυτών των απαιτήσεων. Ο νόμος τροποποιήθηκε στις 21 Ιανουαρίου 2010.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Η Εσθονία τροποποίησε τον Ποινικό της Κώδικα το 2002 και επικύρωσε τη σύμβαση του Συμβούλιου της Ευρώπης για το έγκλημα στον κυβερνοχώρο στις 12 Μαΐου 2003. Τα ακόλουθα άρθρα της Εσθονίας Ποινικού Κώδικα [193] σχετίζονται με το έγκλημα στον κυβερνοχώρο και την ασφάλεια:

Άρθρο 206 Δολιοφθορά υπολογιστή.

Άρθρο 207 Καταστροφή δίκτυού υπολογιστών.

Άρθρο 208 Εξάπλωση ιών υπολογιστών.

Άρθρο 217 Παράνομη χρήση των ηλεκτρονικών υπολογιστών, συστήματος ηλεκτρονικού υπολογιστή ή δικτύου υπολογιστών.

Άρθρο 284 Αποκάλυψη κωδικών προστασίας.

9.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Από την κεντρική κυβέρνηση το Υπουργείο Εθνικής Οικονομίας και Επικοινωνιών [194] είναι υπεύθυνο για την ανάπτυξη και την εφαρμογή των πολιτικών ασφάλειας ενώ το Υπουργείο Εσωτερικών [195] συμμετέχει στη διαχείριση κρίσεων, την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο και είναι υπεύθυνο για το συντονισμό της Ασφάλειας Πληροφοριών της Εσθονίας. Το Υπουργείο Άμυνας [196] συνεργάζεται με το MEAC σχετικά με την ενημέρωση της πολιτικής ασφάλειας στους τομείς της διαχείρισης κρίσεων, του ηλεκτρονικού εγκλήματος, της εκπαίδευσης και της κατάρτισης. Το Γραφείο Εγκλημάτων Η/Υ της Κεντρικής Αστυνομίας [197] είναι υπεύθυνο για τον εντοπισμό και τη διερεύνηση των εγκλημάτων πληροφορικής. Η Επιθεώρηση Προστασίας Δεδομένων [198] έχει ως καθήκον την προστασία των προσωπικών δεδομένων και τη διαχείριση των πληροφοριών του δημόσιου στο διαδίκτυο. Το Τμήμα Πληροφοριακών Συστημάτων (RISO) [1] δημιουργήθηκε για το συντονισμό των κρατικών δράσεων, των πολιτικών πληροφορικής και των σχεδίων ανάπτυξης στον τομέα των κρατικών συστημάτων διοίκησης. Το τμήμα είναι παράρτημα υπό τον διοικητικό έλεγχο του MEAC. Το Γραφείο του Εθνικού Συντονισμού Ασφαλείας [199] συμβουλεύει τον Πρωθυπουργό για θέματα που σχετίζονται με την εθνική ασφάλεια. Το Τμήμα για την Προστασία Κρίσιμων Υποδομών Πληροφοριών (CIIP) [200] ασχολείται με την προστασία των σημαντικών πληροφοριακών συστημάτων στην Εσθονία. Είναι ένα ξεχωριστό τμήμα εντός του Κέντρου Πληροφορικής της Εσθονίας (RIA) [201] και εργάζεται στο στρατηγικό επίπεδο της Ασφάλειας Πληροφοριών.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας

Η CERT-EE [202] είναι η επίσημη εθνική CERT και λειτουργεί ως ένα ξεχωριστό τμήμα εντός του Κέντρου Πληροφορικής [201] που είναι αρμόδιο για τη διαχείριση

των περιστατικών ασφάλειας σε δίκτυα υπολογιστών. Επίσης είναι το σημείο επαφής για τη διεθνή συνεργασία στον τομέα της ασφάλειας πληροφορικής.

Ιδιωτικοί φορείς

Η Εσθονική Κοινωνία της Πληροφορικής (EITS) [203] είναι ένας ιδιωτικός φορέας υπεύθυνος για την εποπτεία της νομιμότητας της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, διατηρώντας βάσεις δεδομένων, σε θέματα διαδικασίας παραβίασης διοικητικού δικαίου στις περιπτώσεις που προβλέπονται από το νόμο. Η EITS συνεργάζεται με τις εθνικές αρχές. Η Εσθονική Ένωση της Πληροφορικής και των Τηλεπικοινωνιών (ITL) [204] έχει ως στόχο να ενώσει όλες τις εσθονικές εταιρείες πληροφορικής και τηλεπικοινωνιών και να προωθήσει τη συνεργασία μεταξύ τους για την ανάπτυξη της κοινωνίας της πληροφορίας. Το Ινστιτούτο Estonian Forensic Science Institute (EFSI) [205] είναι ένας ιδιωτικός οργανισμός επιβολής του νόμου που δραστηριοποιείται στην ψηφιακή εγκληματολογία και την κυβερνοασφάλεια.

Ακαδημαϊκοί φορείς

Το Πανεπιστήμιο Τεχνολογίας του Ταλίν [206] μέσω τον προγραμμάτων του παραδίδει μαθήματα που περιλαμβάνουν επιθέσεις δικτύων υπολογιστών και Μηχανισμούς Άμυνας, Εφαρμογές Δικτύων, Δίκτυα Υπολογιστών, και Εισαγωγή στην Ασφάλεια Δεδομένων. Το Πανεπιστήμιο του Tartu [207] δραστηριοποιείται επίσης στο χώρο της έρευνας της ασφάλειας στον κυβερνοχώρο.

Συνεργασία μεταξύ φορέων

Στην Εσθονία υπάρχουν πολλά υπουργεία των οποίων αντίστοιχες υπομονάδες συμμετέχουν άμεσα στην ασφάλεια των ΤΠΕ. Τα κύρια καθήκοντα συντονισμού έχουν ανατεθεί στο Υπουργείο Οικονομικών και Επικοινωνιών. Το MEAC διαδραματίζει ηγετικό ρόλο στην ασφάλεια των πληροφοριών, με δύο κεντρικές υπηρεσίες τις RISO και RIA. Η CERT-EE είναι υπεύθυνη για τη διαχείριση των περιστατικών ασφάλειας στην Εσθονία. Καθήκον της είναι η εφαρμογή προληπτικών μέτρων προκειμένου να μειωθούν οι πιθανές ζημιές από περιστατικά ασφαλείας και να η παροχή βοήθειας στην αντιμετώπιση των απειλών. Η CERT-EE ασχολείται επίσης με την ασφάλεια συμβάντων στα εσθονικά δίκτυα, σε περιστατικά πού ξεκίνησαν εκεί είτε στο εξωτερικό.

9.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Κύρια δράση είναι το Πρόγραμμα «Ενίσχυση της ευαισθητοποίησης της κοινωνίας της πληροφορίας» [208][209]. Ο στόχος του προγράμματος είναι η προώθηση της ανάπτυξης νέων ηλεκτρονικών υπηρεσιών και η εξασφάλιση της αειφόρου ανάπτυξης της κοινωνίας της πληροφορίας μέσω της ευαισθητοποίησης στην ασφάλειας των πληροφοριών. Αρκετές ιστοσελίδες λειτουργούν στην Εσθονία με σκοπό την ευαισθητοποίηση του ευρύτερου κοινού. Επίσης, η εσθονική αρχή εποπτείας της προστασίας δεδομένων ενημερώνει και προειδοποιεί για spam στο δικτυακό της τόπο. Η μη κερδοσκοπική Ένωσης Παιδικής Πρόνοιας (EUCW) είναι ο γενικός συντονιστής του Κέντρου Ασφαλέστερου Διαδίκτυου της Εσθονίας, «Targalt Internetis SIC EE II» [210]. Το κέντρο μέσω εκπαιδεύσεων και άλλων δραστηριοτήτων επιδιώκει την κατάρτιση και την ευαισθητοποίηση. Το Κέντρο επίσης λειτουργεί τηλεφωνική γραμμή αναφοράς περιστατικών. Η Αστυνομία της Εσθονίας συνδράμει στο έργο του. Επιπλέον, η βιομηχανία ΤΠΕ διοργανώνει μια σειρά συνεδρίων ασφάλειας πληροφορικής στα οποία οι συμμετέχοντες μοιράζονται πληροφορίες σχετικά με τις μελλοντικές τάσεις της τεχνολογίας και δίνονται συμβουλές για το πώς να παραμείνει κανείς ασφαλείς στο δικτυωμένο κόσμο [211]. Τέλος, Στην Εσθονία έχουν πραγματοποιηθεί οι ασκήσεις Κυβερνοασφάλειας εθνικής κλίμακας Tallinn CIIP 2010 Cyber Hedgehog 2010 και Cyber Fever 2012 [28][212].

9.5 Διεθνής Συνεργασία

Η Εσθονία συμμετέχει στο κέντρο εκπαίδευσης και έρευνας του NATO με την ονομασία CCDCOE, μαζί με τις: Λετονία, Γερμανία, Ιταλία, Ουγγαρία, Λιθουανία, Δημοκρατία της Σλοβακίας και Ισπανία. ΤΟ CCD COE [213] βρίσκεται στην Εσθονία και είναι ανοικτό σε όλες τις χώρες του NATO. Πρώτες προτεραιότητές του είναι να παρέχει πληροφορίες, τεχνογνωσία εμπειρογνωμόνων και βοήθεια στο NATO σχετικά με διάφορες πτυχές της άμυνας στον κυβερνοχώρο. Το Κέντρο διεξάγει αμυντικές ασκήσεις κυβερνοχώρου, το οποίο επιτρέπει στους συμμετέχοντες να μάθουν και να δοκιμάσουν τις δεξιότητες που απαιτούνται για να αποκρούσουν μια πραγματική επίθεση. Η πρώτη άσκηση έλαβε χώρα το 2008 ως κοινή εκδήλωση μεταξύ των Σουηδικών Εσθονικών Πανεπιστημίων. Διοργανώθηκε από το Σουηδικό Εθνικό

Κολλέγιο Άμυνας και τις Ένοπλες Δυνάμεις της Εσθονίας. Ακολούθησε τη Baltic Cyber Shield 2010. Από το 2012 η άσκηση ονομάζεται Locked Shields [212] [214]. Παράλληλα η Εσθονία ως μέλος της Ε.Ε. και του ΝΑΤΟ συνεργάζεται με τα αρμόδια όργανα σε θέματα Κυβερνοασφάλειας. Το Τμήμα Πληροφοριακών Συστημάτων του Υπουργείου Οικονομικών είναι ο κύριος εκπρόσωπος της χώρας στον ENISA και συμμετείχε στην άσκηση Cyber Europe [28][215]. Επίσης το 2013 η Εσθονία φιλοξένησε τη Νατοϊκή άσκηση Κυβερνοασφάλειας Cyber Coalition 2013 [216]. Το 2010 η αρχής κυβερνοάμυνας της Γαλλίας και της Εσθονίας υπέγραψαν συμφωνία συνεργασίας [217] στον τομέα της κυβερνοάμυνας και της ασφάλειας πληροφοριακών συστημάτων. Αναγνωρίζοντας ότι η Γαλλία και η Εσθονία μπορούν να αντιμετωπίσουν τις ίδιες απειλές και κρίσεις, η συμφωνία συνεργασίας προβλέπει ότι οι αρχές κυβερνοάμυνας τους θα μοιράζονται τις πληροφορίες και την εμπειρία κάθε φορά που θα είναι χρήσιμες. Τέλος η CERT-EE είναι μέλος του διεθνούς φόρουμ FIRST[32] και μέλος της TI και του Ceenet [218].

Κεφάλαιο 10ο

Ηνωμένο Βασίλειο

10.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η στρατηγική του Ηνωμένου Βασίλειου για την ασφάλεια στον κυβερνοχώρο βασίζεται στην εμπειρία δέκα ετών επιδιώκοντας την προστασία των κυβερνητικών πληροφοριακών συστημάτων και δικτύων. Το 2001 η Εθνική Αρχή Ασφάλειας Πληροφοριών CESG αναγνώρισε τη σημασία της προστασίας της ασφάλειας των δεδομένων και εισηγήθηκε τη δημιουργία ενός κεντρικού οργανισμού για να καθορίσει την πολιτική διαχείρισης και διασφάλισης των κυβερνητικών δεδομένων. Μέχρι το 2004 η κυβέρνηση είχε δημοσιεύσει μια εθνική στρατηγική για τη διασφάλιση των πληροφορίων με στόχο την προώθηση μιας κουλτούρας προστασίας [219]. Το 2009 η κυβέρνηση αναγνώρισε τις αναδυόμενες απειλές και τους σημαντικούς κινδύνους στον κυβερνοχώρο και δημοσίευσε την πρώτη Στρατηγική Ασφάλειας στον Κυβερνοχώρο [220]. Ο στόχος ήταν να διευρύνει το ρόλο της πέρα από αυτόν της προστασίας των κυβερνητικών πληροφοριών και συστημάτων. Επίσης, ήθελε να εργαστεί μαζί με τη βιομηχανία και τους πολίτες για την προστασία της ευρύτερης οικονομίας και της κοινωνίας του Ηνωμένου Βασιλείου από τις κυβερνοαπειλές. Ως μέρος της στρατηγικής, η κυβέρνηση δημιούργησε το Γραφείο Κυβερνοασφάλειας στο Υπουργικό Συμβούλιο. Το Νοέμβριο του 2011, η κυβέρνηση δημοσίευσε μια νέα Στρατηγική [221] Κυβερνοασφάλειας. Αυτή καθορίζει πώς η κυβέρνηση θα υλοποιήσει την Εθνική ασφάλεια στον κυβερνοχώρο μέχρι το 2015. Η Στρατηγική καθορίζει τέσσερις βασικούς στόχους, έξι κεντρικές υπηρεσίες και άλλους εννέα κυβερνητικούς οργανισμούς ως υπεύθυνους με συγκεκριμένες αρμοδιότητες και δράσεις για την Κυβερνοασφάλεια. Οι βασικοί στόχοι της στρατηγικής είναι:

- Αντιμετώπιση της εγκληματικότητας στον κυβερνοχώρο ώστε το Ηνωμένο Βασίλειο να είναι από τα πιο ασφαλή μέρη του κόσμου για επιχειρήσεις.
- Το Ηνωμένο Βασίλειο να είναι πιο ανθεκτικό σε επιθέσεις στον κυβερνοχώρο και να είναι σε θέση να προστατεύσει τα συμφέροντά του στον κυβερνοχώρο.
- Να συμβάλει στη διαμόρφωση ενός ανοιχτού, σταθερού και ζωντανού κυβερνοχώρου όπου το κοινό του Η.Β. θα μπορεί να χρησιμοποιεί με ασφάλεια.

- Διατομεακή ανάπτυξη των γνώσεων, των δεξιοτήτων και των ικανοτήτων που θα στηρίξουν την ασφάλεια στον κυβερνοχώρο.

10.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας ιδιωτικότητας / Προστασίας Προσωπικών Δεδομένων [222]

Ο νόμος περί προστασίας δεδομένων του 1998 έλαβε βασιλική έγκριση τον Ιούλιο του 1998 και τέθηκε σε ισχύ την 1η Μαρτίου 2000, εφαρμόζοντας την οδηγία για την προστασία των δεδομένων της ΕΕ (95/46/ΕΚ). Θεσπίζει κανόνες για τον τρόπο που οι οργανισμοί οφείλουν να διαχειρίζονται τα προσωπικά δεδομένα. Η Αρχή προστασίας δεδομένων πρέπει να ελέγχει ότι όλα τα δεδομένα υφίστανται θεμιτή και νόμιμη επεξεργασία, λαμβάνονται και χρησιμοποιούνται μόνο για συγκεκριμένους και νόμιμους σκοπούς, είναι κατάλληλα, συναφή και όχι υπερβολικά. Επίσης ελέγχει ότι είναι ακριβή και όπου χρειάζεται ενημερώνονται, δεν διατηρούνται για χρόνο περισσότερο από ό, τι είναι απαραίτητο, φυλάσσονται με ασφάλεια και μεταβιβάζονται μόνο σε χώρες που προσφέρουν επαρκή προστασία.

Νομοθεσία ηλεκτρονικού εμπορίου[222]

Οι Κανονισμοί Ηλεκτρονικού Εμπορίου του 2002 μεταφέρουν στο δίκαιο του Ηνωμένου Βασιλείου τη πλειονότητα των διατάξεων της οδηγίας της ΕΕ για το ηλεκτρονικό εμπόριο (2000/31/ΕΚ) σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, και το ηλεκτρονικό εμπόριο, ιδίως στην εσωτερική αγορά.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [222]

Βασικά στοιχεία του πλαισίου της ΕΕ για τις ηλεκτρονικές επικοινωνίες, όπως η οδηγία πλαίσιο (2002/21/ΕΚ), η οδηγία για την πρόσβαση (2002/19/ΕΚ), η οδηγία για την αδειοδότηση (2002/20/ΕΚ) και η οδηγία για την καθολική υπηρεσία (2002/22/ΕΚ), τέθηκαν σε εφαρμογή στο Ηνωμένο Βασίλειο, μέσω του νόμου περί επικοινωνιών του 2003.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Ο Νόμος περί κατάχρησης Η/Υ και ο Νόμος περί Αστυνομίας και Δικαιοσύνης περιγράφουν τα αδικήματα που σχετίζονται με το έγκλημα στον κυβερνοχώρο.

Νόμος περί κατάχρησης Η/Υ [223]

Άρθρο 1. Μη εξουσιοδοτημένη πρόσβαση στο υλικό του υπολογιστή.

Άρθρο 2. Μη εξουσιοδοτημένη πρόσβαση με πρόθεση να διαπραχθεί ή να διευκολυνθεί διάπραξη νέων αδικημάτων.

Άρθρο 3. Μη εγκεκριμένες πράξεις με πρόθεση να βλάψουν, ή να δυσχεράνουν τη λειτουργία του υπολογιστή, κλπ.

Άρθρο 3Α. Δημιουργία, παροχή ή απόκτηση αντικειμένων για χρήση σε αδίκημα μέσω του άρθρου 1 ή 3.

Νόμος περί Αστυνομίας και η Δικαιοσύνης του 2006 Μέρος 5 [224]

Άρθρο 35 Μη εξουσιοδοτημένη πρόσβαση στο υλικό του υπολογιστή.

Άρθρο 36 Μη εγκεκριμένες πράξεις με πρόθεση να βλάψουν τη λειτουργία του υπολογιστή, κλπ.

Άρθρο 37 Δημιουργία, παροχή ή η απόκτηση αντικειμένων για χρήση σε αδικήματα κατάχρησης υπολογιστών.

10.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Υπουργείο Επιχειρήσεων, Καινοτομίας και Δεξιοτήτων (BIS) [225] είναι υπεύθυνο για τομείς όπως η Ασφάλεια Πληροφοριών, το ηλεκτρονικό εμπόριο, οι Ηλεκτρονικές υπηρεσίες και οι υπηρεσίες πληροφορικής. Το Υπουργείο Εσωτερικών [226] μεταξύ άλλων είναι υπεύθυνο για τη καταπολέμηση του εγκλήματος και της τρομοκρατίας. Στις αρμοδιότητες του είναι η αντιμετώπιση της εγκληματικότητας στον κυβερνοχώρο, η μείωση των ευπαθειών και η προώθηση αποτελεσματικών εταιρικών σχέσεων. Το Υπουργείο Άμυνας [227] διασφαλίζει ότι το Ηνωμένο Βασίλειο έχει τη δυνατότητα να προστατεύει τα συμφέροντα του στον κυβερνοχώρο εντοπίζοντας απειλές στον κυβερνοχώρο και αποτρέποντας τις επιθέσεις. Το Υπουργικό Συμβούλιο μέσω του Γραφείου για την Ασφάλεια στον Κυβερνοχώρο και τη διασφάλιση της Πληροφορίας (Ocsia) [228], παρέχει στρατηγική κατεύθυνση και συντονίζει τις ενέργειες που αφορούν την ενίσχυση της ασφάλειας του κυβερνοχώρου και τη διασφάλιση της πληροφορίας στο Ηνωμένο Βασίλειο. Το Κέντρο για την Προστασία των Εθνικών Υποδομών (CPNI) [229] είναι η κυβερνητική αρχή που παρέχει συμβουλές ασφάλειας για την εθνική υποδομή. Στοχεύει στη μείωση της ευπάθειας της εθνικής υποδομής από την τρομοκρατία και άλλες απειλές, συμπεριλαμβανομένων των κυβερνοαπειλών, διατηρώντας τις βασικές υπηρεσίες του Ηνωμένου Βασιλείου ασφαλείς. Η Εθνική Αρχή Ασφάλειας Πληροφοριών CESG [230] είναι τμήμα του Αρχηγείου Επικοινωνιών

της κυβέρνησης (GCHQ) και προστατεύει τα ζωτικά συμφέροντα του Ηνωμένου Βασιλείου με την παροχή πολιτικών και βοήθειας σχετικά με την ασφάλεια των επικοινωνιών και των ηλεκτρονικών δεδομένων, σε συνεργασία με τη βιομηχανία και την ακαδημαϊκή κοινότητα. Η Κεντρική Μονάδα ηλεκτρονικού εγκλήματος της Μητροπολιτικής Αστυνομίας [231] παρέχει έρευνα για τα πιο σοβαρά περιστατικά της εγκληματικότητας στον κυβερνοχώρο. Η Εθνική Αρχή Απάτης [232] έχει αναλάβει το καθήκον της καταπολέμησης της απάτης σε όλους τους τομείς συμπεριλαμβανομένου του Κυβερνοχώρου. Η Εθνική Μονάδα Κυβερνοεγκλήματος [233] άρχισε να λειτουργεί την άνοιξη του 2013 στο πλαίσιο του Εθνικού Οργανισμού Εγκλήματος. Έχει εκπαιδεύσει περίπου 4.000 υπαλλήλους ως ψηφιακούς ερευνητές με στόχο κάθε Περιφερειακή Μονάδα Οργανωμένου Εγκλήματος να έχει μια ειδική μονάδα για τον κυβερνοχώρο. Το Γραφείο Επιτρόπου Πληροφοριών [234] είναι ανεξάρτητη αρχή του Ηνωμένου Βασιλείου που έχει συσταθεί για την προώθηση της πρόσβασης σε επίσημες πληροφορίες και την προστασία των προσωπικών δεδομένων.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η GovCertUK είναι η Ομάδα της κυβέρνηση του Ηνωμένου Βασιλείου και λειτουργεί εντός του CESG. Βοηθάει τους οργανισμούς του δημόσιου τομέα στην αντιμετώπιση των περιστατικών ασφάλειας του υπολογιστή και παρέχει συμβουλές για τη μείωση της έκθεσης στις απειλές. Στο Ηνωμένο Βασίλειο υπάρχει μεγάλη ανάπτυξη όσον αφορά τις ομάδες CERT και ένα πλήθος από αυτές δραστηριοποιούνται ανάλογα με τον τομέα στον οποίο απευθύνονται όπως φαίνεται στον πίνακα 10.1.

Χρηματοπιστωτικός τομέας **CITIGROUP** http://www.citigroup.com **MLCIRT** http://www.ml.com **RBSG-ISIRT** http://www.rbs.co.uk	**Εμπορικών Οργανώσεων** **DCSIRT** http://www.diageo.com **KPMG-CSIRT** http://www.kpmg.co.uk/cyber **P-CIRF** http://www.portcullis-security.com
Εθνικά / κυβερνητικά / Στρατιωτικά **GovCertUK** http://www.govcertuk.gov.uk/	**Έρευνας και Εκπαίδευσης** **DAN-CERT** http://www.dante.net/dancert **EUCS-IRT**

CSIRTUK http://www.cpni.gov.uk/ **MODCERT** http://www.mod.uk/cert/	http://www.ed.ac.uk/home **Janet CSIRT** http://www.ja.net/csirt/ **OxCERT** http://www.oucs.ox.ac.uk/network/security/ **UCL CERT** http://www.ucl.ac.uk/cert **WAR-CSIIRT** http://www.warwick.ac.uk
Παρόχων υπηρεσιών **BTCERTCC** http://bt.com **CIS-CERT** http://www.contextis.co.uk **E-CERT** http://cert.energis2.net/ **ESISS** http://www.esiss.ac.uk **Q-CIRT** http://www.qinetiq.com	**Τομέας Ενέργειας** **NGRID-CSIRT** http://www.nationalgrid.com
ISP **Bunker** http://www.thebunker.net	

Πίνακας 10.1 Cert Ηνωμένου Βασιλείου

Ιδιωτικοί φορείς

Ο tScheme [235] είναι ανεξάρτητος ιδιωτικός οργανισμός, που έχει συσταθεί για τη δημιουργία αυστηρών κριτηρίων αξιολόγησης για την έγκριση υπηρεσιών εμπιστοσύνης. Ως εκ τούτου, η έγκριση της tScheme θα αποτελέσει βασικό στοιχείο για την παροχή ενός επιπέδου αξιοπιστίας σε ιδιώτες και εταιρείες που χρησιμοποιούν ηλεκτρονικές συναλλαγές. Το Mobile Industry Crime Action Forum [236] είναι ένα φόρουμ για την ανταλλαγή πληροφοριών και την προώθηση μιας συντονισμένης προσπάθειας κατά της εγκληματικής δραστηριότητας στον τομέα των τηλεπικοινωνιών. Το Φόρουμ επιδιώκει να αυξήσει την ευαισθητοποίηση σε θέματα

εγκληματικότητας που επηρεάζουν τη βιομηχανία βοηθώντας στον εντοπισμό και την ανάπτυξη αντίμετρων στα εγκλήματα τηλεπικοινωνιών, καθώς και αναπτύσσοντας διαδικασίες για την καταπολέμηση των εγκλημάτων μέσω του κινητού τηλεφώνου στο Ηνωμένο Βασίλειο.

Ακαδημαϊκοί φορείς

Το Ινστιτούτο για επαγγελματίες Ασφάλειας Πληροφοριών (IISP) [237] έχει κύριο ρόλο στην ανάπτυξη του τομέα των επαγγελματιών της Ασφάλειας Πληροφορικής. Συνεργάζεται με την ακαδημαϊκή κοινότητα για να βοηθήσει στην ανάπτυξη νέων μαθημάτων, καθώς και με εταιρείες και κυβερνητικούς οργανισμούς. Η Ομάδα Ασφάλειας Πληροφοριών (ISG) του Royal Holloway College of London [238] είναι μια παγκοσμίως πρωτοπόρα διεπιστημονική ερευνητική ομάδα αφοσιωμένη στην έρευνα και την εκπαίδευση στον τομέα των της ασφάλειας πληροφοριών και στις κυβερνοεπιθέσεις. Η Σκωτσέζικη Συμμαχία Πληροφορικής και Επιστήμης Υπολογιστών SICSA [239] είναι μια συνεργασία των κορυφαίων Σκωτσέζικων πανεπιστήμιων. Το πρόγραμμα της SICSA για την ασφάλεια στον κυβερνοχώρο έχει ως στόχο την προώθηση της έρευνας, την ανταλλαγή γνώσεων και τη συνεργασία μεταξύ της βιομηχανίας, του ακαδημαϊκού κόσμου, της κυβέρνησης και των οργανισμών ασφαλείας. Το Janet [240] είναι το δίκτυο των πανεπιστημίων του Ηνωμένου Βασιλείου, χρηματοδοτείται από την κυβέρνηση, με πρωταρχικό στόχο την παροχή και την ανάπτυξη μιας δικτυακής υποδομής που να ανταποκρίνεται στις ανάγκες των κοινοτήτων της έρευνας και της εκπαίδευσης. Το Ακαδημαϊκό Κέντρο Αριστείας του Πανεπιστημιακού Κολλεγίου του Λονδίνου (UCL), για την έρευνα για την ασφάλεια στον κυβερνοχώρο [241] ιδρύθηκε το 2012 και φιλοξενεί κορυφαίους ερευνητές, που καλύπτουν ένα ευρύ φάσμα τομέων όπως η κρυπτογράφηση, ο ανθρώπινος παράγοντας στην ασφάλεια, η ασφάλεια σε end-to-end συστήματα κ.α. Το UCL είναι ένα από τα έντεκα πανεπιστήμια του Ηνωμένου Βασιλείου που διεξάγουν έρευνα στον τομέα της ασφάλειας στον κυβερνοχώρο και στα οποία έχει χορηγηθεί καθεστώς «Κέντρου Αριστείας». Τα άλλα δέκα κέντρα είναι το Πανεπιστήμιο του Μπρίστολ, Πανεπιστήμιο του Μπέρμιγχαμ, το Πανεπιστήμιο του Κέμπριτζ, το Imperial College του Λονδίνου, το Πανεπιστήμιο του Λάνκαστερ, το Πανεπιστήμιο του Νιούκαστλ, το Πανεπιστήμιο της Οξφόρδης, το Πανεπιστήμιο Queen του Μπέλφαστ, το Royal Holloway College of London, και το Πανεπιστήμιο του Σαουθάμπτον. Μέρος του στόχου για τη δημιουργία των κέντρων είναι να ενθαρρύνει τη συνεργασία, και να

ενισχύσει τη γνωστική βάση του Ηνωμένου Βασιλείου στην παροχή υψηλής ποιότητας μεταπτυχιακής εκπαίδευσης, υποστηρίζοντας τη GCHQ.

Συνεργασία μεταξύ φορέων

Το Γραφείο για την Ασφάλεια στον Κυβερνοχώρο συντονίζει τις εργασίες που διεξάγονται στο πλαίσιο του Εθνικού Προγράμματος ασφάλειας στον Κυβερνοχώρο και συνεργάζεται με δημόσιες υπηρεσίες και οργανισμούς όπως το Υπουργείο Εσωτερικών, το Υπουργείο Εθνικής Άμυνας, το Αρχηγείο Επικοινωνιών, το Κέντρο για την Προστασία των Εθνικών Υποδομών, το Υπουργείο Εξωτερικών και το Υπουργείο Επιχειρήσεων, Καινοτομίας και Δεξιοτήτων. Η CPNI είναι η κυβερνητική αρχή που παρέχει το προσωπικό, πληροφορίες και συμβουλές ασφάλειας για την εθνική υποδομή. [242] Το πρόγραμμα CISP (Συνεργασία Ανταλλαγής Πληροφοριών Κυβερνοασφάλειας) επιτρέπει στην κυβέρνηση και τη βιομηχανία να ανταλλάσσουν πληροφορίες σχετικά με τις τρέχουσες απειλές και τη διαχείριση συμβάντων σε μια ασφαλή πλατφόρμα. Στο πρόγραμμα συμμετέχουν 160 εταιρείες από 5 τομείς. Το πρόγραμμα είναι ανοικτό σε εταιρείες πέραν των κρίσιμων εθνικών υποδομών, συμπεριλαμβανομένων των μικρών και μεσαίων επιχειρήσεων. Το CISP περιλαμβάνει μια ομάδα αναλυτών που υποστηρίζεται από τις υπηρεσίες ασφαλείας της κυβέρνησης, το GCHQ και τον Εθνικό Οργανισμό Εγκλήματος μαζί με αναλυτές των εταιρειών [243].

10.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Το πρόγραμμα WARP [244] είναι μέρος της στρατηγικής της Ανταλλαγής Πληροφοριών του CPNI. Τα WARP είναι ένας τρόπος όπου ένας οργανισμός μπορεί να μοιραστεί πληροφορίες. Τα WARP έχουν αναπτυχθεί για να παρέχουν μια οικονομικά αποδοτική μέθοδο για να υποστηρίξουν την άμυνα κατά των επιθέσεων. Σκοπός τους είναι να παρέχουν σε μια συγκεκριμένη κοινότητα την ικανότητα να μοιράζονται σχετικές με την ασφάλεια πληροφορίες και λύσεις και ως εκ τούτου να αναπτύξουν ένα ασφαλέστερο και ανταποδοτικό περιβάλλον. Η κυβέρνηση συνεργάζεται με τον ιδιωτικό τομέα για την αύξηση της ευαισθητοποίησης του κοινού, με βάση το έργο του GetSafeOnline.org του BIS και εκστρατείες από την Εθνική Αρχή Απάτης, όπως η «The devil's in your details». Το φυλλάδιο 10 Βήματα για την Κυβερνοασφάλεια παρέχει σαφείς και συνοπτικές συμβουλές για το πώς να διασφαλιστούν τα πιο πολύτιμα περιουσιακά στοιχεία μιας εταιρείας , όπως προσωπικά

δεδομένα και online υπηρεσίες. Η καθοδήγηση παρέχει κοινές συμβουλές από το GCHQ, το Υπουργείο Επιχειρήσεων, Καινοτομίας και Δεξιοτήτων και των Υπηρεσιών Ασφάλειας για να βοηθήσει τις επιχειρήσεις να εντοπίζουν κινδύνους και να θέσουν σε εφαρμογή τις απαιτούμενες διαδικασίες για την ελαχιστοποίηση των κινδύνων. Επίσης έχει δημοσιευθεί το εγχειρίδιο «Προσαρμοσμένη καθοδήγηση για τις μικρές επιχειρήσεις.» [245]. Η κυβέρνηση σε συνεργασία με τη βιομηχανία του Διαδικτύου έχουν δημοσιεύσει κατευθυντήριες αρχές σχετικά με το πώς να λειτουργούν αποτελεσματικά στο διαδίκτυο. Οι κατευθυντήριες αρχές έχουν αναπτυχθεί για να βοηθήσουν, να ενημερώσουν, να εκπαιδεύσουν και να προστατεύσουν τους πελάτες των ISPs από τις κυβερνοαπειλές [246]. Η Υπηρεσία Απάτης έχει θεσπιστεί ένα ενιαίο σύστημα αναφοράς για κυβερνοεγκλήματα που αφορούν κυρίως οικονομικά κίνητρα. Η καταγραφή των περιστατικών απάτης επιτρέπει την κεντρική επεξεργασία και ανάλυση των εγκλημάτων με αποτέλεσμα πιο στοχευμένες ενέργειες επιβολής του νόμου. Για την στήριξη της ανάπτυξης του κλάδου της ασφάλειας στον κυβερνοχώρο έχει δημοσιευτεί η Στρατηγική Εξαγωγών Κυβερνοασφάλειας με σκοπό να καθοριστεί το πεδίο εφαρμογής των ευκαιριών και των δράσεων για τις επιχειρήσεις που παρέχουν προϊόντα και υπηρεσίες ασφάλειας στον κυβερνοχώρο και για τον καθορισμό στόχων για τη μελλοντική ανάπτυξη των εξαγωγών [247]. Με στόχο να συνεχιστεί η παγκόσμια συζήτηση για το μέλλον του Διαδικτύου και για τη θέσπιση κανόνων συμπεριφοράς στον κυβερνοχώρο το Η.Β. φιλοξένησε τη Διάσκεψη του Λονδίνου για Κυβερνοχώρο το 2011 [248]. Για τη Βελτίωση των δεξιοτήτων στον κυβερνοχώρο και την εκπαίδευση νέων επαγγελματιών υποστηρίζεται πρόγραμμα "make it happy"και χρηματοδοτούνται σχολικοί διαγωνισμοί, όπως ο «Cybersecurity Challenge και ο «National Cipher Challenge"[249].

10.5 Διεθνής Συνεργασία

Το Υπουργείο Επιχειρήσεων, Καινοτομίας και Δεξιοτήτων και η Εθνική Αρχή Ασφάλειας Πληροφοριών CESG είναι οι κύριοι αντιπρόσωποι της χώρας στους αντίστοιχους διεθνείς οργανισμούς, συνήθως μέσα από τις δομές της ΕΕ και του NATO. Το Η.Β συμμετείχε στην άσκηση κυβερνοάμυνας Cyber Europe και στην κοινή άσκηση Ε.Ε – Η.Π.Α. Cyber Atlantic[28][250]. Επίσης ως μέλος του NATO συμμετέχει στις ασκήσεις Cyber Coalition και έχει δηλώσει την πρόθεσή του να γίνει μέλος του CCDCOE[251]. Η Ασφάλεια στον κυβερνοχώρο είναι επίσης μια

αναπτυσσόμενη περιοχή συνεργασίας μεταξύ των Ηνωμένων Πολιτειών και του Ηνωμένου Βασιλείου [252]. Οι δυο χώρες συνεργάστηκαν στην άσκηση Cyber Storm [253]. Επίσης συμφωνίες συνεργασίας έχουν υπογραφεί με την Ινδία και την Ιαπωνία [254][258]. Όσον αφορά τις CERT, οι CSIRTUK και GovCertUK είναι μέλη της ομάδας των κυβερνητικών CERT της Ευρώπης [31].Επίσης δεκαπέντε CERT του Η.Β. είναι μέλη του διεθνούς φόρουμ FIRST [32].

Κεφάλαιο 11ο

Ιρλανδία

11.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Ιρλανδία μέχρι σήμερα δεν έχει δημοσιεύσει Εθνική Στρατηγική Κυβερνοασφάλειας. Τον Ιούλιο του 2013 το Υπουργείο Επικοινωνιών, Ενέργειας και Φυσικών Πόρων δημοσίευσε την Εθνική Ψηφιακή Στρατηγική [259] με σκοπό να βοηθήσει την Ιρλανδία να αποκομίσει όλα τα οφέλη μιας ψηφιακά ενεργοποιημένης κοινωνίας. Παρόλο που η στρατηγική θέτει αρκετά μέτρα και στόχους για την ψηφιακή ανάπτυξη της Ιρλανδίας, ενεργοποιώντας τόσο τις κυβερνητικές αρχές, τις ιδιωτικές εταιρείες αλλά και τους πολίτες της Ιρλανδίας εντούτοις υπάρχει μικρή αναφορά σε δραστηριότητες που αφορούν την ασφάλεια του κυβερνοχώρου. Τα μέτρα αφορούν κυρίως την προστασία των χρηστών (με έμφαση στα παιδιά) από τους κινδύνους του διαδικτύου.

11.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας ιδιωτικότητας / Προστασίας Προσωπικών Δεδομένων [260]

Ο νόμος περί προστασίας δεδομένων του 1988 τροποποιήθηκε το 2003 για να εξασφαλίσει την πλήρη συμμόρφωση με την οδηγία για την προστασία των δεδομένων της ΕΕ (95/46/ΕΚ). Σκοπός της οδηγίας είναι η θέσπιση κοινών προτύπων προστασίας των δεδομένων σε όλα τα κράτη μέλη, με σκοπό την προστασία της ιδιωτικής ζωής και τη διασφάλιση της ομαλής λειτουργίας της εσωτερικής αγοράς, με ταυτόχρονη εξασφάλιση επαρκών επιπέδων προστασίας των δεδομένων σε χώρες εκτός του Ευρωπαϊκού Οικονομικού Χώρου. Η Επίτροπος Προστασίας Δεδομένων επιβλέπει την εφαρμογή του νόμου.

Νομοθεσία ηλεκτρονικού εμπορίου [260]

Ο νόμος για το ηλεκτρονικό Εμπόριο ψηφίστηκε στις 20 Σεπτεμβρίου 2000. Υλοποιεί την οδηγία της ΕΕ σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές (1999/93/ΕΚ) και, εν μέρει, την οδηγία της ΕΕ για το ηλεκτρονικό εμπόριο (2000/31/ΕΚ). Ο νόμος προβλέπει τη νομική αναγνώριση των ηλεκτρονικών

υπογραφών, των ηλεκτρονικών γραπτών και των ηλεκτρονικών συμβάσεων. Επιτρέπει τη χρήση της κρυπτογράφησης και καθορίζει τα δικαιώματα και τις υποχρεώσεις των παρόχων υπηρεσιών πιστοποίησης.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [260]

Μέσω του κανονισμού Επικοινωνιών του 2002 και του παράγωγου δικαίου (μια σειρά από νομοθετικές πράξεις), η Ιρλανδία μετέφερε όλες τις οδηγίες του κανονιστικού πλαισίου της ΕΕ για τις ηλεκτρονικές επικοινωνίες και συγκεκριμένα: τις οδηγίες 2002/21/ΕΚ (οδηγία-πλαίσιο) 2002/20 / ΕΚ (οδηγία για την αδειοδότηση) 2002/19/ΕΚ (οδηγία για την πρόσβαση) 2002/22/ΕΚ (οδηγία για την καθολική υπηρεσία) και 2002/58/ΕΚ (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες).

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [37]

Στην Ιρλανδία υπάρχουν δύο νόμοι που αναφέρονται σε αδικήματα του κυβερνοχώρου: Ο Νόμος περί Ποινικών Φθορών 1991, Ενότητα 5 Μη εξουσιοδοτημένη πρόσβαση σε δεδομένα και ο Νόμος για την ποινική δικαιοσύνη (κλοπές και απάτες)(2001), Ενότητα 9 Χρήση Η/Υ με σκοπό παράνομες πράξεις.

11.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Υπουργείο Επικοινωνιών, Ενέργειας και Φυσικών Πόρων (DCENR) [261] έχει την ευθύνη για τις τηλεπικοινωνίες, τις ραδιοτηλεοπτικές μεταδόσεις και τον τομέα Ενέργειας. Είναι υπεύθυνο για την Εθνική Ψηφιακή Στρατηγική καθώς και για το πρόγραμμα ευαισθητοποίησης «make IT secure». Ο Επίτροπος Προστασίας Δεδομένων [262] είναι υπεύθυνος για την προάσπιση των δικαιωμάτων των ατόμων σε σχέση με τα προσωπικά δεδομένα. Τα άτομα που αισθάνονται τα δικαιώματά τους να παραβιάζονται μπορούν να υποβάλουν καταγγελία στον Επίτροπο, ο οποίος θα ερευνήσει το θέμα, και θα λάβει τα κατάλληλα μέτρα που είναι απαραίτητα για την επίλυσή του. Η Εθνική Υπηρεσία της Αστυνομίας της Ιρλανδίας μέσω του Γραφείου Διερεύνησης Απάτης [263] ερευνά σοβαρές και πολύπλοκες υποθέσεις απάτης, όπως τα εγκλήματα πληροφορικής. Χωρίζεται σε πέντε επιχειρησιακές μονάδες, ανάλογα με τον επιχειρησιακό τομέα μία εκ των οποίων είναι η μονάδα διερεύνησης εγκλημάτων πληροφορικής.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CSIRT.IE είναι η Εθνική CERT της Ιρλανδίας η οποία θεσμοθετήθηκε το 2013 χωρίς όμως να έχει λειτουργήσει μέχρι σήμερα. Η HEAnet CERT [264] είναι ομάδα του Ερευνητικού Δικτύου του Υπουργείου Εθνικής Παιδείας και συνδέεται με τα Εκπαιδευτικά και Ερευνητικά ιδρύματα σε όλη την Ιρλανδία. Η IRISS CERT [265] ανήκει στην Υπηρεσία Αναφορών και Ασφαλείας Πληροφορικής, μιας ανεξάρτητης μη κερδοσκοπικής εταιρείας περιορισμένης ευθύνης που παρέχει μια σειρά από δωρεάν υπηρεσίες σε ιρλανδικές επιχειρήσεις και καταναλωτές για να βοηθήσει στην αντιμετώπιση των απειλών στον ιρλανδικό κυβερνοχώρο. Είναι η πρώτη ομάδα που δημιουργήθηκε στην Ιρλανδία με σκοπό την παροχή υπηρεσιών σε όλους τους χρήστες εντός της Ιρλανδίας. Παρέχει ένα ευρύ φάσμα υπηρεσιών προστασίας των πληροφοριακών συστημάτων και έχει ως στόχο να κάνει το ιρλανδικό χώρο διαδικτύου ένα ασφαλέστερο περιβάλλον. Η POPCAP-CSIRT ανήκει στην εταιρεία κατασκευής ηλεκτρονικών παιχνιδιών POPCAP.

Ιδιωτικοί φορείς

Στη Ιρλανδία δραστηριοποιούνται εκατοντάδες εταιρείες πληροφορικής, πολλές από τις οποίες είναι κορυφαίες του χώρου παγκοσμίως και διατηρούν τα κεντρικά τους γραφεία για την Ευρώπη στην Ιρλανδία. Ανάμεσα τους είναι η Microsoft, η IBM, η Intel, η Google η Oracle και η Apple. Επίσης στη Ιρλανδία δραστηριοποιούνται πολλές εταιρείες που ασχολούνται αποκλειστικά με την παραγωγή προϊόντων ασφάλειας πληροφορικής. Και σε αυτό τον τομέα ορισμένες από τις παγκοσμίως κορυφαίες εταιρίες διατηρούν τα κεντρικά για γραφεία τους για την Ευρώπη στην Ιρλανδία. Ορισμένες εξ' αυτών είναι η Symantec, η McAfee, η Trend Micro και η WebSense [266]. Στην Ιρλανδία υπάρχουν επίσης αρκετές ενώσεις και οργανισμοί που στοχεύουν στην εξυπηρέτηση των συμφερόντων των μελών τους. Η ICT Ireland [267] είναι η ένωση του τομέα της πληροφορικής και επικοινωνιών στην και αντιπροσωπεύει πάνω από 300 εταιρείες. Είναι ο εκπρόσωπος της ομάδας πίεσης για την υψηλή τεχνολογία. Η Telecommunications and Internet Federation (TIF) [268] είναι η κύρια εμπορική ένωση για τη βιομηχανία των ηλεκτρονικών επικοινωνιών στην Ιρλανδία δραστηριοποιείται στην παρακολούθηση του ρυθμιστικού περιβάλλοντος, τόσο σε εγχώριο επίπεδο όσο και σε επίπεδο ΕΕ, για τη σύνταξη της νομοθεσίας. Η Irish Information Security Forum (IISF) [269] έχει καθιερωθεί ως ένωση χωρίς νομική προσωπικότητα και είναι ένα αποτελεσματικό όργανο που δραστηριοποιείται στον

τομέα της απάτης των τηλεπικοινωνιών και σε θέματα ασφάλειας στους κόλπους της βιομηχανίας.

Η ένωση Internet Service Providers Association of Ireland (ISPAI) [270] ιδρύθηκε τον Ιανουάριο του 1998 από τους κορυφαίους παρόχους υπηρεσιών Διαδικτύου της Ιρλανδίας. Ο σκοπός του συλλόγου είναι να εκπροσωπεί την ιρλανδική βιομηχανία ISP σε εθνικό και διεθνές επίπεδο. Η ISPAI έχει συμφωνήσει με την ιρλανδική κυβέρνηση ότι η προσέγγιση αυτορρύθμισης της βιομηχανίας έχει μεγαλύτερες δυνατότητες για επιτυχία και αποτελεσματικότητα. Στο πλαίσιο αυτό, η ISPAI έχει συστήσει την υπηρεσία www.hotline.ie για την καταπολέμηση του παράνομου περιεχομένου, που φιλοξενείται και διανέμεται μέσω του Διαδικτύου.

Ακαδημαϊκοί φορείς

Το τμήμα School of Computer Science and Informatics του University College Dublin (UCD) [271] εκτός των σχετικών με την ασφάλεια της πληροφορικής προγραμμάτων και μαθημάτων λειτουργεί το UCD Κέντρο για το Έγκλημα στον Κυβερνοχώρο [272], το οποίο εκτελεί δραστηριότητες έρευνας και εκπαίδευσης.

Το HEAnet είναι Ερευνητικό Δίκτυο του Υπουργείου Εθνικής Παιδείας της Ιρλανδίας. Στο πλαίσιο του HEAnet λειτουργεί η HEAnet CERT. Επίσης το HEAnet σε συνεργασία με τις SpamHaus.org και την TrendMicro.com προσφέρουν μια Anti-Spam υπηρεσία.

Συνεργασία μεταξύ φορέων

Στην Ιρλανδία δεν υπάρχουν κυβερνητικές αρχές που να συντονίζουν την κυβερνοάμυνα της Χώρας. Ωστόσο η δημιουργία του Κέντρου Αριστείας για το Κυβερνοέγκλημα αναμένεται να λύσει αρκετά από τα προβλήματα. Μέχρι σήμερα κύριος φορέας συντονισμού ήταν το Υπουργείο Επικοινωνιών αν και οι περισσότερες δράσεις πραγματοποιούνταν από πρωτοβουλίες του ιδιωτικού τομέα. Γενικότερα η κυβερνοάμυνα της Ιρλανδίας στηρίζεται σε μεγάλο βαθμό στην αυτορρύθμιση και στις συμφωνίες που συνάπτονται μεταξύ των επαγγελματικών ενώσεων, της κυβέρνησης και των εταιρειών.

11.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Η ιρλανδική εθνική εκστρατεία "make it secure" [273] είναι η κύρια μορφή ευαισθητοποίησης σχετικά με την ασφάλεια στο διαδίκτυο. Ο στόχος της είναι να εξασφαλιστεί ότι η χρήση ηλεκτρονικών υπολογιστών, ευρυζωνικότητας και

Διαδικτύου είναι μια θετική εμπειρία, παρέχοντας βασικές πληροφορίες σχετικά με τα ζητήματα που ενδέχεται να επηρεάσουν τους χρήστες υπολογιστών. Τα βασικά θέματα ευαισθητοποίησης σε θέματα ασφάλειας πληροφοριών αφορούν: το Phishing, την κλοπή ταυτότητας, τους κινδύνους κοινωνικής δικτύωσης, τα Spyware και τους ιούς. Η εκστρατεία απευθύνεται και παρέχει συμβουλές τόσο σε απλούς χρήστες όσο και σε επιχειρήσεις. Διεξάγεται υπό την αιγίδα του υπουργείου Επικοινωνιών, Ενέργειας και Φυσικών Πόρων και υποστηρίζεται από εταιρείες όπως η Microsoft και η Symantec.
Το Γραφείο για την Ασφάλεια στο Διαδίκτυο [274][275] είναι ένα Εκτελεστικό Γραφείο του Υπουργείου Δικαιοσύνης και Ισότητας. Έχει την ευθύνη για το συντονισμό μέτρων, έτσι ώστε να εξασφαλιστεί ένα ασφαλέστερο διαδικτυακό περιβάλλον, ιδίως για τα παιδιά και τους νέους, μέσα σε ένα πλαίσιο αυτορρύθμισης. Το Γραφείο έχει δημοσιεύσει μια σειρά συμβουλευτικών εγχειριδίων σχετικά με θέματα ασφάλειας του Διαδικτύου όπως ο «οδηγός για γονείς και νέες τεχνολογίες», ο οδηγός για Ιστοσελίδες κοινωνικής δικτύωσης και ένας οδηγός για το Cyberbullying. Το Γραφείο διαχειρίζεται το έργο Safer Internet στην Ιρλανδία, το οποίο χρηματοδοτείται από την Ευρωπαϊκή Ένωση. Μέσω του προγράμματος λειτουργεί hotline που ασχολείται με εμπιστευτικές εκθέσεις του παράνομου περιεχομένου στο διαδίκτυο. Επίσης το γραφείο είναι υπεύθυνο για την ανάπτυξη των εκστρατειών ευαισθητοποίησης για την ασφάλεια στο διαδίκτυο, ιδίως σε συνεργασία με το Εθνικό Κέντρο για την Τεχνολογία στην Εκπαίδευση που λειτουργεί τον ιρλανδικό κόμβο ενημέρωσης για την ασφάλεια στο διαδίκτυο www.webwise.ie. Τέλος στην Ιρλανδία πραγματοποιούνται μια σειρά από συνέδρια με θέματα που αφορούν την ασφάλεια της πληροφορικής όπως τα IIEA Cybersecurity Conference [276], IRISSCERT Cyber Crime Conference [277] και International Computer Security Symposium [278]. Η Gaillean Exercise είναι άσκηση εθνικής κλίμακας που πραγματοποιήθηκε στην Ιρλανδία το 2010 [28].

11.5 Διεθνής Συνεργασία

Η Ιρλανδία συνεργάζεται με τον ENISA μέσω του Υπουργείου Επικοινωνιών, Ενέργειας και Φυσικών Πόρων [215] και κατά την διάρκεια της προεδρίας της στην Ε.Ε το πρώτο εξάμηνο του 2013 ανέδειξε το ρόλο του Οργανισμού για την αντιμετώπιση των κυβερνοεπιθέσεων ως ένα από τα σημαντικότερα θέματα της Ε.Ε. [279] [280]. Η Ιρλανδία συμμετέχει επίσης στην άσκηση κυβερνοάμυνας Cyber Europe

[28]. Τέλος η Ιρλανδία αν και δεν είναι μέλος του ΝΑΤΟ, συνεργάζεται με τον οργανισμό σε θέματα κυβερνοάμυνας και συμμετείχε στην άσκηση Cyber Coalition [57].

Κεφάλαιο 12ο

Ισπανία

12.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Στις 5 Δεκεμβρίου 2013 το Συμβούλιο Ασφαλείας ενέκρινε την Ισπανική Στρατηγική για την Ασφάλεια στον Κυβερνοχώρο [281]. Η Στρατηγική είναι το πλαίσιο για ένα ολοκληρωμένο μοντέλο και βασίζεται στη συμμετοχή, το συντονισμό και την εναρμόνιση όλων των κρατικών φορέων και των πόρων του δημόσιου και ιδιωτικού τομέα καθώς και τη συμμετοχή των πολιτών. Επίσης, δεδομένης της διακρατικής φύσης της ασφάλειας στον κυβερνοχώρο, η συνεργασία με την Ευρωπαϊκή Ένωση και άλλους διεθνείς ή περιφερειακούς οργανισμούς που είναι αρμόδιοι για το θέμα, αποτελούν ουσιαστικό μέρος αυτού του μοντέλου. Η στρατηγική ορίζει έξι στόχους οι οποίοι πρέπει να επιτευχθούν:

- Τα Πληροφοριακά Συστήματα και τα συστήματα Τηλεπικοινωνιών της Δημόσιας διοίκησης θα πρέπει να έχουν το κατάλληλο επίπεδο ασφάλειας και ανθεκτικότητας.
- Ενίσχυση της ασφάλειας και της ανθεκτικότητας των δικτύων και των συστημάτων στον τομέα των επιχειρήσεων και ιδιαίτερα στις εταιρείες που διαχειρίζονται υποδομές ζωτικής σημασίας.
- Ενίσχυση των ικανοτήτων πρόληψης, ανίχνευσης, έρευνας και συντονισμού κατά της τρομοκρατίας και του εγκλήματος στον κυβερνοχώρο.
- Ευαισθητοποίηση των πολιτών, των επαγγελματιών, των επιχειρήσεων και της Ισπανικής κυβέρνησης για τους κινδύνους του Κυβερνοχώρου.
- Ανάπτυξη των τεχνολογικών δυνατότητων που απαιτούνται για την υποστήριξη των στόχων στην ασφάλεια του κυβερνοχώρου.
- Υποστήριξη της συντονισμένης πολιτικής ασφάλειας του κυβερνοχώρου στην Ευρωπαϊκή Ένωση και στους διεθνείς οργανισμούς.

12.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας ιδιωτικότητας / Προστασίας Προσωπικών Δεδομένων [282]

Ο νόμος 15/1999 σχετικά με την προστασία των προσωπικών δεδομένων ευθυγράμμισε την ισπανική νομοθεσία με την οδηγία για την προστασία των δεδομένων της ΕΕ (95/46/ΕΚ). Ο νόμος αυτός ρυθμίζει την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο δημόσιο και στον ιδιωτικό τομέα και παρέχει στους πολίτες το δικαίωμα να έχουν πρόσβαση και διόρθωση των προσωπικών στοιχείων στα μητρώα που τηρούνται από δημόσιους και ιδιωτικούς φορείς. Οι προσωπικές πληροφορίες μπορούν να χρησιμοποιούνται (ή να αποκαλυφθούν σε τρίτους) μόνο με τη συναίνεση του ατόμου, και μόνο για τους σκοπούς για τους οποίους συλλέχθηκαν. Η εφαρμογή του επιβλέπεται από την ισπανική υπηρεσία προστασίας δεδομένων.

Νομοθεσία ηλεκτρονικού εμπορίου [282]

Ο Νόμος 34/2002 για τις υπηρεσίες της κοινωνίας και του ηλεκτρονικού εμπορίου της 11ης Ιουλίου εφαρμόζει την οδηγία της ΕΕ σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά (οδηγία 2000/31/ΕΚ για το «ηλεκτρονικό εμπόριο»). Πρέπει να σημειωθεί ότι ο νόμος 56/2007 σχετικά με τα μέτρα για την προώθηση της κοινωνίας της πληροφορίας τροποποιεί το νόμο σχετικά με τις υπηρεσίες της κοινωνίας της πληροφορίας και του ηλεκτρονικού εμπορίου με τη θέσπιση υποχρεώσεων για την ηλεκτρονική προσβασιμότητα.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [282]

Ο γενικός νόμος περί τηλεπικοινωνιών 32/2003 της 3ης Νοεμβρίου εφαρμόζει στο ισπανικό δίκαιο το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Η Ισπανία έχει τροποποιήσει τον Ποινικό Κώδικα για να συμπεριλάβει τα εγκλήματα του κυβερνοχώρου [37].

Άρθρο 197: άρθρο 198 Παράνομη προσπέλαση, Παράνομη υποκλοπή.

Άρθρο 256: άρθρο 248 Μη εξουσιοδοτημένη χρήση Τηλεπικοινωνιακού εξοπλισμού.

Άρθρο 264: Παρεμβολή σε δεδομένα, παρεμβολή σε σύστημα.

Άρθρο 278: Παράνομη υποκλοπή σε επιχειρήσεις.

Άρθρο 415: Παράνομη προσπέλαση(Δημόσιες Υπηρεσίες).

Άρθρο 560: Καταστροφή τηλεπικοινωνιακού εξοπλισμού.

Άρθρο 413: Παρεμβολή σε δεδομένα.

12.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Εθνικό Κέντρο Κρυπτογραφίας (Centro Nacional Criptológico, CCN) [283], το οποίο υπάγεται στο Εθνικό Κέντρο Πληροφοριών (Centro Nacional de Inteligência, CNI) [284] έχει ως στόχο τη διαχείριση της ασφάλειας στον κυβερνοχώρο και τον συντονισμό στα τρία επίπεδα της δημόσιας διοίκησης (κρατικό, περιφερειακό και τοπικό). Επιπλέον, ο οργανισμός αυτός είναι το ανώτατο όργανο με ευθύνη για τις διαβαθμισμένες πληροφορίες. Το Εθνικό Ινστιτούτο Τεχνολογιών Επικοινωνίας (INTECO) [285], υπάγεται στο Υπουργείο Βιομηχανίας, Τουρισμού και Εμπορίου, και αποστολή του είναι να προωθήσει και να αναπτύξει έργα καινοτομίας στην κοινωνία της πληροφορίας που σχετίζονται με τις ΤΠΕ. Το ινστιτούτο είναι υπεύθυνο για την προστασία του κυβερνοχώρου για τις μικρές και μεσαίες επιχειρήσεις και τους πολίτες της Ισπανίας. Το Εθνικό Κέντρο για την Προστασία Κρίσιμων Υποδομών (CNPIC [286]), υπάγεται στο Υπουργείο Εσωτερικών της Ισπανίας και προωθεί την ασφάλεια στον κυβερνοχώρο σχετικά με αυτές τις υποδομές. Η Ομάδα Τηλεματικού Εγκλήματος της Πολιτικής Φρουράς [287] και η Εθνική Μονάδα Πληροφοριών της Αστυνομίας [288], υπάγονται στο Υπουργείο Εσωτερικών, και εργάζονται για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Τέλος, η ισπανική Υπηρεσία Προστασίας Δεδομένων (AGPD) [289], υπάγεται στο Υπουργείο Δικαιοσύνης, και επιβάλλει τη συμμόρφωση με τους κανονισμούς προστασίας των προσωπικών δεδομένων.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CCN-CERT [290] είναι η ομάδα του Εθνικού Κέντρου Κρυπτογράφησης. Δημιουργήθηκε στα τέλη του 2006, ως η ισπανική κυβερνητική CERT. Η αποστολή της είναι να καταστεί Εθνικό Κέντρο Προειδοποίησης, να συνεργαστεί και να βοηθήσει τη Δημόσια Διοίκηση δίνοντας μια γρήγορη και αποτελεσματική αντιμετώπιση περιστατικών ασφαλείας. Κύριοι στόχοι της είναι η παροχή κεντρικής διαχείρισης περιστατικών ασφαλείας ο συντονισμός σε περιστατικά ασφαλείας, η παροχή άμεσης τεχνικής υποστήριξης, όπου απαιτείται και η δημιουργία σχέσεων με άλλες ομάδες CERT. Στην Ισπανία λειτουργούν πολλές ομάδες CERT αναλόγως του τομέα στον οποίο αναφέρονται. Έτσι στις Εθνικές και κυβερνητικές ομάδες εκτός του CCN-CERT ανήκουν οι INTECO-CERT [291], Andalucia CERT, CESICAT-CERT [292] και CSIRTCV [293]. Στον Χρηματοπιστωτικό τομέα λειτουργούν οι e-LC CSIRT [294],

MAPFRE-CCG-CERT [295]. Στον τομέα Έρευνας και Εκπαίδευσης οι esCERT-UPC [296], IRIS-CERT [297], CESCA-CSIRT [298]. Στον τομέα Πάροχων υπηρεσιών πελατειακής βάσης είναι οι ομάδες 21sec CERT [299], CyberSOC-CERT [300] και TBSecurity-CERT [301]. Η COSDEF-CERT είναι η στρατιωτική CERT, και τέλος η Telefonica CSIRT του παρόχου ίντερνετ Telefonica.

Ιδιωτικοί φορείς

Το ISMS Forum [302] είναι ένα δίκτυο ανοικτής γνώσης που συνδέει επιχειρήσεις, δημόσιους και ιδιωτικούς φορείς, ερευνητές με σκοπό την επαγγελματική ανάπτυξη της Ασφάλειας Πληροφοριών στην Ισπανία με μέλη πάνω από 120 εταιρείες και πάνω από 800 επαγγελματίες. Η Εθνική Συμβουλευτική Επιτροπή για την ασφάλεια στον κυβερνοχώρο (CNCCS) είναι μια ιδιωτική πρωτοβουλία που ξεκίνησε Μάιο του 2009 από την ισπανική βιομηχανία ασφάλειας. Το Συμβούλιο συγκεντρώνει όλες τις ισπανικές κορυφαίες εταιρείες του κλάδου στην Ασφάλεια Υπολογιστών όπως οι Panda Security, S21sec, Hispasec Συστημάτων και Secuware.

Ακαδημαϊκοί φορείς

Το Δίκτυο Κρυπτογραφίας και Ασφάλειας Πληροφοριών criptored.upm [303] που δημιουργήθηκε το 1999, έχει πάνω από 800 μέλη, ερευνητές από 214 πανεπιστήμια και 300 επιχειρήσεις από την Ισπανία και την Λατινική Αμερική. Το NICS Lab [304] είναι διεθνές ερευνητικό Κέντρο Ασφαλείας του Τμήματος Επιστήμης Υπολογιστών του Πανεπιστημίου της Μάλαγα.

Συνεργασία μεταξύ φορέων

Το Εθνικό Κέντρο Κρυπτογραφίας είναι ο οργανισμός που είναι υπεύθυνος για το συντονισμό των δραστηριοτήτων των διαφόρων οργανισμών στον τομέα της δημόσιας διοίκησης όσον αφορά την ασφάλεια των τεχνολογιών των πληροφοριών σε όλους τους τομείς. Το CCN ενεργεί επίσης ως φορέας πιστοποίησης και λειτουργεί το CCN - CERT. Σύμφωνα με το νόμο, το Κέντρο πρέπει να θεσπίσει τις αναγκαίες σχέσεις και την υπογραφή των αντίστοιχων συμφωνιών με ομοειδείς οργανισμούς άλλων χωρών, με σκοπό την εκτέλεση των καθηκόντων του. Για την ανάπτυξη αυτών των λειτουργιών, το CCN μπορεί να καθορίσει τον κατάλληλο συντονισμό με τις εθνικές επιτροπές στις οποίες ο νόμος αναθέτει αρμοδιότητες στον τομέα των συστημάτων των τεχνολογιών της πληροφορικής και των επικοινωνιών. Στον ιδιωτικό τομέα η CNCCS έχει αναλάβει το ρόλο συντονισμού και συνεργασίας των επιχειρήσεων όσον αφορά την προστασία των εταιρικών πληροφοριών, την προστασία της ταυτότητας του

καταναλωτή, και τη γενικότερη βελτίωση και υποστήριξη της οικονομικής ευημερίας και της εθνικής ασφάλειας. Στης Ισπανία λειτουργεί επίσης το Εθνικό Κέντρο Αριστείας για το Κυβερνοέγκλημα [305] με σκοπό τη συνεργασία όλων των φορέων για την αύξηση της αποτελεσματικότητας του αγώνα κατά του κυβερνοεγκλήματος.

12.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Το Κέντρο ασφαλούς διαδικτύου [306], στο πλαίσιο του προγράμματος Safer Internet της ευρωπαϊκής επιτροπής, στοχεύει στην παροχή ενός ασφαλούς περιβάλλοντος στη χρήση του διαδικτύου, κινητής τηλεφωνίας και των ΤΠΕ γενικά. Για το σκοπό αυτό, στο κέντρο λειτουργεί γραμμή για λήψη καταγγελιών σχετικά με το περιεχόμενο του Διαδικτύου, Γραμμή Βοήθειας η οποία ανταποκρίνεται στις απαιτήσεις των παιδιών, των οικογενειών τους ή / και τα σχολεία, σε όλα τα θέματα που σχετίζονται με την ασφαλή χρήση των ΤΠΕ και υλοποιεί δράσεις και εκστρατείες κατάρτισης και ευαισθητοποίησης, στα σχολεία, στους συλλόγους γονέων των μαθητών, στα όργανα επιβολής του νόμου και στους επαγγελματίες από διάφορους τομείς που εργάζονται με παιδιά. Όλες οι ομάδες CERT της Ισπανίας συμβάλλουν μέσα από ενημερώσεις και δράσεις στη δημιουργία ευαισθητοποίησης στο κοινό. Ένα παράδειγμα δράσης είναι το πρόγραμμα Oficina de Seguridad del Internauta (OSI) [307], του ινστιτούτου INTECO. Το OSI είναι ένα σημείο επαφής που παρέχει βοήθεια σε θέματα ασφαλείας για τους χρήστες του Διαδικτύου και παρέχει πληροφορίες και υποστήριξη για την πρόληψη και την επίλυση των προβλημάτων ασφάλειας. Η αποστολή του είναι να αυξηθεί η κουλτούρα της ασφάλειας, της πρόληψης, ευαισθητοποίησης και κατάρτισης παρέχοντας σαφείς και ακριβείς πληροφορίες και εργαλεία για την ασφάλεια, καθώς και η προώθηση της έγκαιρης ανίχνευσης και καταγγελίας των κάθε είδους απειλών, απάτης και επιθέσεων στο Internet. Το CCN - CERT έχει ένα σχέδιο επικοινωνίας και ευαισθητοποίησης, των ανθρώπων που είναι επιφορτισμένοι με την ασφάλεια της πληροφορικής και των επικοινωνιών στη Δημόσια Διοίκηση. Ομοίως, η ισπανική κυβερνητική CERT διεξάγει σεμινάρια και εργαστήρια σχετικά με την αύξηση της ευαισθητοποίησης, με στόχο την εκπαίδευση και την αναβάθμιση των γνώσεων του προσωπικού διοίκησης στον τομέα της ασφάλειας των πληροφοριών. Επιπλέον ο INTECO διοργανώνει ένα ετήσιο συνέδριο ΤΠΕ που ονομάζεται Διεθνής Συνάντηση της Ασφάλειας Πληροφοριών (ENISE) για τις Τεχνολογικές προκλήσεις στην Ασφάλεια των ΤΠΕ . Ο πάροχος υπηρεσιών TELEFONICA διαδραματίζει ενεργό ρόλο

στη διαδικασία ευαισθητοποίησης και ενημερώνει τους πελάτες του σχετικά με την καταπολέμηση των spam και πώς να αποφεύγουν άλλες δόλιες πρακτικές στο Διαδίκτυο. Επίσης προσφέρει στους πελάτες του διάφορα εργαλεία για την καταπολέμηση των αυτόκλητων μηνυμάτων, του κατασκοπευτικού και του κακόβουλου λογισμικού. Τέλος στην Ισπανία έχουν διοργανωθεί οι εθνικές ασκήσεις κυβερνοάμυνας Ejercicio de Cyberdefensa το 2010 και το 2011 και Jornadas PSCIC το 2012 [28].

12.5 Διεθνής Συνεργασία

Η Ισπανία είναι μέλος των διεθνών οργανισμών που προωθούν την προστασία του κυβερνοχώρου . Μερικά τέτοια παραδείγματα περιλαμβάνουν τη συμμετοχή της χώρας στο CCDCOE, τον IMPACT [33] και τον ENISA. Στα πλαίσια αυτά η Ισπανία συμμετείχε στην άσκηση Cyber Europe το 2010 και το 2012 [308][309], στη Cyber Coalition το 2013 [310] καθώς και στη άσκηση μεταξύ Ε.Ε και Η.Π.Α Cyber Atlantic το 2011 [309][311]. Διεθνή συνεργασία έχουν αναπτύξει και οι ισπανικές CERT καθώς δέκα από τις δεκαπέντε ομάδες που λειτουργούν είναι μέλη του διεθνούς φόρουμ FIRST [32]. Επίσης το CNN-CERT είναι μέλος της ομάδας κυβερνητικών CERT της Ευρώπης [31].

Κεφάλαιο 13ο

Ιταλία

13.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Ιταλία δεν έχει εκδώσει επίσημη στρατηγική Κυβερνοασφάλειας ωστόσο, το διάταγμα του προέδρου του συμβουλίου των υπουργών της 24η Ιανουαρίου 2013 [312] καθορίζει τις κατευθυντήριες γραμμές για την προστασία της εθνικής ασφάλειας στον κυβερνοχώρο και μπορεί να θεωρηθεί ως ένα πρώιμο στάδιο ανάπτυξης στρατηγικής. Σύμφωνα με αυτό κρίνεται αναγκαίο να δημιουργηθεί ένα εθνικό στρατηγικό πλαίσιο, με τον προσδιορισμό των ρόλων, των θεσμικών συνιστωσών για την ασφάλεια στον κυβερνοχώρο της χώρας και την καθιέρωση διαδικασιών και μηχανισμών δράσης, σε μια διεπιστημονική και συντονισμένη προσέγγιση. Θεωρείται επίσης αναγκαίο οι θεσμικές συνιστώσες να αλληλοεπιδρούν με τις αντίστοιχες αρχές του εξωτερικού, έτσι ώστε η Ιταλία να μπορεί να συμμετέχει πλήρως στα φόρα συνεργασίας σε διεθνές επίπεδο, όπως στην ΕΕ και στο ΝΑΤΟ. Γι' αυτό το λόγο ορίζεται ότι θα πρέπει να αναπτυχθεί μια αρχιτεκτονική σε τρία διαφορετικά επίπεδα παρέμβασης.

Στο πρώτο επίπεδο θα πρέπει να γίνει πολιτικός και στρατηγικός συντονισμός για τον εντοπισμό των λειτουργικών στόχων και για τη εθνική προστασία των πληροφοριών μέσω της ανάπτυξης ενός εθνικού σχεδίου για την ασφάλεια του κυβερνοχώρου.

Σε δεύτερο επίπεδο θα πρέπει να γίνει η σύνδεση των λειτουργιών των διοικητικών και των ρυθμιστικών αρχών, στην κατεύθυνση της υλοποίησης των στόχων και των γραμμών δράσης που υποδεικνύονται από τον εθνικό προγραμματισμό.

Στο τρίτο επίπεδο, θα πρέπει να γίνεται διαχείριση κρίσεων με συντονισμένη ανταπόκριση όλων των ενδιαφερομένων και αποκατάσταση της λειτουργικότητας των συστημάτων.

Για τις ειδικές ανάγκες του συντονισμού και την έγκριση των αναγκαίων μέτρων για την αποκατάσταση των συστημάτων θα πρέπει να δημιουργηθεί ένα διυπουργικό όργανο που θα ενεργοποιείται σε εκδήλωση κρίσης. Για τις τεχνικές πτυχές αντιμετώπισης καταστάσεων έκτακτης ανάγκης θα συσταθεί εθνικό CERT στο Υπουργείο Οικονομικής Ανάπτυξης.

13.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας ιδιωτικότητας / Προστασίας Προσωπικών Δεδομένων [313]

Ο Κώδικας Προστασίας Προσωπικών Δεδομένων που τέθηκε σε ισχύ την 1η Ιανουαρίου 2004 αντικαθιστά τον προηγούμενο νόμο προστασίας δεδομένων (Νόμος. 675/1996), καθώς και μια σειρά άλλων νομοθετικών και κανονιστικών διατάξεων. Ολοκληρώνει και ενοποιεί τη νομοθεσία περί προστασίας δεδομένων (1996), εισάγοντας σημαντικές καινοτομίες και συμμορφώνει την εθνική νομοθεσία με τους ευρωπαϊκούς κανονισμούς, ιδίως την οδηγία για την προστασία των δεδομένων (95/46/ΕΚ) και την οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες (2002/58/ΕΚ). Ο νόμος έχει ως στόχο να ενισχύσει τα δικαιώματα προστασίας των δεδομένων των φυσικών προσώπων. Ο Επίτροπος Προστασίας Δεδομένων (Privacy Garante) είναι υπεύθυνος για την εποπτεία της εφαρμογής του.

Νομοθεσία ηλεκτρονικού εμπορίου [313]

Το Νομοθετικό Διάταγμα τέθηκε σε ισχύ στις 14 Μαΐου 2003. Ρυθμίζει τη χρήση του ηλεκτρονικού εμπορίου μέσα στην Ιταλία. Το διάταγμα μεταφέρει την οδηγία 2000/31/ΕΚ σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»).

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [313]

Ο Κώδικας Ηλεκτρονικών Επικοινωνιών τέθηκε σε ισχύ στις 16 Σεπτεμβρίου 2003. Και ενσωματώνει τέσσερις από τις οδηγίες του κανονιστικού πλαισίου της ΕΕ για τις ηλεκτρονικές επικοινωνίες,

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [314]

Η Γερουσία του ιταλικού Κοινοβουλίου ενέκρινε στις 27 Φεβρουαρίου 2008 τη Σύμβαση για το έγκλημα στον κυβερνοχώρο του συμβουλίου της Ευρώπης και αναθεώρησέ τον Ποινικό Κώδικα της Ιταλίας.

Ποινικός Κώδικας

Άρθρο 615 Παράνομη Πρόσβαση, Κακή χρήση ηλεκτρονικών συσκευών.

Άρθρο 617 Παράνομη Υποκλοπή.

Άρθρο 635 Παρεμβολή Δεδομένων, Παρεμβολή συστήματος.

Άρθρο 491 Πλαστογραφία με Η/Υ.

Άρθρο 640 Απάτη με Η/Υ.

13.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Ανώτερο Ινστιτούτο Επικοινωνιών και Τεχνολογιών Πληροφορικής (ISCOM) [315] λειτουργεί στο πλαίσιο του Υπουργείου Οικονομικής Ανάπτυξης - Επικοινωνιών ως τεχνικό-επιστημονικό όργανο. Οι δραστηριότητες του Ινστιτούτου στον τομέα της έρευνας έχουν ως στόχο την ανάπτυξη και βελτίωση των ΤΠΕ. Το Ινστιτούτο στοχεύει στην προώθηση της ανάπτυξης των τηλεπικοινωνιών και την εφαρμογή καινοτόμων τεχνολογιών και έχει επίσης τον ρόλο του Φορέα Πιστοποίησης της ασφάλειας συστημάτων και προϊόντων εμπορικών πληροφοριών (OCSI) [316]. Ο Οργανισμός για την ψηφιακή Ιταλία (DigitPA) [317] παρέχει τεχνική υποστήριξη προς την κυβέρνηση. Κύριοι τεχνικοί τομείς του είναι: το PKI, οι ηλεκτρονικές υπογραφές, η ευαισθητοποίηση στο τομέα των ΤΠΕ και η ηλεκτρονική διακυβέρνηση. Ο Οργανισμός για την ψηφιακή Ιταλία υπαγορεύει συστάσεις, στρατηγικές, και τεχνικές προδιαγραφές σε σχέση με την ευαισθητοποίηση στον τομέα της ασφάλειας των πληροφοριών και των σχετικών καταστάσεων έκτακτης ανάγκης. Ο DigitPA λειτουργεί και ως ένα κέντρο αριστείας επιχειρησιακής συνέχειας, το οποίο ασχολείται με την προστασία των δεδομένων και των εφαρμογών της πληροφορικής στην κυβέρνηση. Το Κέντρο έχει ετοιμάσει τις "Κατευθυντήριες γραμμές για τη συνέχιση της λειτουργίας της δημόσιας διοίκησης". Το Εθνικό Κέντρο για το έγκλημα στον κυβερνοχώρο και την προστασία των υποδομών ζωτικής σημασίας (CNAIPIC) [318] είναι Μονάδα της Αστυνομίας που ειδικεύεται σε επιθέσεις προς τις Υποδομές Ζωτικής Σημασίας. Το CNAIPIC είναι υπεύθυνο για τη πρόληψη και τη δίωξη των εγκλημάτων πληροφορικής, Έχει εξειδικευμένο προσωπικό στον τομέα της καταπολέμησης του εγκλήματος στον κυβερνοχώρο, το οποίο έχει επίσης αποκτήσει πρακτική πείρα στους τομείς της λεγόμενης κυβερνο-τρομοκρατίας και κατασκοπείας. Η Ιταλική Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα [319] είναι υπεύθυνη για όλες τις περιοχές, δημόσιες και ιδιωτικές, όπου θα πρέπει να διασφαλιστεί η σωστή επεξεργασία των δεδομένων και ο σεβασμός στα δικαιώματα των ατόμων .

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CERT-IT [320] είναι η εθνική ομάδα της Ιταλίας και υποστηρίζεται από το πανεπιστήμιο του Μιλάνου. Προς το παρόν δεν είναι πλήρως επιχειρησιακή. Η GARR-

CERT [321]ανήκει στο Ιταλικό Ακαδημαϊκό και Ερευνητικό Δίκτυο (GARR). Η CERT Poste Italiane [322] είναι υπεύθηνη για την πρόληψη και την αντιμετώπιση των απειλών στον κυβερνοχώρο που επηρεάζουν τις πληροφορίες και τα περιουσιακά στοιχεία του Ιταλικού Ταχυδρομείου (Poste Italiane). Η CERT-Difesa [323] έχει ως αποστολή να βοηθήσει τον εθνικό στρατό στην προστασία των δικτύων επικοινωνίας και την προώθηση της ανταλλαγής πληροφοριών γύρω από την ασφάλεια των ΤΠΕ. Η.S2OC [324] είναι η CERT του τηλεπικοινωνιακού παρόχου Telecom Italia Group. Η CERT ENEL [325] ανήκει στην εταιρεία ENEL, που δραστηριοποιείται στον τομέα της ενέργειας. Η CERT-RAFVG [326] δημιουργήθηκε το 2005 από την Αυτόνομη Περιφέρεια Friuli Venezia Giulia, και λειτουργεί ως σημείο αναφοράς για τις δραστηριότητες της ασφάλειας στον κυβερνοχώρο εντός της περιοχής. Τέλος η SICEI-CERT [327] ιδρύθηκε για να στηρίξει την Ιταλική Εκκλησία.

Ιδιωτικοί φορείς

Η Ένωση Τηλεπικοινωνιών, Πληροφορικής και Ηλεκτρονικών (ANITEC) [328] συγκεντρώνει τις Ιταλικές Βιομηχανίες που δραστηριοποιούνται στον τομέα των τηλεπικοινωνιών, της πληροφορικής και των καταναλωτικών ηλεκτρονικών με σκοπό να συμβάλλει στην ανάπτυξη και την ανάπτυξη των ψηφιακών τεχνολογιών. Η Ιταλική Ένωση Επαγγελματιών Ασφάλειας [329] εκπροσωπεί την κοινότητα των επαγγελματιών της ασφάλειας. Είναι η ιταλική εκπρόσωπος της ISSA (Information Systems Security Association), με κύριες δραστηριότητες την οργάνωση εκπαιδευτικών φόρουμ και την ανταλλαγή απόψεων μεταξύ των εμπειρογνωμόνων σε θέματα ασφάλειας, προκειμένου να βελτιώσουν τις γνώσεις τους, για τη σωστή διαχείριση της ασφάλειας σε δημόσιους και ιδιωτικούς οργανισμούς. Η CLUSIT [330] είναι μια ένωση εμπειρογνωμόνων που έχει ως στόχο την ευαισθητοποίηση για την ασφάλεια της πληροφορικής στο χώρο των επιχειρήσεων, της δημόσιας διοίκησης και των πολιτών. Συμβάλλει στην ανάπτυξη των νόμων, και των πρακτικών για τη σωστή συμπεριφορά στην ασφάλεια των υπολογιστών, τόσο σε εθνικό όσο και σε διεθνές επίπεδο, στον καθορισμό προγραμμάτων μάθησης και πιστοποιήσεων για επαγγελματίες της ασφάλειας υπολογιστών και προωθεί την υιοθέτηση μεθοδολογιών και τεχνολογιών που μπορούν να συμβάλλουν στη βελτίωση της ασφάλειας των υποδομών πληροφοριών σε όλα τα επίπεδα.

Ακαδημαϊκοί φορείς

Το εργαστήριο Computer and Network Security Lab (LaSER) [331] είναι μια ερευνητική δομή του Τμήματος της Επιστήμης των Υπολογιστών, στο Università degli Studi di Milano. Η έρευνα εστιάζει σε θέματα σχετικά με την ασφάλεια των υπολογιστών. Το Ιταλικό Δίκτυο Έρευνας και Εκπαίδευσης GARR σχεδιάζει και διαχειρίζεται το δίκτυο των Πανεπιστημίων και Επιστημονικής Έρευνας και λειτουργεί την ομάδα GARR-CERT.

Συνεργασία μεταξύ φορέων

Σύμφωνα με το νόμο 132/2013 ο Οργανισμός για την ψηφιακή Ιταλία DigitPA ορίστηκε ως ο κεντρικός κόμβος συνεργασίας για την ψηφιακή ανάπτυξη στην Ιταλία Σε θέματα ασφάλειας ασχολείται με τη θέσπιση τεχνικών κανόνων και τη διαμμόρφωση κατευθυντήριων οδηγιών. Επίσης υπαγορεύσει τις συστάσεις, τις στρατηγικές, και τις τεχνικές προδιαγραφές σε σχέση με την ευαισθητοποίηση και την εκπαίδευση του προσωπικού στον τομέα της ασφάλειας των πληροφοριών και των καταστάσεων έκτακτης ανάγκης. Μέσω της Υπηρεσίας Ασφάλειας Πληροφοριών και Επιχειρησιακής Συνέχειας, αξιολογεί σε τακτά χρονικά διαστήματα το επίπεδο ασφάλειας και εμπιστευτικότητας των συστημάτων πληροφορικής και δικτύων ηλεκτρονικών υπολογιστών που χρησιμοποιούνται από τις τοπικές αρχές, προτείνει διορθωτικές ενέργειες για την αντιμετώπιση τυχόν ελλείψεων και προτείνει τεχνικά, διαδικαστικά και οργανωτικά μέτρα. Στον οργανισμό έχεις συσταθεί μια επιτροπή με εκπροσώπους όλων των υπουργείων για την καλύτερη συνεργασία εντός της κυβέρνησης.

13.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Η σημαντικότερη δράση ευαισθητοποίησης στην Ιταλία προέρχεται από το κέντρο Sicurinrete.it [332] στα πλαίσια του προγράμματος της Ευρωπαϊκής Επιτροπής Safer Internet. Το κέντρο έχει ως στόχο την αύξηση της γνώσης της χρήσης του Διαδικτύου και των νέων μέσων από τους νέους, τους γονείς, τους δασκάλους και όλους εκείνους που χρειάζονται βοήθεια. Στο κέντρο μπορεί κανείς να αναφέρει αν ήρθε σε επαφή με κακόβουλο περιεχόμενο ή παιδική πορνογραφία. Επίσης το κέντρο έχει δημοσιεύσει και διανείμει αρκετά ενημερωτικά φυλλάδια σχετικά με την ασφαλή χρήση του διαδικτύου.

Η ιστοσελίδα της Ιταλικής Αστυνομίας παρέχει επίσης πληροφόρηση σχετικά με τα εγκλήματα του διαδικτύου. Η Telecom Italia [333] παρέχει μέσω της ιστοσελίδας της ενημέρωση σχετικά με την ασφάλεια στο διαδίκτυο που περιλαμβάνει βέλτιστες

πρακτικές, προειδοποιήσεις καθώς και τεχνική βοήθεια. Τέλος στην Ιταλία διεξάγονται οι εθνικές άσκησες κυβερνοασφάλειας Cyber Italy και HACKCERT [28][334][335].

13.5Διεθνής Συνεργασία

Ο DigitPa, είναι ο κύριος φορέας συνεργασίας με την Ε.Ε. και τον οργανισμό ENISA. Το 2012 έλαβε μέρος στην άσκηση «Cyber Europe 2012» [336][337]. Συμμετείχαν από την Ιταλία επίσης η CNAIPIC και το CERT-Difesa. Η Ιταλία, ως μέλος του NATO, συνεργάζεται σε θέματα Κυβερνοασφάλειας με τις υπόλοιπες χώρες μέλη, συμμετείχε στις ασκήσεις Locked Shields και Cyber Coalition καθώς και στην άσκηση μεταξύ Ε.Ε. και Η.Π.Α cyber atlantic[337][338]. Είναι επίσης μέλος του NATO CCDCoE από το 2008 [130]. Ακόμη στο πλαίσιο συνεργασίας με τις Η.Π.Α. συμμετείχε στην άσκηση Cyber Storm που διοργάνωσε το Υπουργείο Εσωτερικής Ασφάλειας των Η.Π.Α [253]. Τέλος, η Ιταλία είναι του IMPACT [33].

Κεφάλαιο 14ο

Κροατία

14.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Μέχρι σήμερα η Κροατία δεν έχει δημοσιεύσει επίσημη Εθνική Στρατηγική Κυβερνοασφάλειας. Ωστόσο μπορεί κανείς να παρατηρήσει δράσεις και πολιτικές που μπορούν να θεωρηθούν ως πρώιμο στάδιο ανάπτυξης μιας εθνικής στρατηγικής μέσα από την διακήρυξη για την ασφάλεια στην πληροφορική που ψήφισε το κροατικό κοινοβούλιο στις 13 Ιουλίου 2007 [339]. Η διακήρυξη ορίζει την έννοια των μέτρων ασφάλειας πληροφορικής, τα πρότυπα της ασφάλειας, καθώς και τις αρμόδιες αρχές για την υιοθέτηση, εφαρμογή και παρακολούθηση των μέτρων και προτύπων ασφάλειας. Επίσης προβλέπει τη συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα.

14.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας ιδιωτικότητας / Προστασίας Προσωπικών Δεδομένων [340]

Ο νόμος περί προστασίας προσωπικών δεδομένων εγκρίθηκε τον Ιούνιο του 2003, για μεταφέροντας στο εθνικό δίκαιο την οδηγίας της ΕΕ (95/46/ΕΚ). Η τελευταία τροποποίηση έλαβε χώρα στις 3 Απριλίου 2008 (NN 41/08).

Νομοθεσία ηλεκτρονικού εμπορίου[340]

Ο νόμος για το ηλεκτρονικό εμπόριο ρυθμίζει την παροχή των υπηρεσιών πληροφορικής, την ευθύνη των παρόχων και καθορίζει τους κανόνες σχετικά με τη σύναψη των συμβάσεων σε ηλεκτρονική μορφή. Οι διατάξεις της δεν ισχύουν για την προστασία των δεδομένων, τη φορολογία, και τη συμβολαιογραφική δραστηριότητα. Ο νόμος εγκρίθηκε για πρώτη φορά στις 15 Οκτωβρίου 2003 (NN 173/03) ενώ η τελευταία έκδοσή του ψηφίστηκε στις 13 Μαρτίου 2009 (NN 36/09).

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [340]

Ο νόμος περί ηλεκτρονικών επικοινωνιών εξασφαλίζει την υλοποίηση των βασικών αρχών και στόχων στον τομέα των ηλεκτρονικών επικοινωνιών, όπως η περαιτέρω ενοποίηση και απλούστευση του υπάρχοντος νομοθετικού πλαισίου των ηλεκτρονικών

επικοινωνιών και τη εφαρμογή άλλων λύσεων, σύμφωνα με τις βέλτιστες πρακτικές στα κράτη μέλη της Ευρωπαϊκής Ένωσης.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [341]

Ποινικός Κώδικας

Η Κροατία επικύρωσε τη σύμβαση για το κυβερνοέγκλημα του Συμβουλίου της Ευρώπης, στις 17 Οκτωβρίου 2002. Ο Ποινικός Κώδικας τροποποιήθηκε ώστε να είναι σύμφωνος με τη Σύμβαση, και τέθηκε σε ισχύ την1η Οκτωβρίου 2004. Στο κώδικα περιγράφονται οι παρακάτω κατηγορίες εγκλημάτων:

Άρθρο 223-1: Παράνομη πρόσβαση.

Άρθρο 223-3: Παρεμβολή σε δεδομένα, παρεμβολή σε σύστημα.

Άρθρο 223-4: Παράνομη υποκλοπή.

Άρθρο 223-6: Κακή χρήση ηλεκτρονικών συσκευών.

Άρθρο 223α: Πλαστογραφία με Η/Υ.

Άρθρο 224α: Απάτη με Η/Υ.

Νόμος περί Ασφάλειας Πληροφοριών [339]

Ο νόμος ορίζει την έννοια των μέτρων ασφάλειας πληροφορικής, τα πρότυπα της ασφάλειας, καθώς και τις αρμόδιες αρχές για την υιοθέτηση, εφαρμογή και παρακολούθηση των μέτρων και προτύπων ασφάλειας. Επίσης θεσπίζει τη συνεργασία μεταξύ δημόσιου και ιδιωτικού τομέα.

Κανονισμός για τα Μέτρα Ασφάλειας Πληροφοριών [342]

Με το άρθρο 7 του νόμου περί Ασφάλειας Πληροφοριών η κροατική κυβέρνηση, ενέκρινε τον Κανονισμό που καθορίζει τα μέτρα ασφάλειας για το χειρισμό των διαβαθμισμένων δεδομένων.

14.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς [1]

Το Γραφείο του Συμβουλίου Εθνικής Ασφάλειας [343] είναι ο κεντρικός φορέας για την ασφάλεια των πληροφοριών και για τον συντονισμό στην υιοθέτηση και την εφαρμογή των μέτρων και των προτύπων για την ασφάλεια των πληροφοριών της Δημοκρατίας της Κροατίας καθώς και για την ανταλλαγή διαβαθμισμένων και μη πληροφοριών μεταξύ της Κροατίας και ξένων χωρών και οργανισμών.

Το Τμήμα Ασφάλειας Πληροφοριακών Συστημάτων [344] είναι ένα όργανο της κεντρικής κυβέρνησης για την εκτέλεση των τεχνικών μέτρων ασφάλειας, συμπεριλαμβανομένων των προτύπων ασφάλειας συστημάτων πληροφορικής, των διαπιστεύσεων ασφαλείας των πληροφοριακών συστημάτων, και το συντονισμό για την πρόληψη και την αντιμετώπιση των απειλών.

Η Αστυνομική Υπηρεσία για την καταπολέμηση της διαφθοράς και του οργανωμένου εγκλήματος μέσω του τμήματος εγκλημάτων υψηλής τεχνολογίας [345] πραγματοποιεί συστηματική ανάλυση, παρακολούθηση και μελέτη των εγκλημάτων στον κυβερνοχώρο και προτείνει λύσεις, στην καταπολέμηση του, υλοποιεί άμεσα ποινικές έρευνες στον τομέα των αξιόποινων πράξεων που διαπράττονται εις βάρος και από πληροφοριακά συστήματα και δίκτυα, και παρέχει εξειδικευμένη υποστήριξη σε άλλες οργανωτικές μονάδες της αστυνομίας και κρατικούς φορείς. Τέλος, η Αρχή Προστασίας Προσωπικών δεδομένων (AZOP) είναι υπεύθυνη για την εφαρμογή του νόμου περί προστασίας των προσωπικών δεδομένων και της ιδιωτικότητας.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η HR-CERT [9] είναι η εθνική CERT της Κροατίας. Σκοπός της είναι να βοηθήσει τους χρήστες του Διαδικτύου στην εφαρμογή προληπτικών μέτρων για τη μείωση των κινδύνων των περιστατικών ασφάλειας στους υπολογιστές και να βοηθήσει στην καταπολέμηση των επιπτώσεων που προκύπτουν από περιστατικά ασφάλειας. Ιδρύθηκε σύμφωνα με τη νομοθεσία για την ασφάλεια των πληροφοριών και κύρια αποστολή της είναι η επεξεργασία των συμβάντων στο Διαδίκτυο. Σύμφωνα με την πολιτική της, ασχολείται με περιστατικά τα οποία αφορούν το χώρο διευθύνσεων IP της Κροατίας ή τον τομέα του Διαδικτύου. Η CERT ZSIS [346] Αποτελεί την κυβερνητική CERT. Το πεδίο των εργασιών της αφορά κυρίως την εφαρμογή προληπτικών μέτρων που αποσκοπούν στην μείωση των κίνδυνων και στην αντιμετώπιση των περιστατικών ασφάλειας στις κρατικές αρχές της Δημοκρατίας της Κροατίας.

Ιδιωτικοί φορείς

Το Poslovni Forum[348] είναι ένα επιχειρηματικό Φόρουμ που ιδρύθηκε το 2002 και συγκέντρωσε εμπειρογνώμονες από τον τομέα της οικονομίας, του δικαίου και της επιστήμης των υπολογιστών. Στους τομείς ενδιαφέροντός του συμπεριλαμβάνεται και η ασφάλεια των δικτύων υπολογιστών.

Ακαδημαϊκοί φορείς

Το Laboratory for Systems and Signals [348] είναι ένα εργαστήριο του Τμήματος Ηλεκτρολόγων Μηχανικών και Πληροφορικής του Πανεπιστημίου του Ζάγκρεμπ το οποίο ασχολείται με την ασφάλεια της πληροφορικής από το 1995. Ξεκίνησε τη Κροατική Εθνική CERT και συνέγραψε το «Εθνικό Πρόγραμμα για την Ασφάλεια της Πληροφορίας». Επίσης παρείχε βοήθεια σε εκατοντάδες οργανώσεις στην Κροατία με την εκτίμηση της τρωτότητας των πληροφοριακών συστημάτων τους ή/και σχεδιάζοντας την προστασία τους. Το CARNet [349] είναι το κροατικό Ακαδημαϊκό και Ερευνητικό Δίκτυο που ιδρύθηκε το 1991 από του Υπουργείο Επιστήμης και Τεχνολογίας της Δημοκρατίας της Κροατίας. Το Τμήμα Ασφάλειας Ηλεκτρονικών Υπολογιστών στοχεύει στην προστασία και στην ευαισθητοποίηση των υπηρεσιών και των χρηστών του δικτύου έναντι των απειλών.

Συνεργασία μεταξύ φορέων

Ο συντονισμός στην υιοθέτηση και εφαρμογή των μέτρων και προτύπων για την ασφάλεια των πληροφοριών είναι ευθύνη του Γραφείου του Συμβουλίου Εθνικής Ασφάλειας. Τα περιστατικά ασφαλείας θα πρέπει να αναφέρονται στην εθνική CERT. Αυτή συνεργάζεται με τις αρμόδιες αρχές (Τμήμα Πληροφοριακών Συστημάτων Ασφαλείας - ISSB, το γραφείο του Συμβουλίου Εθνικής Ασφάλειας και το Υπουργείο Εσωτερικών), καθώς επίσης και με διεθνή CERT για την αντιμετώπισή τους.

14.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Το πρόγραμμα ευαισθητοποίησης (safe internet) της Ευρωπαϊκής επιτροπής δεν έχει υλοποιηθεί ακόμα στην Κροατία. Κύριος φορέας ενημέρωσης και ευαισθητοποίησης είναι η εθνική CERT. Η εθνική CERT ενημερώνει για το επίπεδο ασφάλειας στην χώρα και παρέχει μέσα από την ιστοσελίδα του συστάσεις και ειδοποιήσεις προς τους απλούς χρήστες του διαδικτύου. Στην Κροατία διεξάγεται επίσης κάθε χρόνο το συνέδριο FSec [350]. Το Συνέδριο καλύπτει αρκετούς τομείς ενδιαφέροντος όπως η ψηφιακή εγκληματολογία, εφαρμογές για την ασφάλεια στο διαδίκτυο, κρυπτογραφία και κρυπτανάλυση, απόρρητο και ανωνυμία κ.α.

14.5 Διεθνής Συνεργασία

Η Κροατία έγινε το 28ο κράτος μέλος της Ευρωπαϊκής Ένωσης τον Ιούλιο του 2013. Ως το πιο πρόσφατο μέλος η συνεργασία με τους ευρωπαϊκούς θεσμούς είναι ακόμα σε πρώιμο στάδιο. Τον Σεπτέμβριο του 2013 αντιπροσωπεία με εκπροσώπους του εθνικού και κυβερνητικού CERT συναντήθηκε με τους εμπειρογνώμονες του ENISA[351]. Ο στόχος της συνάντησης ήταν να συζητήσουν την τρέχουσα κατάσταση σχετικά με την ασφάλεια του κυβερνοχώρου της Κροατίας, τη συμμετοχή της Κροατίας στην αντιμετώπιση των περιστατικών ασφαλείας στην Ευρώπη καθώς και την συμμετοχή της σε πανευρωπαϊκές ασκήσεις όπως η Cyber Europe. Η Κροατία αποτελεί επίσης μέλος του NATO. Το εθνικό CERT συμμετείχε το 2013 για πρώτη φορά ενεργά στην άσκηση Cyber Coalition [352]. Στην άσκηση συμμετείχαν επίσης εμπειρογνώμονες του Κροατικού στρατού, καθώς και εμπειρογνώμονες από το τμήμα Ασφάλειας Πληροφοριακών Συστημάτων. Η Κροατία είναι επίσης μέλος του IMPACT [33]. Τέλος, η Κροατία είναι μέλος της Ένωσης Δικτύωσης Κεντρικής και Ανατολικής Ευρώπης (CEENet) [79] και οι τρείς CERT της Χώρας είναι μέλη του διεθνούς Φόρουμ FIRST [32].

Κεφάλαιο 15ο

Κύπρος

15.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας [353]

Η Εθνική Στρατηγική Κυβερνοασφάλειας της Κύπρου διαμορφώθηκε το 2012 με στόχο την εδραίωση ενός ασφαλούς ηλεκτρονικού περιβάλλοντος με ειδικές πρόνοιες και δράσεις προκειμένου να προστατευτούν οι κρίσιμες υποδομές πληροφορίας, από ενδεχόμενη διατάραξη ή καταστροφή διότι σε αυτή τη περίπτωση οι επιπτώσεις θα ήταν ζωτικής σημασίας για την κοινωνία. Σύμφωνα με τις ανάγκες της Κυπριακής Δημοκρατίας προτεραιότητα δόθηκε :

- Στην οργάνωση των αρμόδιων φορέων του κράτους ώστε να διασφαλίζεται η σωστή και αποτελεσματική τους συνεργασία.
- Στη δημιουργία ολοκληρωμένου νομοθετικού πλαισίου από τις αρμόδιες υπηρεσίες του κράτους ώστε να καλύπτονται όλες οι πτυχές της ασφάλειας δικτύων και πληροφοριών, συμπεριλαμβανομένου του κυβερνοεγκλήματος και της προστασίας των προσωπικών δεδομένων.
- Στη διαμόρφωση τεχνικών και οργανωτικών μέτρων αλλά και διαδικασιών για την αύξηση της ασφάλειας στον απαιτούμενο βαθμό τόσο στους χώρους αλλά και κυρίως στον εξοπλισμό και στο λογισμικό,
- Στην κατάρτιση σε θέματα ασφάλειας αλλά και στην ανάπτυξη των απαραίτητων ικανοτήτων τόσο των άμεσα εμπλεκομένων όσο και του λοιπού πληθυσμού.
- Στην αποδοτική συνεργασία του κράτους με αρμόδιους φορείς του δημόσιου και ιδιωτικού τομέα, τόσο σε εθνικό όσο και σε διεθνές επίπεδο.
- Στη δημιουργία ή την προσαρμογή των δομών και μηχανισμών των αρμοδίων υπηρεσιών, ώστε να διασφαλιστούν οι απαιτήσεις και οι δυνατότητες άμεσης ανταπόκρισης σε συμβάντα.

15.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [354]

Ο νόμος περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) (Ν.138 (Ι) / 2001) που τέθηκε σε ισχύ το Νοέμβριο του 2001 όπως τροποποιήθηκε με το Ν.37 (Ι) / 2003, είναι συμβατός με το κοινοτικό κεκτημένο και κυρίως με την Ευρωπαϊκή Οδηγία 95/46/ΕΚ για την προστασία των δεδομένων.

Νομοθεσία ηλεκτρονικού εμπορίου [354]

Ο νόμος εξυπηρετεί την εφαρμογή της οδηγίας 2000/31/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 8ης Ιουνίου 2000, για ορισμένες νομικές πτυχές υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου στην εσωτερική αγορά.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [354]

Η Κύπρος έχει υιοθετήσει δύο νόμους. Ο πρώτος αναφέρεται στις ηλεκτρονικές επικοινωνίες και ο δεύτερος είναι η τροποποίηση του νόμου 2002 περί Ραδιοεπικοινωνιών.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [355]

Στο Νόμο 22 (ΙΙΙ) του 2004 περιγράφονται αδικήματα που συνιστούν τις παρακάτω κατηγορίες εγκλημάτων:

Άρθρο 2 Παράνομη πρόσβαση.

Άρθρο 3 Παράνομη Υποκλοπή.

Άρθρο 4 Παρεμβολή σε δεδομένα.

Άρθρο 5 Παρεμβολή σε Σύστημα.

Άρθρο 6 Κακή χρήση συσκευών.

Άρθρο 7 Πλαστογραφία με χρήση Η/Υ.

Άρθρο 8 Απάτη με χρήση Η/Υ.

15.3 Αρχές και Οργανισμοί [1]

Δημόσιοι φορείς

Το Γραφείο Επιτρόπου Ρυθμίσεως Ηλεκτρονικών Επικοινωνιών και Ταχυδρομείων (ΓΕΡΗΕΤ) [356] είναι κατά νόμο αρμόδιο για τον συντονισμό των θεμάτων της ασφάλειας δικτύων ηλεκτρονικών επικοινωνιών και πληροφοριών στην επικράτεια της Κυπριακής Δημοκρατίας. Επίσης το ΓΕΡΗΕΤ εκπροσωπεί τη χώρα στο Διοικητικό Συμβούλιο του ENISA και ενεργεί ως κεντρικός σύνδεσμος επικοινωνίας και συντονισμού όλων των υπόλοιπων φορέων. Ακόμη, στο πλαίσιο των αρμοδιοτήτων του είναι ο συντονισμός αλλά και η αμφίδρομη ενημέρωση των κυπριακών αρχών, των

ενδιαφερομένων μερών και των καταναλωτών εντός της Κυπριακής Δημοκρατίας με τις αρμόδιες υπηρεσίες της Ευρωπαϊκής Ένωσης, για θέματα και δραστηριότητες που αφορούν την ασφάλεια δικτύων και πληροφοριών.

Το Τμήμα Υπηρεσιών Πληροφορικής (ΤΥΠ) του Υπουργείου Οικονομικών [357] είναι αρμόδιο για θέματα σχετικά με την προώθηση και εφαρμογή της πληροφορικής και της διακυβέρνησης στο δημόσιο τομέα. Η αστυνομία της Κύπρου μέσω του Γραφείου Καταπολέμησης Ηλεκτρονικού Εγκλήματος, (ΓΚΗΕ) [358], σύμφωνα με την, Αστυνομική Διάταξη 3/45, έχει ως αποστολή τη διερεύνηση εγκλημάτων που γίνονται μέσω διαδικτύου και ηλεκτρονικών υπολογιστών κατά παράβαση του Νόμου 22(ΙΙΙ)/2004. Το Γενικό Επιτελείο Εθνικής Φρουράς (ΓΕΕΦ), μέσω της Αρχής Ασφαλείας Πληροφοριών Τεχνικής Φύσης (INFOSEC) [359] έχει αποστολή τον προσδιορισμό και την εφαρμογή μέτρων ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών. Η Κεντρική Υπηρεσία Πληροφοριών (ΚΥΠ) [360] υπάγεται απευθείας στον Πρόεδρο της Δημοκρατίας και είναι αρμόδια για θέματα που σχετίζονται με τη συλλογή, την αξιολόγηση και εκμετάλλευση πληροφοριών που αφορούν την ασφάλεια του Κράτους. Το Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα [361] είναι υπεύθυνο για την προστασία των προσωπικών δεδομένων. Οι υπεύθυνοι επεξεργασίας προσωπικών δεδομένων τόσο από ιδιωτικές εταιρείες όσο και από δημόσιους οργανισμούς κοινοποιούν στο Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα τα μέτρα που λαμβάνουν για την ασφάλεια και την προστασία των δεδομένων. Το Υπουργείο Συγκοινωνιών και Έργων (ΥΣΕ) [362] σύμφωνα με Ν. 112(Ι)/2004, είναι η αρμόδια αρχή στα θέματα πολιτικής στον τομέα της ασφάλειας των δικτύων. Το Τμήμα Ηλεκτρονικών Επικοινωνιών (ΤΗΕ) [363] είναι υπεύθυνο για την προστασία των ασύρματων δικτύων ηλεκτρονικών επικοινωνιών από επιβλαβείς παρεμβολές. Τέλος, η Δύναμη Πολιτικής Άμυνας [364] είναι αρμόδια για το δίκτυο πληροφοριών προειδοποίησης για τις υποδομές ζωτικής σημασίας (CIWIN). Επίσης, ο συγκεκριμένος φορέας ανταλλάσσει πληροφορίες με άλλα κράτη μέλη της Ε.Ε για τις βέλτιστες πρακτικές που χρησιμοποιούνται στην ασφάλεια των κρίσιμων υποδομών.

Ομάδες αντιμετώπισης περιστατικών ασφαλείας [13]

Η Cyprus Research and Academic CSIRT [365] είναι η μόνη ομάδα αντιμετώπισης περιστατικών ασφαλείας στην Κύπρο κα λειτουργεί από το Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο. Προς το παρόν δεν είναι πλήρως επιχειρησιακή.

Ιδιωτικοί φορείς

Ο οργανισμός Cyprus Computer Society [366] ιδρύθηκε από εταιρείες και επαγγελματίες του κλάδου της πληροφορικής, προκειμένου να εκπροσωπεί τις απόψεις τους στις εθνικές αρχές επί γενικών θεμάτων του κλάδου αλλά και για τη διαμόρφωση στρατηγικής. Επίσης συμμετέχει σε προγράμματα ανάπτυξης συνεργασιών με άλλους φορείς από ευρωπαϊκά κράτη, με την ακαδημαϊκή κοινότητα, την κυβέρνηση, δημόσιες, ιδιωτικές και μη κυβερνητικές οργανώσεις. Ο οργανισμός έχει καθοριστικό ρόλο στην προώθηση της ασφάλειας στις ΤΠΕ με τη διοργάνωση και τη χορηγία συνεδρίων και ημερίδων στην Κύπρο, που εξυπηρετούν την τοπική βιομηχανία, την κυβέρνηση, την ακαδημαϊκή κοινότητα και το ευρύ κοινό.

Ακαδημαϊκοί φορείς

Το Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο (ΚΕΑΔ) [367] παρέχει την υποδομή δικτύου για την Κυπριακή Ερευνητική και Ακαδημαϊκή Κοινότητα και συνδέει τους οργανισμούς τριτοβάθμιας εκπαίδευσης με ερευνητικούς. Στο πλαίσιο του δικτύου λειτουργεί η CSIRT.

Συνεργασία μεταξύ φορέων

Όπως έχει αναφερθεί, το ΓΕΡΗΕΤ είναι αρμόδιο για το συντονισμό των θεμάτων της ασφάλειας δικτύων ηλεκτρονικών επικοινωνιών και πληροφοριών. Στο πλαίσιο της ευθύνης του είναι και ο συντονισμός ενεργειών των αρμοδίων φορέων για τη δημιουργία σχεδίου άμεσης ανταπόκρισης για συμβάντα που σχετίζονται με την Ασφάλεια Δικτύων και Πληροφοριών (CSIRTs - Computer Security Incident Response Teams ή CERTs - Computer Emergency Response Teams), στην Κύπρο. Επιπλέον, έχει την ευθύνη για το πλαίσιο παραλαβής και κοινοποίησης παραβιάσεων ασφάλειας στα δίκτυα και συνεργάζεται όπου απαιτείται, τόσο σε εθνικό αλλά σε και ευρωπαϊκό επίπεδο, με φορείς των άλλων κρατών μελών, με τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) καθώς και την Ευρωπαϊκή Επιτροπή. Επίσης συμβουλεύει τον Υπουργό Συγκοινωνιών για θέματα στρατηγικής στον τομέα της ασφάλειας δικτύων και πληροφοριών, συμπεριλαμβανομένης της προστασίας Κρίσιμων Υποδομών Πληροφοριών και συντονίζει τις δράσεις για την εφαρμογή της σχετικής πολιτικής του κράτους. Τέλος ενημερώνει όλα τα ενδιαφερόμενα μέρη αλλά και το κοινό σε θέματα ασφάλειας. Όσον αφορά τη συνεργασία μεταξύ κράτους και ιδιωτικού Τομέα αν και υπάρχει ενθάρρυνση από το ΓΕΡΗΕΤ, αυτή βρίσκεται ακόμα σε πρώιμο στάδιο και εστιάζεται κυρίως στην ανταλλαγή πληροφοριών. Ωστόσο, το

έργο CyberEthics που άρχισε την 1η Σεπτεμβρίου 2006 με σκοπό να λειτουργήσει ως κόμβος ευαισθητοποίησης στην Κύπρο προέκυψε από μια εταιρική σχέση μεταξύ των δημοσίων φορέων, του Τύπου, ομάδων των μέσων ενημέρωσης και των ενώσεων ISP. Επίσης το τμήματος της αστυνομίας για το έγκλημα στον κυβερνοχώρο συνεργάζεται με ιδιωτικές εταιρείες, όπως η Microsoft για τη διεξαγωγή των ερευνών.

15.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Τα τελευταία χρόνια έχουνε πραγματοποιηθεί διάφορες δράσεις για ενημέρωση, εκπαίδευση και προστασία των πολιτών και των φορέων, μια εκ των οποίων είναι και ο δικτυακός τόπος CyberEthics [368] που είναι μέλος του ευρωπαϊκού προγράμματος Insafe. Έχουν γίνει παρουσιάσεις σε σχολεία και άλλα δημόσια φόρουμ τις οποίες έχουν παρακολουθήσει πάνω από 15.532 φοιτητές, 1.705 εκπαιδευτικοί και πάνω από 2.276 γονείς μεταξύ 2008-2010. Εκπρόσωποι του CyberEthics κλήθηκαν σε περισσότερες από 48 τηλεοπτικές και 25 ραδιοφωνικές εκπομπές, ενώ άρθρα σε εφημερίδας και περιοδικά προωθούν το έργο του. Μέσω του κέντρου παρέχεται τηλεφωνική γραμμή ως ένα σημείο επικοινωνίας για τους χρήστες που επιθυμούν την ποινική δίωξη και την αφαίρεση του παράνομου περιεχομένου από το Διαδίκτυο. Επιπλέον, για την παροχή πληροφοριών και οδηγιών προς τους γονείς σχετικά με το Διαδίκτυο και την ασφαλή χρήση του, ο πάροχος Cytanet προσφέρει το εκπαιδευτικό πρόγραμμα «Το Διαδίκτυο και τα παιδιά μας - Ασφαλής και υπεύθυνη χρήση» σε συνεργασία με τους συλλόγους γονέων. Στο ευρύτερο πλαίσιο των προσπαθειών της η Cytanet κάνει επίσης παρουσιάσεις σχετικά με την ασφαλή χρήση του Διαδικτύου για άλλες οργανωμένες ομάδες, δήμους, κλπ. Παίρνει επίσης μέρος σε συζητήσεις μέσα ενημέρωσης σχετικά με θέματα ασφάλειας στο Διαδίκτυο και συμμετέχει σε άλλα συναφή έργα και προγράμματα. Η Cytanet παρέχει επίσης σεμινάρια για τους μαθητές, τους εκπαιδευτικούς και τα μέσα ενημέρωσης και συμμετέχει σε σεμινάρια που οργανώνονται από την Αστυνομία, το κράτος, την Εκκλησία και άλλους φορείς. Κάθε χρόνο, σε συνεργασία με άλλους φορείς, η Cytanet διοργανώνει μια ειδική εκδήλωση για τον εορτασμό της «Ημέρας Ασφαλέστερου Διαδίκτυου». Επίσης η Κυπριακή αστυνομία έχει τη δική της ιστοσελίδα όπου παρέχει συμβουλές σχετικά με την πρόληψη της διαδικτυακής απάτης. Η εθνική αρχή προστασίας δεδομένων της Κύπρου έχει εκδώσει κατευθυντήριες οδηγίες για το κοινό σχετικά με την προστασία από το

spam ενώ κάθε χρόνο πραγματοποιείται το Κυπριακό συνέδριο Infosec που έχει ως στόχους την προώθηση και την ευαισθητοποίηση των επιχειρήσεων και γενικότερα των επαγγελματιών της πληροφορικής στις πλέον πρόσφατες εξελίξεις στον τομέα της ασφάλειας των πληροφοριών. [369]

15.5 Διεθνής Συνεργασία

Η Κυπριακή Δημοκρατία, μέσω των δραστηριοτήτων του ΓΕΡΗΕΤ αλλά και άλλων αρμόδιων αρχών, ήδη εκπροσωπείται σε μεγάλο βαθμό στις πλείστες σχετικές ομάδες εργασίας και διεθνή φόρα τα οποία λειτουργούν κάτω από την επίβλεψη της Ευρωπαϊκής Επιτροπής και του ENISA. Στόχοι της Κυπριακής Δημοκρατίας είναι να δημιουργηθούν στενοί δεσμοί με τους αντίστοιχους αρμόδιους φορείς σε άλλα κράτη μέλη της Ευρωπαϊκής Ένωσης με σκοπό την διαρκή ανάπτυξη και βελτίωση της στρατηγικής στα θέματα ηλεκτρονικής ασφάλειας. Τέλος η Κύπρος είναι μέλος της συμμαχίας κατά του κυβερνοεγκλήματος IMPACT [33].

Κεφάλαιο 16ο

Λετονία

16.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Λετονία έχει εκδώσει μια σειρά από στρατηγικές που αφορούν την ανάπτυξη της πληροφορικής, των τηλεπικοινωνιών, της ηλεκτρονικής διακυβέρνησης και της κοινωνίας της πληροφορίας όπως το Εθνικό Σχέδιο Ανάπτυξης 2007-2013, το Σχέδιο Ανάπτυξης της Ηλ. Διακυβέρνησης (2011-2013) και η Πολιτική για την Κοινωνία της Πληροφορίας (2006-2013) [370] χωρίς όμως να έχει εκδώσει ακόμη Εθνική Στρατηγική για την Κυβερνοασφάλεια. Ωστόσο, ο Νόμος για την ασφάλεια της Πληροφορικής ψηφίστηκε με σκοπό να προσδιορίσει τις πιο σημαντικές απαιτήσεις, προκειμένου να διασφαλιστεί η λειτουργία των εν λόγω τεχνολογιών [371]. Ο νόμος ορίζει ότι η κρίσιμη υποδομή των τεχνολογιών της πληροφορικής θα πρέπει να υποστηριχθεί προκειμένου να παρέχει λειτουργίες ουσιώδους σημασίας για το κράτος και την κοινωνία. Επιπλέον, θα πρέπει να εξασφαλίζεται η ακεραιότητα, η διαθεσιμότητα και η εμπιστευτικότητα αυτών των υποδομών. Οι διαδικασίες για το σχεδιασμό και την εφαρμογή των μέτρων ασφαλείας καθορίζονται από το Υπουργικό Συμβούλιο. Επίσης ορίζει ότι η Ομάδα Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας θα προωθεί την ασφάλεια της πληροφορικής στη Δημοκρατία της Λετονίας. Οι κυβερνητικοί φορείς και τα νομικά πρόσωπα ιδιωτικού δικαίου έχουν την υποχρέωση να συνεργάζονται με την Ομάδα, παρέχοντας την απαραίτητη πληροφόρηση και εφαρμόζοντας τα νόμιμα αιτήματά της. Τέλος ο νόμος προβλέπει τη συγκρότηση Εθνικού Συμβούλιου για την Ασφάλεια της πληροφορικής.

16.2 Νομοθετικό Πλαίσιο

Νόμος για την ασφάλεια της Πληροφορικής [372]

Ο νόμος εγκρίθηκε από το Κοινοβούλιο στις 28 Οκτωβρίου 2010, τέθηκε σε ισχύ την 1η Φεβρουαρίου 2011 και αποσκοπεί στη βελτίωση της ασφάλειας της πληροφορικής, καθορίζοντας τις βασικές απαιτήσεις για τους οργανισμούς ώστε να διασφαλίσει την ασφάλεια των ηλεκτρονικών υπηρεσιών.

Νόμος για τα κρατικά Πληροφοριακά Συστήματα [372]

Εγκρίθηκε τον Μάιο του 2002 και με τις τροποποιήσεις της 1η Ιανουαρίου 2011, ο εν λόγω νόμος έχει ως στόχο την εξασφάλιση της διαθεσιμότητας και της ποιότητας των υπηρεσιών πληροφοριών που παρέχονται από το κράτος και την τοπική αυτοδιοίκηση.

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [372]

Ο νόμος περί προστασίας προσωπικών δεδομένων εγκρίθηκε από το Κοινοβούλιο στις 23 Μαρτίου 2000 και, τροποποιήθηκε το 2009. Είναι πλήρως συμβατός με την οδηγία για την προστασία των δεδομένων της ΕΕ (95/46/ΕΚ). Σκοπός του παρόντος νόμου είναι η προστασία των θεμελιωδών ανθρωπίνων δικαιωμάτων και ελευθεριών των φυσικών προσώπων, ιδίως το απαραβίαστο της ιδιωτικής ζωής όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Η Εφαρμογή του Νόμου εποπτεύεται από την Επιθεώρηση Δεδομένων, η οποία είναι επίσης υπεύθυνη και για την εποπτεία του spam.

Νομοθεσία ηλεκτρονικού εμπορίου [372]

Ο Νόμος για τις Ηλεκτρονικές Επικοινωνίες τέθηκε σε ισχύ την 1η Δεκεμβρίου 2004, και τροποποιήθηκε στις 19 Μαΐου 2011. Στόχος του είναι να προωθήσει και να ρυθμίσει την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών, μεταφέροντας το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες. Ο νόμος προβλέπει τις μορφές των διαφόρων ηλεκτρονικών δικτύων, συμπεριλαμβανομένων των δημόσιων και ιδιωτικών ηλεκτρονικών δικτύων. Επιπλέον, προβλέπει τα δικαιώματα και τις υποχρεώσεις των παρόχων, των συνδρομητών και των χρηστών των ηλεκτρονικών δικτύων.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Η Λετονία ενέκρινε το ισχύον Ποινικό Δίκαιο [373] στις 17 Ιουνίου του 1998. Τα άρθρα που σχετίζονται με το έγκλημα στον κυβερνοχώρο είναι:

Άρθρο 241: Αυθαίρετη Πρόσβαση σε Συστήματα Υπολογιστών.

Άρθρο 242: Μη εξουσιοδοτημένη απόκτηση λογισμικού υπολογιστών.

Άρθρο 243: Ζημίωση λογισμικού υπολογιστών.

Άρθρο 244: Διάδοση ενός ιού υπολογιστών.

Άρθρο 245: Παραβίαση των διατάξεων Ασφάλειας των Πληροφοριακών Συστημάτων.

16.3 Αρχές και Οργανισμοί [374]

Δημόσιοι φορείς

Το Υπουργείο Μεταφορών και Επικοινωνιών [375] είναι το υπουργείο με αρμοδιότητα τα θέματα ασφάλειας πληροφορικής και τηλεπικοινωνιών στη Λετονία. Στις αρμοδιότητές του είναι η εκπόνηση των πολιτικών και ο συντονισμός της εφαρμογή τους. Το Εθνικό Συμβούλιο Ασφαλείας Πληροφορικής υπάγεται στο υπουργείο Μεταφορών και Επικοινωνιών και σκοπός λειτουργίας του είναι να συντονίζει τον προγραμματισμό και την εκτέλεση των ενεργειών που σχετίζονται με τις τεχνολογίες της ασφάλειας πληροφοριών [376]. Το Υπουργείο Άμυνας απαίτησε στενότερη συνεργασία με τον ιδιωτικό τομέα στην ανάπτυξη μιας ειδικής μονάδας εμπειρογνωμόνων της πληροφορικής η οποία σε μελλοντική κρίση ασφάλειας ή κατάστασης απειλής σε συνεργασία με τη CERT θα μπορεί να στηρίξει τον δημόσιο και τον ιδιωτικό τομέα [377] με αποτέλεσμα την ίδρυση στις 30 Ιουλίου 2013 της Μονάδας Κυβερνοάμυνας [378]. Η μονάδα έχει σχεδιαστεί σύμφωνα με τους νόμους που διέπουν την Εθνική Φρουρά. Η Κρατική Επιθεώρηση Δεδομένων [379] ελέγχει και εποπτεύει την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε επίπεδο πολιτείας σύμφωνα με τις απαιτήσεις του νόμου Προστασίας Προσωπικών Δεδομένων.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας

Η CERT.LV [380] είναι η εθνική ομάδα της Λετονίας και αποστολή της είναι η προώθηση της ασφάλειας της Πληροφορικής. Μέχρι την 31η, Δεκεμβρίου του 2012 λειτουργούσε κάτω από το Υπουργείο Μεταφορών. αλλά τώρα λειτουργεί στο πλαίσιο του Υπουργείου Άμυνας και ρυθμίζεται από το νόμο Ασφάλειας Πληροφορικής. Κύρια καθήκοντα της είναι η διατήρηση και ενημέρωση των πληροφοριών σχετικά με τις απειλές στον κυβερνοχώρο, η παροχή στήριξης σε περίπτωση έκτακτου περιστατικού ασφάλειας, η παροχή συμβουλών σε κυβερνητικούς θεσμούς και η οργάνωση ενημερωτικών και εκπαιδευτικών δραστηριοτήτων για τους κυβερνητικούς υπαλλήλους, τους επαγγελματίες της ασφάλειας και το ευρύ κοινό.

Ιδιωτικοί φορείς

Η Λετονική Ένωση Τεχνολογιών Πληροφορίας και Επικοινωνίας (LIKTA) [381] είναι ένας επαγγελματικός σύλλογος που συγκεντρώνει πάνω από 85 σημαντικούς παρόχους προϊόντων και υπηρεσιών πληροφορικής και τηλεπικοινωνιών. Η LIKTA παρέχει επαγγελματική εκπαίδευση και συμμετέχει σε έργα εθνικής σημασίας και σε διεθνείς δραστηριότητες.

Ο Λετονικός Οργανισμός για το Internet (LIA) [382] είναι ένας οργανισμός αποτελούμενος από τις εταιρείες που δραστηριοποιούνται σε διάφορες υπηρεσίες

διαδικτύου. Η Ομάδα Εμπειρογνωμόνων της Πληροφορικής και των Συστημάτων Ασφαλείας (DEG) αποτελείται από εμπειρογνώμονες σε θέματα ασφάλειας από διάφορες οργανώσεις. Η ομάδα συνεδριάζει μηνιαίως και βασικοί της στόχοι είναι η ενίσχυση του επιπέδου ασφάλειας της πληροφορικής στη Δημοκρατία της Λετονίας, η διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ των μελών της ομάδας, η εκπαίδευση του ευρέως κοινού σε θέματα ασφάλειας και η υποστήριξη της CERT.LV.

Συνεργασία μεταξύ φορέων

Σύμφωνα με τον νόμο για την ασφάλεια της Πληροφορικής, οι κρατικοί φορείς και τα νομικά πρόσωπα ιδιωτικού δικαίου έχουν την υποχρέωση να συνεργάζονται με τη CERT.LV παρέχοντας την απαραίτητη πληροφόρηση και εφαρμόζοντας. Σε περίπτωση κινδύνου για το κράτος, το Υπουργικό Συμβούλιο μπορεί να λάβει απόφαση για τη μεταβίβαση των καθηκόντων, των δικαιωμάτων και των πόρων στις Εθνικές Ένοπλες Δυνάμεις. Η CERT.LV παρέχει υποστήριξη και συντονισμό για την πρόληψη των περιστατικών ασφαλείας. Στο πλαίσιο αυτό διατηρεί στην ιστοσελίδα του συστάσεις σχετικά με την πρόληψη των κινδύνων, επιβλέπει τους κρατικούς και ιδιωτικούς φορείς των ηλεκτρονικών επικοινωνιών ως προς την εκπλήρωση των καθηκόντων τους και συνεργάζεται με τους διεθνείς εταίρους. Σε περίπτωση περιστατικού ασφάλειας σε κρατικό φορέα ή νόμιμο κάτοχο υποδομής ζωτικής σημασίας θα πρέπει να ενημερώνεται άμεσα η CERT.LV ώστε η ομάδα να παρέχει την απαραίτητη υποστήριξη. Στη συνέχεια εάν ανιχνεύσει ότι το συμβάν ασφαλείας, θέτει σε κίνδυνο την εθνική ασφάλεια, ενημερώνει τον Υπουργό Μεταφορών, τον αρμόδιο υπουργό για τον τομέα και τον αρμόδιο φορέα ασφάλειας του κράτους. Επίσης υποβάλλει προτάσεις για τις αναγκαίες ενέργειες, και εφόσον κριθεί απαραίτητο, ενημερώνονται τα θεσμικά όργανα της Ευρωπαϊκής Ένωσης.[383]

16.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Το Net-Safe Latvia [384] είναι το Κέντρο Safer Internet που δημιουργήθηκε για να εκπαιδεύσει το κοινό στην ασφαλή χρήση του διαδικτύου και λειτουργεί από τον Λετονικό Οργανισμό για το Internet. Το πρόγραμμα συγχρηματοδοτείται από το πρόγραμμα Safer Internet της Ευρωπαϊκής Επιτροπής. Δραστηριότητες του Κέντρου Ασφαλούς Διαδικτύου είναι το εκπαιδευτικό έργο, μέσω του οποίου τα παιδιά, οι νέοι, οι εκπαιδευτικοί και οι γονείς ενημερώνονται και εκπαιδεύονται για την ασφάλεια του

περιεχομένου στο διαδίκτυο, τους πιθανούς κινδύνους και τις απειλές στο διαδίκτυο. Μέσω τηλεφωνικής γραμμής δίνεται η δυνατότητα στα παιδιά και στους νέους να αναφέρουν παραβιάσεις στο Διαδίκτυο. Το 2010 υπεγράφη συμφωνία συνεργασίας μεταξύ του εθνικού Κέντρου Ασφαλούς Διαδικτύου και της Αστυνομίας για την επεξεργασία των εκθέσεων σχετικά με το παράνομο περιεχόμενο και τις δραστηριότητες του διαδικτύου. Επιπλέον, το Κέντρο αναπτύσσει εκπαιδευτικό υλικό και σημειώσεις, παρουσιάσεις και εγχειρίδια για τους καθηγητές που θα χρησιμοποιηθούν ως εργαλεία για την εκπαίδευση σε θέματα ασφάλειας στο διαδίκτυο σε τακτική βάση [385]. Η ιστοσελίδα www.esidross.lv λειτουργεί από τη CERT.LV και προορίζεται για όποιον ενδιαφέρεται για την ασφάλεια του υπολογιστή και του διαδικτύου. Εμπειρογνώμονες από την ομάδα DEG παρέχουν επίσης συμβουλές, και απαντούν σε σχετικές ερωτήσεις [386]. Τέλος, η άσκηση CERT.LV Technical IT Security διοργανώθηκε το 2011σε εθνικό επίπεδο [28].

16.5 Διεθνής Συνεργασία

Η Λετονία μέσω του Υπουργείου Μεταφορών συνεργάζεται με τον Ευρωπαϊκό οργανισμό ENISA, σε θέματα ασφάλειας πληροφορικής. Τόσο το 2010 όσο και το 2012 συμμετείχε στην άσκηση Cyber Europe με ομάδες που αντιπροσώπευαν τη CERT.LV, την επιτροπή Χρηματοοικονομικών Υπηρεσιών και Κεφαλαιαγοράς, τη Λετονική κρατική ραδιοφωνία και τηλεόραση, το Υπουργείο Μεταφορών και τις εταιρείες SEB, Swedbank, Telia [387][388]. Η Λετονία είναι από τα ιδρυτικά κράτη μέλη του CCD COE,στο οποίο συμμετέχει από το 2008.[130]. Επίσης συμμετέχει στις Νατοϊκές ασκήσεις Cyber Coalition και Locked Shields μέσω της CERT.LV [388][389][390]. Τέλος η CERT.LV είναι μέλος του διεθνούς φόρουμ FIRST [32] και του TF-CSIRT[391].

Κεφάλαιο 17ο

Λιθουανία

17.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Κυβέρνηση της Λιθουανίας ψήφησε τον Ιούνιο του 2011 το Πρόγραμμα για την Ανάπτυξη της ασφάλειας των ηλεκτρονικών πληροφοριών (cyber-security) για το 2011-2019.[392] Ο σκοπός του προγράμματος είναι να καθορίσει τους στόχους προκειμένου να διασφαλιστεί η εμπιστευτικότητα, η ακεραιότητα και η προσβασιμότητα των ηλεκτρονικών πληροφοριών και των υπηρεσιών που παρέχονται στον κυβερνοχώρο. Επίσης το πρόγραμμα στοχεύει στην προστασία των δικτύων ηλεκτρονικών επικοινωνιών και των πληροφοριακών συστημάτων των υποδομών ζωτικής σημασίας από επεισόδια και επιθέσεις στον κυβερνοχώρο καθώς και στην προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωή. Τέλος ορίζει τα μέτρα η εφαρμογή των οποίων θα επιτρέπει την πλήρη ασφάλεια του κυβερνοχώρου και των φορέων που δραστηριοποιούνται σε αυτόν. Η ασφάλεια στον κυβερνοχώρο των κατοίκων της Λιθουανίας. Προκειμένου να επιτευχθούν οι στόχοι το πρόγραμμα προβλέπει:

- Τη βελτίωση του συντονισμού και της εποπτείας της ασφάλειας στον κυβερνοχώρο.
- Τη βελτίωση του κανονιστικού πλαισίου ασφάλειας στον κυβερνοχώρο.
- Την επέκταση και βελτίωση μιας ασφαλούς εθνικής υποδομής πληροφοριών.
- Την προώθηση των εφαρμογών ασφάλειας.
- Την ανάπτυξη της διεθνούς συνεργασίας.
- Την ενίσχυση της κουλτούρας της ασφάλειας πληροφοριών.

17.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [393]

Ο νόμος για την προστασία των δεδομένων προσωπικού χαρακτήρα εκδόθηκε στις 11 Ιουνίου 1996 και τροποποιήθηκε 1η Ιανουαρίου 2009. Ο κύριος σκοπός του είναι η προστασία της ιδιωτικής ζωής όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Ο νόμος είναι πλήρως συμβατός με την οδηγία της ΕΕ (95/46/ΕΚ).για την προστασία των δεδομένων.

Νομοθεσία ηλεκτρονικού εμπορίου [393]

Νόμος σχετικά με τις υπηρεσίες της κοινωνίας της πληροφορίας (2006)

Ο νόμος εγκρίθηκε τον Μάιο του 2006 προκειμένου να εξασφαλιστεί η εφαρμογή της κοινοτικής οδηγίας 2000/31/ΕΚ για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως για το ηλεκτρονικό εμπόριο στην εσωτερική αγορά. Ο κύριος σκοπός είναι να δημιουργηθεί ένα νομικό πλαίσιο για τη ρύθμιση της παροχής υπηρεσιών της κοινωνίας της πληροφορίας. Ο νόμος καθορίζει τις απαιτήσεις για τις πληροφορίες που παρέχονται για τη σύναψη συμφωνιών με ηλεκτρονικά μέσα, ρυθμίζει τις αρμοδιότητες, τα δικαιώματα τις υποχρεώσεις και τις δραστηριότητες των παρόχων υπηρεσιών και, επιπλέον, καθορίζει τα μέσα επίλυσης των διαφορών.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [393]

Ο νόμος ψηφίστηκε το 2004 και τροποποιήθηκε για το Μάρτιο του 2009 και ρυθμίζει τις υπηρεσίες ηλεκτρονικών επικοινωνιών και δικτύων, τη χρήση των πόρων ηλεκτρονικών επικοινωνιών (συμπεριλαμβανομένου του ραδιοφώνου και του τερματικού εξοπλισμού) και την ηλεκτρομαγνητική συμβατότητα. Ο νόμος μεταφέρει το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [394]:

Η Λιθουανία επικύρωσε τη σύμβαση του Συμβουλίου της Ευρώπης για το κυβερνοέγκλημα στις 22 Ιανουαρίου 2004. Τα ειδικά άρθρα στον Ποινικό Κώδικα σχετικά με το έγκλημα στον κυβερνοχώρο είναι:

Άρθρο 196 Καταστροφή ή παρεμβολή ηλεκτρονικών δεδομένων.

Άρθρο 197 Καταστροφή ή παρεμβολή προγράμματος ηλεκτρονικού υπολογιστή.

Άρθρο 198 Υποκλοπή και διανομή ηλεκτρονικών δεδομένων.

17.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Υπουργείο Μεταφορών και Επικοινωνιών [395] είναι υπεύθυνο για την ανάπτυξη και την εφαρμογή των προτύπων και των πολιτικών ασφάλειας πληροφορικής.

Η Δημόσια επιχείρηση Infostruktūra [396] ιδρύθηκε το 1992 για την υλοποίηση του στρατηγικού προγράμματος δημιουργίας υποδομών πληροφορίων. και υπάγεται στο Υπουργείο Εσωτερικών. Ο κύριος στόχος της είναι η ανάπτυξη μιας ασφαλής υποδομής τηλεματικών υπηρεσιών για να επικοινωνούν τα υπουργεία μεταξύ τους και με τα θεσμικά όργανα της ΕΕ. Η επιχείρηση παρέχει μια σειρά από υπηρεσίες ασφαλείας όπως το σύστημα SSDCN. Με τη χρήση αυτής της υπηρεσίας, παρέχεται προστασία κατά της διείσδυσης στα δημόσια δίκτυα, της κλοπής δεδομένων και από επιθέσεις στον κυβερνοχώρο. Το SSDCN προσφέρεται για τις κυβερνητικές και τοπικές υπηρεσίες καθώς και για τις εταιρείες και τα άλλα νομικά πρόσωπα που ασκούν δημόσια καθήκοντα. Η Ρυθμιστική Αρχή Επικοινωνιών (RRT) [397] είναι ένας Ανεξάρτητος Οργανισμός στον τομέα των εθνικών επικοινωνιών, που έχει συσταθεί βάσει του νόμου περί τηλεπικοινωνιών. Έχει ως στόχο να εξασφαλίσει για τη Λιθουανία τεχνολογικά προηγμένες, υψηλής ποιότητας, ασφαλείς και οικονομικά προσιτές ΤΠΕ. Η αρχή είναι υπεύθυνη για τη λειτουργία του λιθουανικού εθνικού CERT, του προγράμματος Safer Internet καθώς και άλλων δράσεων που στοχεύουν στην ασφάλεια του κυβερνοχώρου. Επίσης είναι ο κύριος σύνδεσμος της Λιθουανίας με τον ευρωπαϊκό οργανισμό ENISA. Η Επιθεώρηση Προστασίας Δεδομένων [398] είναι υπεύθυνη για την εποπτεία και τον έλεγχο της εφαρμογής του νόμου περί Προστασίας Προσωπικών Δεδομένων. Η Λιθουανική Αστυνομία μέσω του Τμήμα Έρευνας Κυβερνοεγκλήματος [399] έρευνά τα περιστατικά εγκληματικότητας στον κυβερνοχώρο.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CERT-LT [400][401] είναι η εθνική ομάδα της Λιθουανίας. Η αποστολή της είναι να προωθήσει την ασφάλεια στην κοινωνία της πληροφορίας, με την πρόληψη, την παρατήρηση και την επίλυση των περιστατικών ασφάλειας και τη διάδοση πληροφοριών σχετικά με τις απειλές. Καθήκοντά της είναι η διερεύνηση των περιστατικών ασφάλειας δικτύων και πληροφοριών στα λιθουανικά ηλεκτρονικά δίκτια, ο συντονισμός των δράσεων των φορέων παροχής υπηρεσιών Διαδικτύου και τηλεπικοινωνιακών δικτύων και των υπόλοιπων ομάδων CER. Επίσης η διερεύνα για τρωτά σημεία των δικτύων και των πληροφοριακών συστημάτων για την πρόληψη περιστατικών ασφάλειας δικτύων και πληροφοριών. Επιπλέον στοχεύει στην

προώθηση της δημιουργίας νέων ομάδων CERT. Η SVDPT-CERT [402] είναι η κυβερνητική CERT και ανταποκρίνεται σε περιστατικά ασφάλειας των θεσμικών οργάνων του λιθουανικού κράτους και των τοπικών διοικήσεων.

Η LTU MOD CIRT ανήκει στο Υπουργείο Άμυνας και η LITNET CERT [403] είναι η ομάδα του Λιθουανικού δικτύου Πανεπιστημίων και εκπαιδευτικών ιδρυμάτων.

Ιδιωτικοί φορείς

Η Infobalt [404] είναι μια ένωση επιχειρήσεων με αποστολή την προώθηση της χρήσης των Τεχνολογιών Πληροφορίας και Επικοινωνιών προς όφελος της κοινωνίας, των επιχειρήσεων και του δημόσιου τομέα. Η Ένωση έχει περισσότερα από 130 μέλη, συμπεριλαμβανομένων των εθνικών επιχειρήσεων, πανεπιστήμιων και τα κολλεγίων που εμπλέκονται στην εκπαίδευση των ΤΠΕ, καθώς και ερευνητικά ιδρύματα, απασχολώντας περισσότερους από 10.000 έμπειρους επαγγελματίες των ΤΠΕ.

Ακαδημαϊκοί φορείς

Η LITNET είναι μια ένωση των ακαδημαϊκών, ερευνητικών και άλλων μη κερδοσκοπικών οργανώσεων. Τα μέλη της διαχειρίζονται και αναπτύσσουν το ερευνητικό δίκτυο LITNET και λειτουργούν την ομάδα LITNET CERT.

17.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Η ιστοσελίδα www.draugiskasinternetas.lt αποτελεί το επίσημο πρόγραμμα Safer Internet της Λιθουανίας. Ο στόχος του έργου που συγχρηματοδοτείται από την Ε.Ε είναι να επιστήσει την προσοχή του κοινού σε παράνομες και βλαβερές πληροφορίες του Διαδικτύου και να προωθήσει την ασφαλέστερη χρήση του405]. Στο κέντρο λειτουργεί τηλεφωνική γραμμή επικοινωνίας υπο την ευθύνη της Ρυθμιστικής Αρχής Επικοινωνιών, στην οποία μπορεί να αναφερθεί το επιβλαβές περιεχόμενο. Επίσης διοργανώνει εκστρατείες ευαισθητοποίησης σχετικά με τη διαδικτυακή ασφάλεια [406]. Από το 2012 όλοι οι χρήστες των ηλεκτρονικών υπηρεσιών μπορούν να επισκεφθούν την εξειδικευμένη ιστοσελίδα www.esaugumas.lt της Ρυθμιστικής Αρχής Επικοινωνιών (RRT), η οποία παρέχει αναλυτικές πληροφορίες σχετικά με την ασφάλεια στον κυβερνοχώρο. Σε αυτή την ιστοσελίδα υπάρχουν πληροφορίες για τα πιο κοινά προβλήματα του διαδικτύου όπως οι ιοί ηλεκτρονικών υπολογιστών και κινητών συσκευών, τα ανεπιθύμητα e-mail, τεχνικές απάτης και άλλες πιθανές απειλές. Παρέχεται επίσης καθοδήγηση και συμβουλές για το πώς να αποφευχθεί το ενδεχόμενο

επεισοδίων. Επιπλέον υπάρχει ένα ειδικό τμήμα για τους χρήστες e-banking το οποίο περιλαμβάνει την παροχή βασικών κανόνων σε αυτές τις υπηρεσίες και συμβουλές για το πώς να επιλέγονται οι κωδικοί πρόσβασης. Οι χρήστες μπορούν να θέτουν ερωτήσεις σχετικά με την ασφάλεια του κυβερνοχώρου, οι οποίες απαντούνται από επαγγελματίες της RRT [407].

17.5 Διεθνής Συνεργασία

Η Λιθουανία συνεργάζεται με τους θεσμούς της Ε.Ε. και με τον οργανισμό ENISA μέσω της Ρυθμιστικής Αρχή Επικοινωνιών [408]. Επίσης συμμετέχει στην ευρωπαϊκή άσκηση κυβερνοάμυνας Cyber Europe [28]. Η Λιθουανία είναι μέλος του NATO και συμμετέχει ενεργά ως ιδρυτικό μέλος στο CCDCOE [130]. Έχει συμμετάσχει στις ασκήσεις του CCD COE Baltic Shield και Cyber Shield καθώς και στην Ναtοϊκή άσκηση Cyber Coalition [409]. Επίσης είναι μέλος του IMPACT [33]. Όσον αφορά τις συνεργασίες των CERT οι LITNET CERT, LTU MOD CIRT, και CERT-LT είναι μέλη του διεθνούς φόρουμ FIRST και του TI [32][401]. Η LITNET CERT είναι επίσης μέλος του δικτύου Ceenet [79].

Κεφάλαιο 18ο

Λουξεμβούργο

18.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Στις 23 του Νοεμβρίου του 2011 κατά τη διάρκεια ενός συνεδρίου που πραγματοποιήθηκε στο Λουξεμβούργο με θέμα την Κυβερνοασφάλεια [410] ανακοινώθηκε από το Υπουργείο Δικαιοσύνης η Εθνική Στρατηγική Κυβερνοασφάλειας [411]. Αυτό το έγγραφο καθορίζει τις γραμμές δράσης για την ενίσχυση της ασφάλειας και της ανθεκτικότητας των υποδομών και έτσι συμβάλλει στην προστασία των πολιτών των επαγγελματιών και των συμμετεχόντων στη δημόσια ζωή, στο ψηφιακό περιβάλλον. Για την επίτευξη των παραπάνω η Στρατηγική ορίζει πέντε πυλώνες.

1. Τη διασφάλιση τη λειτουργικότητας της υποδομής των συστημάτων επικοινωνίας και επεξεργασίας πληροφοριών. Τα επιχειρησιακά μέτρα που αποσκοπούν στην επίτευξη αυτού του στόχου είναι η καθιέρωση Σχέδιου Έκτακτης Ανάγκης, η εκτέλεση ασκήσεων σχετικά με την ανταπόκριση σε περιστατικά που αφορούν την ασφάλεια των πληροφοριακών συστημάτων και ευαίσθητες ή κρίσιμες επικοινωνίες, η συμμετοχή σε ευρωπαϊκές ασκήσεις, και η σύσταση εξειδικευμένων CERT ικανών να αναλάβουν τα περιστατικά ασφάλειας.
2. Ο εκσυγχρονισμός του νομικού πλαισίου έτσι ώστε να ανταποκρίνεται στις μεταβολές της τεχνολογίας και στο διεθνοποιημένο περιβάλλον του κυβερνοχώρου.
3. Η ανάπτυξη της εθνικής και διεθνούς συνεργασίας. Σε εθνικό επίπεδο, η αποτελεσματική συνεργασία μεταξύ όλων των φορέων καθορίζεται ως προϋπόθεση για την εφαρμογή της στρατηγικής. Σε διεθνές επίπεδο, η συνεργασία μπορεί να βασίζεται σε πολυμερείς σχέσεις με τις χώρες της BENELUX, την Interpol και την Europol, την Ε.Ε., το Συμβούλιο της Ευρώπης, το ΝΑΤΟ, τον ΟΟΣΑ και τον ΟΑΣΕ.
4. Ενημέρωση, εκπαίδευση και ευαισθητοποίηση σχετικά με τους κινδύνους σε όλα τα ενδιαφερόμενα μέρη, δηλαδή τελικούς χρήστες, μαθητές, γονείς, εκπαιδευτικούς, υπάλληλους του κράτους, μικρές και μεσαίες επιχειρήσεις, πάροχους υπηρεσιών και φορείς εκμετάλλευσης των υποδομών ζωτικής σημασίας.

5. Καθιέρωση προτύπων για τις μεθόδους ανάλυσης κινδύνου, πολιτικών και πρότυπων ασφαλείας.

18.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [412]

Ο νόμος για την προστασία των δεδομένων της 2ας Αυγούστου 2002, όπως τροποποιήθηκε από το νόμο της 27ης Ιουλίου 2007 αποτελεί την εφαρμογή της οδηγίας 95/46/ΕΚ σχετικά με την προστασία των προσωπικών δεδομένων προσωπικού χαρακτήρα στο Λουξεμβούργο.

Νομοθεσία ηλεκτρονικού εμπορίου[412]

Ο νόμος για το ηλεκτρονικό εμπόριο της 14ης Αυγούστου 2000 συμπληρωμένος με τον κανονισμό της 1ης Ιουνίου 2001 για τις ηλεκτρονικές υπογραφές και τις ηλεκτρονικές πληρωμές, μεταφέρει την οδηγία της ΕΕ για τις ηλεκτρονικές υπογραφές (1999/93/ΕΚ).

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [412]

Ο νόμος της 30ής Μαΐου 2005 μεταφέρει το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες (Οδηγίες 2002/19/ΕΚ, 2002/20/ΕΚ, 2002/21/ΕΚ, 2002/22/ΕΚ). Αποτελεί μέρος του νομοθετικού πακέτου των τηλεπικοινωνιών του Λουξεμβούργου, περιλαμβάνοντας επίσης έναν ειδικό νόμο για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών. Ο νόμος ρυθμίζει την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και τη διασύνδεσή τους με τη δημιουργία ενός βιώσιμου και ανταγωνιστικού περιβάλλοντος, καθώς και την εξασφάλιση της διαλειτουργικότητας των υπηρεσιών ηλεκτρονικών επικοινωνιών.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Ο Ποινικός Κώδικας του Λουξεμβούργου [37] περιέχει άρθρα που αναφέρονται σε εγκλήματα του κυβερνοχώρου. Συγκεκριμένα:

Άρθρο 509-1 Παράνομη προσπέλαση, Απάτη με Η/Υ, Πλαστογραφία με Η/Υ, Κακή χρήση ηλεκτρονικών συσκευών.

Άρθρο 509-2 Παράνομη υποκλοπή.

Άρθρο 509-3 Παρεμβολή σε δεδομένα, Παρεμβολή σε σύστημα.

18.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Η Ύπατη Αρμοστεία Εθνικής Προστασίας (HCPN) [413] είναι διυπηρεσιακή και πολιτικο-στρατιωτική επιτροπή διαβούλευσης, συντονισμού και σχεδιασμού των διαφόρων τομέων της εθνικής προστασίας. Η Εθνική Επιτροπή για τις υποδομές ζωτικής σημασίας (CONATIC) [414] απαρτίζεται από εκπροσώπους και εμπειρογνώμονες των υπουργείων και των οργανισμών που ασχολούνται με την προστασία των κρίσιμων υποδομών και καλύπτει το στόχο της κατάρτισης ενός καταλόγου του συνόλου των υποδομών ζωτικής σημασίας, καθώς και της αλληλεξάρτησης τους, ορίζει τις προτεραιότητες προστασίας, ελέγχει την καταλληλόλητα των σχεδίων και των διαδικασιών μέσω προσομοιώσεων και ασκήσεων. Η εθνική επιτροπή τηλεπικοινωνιών (CONATEL) [415] έχει ως στόχους την κατάρτιση ενός καταλόγου των υπηρεσιών δικτύων και τηλεπικοινωνιών και καθορίζει τις απαιτήσεις ασφάλειας. Επίσης οργανώνει, συντονίζει και να εκπονεί σχέδια για τη χρήση και την ταχεία επισκευή των τηλεπικοινωνιακών δικτύων και υπηρεσιών σε περίπτωση καταστροφής ή αδυναμίας λειτουργίας. Επίσης εξασφαλίζει ότι οι οδηγίες για την εκτέλεση των ανωτέρω σχεδίων διαβιβάζονται στις αρμόδιες αρχές για να λάβουν όλα τα αναγκαία μέτρα για την εκτέλεση των καθηκόντων τους. Επιπλέον η CONATEL διοργανώνει περιοδικές ασκήσεις και προτείνει αναγκαία μέτρα που. Το Κέντρο Επικοινωνιών [416] είναι διακομιστικό κέντρο της κυβέρνησης για τα δίκτυα που συνδέονται με το ΝΑΤΟ - ΕΕ - ΔΕΕ –ΟΑΣΕ, συμβουλεύει την κυβέρνηση στους τομείς των τηλεπικοινωνιών και της πληροφορικής για την ασφάλεια, βεβαιώνει τις αρχές ασφαλείας για τα συστήματα τηλεπικοινωνιών και πληροφορικής, λειτουργεί ως CA της επικοινωνιακής υποδομής της δημόσιας διοίκησης. Επίσης εκπροσωπεί το Λουξεμβούργο σε διεθνείς οργανισμούς στους τομείς των τηλεπικοινωνιών, της πληροφορικής και της ασφάλειας και παρέχει στην κυβέρνηση και τους βασικούς φορείς του κράτους τα μέσα τηλεπικοινωνιών και πληροφορικής. Το κέντρο προσφέρει συνεχή υπηρεσίας 24 ωρών για την κυβέρνηση ως Κέντρο αντιμετώπισης κρίσεων. Το Κρατικό Κέντρο Τεχνολογιών Πληροφορικής (CTIE) [417] είναι ένα τμήμα πληροφορικής της κυβέρνησης με κύρια καθήκοντά το σχεδιασμό των υπηρεσιών πληροφορικής της εθνικής κυβέρνησης, την ασφάλεια των δεδομένων της και την τυποποίηση των κυβερνητικών ιστοσελίδων. Η Εθνική Επιτροπή για την Προστασία

των Δεδομένων (CNPD) [418] είναι μια ανεξάρτητη αρχή υπεύθυνη για τον έλεγχο της νομιμότητας συλλογής αρχείων και για τις χρήσεις και τις διαβιβάσεις πληροφοριών. Σ' αυτό το πλαίσιο πρέπει να διασφαλίζει το σεβασμό των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων, ιδίως του δικαιώματος στην ιδιωτική ζωή. Η Αστυνομία του Λουξεμβούργου [419] αντιμετωπίζει τα εγκλήματα στον κυβερνοχώρο και μέσω του συμβουλίου πρόληψης εγκλήματος ενημερώνει τους πολίτες σχετικά με τους τρέχοντες κινδύνους και τα θέματα ασφαλείας του διαδικτύου. Ο οργανισμός Security Made In Luxembourg (SMILE) [420] έχει ως αποστολή να υποστηρίξει τις στρατηγικές ασφαλείας των πληροφοριακών και επικοινωνιακών συστημάτων μέσω των προγραμμάτων Cyberworld Awareness & Security Enhancement Services (CASES) και Computer Incident Response Center Luxembourg (CIRL) καθώς και του προγράμματος του Λουξεμβούργου για ασφαλές Internet» (BEE SECURE). Οι υπηρεσίες παρέχονται προς τους πολίτες, τις επιχειρήσεις και τους φορείς τις τοπικής αυτοδιοίκησης. Ο οργανισμός είναι μια κοινοπραξία από τρία υπουργεία (Υπουργείο Οικογένειας και Ένταξης, Υπουργείο Εθνικής Παιδείας και Επαγγελματικής Εκπαίδευσης, Υπουργείο Εθνικής Οικονομίας και Εξωτερικού Εμπορίου).

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η Computer Incident Response Center Luxembourg (CIRCL) [421][422] είναι η Εθνική Ομάδα και κέντρο συντονισμού για το Λουξεμβούργο και υπάγεται στον οργανισμό SMILE. Οι υπηρεσίες που διατίθενται είναι αναφορά συμβάντων ασφαλείας ταυτοποίηση περιστατικών, τεχνική έρευνα, ανάλυση malware, εκτίμηση τρωτότητας ασφάλειας, ανάλυση διαρροής πληροφοριών και εξόρυξη δεδομένων. Η GOVCERT.LU [423] είναι το σημείο επαφής για την αντιμετώπιση όλων των περιστατικών που σχετίζονται με τους κινδύνους των πληροφοριακών συστημάτων της κυβέρνησης και των υποδομών ζωτικής σημασίας. Η Malware.lu CERT [424] είναι η ομάδα CERT της εταιρείας παροχής προϊόντων και υπηρεσιών ασφάλειας πληροφορικής itrust. Η Restena-CSIRT [425] είναι η ομάδα του δικτύου υψηλής ταχύτητας για την εκπαιδευτική και ερευνητική κοινότητα του Λουξεμβούργου. Η CSRRT-LU [426] είναι μια εικονική ερευνητική ομάδα στον τομέα της ασφάλειας πληροφοριών.

Ιδιωτικοί φορείς

Η Κοινωνία του διαδικτύου του Λουξεμβούργου (ISOC) [427] είναι ένας μη-κερδοσκοπικός οργανισμός που δημιουργήθηκε για να συντονίζει και να παρακολουθεί

το διαδίκτυο στο Λουξεμβούργο. Στις δραστηριότητές του περιλαμβάνεται ένα φόρουμ για συζητήσεις σχετικά με την ασφάλεια, τους νόμους, την οικονομία, και την επικοινωνία στο διαδίκτυο. Η επαγγελματική ένωση της Ασφάλειας Πληροφοριών (APSI) [428] είναι μη κερδοσκοπική ένωση επαγγελματιών που εργάζονται στον τομέα της πληροφορικής και έχει ως στόχο να προωθήσει τη δημιουργία δημόσιων και ιδιωτικών πρωτοβουλιών στους τομείς της κοινωνίας της πληροφορίας. Η Ομοσπονδία Επιχειρήσεων του Λουξεμβούργου (Fedil) [429] είναι μια ομοσπονδία των εταιρειών που αντιπροσωπεύουν διάφορους τομείς της βιομηχανίας, των κατασκευών και των υπηρεσιών. Μία από τις πέντε ομάδες εργασίας αποτελούμενες από εμπειρογνώμονες των εταιρειών μελών εξετάζει και προετοιμάζει τις αποφάσεις που λαμβάνονται σχετικά με τα θέματα των Τεχνολογιών Πληροφορικής και Επικοινωνιών Η CLUSIL [430] είναι μια μη κερδοσκοπική ένωση εμπειρογνωμόνων στους τομείς της ασφάλειας της πληροφορικής. Συμβάλλει στην εκπαίδευση στην ασφάλεια της πληροφορικής τη βελτίωση και την ευαισθητοποίηση μέσω δημοσιεύσεων που προκύπτουν από την δραστηριότητα των ομάδων του έργου.

Ακαδημαϊκοί φορείς

Η μονάδα έρευνας LACS του Πανεπιστημίου του Λουξεμβούργου [431] αποτελεί μέρος της Ερευνητικής Μονάδας της Επιστήμης Υπολογιστών και Επικοινωνιών και ερευνά θέματα Κρυπτογραφίας, Υπολογιστικής Θεωρίας Αριθμών, Ασφάλειας Συστημάτων και Δικτύου, και Διαχείρισης Ασφάλειας Πληροφοριών. Το University of Luxembourg, Interdisciplinary Centre for Security, Reliability and Trust [432] είναι ένα εθνικό κέντρο αριστείας και καινοτομίας για ασφαλή, και αξιόπιστα συστήματα και υπηρεσίες ΤΠΕ. Το RESTENA [433] είναι το ερευνητικό δίκτυο του Λουξεμβούργου και πρωταρχικός στόχος του είναι η παροχή υπηρεσιών δικτύου για όλους τους δημόσιους και ιδιωτικούς φορείς και οργανισμούς που εμπλέκονται στον τομέα της εκπαίδευσης και της έρευνας. Το δίκτυο λειτουργεί τη Restena-CSIRT.

Συνεργασία μεταξύ φορέων

Η HCPN, οι σχετικές εθνικές επιτροπές και το κέντρο επικοινωνιών έχουν την αρμοδιότητα για διαχείριση κρίσης. Τα περιστατικά συλλέγονται και αναλύονται από το Circl το οποίο στη συνέχεια ενημερώνει το CASES ώστε να παρέχει άμεση πληροφόρηση και ευαισθητοποίηση για τα συμβάντα. Το CASES συναντάται επίσης με φορείς σε τακτική βάση και δημοσιεύει τις βέλτιστες πρακτικές σε διάφορους τομείς,

που μπορούν να υιοθετηθούν από τον ιδιωτικό τομέα. Ωστόσο, ο ιδιωτικός τομέας δεν είναι υποχρεωμένος να λάβει τα μέτρα.

18.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Η BEE SECURE [434] είναι μια κοινή πρωτοβουλία του Υπουργείου Οικονομίας του Λουξεμβούργου, το Υπουργείου Οικογένειας και του Υπουργείου Παιδείας, με δράσεις ευαισθητοποίησης για την ασφαλή χρήση των τεχνολογιών της πληροφορικής και των επικοινωνιών. Η BEE SECURE εν μέρει υποστηρίζεται από το πρόγραμμα της Ευρωπαϊκής Επιτροπής και συνεργάζεται ως Κέντρο Ασφαλούς Διαδικτύου του Λουξεμβούργου με το ευρωπαϊκό δίκτυο Insafe. Η ιστοσελίδα προσφέρει ενημέρωση για τους κινδύνους του διαδικτύου στους τελικούς χρήστες με έμφαση στα παιδιά και τους γονείς σε θέματα όπως ευπάθειες του υπολογιστή, ανθρώπινες ευπάθειες, κοινωνική δικτύωση, e-banking και e-shopping. Η Οργάνωση διαθέτει και τηλεφωνική γραμμή υποστήριξης(υπηρεσία LISA Stopline) και αναφοράς περιστατικών ασφαλείας στο διαδίκτυο. Το έργο Stopline στοχεύει να παρέχει μια δομή για τις ανώνυμες αναφορές παράνομου περιεχομένου στο διαδίκτυο και τη διερεύνηση αυτών των εκθέσεων σε συνεργασία με τις αρμόδιες αρχές σε εθνικό και διεθνές επίπεδο [435].
Το κέντρο ευαισθητοποίησης και ενίσχυσης της ασφάλειας στον κυβερνοχώρο (CASES) [436] είναι μια εθνική διαδικτυακή πύλη για την ασφάλεια των πληροφοριών. Η πύλη απευθύνεται κυρίως στον χώρο των επιχειρήσεων και παρέχει συμβουλές για την ανάπτυξη πολιτικών ασφαλείας, τις βέλτιστες πρακτικές και τα τεχνικά μέτρα που μπορούν να λάβουν για την αντιμετώπιση των απειλών, την ανάλυση και διαχείριση του κινδύνου καθώς και για τη συμμόρφωση με τα διεθνή πρότυπα.
Το Hack.lu [437] είναι ένα συνέδριο που πραγματοποιείται κάθε χρόνο στο Βέλγιο όπου σχετικά με την ασφάλεια υπολογιστών, την προστασία της ιδιωτικής ζωής, την τεχνολογίας της πληροφορικής και των πολιτιστικών / τεχνικών επιπτώσεων της στην κοινωνία. Το συνέδριο Hack.lu προσελκύει ετησίως μεγάλο μέρος της διεθνούς κοινότητας των ερευνητών ασφάλειας.

18.5 Διεθνής Συνεργασία

Στις 5 Απριλίου 2011, σε ένα συνέδριο ασφάλειας του κυβερνοχώρου στο Maastricht της Ολλανδίας το Λουξεμβούργο μαζί με το Βέλγιο και την Ολλανδία, υπέγραψαν μια

δήλωση προθέσεων για συνεργασία στον τομέα της ασφάλειας στον κυβερνοχώρο, ως αναπόσπαστο μέρος των συνεχών προσπαθειών για την προώθηση της ασφάλειας στις ΤΠΕ. Αποφάσισαν μια στενή συνεργασία μεταξύ των κυβερνήσεών τους, στους τομείς των επιχειρήσεων και της ακαδημαϊκής κοινότητας, με περαιτέρω συμπράξεις δημόσιου-ιδιωτικού τομέα και τακτικές συναντήσεις [438]. Το Λουξεμβούργο συνεργάζεται επίσης με τις υπόλοιπες ευρωπαϊκές χώρες μέσω του ENISA καθώς και άλλων διεθνών οργανισμών όπως η Europol, και το Συμβούλιο της Ευρώπης και συμμετέχει στις ασκήσεις κυβερνοασφάλειας Cyber Europe. Ως χώρα μέλος του NATO συνεργάζεται με τα υπόλοιπα μέλη σε θέματα κυβερνοασφάλειας και συμμετέχει στην διεθνή άσκηση Cyber Coalition [57]. Το Λουξεμβούργο είναι επίσης μέλος της συμμαχίας κατά του κυβερνοεγκλήματος IMPACT [33]. Η CERT.BE είναι μέλος του διεθνούς Φόρουμ FISRT και του TERENA TF-CSIRT [422].

Κεφάλαιο 19ο

Μάλτα

19.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Μάλτα μέχρι σήμερα δεν έχει εκδώσει Εθνική Στρατηγική Κυβερνοασφάλειας. Ωστόσο στο Στρατηγικό Σχέδιο 2009 – 2012 [439] της Υπηρεσίας Πληροφορικής της Μάλτας επικεντρώνεται σε πέντε προτεραιότητες ανάμεσα στις οποίες είναι η διατήρηση μια ισχυρής, ανθεκτικής και ασφαλούς υποδομής ΤΠΕ και υπηρεσιών πληροφορικής. Για την υλοποίηση αυτού του σκοπού η στρατηγική προβλέπει την ανάπτυξη μιας στρατηγικής για την ασφάλεια της πληροφορικής στις επιχειρήσεις, την καθιέρωση ενός ολοκληρωμένου πλαισίου διαχείρισης κινδύνου και την καθιέρωση ενός αυστηρού πλαισίου διαλειτουργικότητας των επιχειρήσεων.

Στη προηγούμενη στρατηγική που είχε δημοσιευτεί από την Υπηρεσία Πληροφορικής για τα έτη 2008-2010 [440] προβλέπονταν επίσης η επανεξέταση του νομοθετικού πλαισίου με έμφαση στο κυβερνοέγκλημα και στην προστασία των δεδομένων, η Καθιέρωση ενός Κέντρου Ασφάλειας Πληροφοριών στη Μάλτα, η καθιέρωση ενός Εθνικού Πλαισίου Ασφάλειας Πληροφοριών, η συνεργασία με όλους τους δημόσιους και μη κυβερνητικούς φορείς για να αναπτυχθεί ένα εκπαιδευτικό πρόγραμμα ευαισθητοποίησης για την πρόληψη και την προστασία των παιδιών από τη φυσική, ψυχολογική ή ηθική κακοποίηση μέσω του διαδικτύου ή άλλων ηλεκτρονικών καναλιών και τέλος, η ενίσχυση της καταπολέμησης του εγκλήματος στον κυβερνοχώρο.

Το 2013 η Υπηρεσία Πληροφορικής της Μάλτας (MITA), σε συνεργασία με την Αρχή Επικοινωνιών της Μάλτας (MCA), διοργάνωσε μια σειρά συναντήσεων εργασίας για την ανάπτυξη μιας εθνικής στρατηγικής για τις ΤΠΕ για την περίοδο 2014-2018 [441].

19.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [442]

Ο νόμος περί προστασίας των δεδομένων ψηφίστηκε στις 14 Δεκεμβρίου 2001 και τέθηκε σε ισχύ τον Ιούλιο του 2003. Εισήχθη για να καταστήσει το δίκαιο της Μάλτας συμβατό με την οδηγία προστασίας δεδομένων της ΕΕ (95/46/ΕΚ). Περιγράφει εννέα αρχές της «καλής επεξεργασίας πληροφοριών» για τη διασφάλιση της προστασίας των προσωπικών δεδομένων. Οι συλλέκτες δεδομένων, όπως εκπαιδευτικά ιδρύματα, εργοδότες και τράπεζες, υποχρεούνται να γνωστοποιούν για τους λόγους της συλλογής πληροφοριών. Ο νόμος περιλαμβάνει επίσης τις απαιτήσεις ακρίβειας και διευκρινίζει ότι «η ρητή» συγκατάθεση από ιδιώτες είναι απαραίτητη, προκειμένου να υποστούν επεξεργασία τα «ευαίσθητα προσωπικά δεδομένα».

Νομοθεσία ηλεκτρονικού εμπορίου [442]

Ο νόμος περί ηλεκτρονικού εμπορίου, δόθηκε στη δημοσιότητα το 2001 και τέθηκε σε ισχύ στις 10 Μαΐου 2002. Σκοπός του είναι να διευκολύνει το ηλεκτρονικό εμπόριο. Οι βασικές διατάξεις του καλύπτουν την νομική ισχύ των ηλεκτρονικών επικοινωνιών και συναλλαγών, το νομικό πλαίσιο για το σχηματισμό των ηλεκτρονικών συμβάσεων το κανονιστικό πλαίσιο για την παροχή των πιστοποιητικών υπογραφής και εξαιρέσεις από την ευθύνη των μεσαζόντων παροχής υπηρεσιών.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [442]

Τον Σεπτέμβριο του 2004 ο νόμος για τις Ηλεκτρονικές Επικοινωνίες (δημοσιεύθηκε στην Εφημερίδα της Κυβερνήσεως της Μάλτας (αριθ. 17 652), μαζί με μια σειρά από συναφείς πράξεις για την τροποποίηση και την κατάργηση της προηγούμενης σχετικής νομοθεσίας. Η νομοθετική αλλαγή μεταφέρει στο δίκαιο της Μάλτας το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες, και συγκεκριμένα τις οδηγίες 2002/21/ΕΚ (οδηγία-πλαίσιο) 2002/20/ΕΚ (οδηγία για την αδειοδότηση) 2002/19/ΕΚ (οδηγία για τη διασύνδεση) 2002/22/ΕΚ (καθολική υπηρεσία και οδηγία για τα δικαιώματα του χρήστη) και 2002/58/ΕΚ (οδηγία για την προστασία της ιδιωτικής ζωής).

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Ο Ποινικός Κώδικας τροποποιήθηκε στις 16 Ιανουαρίου του 2001 [443] και μέσω του άρθρου 337γ προβλέπει μια σειρά από πράξεις οι οποίες εμπίπτουν στα αδικήματα της παράνομης πρόσβασης, παράνομης υποκλοπής, κακής χρήση ηλεκτρονικών συσκευών, απάτης με Η/Υ και πλαστογραφίας με Η/Υ.

19.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Ο ρόλος της Υπηρεσίας Πληροφορικής της Μάλτας (MITA) [444] είναι να διαμορφώνει και να εφαρμόζει τις πολιτικές και τα προγράμματα για τις ΤΠΕ. Επίσης είναι υπεύθυνη για τις υποδομές της κυβέρνησης. Εντός της υπηρεσίας λειτουργεί το Τμήμα Ασφάλειας Πληροφοριών, το οποίο είναι οργανωμένο σε τέσσερις λειτουργικές μονάδες:

- Μονάδα Ασφαλούς Διακυβέρνησης, η οποία είναι υπεύθυνη για την εφαρμογή του πρότυπου ISO27001 και τη διαχείριση του επιχειρηματικού κινδύνου.
- Κέντρο Ασφάλειας των Επιχειρήσεων, το οποίο είναι υπεύθυνο για την Επιχειρησιακή Συνέχεια και την αντιμετώπιση των περιστατικών ασφάλειας.
- Μονάδα Τεχνολογίας Ασφάλειας, η οποία είναι υπεύθυνη για τα εργαλεία της ασφάλειας των πληροφοριών.
- Μονάδα Διαχείρισης Συμμόρφωσης η οποία είναι υπεύθυνη για τους ελέγχους στις ΤΠΕ.

Η Υπηρεσία Επικοινωνιών της Μάλτας (MCA) [445] είναι η εθνική ρυθμιστική αρχή του τομέα των επικοινωνιών στη Μάλτα. Η αρχή αυτή διέπει τις ηλεκτρονικές επικοινωνίες, το ηλεκτρονικό εμπόριο και τον ταχυδρομικό τομέα, και είναι επίσης υπεύθυνη για την εθνική στρατηγική για τις ΤΠΕ, σε θέματα όπως η ασφάλεια στο διαδίκτυο. Η Αστυνομία της Μάλτας μέσω της Μονάδας καταπολέμησης του κυβερνοεγκλήματος [446] βοηθά στη διερεύνηση όλων των εγκλημάτων στα οποία οι υπολογιστές και τα συστήματα πληροφορικής χρησιμοποιούνται ως στόχος της επίθεσης, ή/και χρησιμοποιούνται ως μέσο για να ξεκινήσει οποιαδήποτε επίθεση σε οποιαδήποτε οντότητα. Συλλέγει και διατηρεί αποδεικτικά στοιχεία και τα παρουσιάζει ενώπιον των δικαστικών αρχών. Συνεργάζεται με διεθνείς υπηρεσίες επιβολής του νόμου. Το Γραφείο Επιτρόπου Προστασίας Δεδομένων [447] είναι υπεύθυνο για την προστασία της ιδιωτικής ζωής με την εξασφάλιση της ορθής επεξεργασίας δεδομένων προσωπικού χαρακτήρα και την επίβλεψη της εφαρμογής του νόμου περί προστασίας δεδομένων του 2001. Η Υπηρεσία Προστασίας Πληροφοριών Υποδομών Ζωτικής Σημασίας [448] παρέχει τους κατάλληλους μηχανισμούς έγκαιρης προειδοποίησης, μέσω της ανάπτυξης και της εγκατάστασης ενός εθνικού συστήματος συναγερμού σχετικά με τις απειλές στον κυβερνοχώρο προς τους φορείς εκμετάλλευσης των υποδομών πληροφοριών ζωτικής σημασίας καθώς και σε άλλες επιχειρήσεις και πολίτες. Ως μέρος του σχεδίου για την ενίσχυση της

ασφάλειας και της ανθεκτικότητας των υποδομών ζωτικής σημασίας πληροφορικής και επικοινωνιών η Μονάδα ανέλαβε το έργο για τη δημιουργία της εθνικής ομάδας αντιμετώπισης έκτακτων περιστατικών κυβερνοασφάλειας.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας

Στη Μάλτα λειτουργεί η CSIRTMALTA [449], αποστολή της οποίας είναι να παρέχει στις επιχειρήσεις της Μάλτας πληροφορίες για το πώς να προστατεύσουν τις κρίσιμες πληροφορίες των περιουσιακών στοιχείων τους από τις απειλές του κυβερνοχώρου και τα τρωτά σημεία. Η Ομάδα προωθεί την ανταλλαγή των μη διαβαθμισμένων πληροφοριών οι οποίες μπορεί να είναι χρήσιμες για επιθέσεις στον κυβερνοχώρο και παρέχει ειδοποιήσεις και προειδοποιήσεις,

Ιδιωτικοί φορείς

Η Maltainfosec [450] είναι μια ιδιωτική πρωτοβουλία, στόχος της οποίας είναι να αναδείξει την ανάγκη της ασφάλειας των πληροφοριών σε διάφορους τομείς της πληροφορικής και να δημιουργήσει μια τοπική κοινότητα η οποία θα ανταλλάσσει επαγγελματικές συμβουλές.

Ακαδημαϊκοί φορείς

Το Malta College of Arts, Science & Technology μέσω του Ινστιτούτου Πληροφορικής και Τηλεπικοινωνιών [451] προσφέρει διπλώματα σε όλους τους τομείς της πληροφορικής, ωστόσο δεν έχει αναπτύξει δραστηριότητες σχετικά με την ασφάλεια της πληροφορικής.

Συνεργασία μεταξύ φορέων

Για τη συνεργασία μεταξύ των φορέων, το Συμβούλιο Προστασίας Πληροφοριών Υποδομών Ζωτικής Σημασίας είναι σε συνεχή συνεργασία με όλους τους σχετικούς δημόσιους και ιδιωτικούς οργανισμούς. Συγκεκριμένα, μέσω της CSIRTMalta έχει ήδη δημιουργήσει επαφές με άτομα κλειδιά στις τοπικές επιχειρήσεις του διαδικτύου, στην Υπηρεσία Πληροφορικής, σε σημαντικές τράπεζες και χρηματοπιστωτικά ιδρύματα, σε ιδιωτικούς, και σε διεθνείς οργανισμούς [452].

19.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Η MITA διαδραματίζει σημαντικό ρόλο στην ευαισθητοποίηση για την Ασφάλειας των Πληροφοριών στη Μάλτα, παρέχοντας μια σειρά από συναφείς υπηρεσίες [453]. Οι τελευταίες εκστρατείες ευαισθητοποίησης αφορούν θέματα όπως η χρήση ισχυρών κωδικών πρόσβασης, οδηγίες χρήσης E-Mail, οδηγίες χρήσης του διαδικτύου, φυσική

ασφαλείας στην πρόσβαση, phishing κ.α. Το Κέντρο Ασφαλούς Διαδικτύου Μάλτας έχει δημιουργηθεί ως αποτέλεσμα του προγράμματος safer internet, της Ευρωπαϊκής Επιτροπής [454][455]. Αποτελείται από τέσσερις οργανώσεις: Αρχή Επικοινωνιών της Μάλτας (MCA), το Ίδρυμα Κοινωνικής Ευημερίας (FSWS) και Διεύθυνση Εκπαιδευτικών Υπηρεσιών (DES) και το Γραφείο του Επίτροπου για τα Παιδιά (CFC). Η MCA συντονίζει τις δραστηριότητες του κέντρου ευαισθητοποίησης, ενώ το FSWS είναι υπεύθυνο για την τηλεφωνική γραμμή υποστήριξης. Η ανοιχτή τηλεφωνική γραμμή συντονίζεται από το FSWS σε στενή συνεργασία με τη Μονάδα Ηλεκτρονικού Εγκλήματος της Αστυνομίας της Μάλτας. Το κέντρο οργανώνει επίσης εκπαιδεύσεις σχετικά με την ασφάλεια στο διαδίκτυο στις οποίες συμμετέχουν συνολικά 390 εκπαιδευτικοί. Στις εκπαιδεύσεις γίνεται συζήτηση για τους κινδύνους στο διαδίκτυο, μαζί με τις κοινωνικές και νομικές συνέπειες που συνδέονται με τέτοια συμπεριφορά ή κατάχρηση. Η BeSmartOnline [456] είναι η επίσημη ιστοσελίδα του κέντρου.

19.5 Διεθνής Συνεργασία

Η Υπηρεσία Προστασίας Πληροφοριών Υποδομών Ζωτικής Σημασίας συνεργάζεται στενά με τον ENISA. Στο πλαίσιο της συνεργασίας συμμετέχει σε ασκήσεις του οργανισμού με σκοπό την εξοικείωση σε διαδικασίες διασυνοριακής συνεργασίας και στους μηχανισμούς άμυνας [457]. Επίσης συμμετέχει σε συνέδρια του οργανισμού αλλά και σε άλλα διεθνή συνέδρια [452]. Τέλος, η Μάλτα είναι μέλος της διεθνούς συμμαχίας για την καταπολέμηση του κυβερνοεγκλήματος [33].

Κεφάλαιο 20ο

Ολλανδία

20.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Στις 22 Φεβρουαρίου 2011 ο υπουργός Ασφάλειας και Δικαιοσύνης παρουσίασε την πρώτη Ολλανδική Εθνική Στρατηγική για την ασφάλεια στον κυβερνοχώρο [458]. Η Στρατηγική παρουσίαζε το ολλανδικό όραμα για τις βασικές αρχές για την ασφάλεια στον κυβερνοχώρο, ως εξής:

- Συνεργασία δημόσιου-ιδιωτικού τομέα.
- Εστίαση στις δομές.
- Διατύπωση μοντέλου ενδιαφερομένων φορέων.
- Ενίσχυση των ικανοτήτων.
- Αύξηση των μέτρων ανθεκτικότητας (Γενική προσέγγιση).
- Διατύπωση των θεμελιωδών αρχών.
- Αύξηση της ευαισθητοποίηση των ενδιαφερομένων.

Το 2013 η Ολλανδία αναθεώρησε την στρατηγική της παρουσιάζοντας τη δεύτερη Εθνική Στρατηγική για την ασφάλεια στον κυβερνοχώρο[459] έχοντας το εξής όραμα:

- Ιδιωτική- δημόσια Συμμετοχή.
- Έμφαση στα δίκτυα και τις στρατηγικές συμμαχίες.
- Αποσαφήνιση των σχέσεων μεταξύ των διαφόρων φορέων.
- Ανάπτυξη των ικανοτήτων τόσο στο εσωτερικό όσο και στο εξωτερικό.
- Ισορροπία μεταξύ της προστασίας των συμφερόντων, της απειλής για τα συμφέροντα και τους αποδεκτούς κινδύνους στην κοινωνία (Προσέγγιση με βάση τον κίνδυνο).
- Παρουσίαση του πολιτικού οράματος.
- Πέρασμα από την ευαισθητοποίηση στην αύξηση των ικανοτήτων των ενδιαφερομένων.

Για την επίτευξη των στόχων η στρατηγική καθορίζει τους εμπλεκόμενους φορείς, τις δράσεις που θα πρέπει να εφαρμόσουν και το χρονικό διάστημα που θα πρέπει να έχουν επιτευχθεί.

20.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [460]

Ο νόμος περί προστασίας δεδομένων προσωπικού χαρακτήρα, εγκρίθηκε από το ολλανδικό κοινοβούλιο τον Ιούλιο του 2000 και τέθηκε σε ισχύ την 1η Σεπτεμβρίου 2001. Θέτει τους κανόνες για την καταγραφή και τη χρήση προσωπικών δεδομένων, εφαρμόζοντας τη νομοθεσία της ΕΕ. Η εφαρμογή του νόμου εποπτεύεται από την Αρχή Προστασίας Δεδομένων.

Νομοθεσία ηλεκτρονικού εμπορίου [460]

Τον Μάιο του 2004 το Κοινοβούλιο ψήφισε το νόμο για το ηλεκτρονικό εμπόριο για την εφαρμογή της οδηγίας της ΕΕ (2000/31/ΕΚ). Σε αντίθεση με τα περισσότερα άλλα κράτη μέλη της ΕΕ, η εν λόγω μεταφορά δεν λαμβάνει τη μορφή ενός οριζόντιου νόμου για το ηλεκτρονικό εμπόριο, αλλά μάλλον τη μορφή μιας σειράς τροποποιήσεων των υφιστάμενων νόμων και κανονισμών.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [460]

Ο νόμος για τις τηλεπικοινωνίες τέθηκε σε ισχύ στις 19 Μαΐου 2004. Μεταφέρει στο ολλανδικό δίκαιο τις πέντε οδηγίες που αποτελούν το κανονιστικό πλαίσιο της Ε.Ε. για τις ηλεκτρονικές επικοινωνίες.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Στο ολλανδικό κοινοβούλιο ψηφίστηκε στις 31 Μαΐου 2006 νέα νομοθεσία για το έγκλημα στον κυβερνοχώρο συμπεριλαμβάνοντας στον Ποινικό Κώδικα σχετικά άρθρα [461]:

Άρθρο 138 Διείσδυση σε αυτοματοποιημένη συσκευή.

Άρθρο 161 Παρεμπόδιση της λειτουργίας μιας αυτοματοποιημένης συσκευής.

Άρθρο 350 Παράνομη τροποποίηση δεδομένων συστήματος.

Άρθρο 139 Παρεμβολή συστήματος.

20.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Σύμφωνα με την Εθνική Στρατηγική Κυβερνοασφάλειας, τα κύρια εμπλεκόμενα υπουργεία είναι το Υπουργείο Οικονομικών, το Υπουργείο Εσωτερικών και Σχέσεων του Βασιλείου, το Υπουργείο Ασφάλειας και Δικαιοσύνης και το Υπουργείο Άμυνας. Το Υπουργείο Οικονομικών [462] δραστηριοποιείται σχετικά με την ανάπτυξη της αγοράς των ηλεκτρονικών επικοινωνιών και της πληροφορικής, συμπεριλαμβανομένης της ασφάλειας των δικτύων και των πληροφοριών. Το υπουργείο είναι επίσης υπεύθυνο για τον Οργανισμό Ραδιοεπικοινωνιών [463]. Το Υπουργείο Εσωτερικών και Σχέσεων του Βασιλείου [464] διατυπώνει την πολιτική, προετοιμάζει τη νομοθεσία και τους κανονισμούς και είναι επίσης υπεύθυνο για τον συντονισμό, την εποπτεία και την εφαρμογή των πολιτικών. Έχει κύριο ρόλο όσον αφορά την καθοδήγηση και την ανάπτυξη της ηλεκτρονικής διακυβέρνησης μέσω του οργανισμού logius [465] συμπεριλαμβανομένης της ασφάλειας των κυβερνητικών πληροφοριών. Το Υπουργείο Ασφάλειας και Δικαιοσύνης [466] έχει τον κύριο ρόλο στην ασφάλεια δικτύων και πληροφοριών σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Στο υπουργείο λειτουργούν επίσης τα τμήματα Πληροφορικής και Επικοινωνιών, Συντονισμού και Διαχείρισης Κρίσεων. Στο τελευταίο υπάγεται και το Εθνικό Κέντρο Κυβερνοασφάλειας. Στο υπουργείο επίσης υπάγεται η αστυνομία της Ολλανδίας [467] η οποία διαθέτει τμήμα το οποίο επιτηρεί τα δίκτυα και τα συστήματα επικοινωνιών και αντιμετωπίζει τα εγκλήματα που αφορούν την πληροφορική και τις επικοινωνίες.

Το Υπουργείο Άμυνας [468] θέτει ως στόχους του την αντιμετώπιση των απειλών στη θάλασσα, τη γη, τον αέρα, το διάστημα και τον ψηφιακό τομέα - κυβερνοχώρο. Για την προστασία του κυβερνοχώρου το υπουργείο έχει εκδώσει τη δική [469] του στρατηγική και στο πλαίσιο του λειτουργεί η ομάδα DefCERT. Τέλος η Αρχή Προστασίας Δεδομένων [470] επιβλέπει την δίκαιη και νόμιμη χρήση των προσωπικών δεδομένων.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Το NCSC-NL [471] είναι το Εθνικό Κέντρο Κυβερνοασφάλειας. Είναι η συνέχεια της πρώην κυβερνητικής GOVCERT.NL με αυξημένα πλέον καθήκοντα και δυνατότητες. Τα προϊόντα και οι υπηρεσίες που παρέχονται, έχουν στόχο να καταστήσουν ασφαλέστερη την ψηφιακή κοινωνία. Αυτά αφορούν τεχνογνωσία και συμβουλές, ανταπόκριση σε απειλές και περιστατικά καθώς και επιχειρησιακό συντονισμό σε

κρίσεις. Οι υπηρεσίες επικεντρώνονται στην κεντρική κυβέρνηση και τους κρίσιμους τομείς, αλλά μπορούν να προσφερθούν επίσης σε επιχειρήσεις και σε πολίτες. Το κέντρο παρέχει προειδοποιήσεις ασφαλείας και 24ωρη τεχνική βοήθεια και είναι ο κύριος φορέας συνεργασίας μεταξύ δημοσίου και ιδιωτικού τομέα καθώς και με διεθνείς εταίρους.

Εκτός από το Εθνικό Κέντρο Κυβερνοασφάλειας στην Ολλανδία λειτουργούν αρκετές ακόμη CERT ανάλογα με τον τομέα στον οποίο απευθύνονται, όπως φαίνεται στον πίνακα 20.1.

Χρηματοπιστωτικός τομέας AAB GCIRT http://www.abnamro.com/ FIRST member ING Global CIRT http://www.ing.com FIRST member RABOBANK SOC http://www.rabobank.nl FIRST member	**Εμπορικών Οργανώσεων** FoxCERT http://www.foxcert.com
Εθνικά / κυβερνητικά / Στρατιωτικά DefCERT http://www.defcert.nl FIRST member NCSC-NL http://www.govcert.nl FIRST member	**Έρευνας και Εκπαίδευσης** AMC-CERT http://www.amc.uva.nl/cert/ CERT-RU (formerly CERT-KUN) http://www.kun.nl/cert CERT-RUG: http://www.rug.nl/rc/security/ CERT-UU http://www.cs.ruu.nl/cert-uu/ SURFCERT http://cert.surfnet.nl/ FIRST member UvA-CERT:

	http://ic.uva.nl/cert/
Παρόχων υπηρεσιών CERT-IDC http://www.energis-idc.net Edutel-CSIRT https://www.edutel.nl KPN-CERT: http://www.kpn-cert.nl FIRST member	

Πίνακας 20.1 Cert Ολλανδίας.

Ιδιωτικοί φορείς

Η ICT-Office [472] είναι ένωση από περισσότερες από 500 εταιρείες του τομέα πληροφορικής, και τηλεπικοινωνιών. Η ένωση έχει δημιουργήσει μια ομάδα εργασίας για την ασφάλεια των πληροφοριών, με πρωτοβουλίες αντιμετώπισης του εγκλήματος στον κυβερνοχώρο και την οργανωτική προστασία από τους κινδύνους του κυβερνοχώρου.

Ακαδημαϊκοί φορείς

Το Sentinels [473] είναι ένα ολλανδικό ερευνητικό πρόγραμμα για την ασφάλεια στον τομέα των ΤΠΕ, τα δίκτυα και τα συστήματα πληροφοριών. Το πρόγραμμα για τα έτη 2004-2014 στοχεύει να δώσει μια πολύ σημαντική ώθηση στην τεχνογνωσία ασφάλειας στην Ολλανδία με την παροχή και τη διαχείριση των πόρων στον τομέα της ασφάλειας πληροφοριών, με την οικοδόμηση μιας εθνικής κοινότητας ασφάλειας πληροφορικής, και με τη διάδοση των αποτελεσμάτων στη βιομηχανία και την κυβέρνηση. Η SAFE NL [474] είναι μια πλατφόρμα για την ασφάλεια των υπολογιστών. Παρέχει ένα φόρουμ για τους ερευνητές, τους επαγγελματίες από ερευνητικούς οργανισμούς, τη βιομηχανία και τους κρατικούς φορείς για να ανταλλάξουν ιδέες σχετικά με την εξέλιξη στον τομέα της τεχνολογία της ασφάλειας. Το Eindhoven University of Technology [475]και το Radboud University Nijmegen [476] παρέχουν μεταπτυχιακές σπουδές και διεξάγουν έρευνα στον τομέα της ασφάλειας της πληροφορικής.

Συνεργασία φορέων

Το φόρουμ O- IRT (operationeel Incident Response Teams) δημιουργήθηκε από τη GOVCERT.NL το 2002. Αυτή τη στιγμή συμμετέχουν 31 οργανισμοί από τον δημόσιο και τον ιδιωτικό τομέα. Συμμετέχοντες από τον ιδιωτικό τομέα είναι πάροχοι

υπηρεσιών διαδικτύου, τράπεζες, πολυεθνικές και βιομηχανικές επιχειρήσεις. Από τον δημόσιο τομέα συμμετέχουν η Εθνική Αστυνομία, το Εθνικό Κέντρο Κυβερνοασφάλειας και τα Πανεπιστήμια. Το φόρουμ διευκολύνει την ανταλλαγή γνώσεων και τη συνεργασία σε περιπτώσεις έκτακτων περιστατικών ασφάλειας [80].

20.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Κύριος φορέας είναι το Κέντρο Ευαισθητοποίησης Digibewust [477][478] στο πλαίσιο του προγράμματος της ΕΕ για ασφαλέστερη χρήση του διαδικτύου. Πρόκειται για μια συνεργασία της κυβέρνησης, των επιχειρήσεων και κοινωνικών οργανώσεων η οποία ενημερώνει τους Ολλανδούς πολίτες σχετικά με την ασφαλή χρήση του διαδικτύου και των νέων τεχνολογιών. Το κέντρο εισηγείται, συντονίζει και συμμετέχει σε ένα ευρύ φάσμα εθνικών δραστηριοτήτων και πρωτοβουλιών για διαφορετικές ομάδες, συμπεριλαμβανομένων των παιδιών, των γονέων και των εκπαιδευτικών. Οι μικρομεσαίες επιχειρήσεις αποτελούν επίσης ομάδες στόχους του προγράμματος. Το συνέδριο Black Hat [479] διεξάγεται από το 2000 στο Άμστερνταμ της Ολλανδίας και συγκεντρώνει ειδικούς και εμπειρογνώμονες σχετικά με την ασφάλεια των υπολογιστών από τους εταιρικούς, ακαδημαϊκούς και κυβερνητικούς τομείς αλλά και ανεξάρτητους ερευνητές. Το Black Hat είναι ένα από τα καλύτερα και μεγαλύτερα συνέδρια ασφάλειας υπολογιστών παγκοσμίως. Το Hat In The Box (HITB) [480] είναι επίσης ένα συνέδριο παγκοσμίου φήμης που διοργανώνεται στο Άμστερνταμ. Τέλος, στην Ολλανδία έχουν πραγματοποιηθεί οι εθνικές ασκήσεις Shift Control (2007), Copy…Paste (2011) και Cyberstorm III-NL pact (2012) [28] [481].

20.5 Διεθνής Συνεργασία

Η Ολλανδία συνεργάζεται σε θέματα κυβερνοασφάλειας με τους εταίρους της στην Ε.Ε. και το ΝΑΤΟ. Η Ολλανδία είναι επίσης μέλος του CCD COE [130] και του IMPACT [33]. Το NCSC αποτελεί μέλος του δικτύου FIRST [32] και του EGC [31]. Μέλη του FIRST είναι επίσης οι εννέα από τις δεκαέξι CERT που λειτουργούν στη χώρα [32]. Επιπλέον το NCSC συνεργάζεται με τον ENISA καθώς και με τα CERT NASK και CertPolska της Πολωνίας, AusCERT και CERT.au της Αυστραλίας, CertCC και US-CERT των Ηνωμένων Πολιτειών της Αμερικής και το JPCert της Ιαπωνίας βάση διμερών συμφωνιών[482]. Το DefCERT συνεργάζεται επίσης με το Νατοϊκό Computer Incident Response Center (NCIRC). Σ’ αυτά τα πλαίσια η Ολλανδία

συμμετέχει στην ευρωπαϊκή άσκηση Cyber Europe, στη άσκηση Cyber Storm[108] που διοργανώνουν οι ΗΠΑ καθώς και στην άσκηση Cyber Coalition του NATO [483]. Τέλος η Ολλανδία συνεργάζεται στενά με τις υπόλοιπες χώρες της BENELUX βάση συμφωνίας που έχουν υπογράψει μεταξύ τους [58].

Κεφάλαιο 21ο

Ουγγαρία

21.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας [484]

Η κυβέρνηση της Ουγγαρίας ενέκρινε την Εθνική Στρατηγική Κυβερνοασφάλειας με την Κυβερνητική Απόφαση αριθ. 1139/2013 (21 Μαρτίου). Ο σκοπός αυτής της στρατηγικής είναι να καθορίσει τους εθνικούς στόχους, τις στρατηγικές κατευθύνσεις, τα καθήκοντα και τα κυβερνητικά εργαλεία τα οποία θα επιτρέψουν στην Ουγγαρία να προασπίσει τα εθνικά της συμφέροντα στον ουγγρικό κυβερνοχώρο, στο πλαίσιο του παγκόσμιου κυβερνοχώρου. Η στρατηγική ορίζει τους εξής στόχους :

- Μια ελεύθερη, δημοκρατική και ασφαλή λειτουργία του ουγγρικού κυβερνοχώρο που θα βασίζεται στο κράτος δικαίου, με βάση τη συνεργασία με όλους τους δημόσιους και ιδιωτικούς φορείς του παγκόσμιου κυβερνοχώρου.
- Τη διασφάλιση της κοινωνικής ανάπτυξης και ολοκλήρωσης μέσω της επικοινωνίας εξασφαλίζοντας την προστασία των προσωπικών δεδομένων, την ανάπτυξη αποτελεσματικών και καινοτόμων επιχειρήσεων και τη προώθηση καινοτόμων δημόσιων υπηρεσιών
- Την αποτελεσματική διαχείριση κρίσεων και προστασία των χρηστών διαθέτοντας αποτελεσματικές δυνατότητες αντιμετώπισης των απειλών, πληρώντας τις απαιτήσεις των διεθνών βέλτιστων πρακτικών, με ιδιαίτερη έμφαση στην τήρηση των διεθνών πρότυπων πιστοποίησης, διασφαλίζοντας την ποιότητα της εκπαίδευσης, της κατάρτισης, και της έρευνας και διατηρώντας αποτελεσματική ικανότητα ανάκτησης σε περιπτώσεις επιθέσεων.

21.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [485]

Ο νόμος Αρ. LXIII του 1992 για την προστασία των δεδομένων προσωπικού χαρακτήρα και Γνωστοποίησης Δεδομένων του δημοσίου συμφέροντος καθορίζει τους

κανόνες για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα των δημόσιων και ιδιωτικών φορέων. Η εφαρμογή της εποπτεύεται από τον Κοινοβουλευτικό Επίτροπο για την προστασία των δεδομένων και την ελευθερία της πληροφόρησης.

Νομοθεσία ηλεκτρονικού εμπορίου[485]

Ο Νόμος αριθ. CVIII του 2001 για το ηλεκτρονικό εμπόριο και τις υπηρεσίες της κοινωνίας της πληροφορίας της 18 Δεκεμβρίου 2001 θέτει σε εφαρμογή την οδηγία της ΕΕ 2000/31/ΕΚ σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [486]

Ποινικός Κώδικας

Η Ουγγαρία επικύρωσε τη σύμβαση του Συμβουλίου της Ευρώπης για την Εγκληματικότητα στον Κυβερνοχώρο στις 4 του Δεκεμβρίου 2003 ενσωματώνοντας αντίστοιχα άρθρα στον ποινικό της κώδικα:

Άρθρο 300γ και Άρθρο 300ε παράνομη πρόσβαση, παράνομη υποκλοπή, παρεμβολή δεδομένων, κακή χρήση ηλεκτρονικών συσκευών, απάτη με χρήση Η/Υ, πλαστογραφία με χρήση Η/Υ.

21.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Υπουργείο Εθνικής Ανάπτυξης, μέσω της Κρατικής Γραμματείας Πληροφοριών και Επικοινωνιών [487] έχει ως στόχο τη βελτίωση των λειτουργιών στον τομέα των ΤΠΕ και είναι αρμόδιο για την ανάπτυξη των υποδομών πληροφορικής των τηλεπικοινωνιών και των πληροφοριακών συστημάτων της κυβέρνησης. Παραρτήματα της Εθνικής Αρχής Ασφάλειας [488] είναι η Αρχή Διαχείρισης Κυβερνοάμυνας και το Τμήμα Ασφάλειας Πληροφοριών και Κρυπτογράφησης. Βασικές αρμοδιότητες της Αρχής Διαχείρισης Κυβερνοάμυνας είναι η διαχείριση των ευπαθειών, η συμβολή στην αντιμετώπιση προβλημάτων, η αποκάλυψη τρωτών σημείων του δικτύου, και η ανάλυση των κυβερνητικών και εθνικών οργανισμών. Περαιτέρω η αρχή χειρίζεται περιστατικά που αφορούν τον προαναφερθέντα κύκλο και συμβάλλει στην έρευνα των επιθέσεων στον κυβερνοχώρο. Η Αρχή επίσης οργανώνει προγράμματα κατάρτισης και ευαισθητοποίησης με στόχο την ηλεκτρονική ασφάλεια των πληροφοριών και είναι αρμόδια με βάση τα σχετικά μνημόνια συνεννόησης για συνεργασία με τους αρμόδιους

φορείς τόσο της ΕΕ όσο και του ΝΑΤΟ. Το Τμήμα Ασφάλειας Πληροφοριών και Κρυπτογράφησης εκτελεί την άσκηση ελέγχου όσον αφορά τα ηλεκτρονικά συστήματα χειρισμού διαβαθμισμένων πληροφοριών, που λειτουργούν και διαχειρίζονται από κυβερνητικούς οργανισμούς και εταιρείες. Η Εθνική Αρχή Προστασίας Προσωπικών Δεδομένων και Ελευθερίας της Πληροφορίας [489] είναι υπεύθυνη για την εποπτεία και την υπεράσπιση του δικαιώματος στην προστασία των δεδομένων προσωπικού χαρακτήρα και της ελευθερίας της πληροφόρησης. Οι ευθύνες της καλύπτουν τόσο το κράτος όσο και στον ιδιωτικό τομέα. Τέλος, η Ουγγρική Αστυνομία μέσω του Τμήματος Ηλεκτρονικού Εγκλήματος [490] ασχολείται με την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CERT-Hungary [491][492] είναι η κυβερνητική CERT της Ουγγαρίας και λειτουργεί εντός της Ειδικής Υπηρεσίας Εθνικής Ασφάλειας. Ξεκίνησε τη λειτουργία της τον Ιούλιο του 2013 και απευθύνεται σε υποδομές ζωτικής σημασίας στην Ουγγαρία. Τα καθήκοντα της περιλαμβάνουν τον συντονισμό και την ανταπόκριση σε σοβαρές παραβιάσεις της ασφάλειας των κυβερνητικών δικτύων και υποδομών πληροφοριών ζωτικής σημασίας, την προώθηση της ανταλλαγής πληροφοριών, τον συντονισμό με τους εθνικούς και διεθνείς ομολόγους για την ενίσχυση των εθνικών μέτρων ετοιμότητας και την ευαισθητοποίηση στον τομέα της ασφάλειας δικτύων και πληροφοριών. Το πρόγραμμα Ανάπτυξης της Εθνικής Υποδομής Πληροφοριών χρησιμεύει ως πλαίσιο για την ανάπτυξη και τη λειτουργία του δικτύου έρευνας στην Ουγγαρία. Στο πλαίσιο του προγράμματος είναι και λειτουργία της ομάδας NIIF CSIRT [493]. Η HUN-CERT [494] είναι η ομάδα των παρόχων υπηρεσιών διαδικτύου και είναι υπεύθυνη στη παροχή βοήθειας, στην ανάλυση και επεξεργασία περιστατικών. Επίσης συμβάλει στην αύξηση του επιπέδου ευαισθητοποίησης σχετικά με την ασφάλεια πληροφοριών.

Ιδιωτικοί φορείς

Ο Ουγγρικός Σύνδεσμος Επιχειρήσεων Πληροφορικής [495] εκπροσωπεί τα συμφέροντα των εταιρειών πληροφορικής της Ουγγαρίας συμπεριλαμβανομένων αυτών της ασφάλειας. Ο σύλλογος Inforum [496] επικεντρώνεται στην ανάπτυξη του Internet και στην καταπολέμηση των αρνητικών πτυχών του όπως το spam και οι ιοί. Η Ένωση των Ούγγρων παρόχων [497] περιεχομένου δημιουργήθηκε με σκοπό την

επίτευξη ασφαλούς περιεχομένου στο Διαδίκτυο και την ευαισθητοποίηση σχετικά με την ασφάλεια του διαδικτύου.

Ακαδημαϊκοί φορείς

Το πρόγραμμα Ανάπτυξης της Εθνικής Υποδομής Πληροφοριών NIIF [498] χρησιμεύει ως πλαίσιο για την ανάπτυξη και τη λειτουργία του δικτύου έρευνας της Ουγγαρίας. Το κέντρο πληροφορικής του Πανεπιστημίου Τεχνολογίας και Οικονομικών της Βουδαπέστης [499] διαδραματίζει έναν πολύ σημαντικό ρόλο στη δημιουργία και την κατάρτιση μηχανικών υπολογιστών. Το κέντρο είναι επίσης υπεύθυνο για τη λειτουργεία ενός εργαστηρίου ασφάλειας υπολογιστών.

Συνεργασία μεταξύ φορέων

Το CERT Hungary συντονίζει την αντιμετώπιση των περιστατικών. Αρχικά προσδιορίζει την αρχική αιτία του συμβάντος και διευκολύνει την επικοινωνία με άλλους δικτυακούς τόπους που μπορεί να εμπλέκονται. Εάν είναι απαραίτητο έρχεται σε επαφή με τις αρχές επιβολής του νόμου, κάνει αναφορές και βγάζει ανακοινώσεις προς τους χρήστες.

21.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Κύριος φορέας ευαισθητοποίησης για την προώθηση της ασφάλειας των δικτύων είναι η CERT Hugary [500]. Οι δράσεις της αφορούν την προετοιμασία της ουγγρικής κοινωνίας για ασφαλέστερη χρήση του διαδικτύου, την ανάπτυξη εκπαιδευτικού υλικού, δράσεων, και εκστρατειών ευαισθητοποίησης. Στην ιστοσελίδα της παρέχει εγχειρίδια για την αντιμετώπιση επιθέσεων phishing, χρήση των ιστότοπων κοινωνικής δικτύωσης με ασφάλεια, προστασία των παιδιών στο διαδίκτυο και σωστή χρήση των κωδικών πρόσβασης. Η ιστοσελίδα «Biztonságos Internet» δημιουργήθηκε από το Ίδρυμα Puskas ως μια πρωτοβουλία ευαισθητοποίησης στην ασφάλεια της πληροφορικής. Ο δικτυακός τόπος είναι ένα σημείο αναφοράς για παράνομο και επιβλαβές περιεχόμενο στο διαδίκτυο και διοργανώνει εκστρατείες ευαισθητοποίησης σχετικές με την ασφάλειας του διαδικτύου στα σχολεία. Υποστηρίζεται από την Ευρωπαϊκή Επιτροπή ως μέρος του προγράμματος Safer Internet Plus και είναι επίσης υπεύθυνη για τη λειτουργία τηλεφωνικής γραμμής στην οποία οι πολίτες μπορούν να αναφέρουν επιβλαβές περιεχόμενο στο διαδίκτυο [501]. Επιπλέον, το NETWORKSHOP [502] είναι μία ετήσια εκδήλωση που διοργανώνεται από το NIIF

με επίκεντρο λύσεις για υπολογιστές, τη δικτύωση, και την ασφάλεια των ΤΠΕ. Στην Ουγγαρία διεξάγεται η εθνική άσκηση Κυβερνοασφάλειας COMEX [28].

21.5 Διεθνής Συνεργασία

Η Ουγγαρία λαμβάνει μέρος μέσω της Αρχής Διαχείρισης Κυβερνοάμυνας της Εθνικής Αρχής Ασφαλείας στην πανευρωπαϊκή άσκηση για την προστασία κρίσιμων πληροφοριακών υποδομών, Cyber Europe [28][503. Επίσης η Ουγγαρία είναι η 8η χώρα που έγινε μέλος του CCDCOE [504]. Η Αρχή Διαχείρισης Κυβερνοάμυνας συμμετέχει επίσης στη Νατοϊκή άσκηση Cyber Coalition[503][505][506]. και στην άσκηση Cyber Storm, που οργανώνεται από το Αμερικανικό Υπουργείο Εσωτερικής Ασφάλειας (DHS)[503][507]. Το CERT-Hungary συνεργάζεται με τα αντίστοιχα CERT των χωρών της Σλοβακίας [508] της Ρουμανίας, [509] της Κίνας [510] και της Αιγύπτου [511] διεξάγοντας συζητήσεις για τις δυνατότητες ανταλλαγής πληροφοριών, στους τομείς της συνεργασίας για την προστασία κρίσιμων πληροφοριακών υποδομών, και την εκπροσώπηση του κοινού συμφέροντος στις διεθνείς κοινότητες CERT. Τέλος η Ουγγαρία συμμετέχει στην CEENet μέσω της HUNGARNET [79] και η CERT-Hungary είναι αναγνωρισμένο μέλος των TI TF-CSIRT, EGC[31] και FIRST [32][512].

Κεφάλαιο 22ο

Πολωνία

22.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Το «Πρόγραμμα για την προστασία του κυβερνοχώρου της Πολωνίας 2011-2016» [513], αποτελεί σήμερα το πιο σημαντικό έγγραφο που σχεδιάζει τις δράσεις που σχετίζονται με τον πολωνικό κυβερνοχώρο. Το Πρόγραμμα συστείνει τις δράσεις που θα οδηγήσουν στην πρόληψη και την καταπολέμηση των απειλών και περιλαμβάνει προτάσεις για νομικές, οργανωτικές, τεχνικές και εκπαιδευτικές δραστηριότητες. Επιπλέον, ο στόχος του Προγράμματος είναι να προσδιοριστούν οι φορείς που είναι υπεύθυνοι για την ασφάλεια στον κυβερνοχώρο. Επίσης στοχεύει στη δημιουργία ενός συστήματος αξιολόγησης των κινδύνων για τους δημόσιους φορείς (που θα περιλαμβάνει κατευθυντήριες γραμμές και για τους ιδιωτικούς φορείς), και στη δημιουργία ενός συστήματος συντονισμού για την εξουδετέρωση και πρόληψη των απειλών, καθώς και για τη συνεργασία και την ανταλλαγή πληροφοριών με χώρες-εταίρους, διεθνείς οργανισμούς και πάνω από όλα, με τον ιδιωτικό τομέα. Άλλες προτεινόμενες λύσεις που αποσκοπούν στη βελτίωση της ασφάλειας του κυβερνοχώρου περιλαμβάνουν τη δημιουργία Διυπουργικής Ομάδας Συντονισμού, υπεύθυνης για το συντονισμό των ενεργειών που σχετίζονται με την ασφάλεια στον κυβερνοχώρο. Το έργο επίσης Προϋποθέτει αλλαγές στη νομοθεσία σχετικά με την ασφάλεια στον κυβερνοχώρο (π.χ. όσον αφορά το έγκλημα στον κυβερνοχώρο). Επιπλέον, το πρόγραμμα προβλέπει το διορισμό ενός Αντιπρόσωπου της Κυβέρνησης και ένας εκπροσώπου επικεφαλής της οργανωτικής μονάδας στον κυβερνοχώρο για την προστασία της δημόσιας διοίκησης, καθώς και τη δημιουργία μια παρόμοιας θέσης για τον ιδιωτικό τομέα. Το Υπουργείο Εσωτερικών ορίζεται ως υπεύθυνο για να τεθεί το πρόγραμμα σε ισχύ.

22.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [514]

Ο νόμος για την προστασία των δεδομένων προσωπικού χαρακτήρα εγκρίθηκε στις 29 Αυγούστου 1997 και τροποποιήθηκε τρεις φορές κατά τη διάρκεια του 2004. Ο νόμος αυτός ακολουθεί τους κανόνες που έχουν θεσπιστεί από την οδηγία της Ευρωπαϊκής Ένωσης 95/46/ΕΚ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα. Ο Γενικός Επιθεωρητής για την προστασία των δεδομένων προσωπικού χαρακτήρα επιβλέπει την τήρηση του νόμου.

Νομοθεσία ηλεκτρονικού εμπορίου [514]

Ο νόμος για την παροχή ηλεκτρονικών υπηρεσιών τέθηκε σε ισχύ στις 10 Μαρτίου 2003. Υλοποιεί τις διατάξεις της οδηγίας 2000/31/ΕΚ για ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου, στην εσωτερική αγορά («οδηγία για το ηλεκτρονικό εμπόριο»). Μεταξύ άλλων θεμάτων, ο νόμος ρυθμίζει τις υποχρεώσεις και τις ευθύνες των παρόχων ηλεκτρονικών υπηρεσιών, καθώς και την προστασία των δεδομένων προσωπικού χαρακτήρα των φυσικών προσώπων που χρησιμοποιούν ηλεκτρονικές υπηρεσίες. Επίσης, εξετάζεται το ζήτημα του spamming.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [514]

Ο νόμος για τις τηλεπικοινωνίες μεταφέρει το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες, εκδόθηκε τον Ιούλιο του 2004 και τέθηκε σε ισχύ στις 3 Σεπτεμβρίου 2004. Τροποποιήθηκε το 2005 με στόχο την αναβάθμιση της ρυθμιστικής διαδικασίας στον τομέα των τηλεπικοινωνιών, την καλύτερη προσαρμογή των εθνικών διατάξεων στους κανονισμούς της ΕΕ, και την εισαγωγή νέων ρυθμίσεων υπέρ των καταναλωτών.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [37]

Ο Ποινικός Κώδικας της Πολωνίας περιλαμβάνει άρθρα που σχετίζονται με τα εγκλήματα του κυβερνοχώρου:

Άρθρο 269α Παρεμβολή σε δεδομένα, παρεμβολή σε σύστημα.

Άρθρο 269β Παράνομη προσπέλαση.

Άρθρο 267 Παράνομη υποκλοπή, Κακή χρήση ηλεκτρονικών συσκευών.

Άρθρο 268 Πλαστογραφία με Η/Υ, απάτη με Η/Υ.

22.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Υπουργείο Δημόσιας Διοίκησης και Ψηφιοποίησης [515] εκτελεί μια σειρά από εργασίες, συμπεριλαμβανομένων και εκείνων που εμπίπτουν στο πεδίο εφαρμογής της ψηφιοποίησης της δημόσιας διοίκησης, τις τεχνικές και τα πρότυπα, καθώς και στήριξη των επενδύσεων στον χώρο της πληροφορικής, την εφαρμογή λύσεων πληροφορικής στην κοινωνία της πληροφορίας και την ανάπτυξή της. Τέλος, εκπληρώνει τις διεθνείς δεσμεύσεις της Πολωνίας στον τομέα της πληροφορικής. Το υπουργείο είναι υπεύθυνο για τον συντονισμό, την πρόληψη, την αντιμετώπιση και την αποκατάσταση σε περιπτώσεις καταστροφών, συμπεριλαμβανομένων αυτών στους τομείς της πληροφορικής και τηλεπικοινωνιών καθώς ανέλαβε τις αρμοδιότητες αυτές από το Υπουργείο Εσωτερικών. Η Υπηρεσία Εσωτερικής Ασφάλειας (ABW) [516] φροντίζει για την ασφάλεια της Πολωνίας συμπεριλαμβανομένου του πεδίου της ασφάλειας των ΤΠΕ. Η ομάδα CERT.GOV.PL είναι ένα μέρος του Τμήματος Πληροφορικής της υπηρεσίας. Το Κυβερνητικό Κέντρο για την Ασφάλεια (RCB) [517] έχει την ευθύνη για το συντονισμό των ενεργειών που αφορούν τις κρίσιμες υποδομές. Τα ειδικά καθήκοντα του Γραφείου Ηλεκτρονικών Επικοινωνιών (UKE) [518] περιλαμβάνουν, μεταξύ άλλων τη ρύθμιση και την εποπτεία των τηλεπικοινωνιακών υπηρεσιών, τη διαχείριση του ραδιοφάσματος, καθώς και την επιβολή της συμμόρφωσης με τις απαιτήσεις ηλεκτρομαγνητικής συμβατότητας. Ο Γενικός Επιθεωρητής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα [519] ασκεί εποπτεία για τη διασφάλιση της συμμόρφωσης με τις διατάξεις περί προστασίας των προσωπικών δεδομένων, εκδίδει διοικητικές αποφάσεις και εξετάζει σχετικές καταγγελίες. Η Πολωνική Αστυνομία, μέσω του Τμήματος Καταπολέμησης Εγκλημάτων Κυβερνοχώρου [520] συμβάλει στον εντοπισμό και την παρακολούθηση του εγκλήματος στον κυβερνοχώρο, σε συνεργασία με τους διαχειριστές και τους ιδιοκτήτες των δικτύων υπολογιστών, τις εταιρείες τηλεπικοινωνιών και τους παρόχους υπηρεσιών.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CERT.GOV.PL [521] είναι η Κυβερνητική ομάδα και κύριο έργο της είναι η προστασία της δημόσιας διοίκησης από τις κυβερνοαπειλές. Η ομάδα υπάγεται στην Πολωνική Υπηρεσία Εσωτερικής Ασφάλειας και οι υπηρεσίες που παρέχονται περιλαμβάνουν συντονισμό στη διαδικασία αντιμετώπισης περιστατικού, δημοσίευση ανακοινώσεων σχετικά με απειλές κατά της ασφάλειας , ανίχνευση , επίλυση και ανάλυση των περιστατικών ασφάλειας. Το Arakis-GOV είναι ένα σύστημα έγκαιρης προειδοποίησης απειλών το οποίο έχει αναπτυχθεί από την Υπηρεσία Εσωτερικής

Ασφάλειας, σε συνεργασία με την ομάδα CERT Polska. Η CERT POLSKA [522] είναι η εθνική ομάδα και σκοπός της είναι να βοηθήσει τους Πολωνούς χρήστες του Διαδικτύου στην εφαρμογή προληπτικών μέτρων για τη μείωση των κινδύνων υπολογιστή και στην αντιμετώπιση των περιστατικών ασφάλειας. Η OPL CERT [523] είναι ομάδα του τηλεπικοινωνιακού παρόχου OPL και κύριος στόχος της είναι να βοηθήσει τους χρήστες του στην εφαρμογή προληπτικών μέτρων για τη μείωση των κινδύνων των περιστατικών ασφάλειας των υπολογιστών, ιδίως με την παροχή συμβουλευτικών υπηρεσιών και εκπαίδευσης. Η PIONIER-CERT [524] είναι μια ομάδα που έχει συσταθεί για να παρέχει αποτελεσματικές υπηρεσίες αντιμετώπισης περιστατικών στα μέλη και τους χρήστες του Πολωνικού Επιστημονικού Δικτύου PIONIER.

Ιδιωτικοί φορείς

Το Πολωνικό Επιμελητήριο Πληροφορικής και Τηλεπικοινωνιών (PIIT) [525] συγκεντρώνει εταιρείες του τομέα της πληροφορικής και των τηλεπικοινωνιών. Το Επιμελητήριο διοργανώνει συνέδρια και άλλες δράσεις που αφορούν την προστασία των πληροφοριακών συστημάτων των μελών του.

Ακαδημαϊκοί φορείς

Το Ερευνητικό και Ακαδημαϊκό Δίκτυο Υπολογιστών (NASK) [526] έχει την ιδιότητα του ερευνητικού ινστιτούτου. Προσφέρει λύσεις τηλεπικοινωνιών και δεδομένων για τις επιχειρήσεις, τη διοίκηση και τα ακαδημαϊκά ιδρύματα. Η Ομάδα Ασφάλειας Δικτύων και Πληροφοριών υπάρχει ως ξεχωριστή μονάδα στο Τμήμα Έρευνας από το 2009 και καλύπτει όλες τις πτυχές της ασφάλειας στα ερευνητικά πεδία των μεθόδων ανίχνευσης απειλών και μεθόδων ελέγχου πρόσβασης και διαχείρισης κρίσεων στις ΤΠΕ. Ένα μεγάλο μέρος της έρευνας γίνεται σε στενή συνεργασία με την CERT Polska η οποία είναι επίσης μέρος του οργανισμού NASK. Το Ακαδημαϊκό Υπολογιστικό Κέντρο CYFRONET AGH [527] είναι μια αυτόνομη οργανωτική και οικονομική οντότητα του AGH University of Science and Technology. Το κέντρο έχει, μεταξύ άλλων, Τμήματα Λογισμικού, Δικτύων Υπολογιστών και Ασφάλειας Δεδομένων.

Συνεργασία μεταξύ φορέων

Οι CERT Polska, CERT GOV PL και η Εθνική Υπηρεσία Εσωτερικής Ασφάλειας είναι τα κύρια σημεία επαφής για την ασφάλεια πληροφορικής. Την ευθύνη για την καταπολέμηση των απειλών στον κυβερνοχώρο φέρει η CERT.GOV.PL η οποία αποτελεί μια πλατφόρμα συντονισμού για την αντιμετώπιση περιστατικών που

απειλούν την ασφάλεια των συστημάτων πληροφορικής ή δικτύων που χρησιμοποιούνται από τα κρατικά όργανα των οποίων η καταστροφή μπορεί να οδηγήσει σε σοβαρή διαταραχή της λειτουργίας της χώρας . Ένα από τα καθήκοντα της ομάδας είναι να εφαρμόσει και να επιβλέπει το σύστημα έγκαιρης προειδοποίησης Arakis– GOV[528][529]. Το σύστημα δημιουργήθηκε ύστερα από συνεργασία της CERT Polska και της Υπηρεσίας Εσωτερικής Ασφάλειας. Προς το παρόν, οι αισθητήρες του συστήματος είναι εγκατεστημένοι σε πάνω από 60 γραφεία της κεντρικής και της τοπικής διοίκησης. Το κέντρο GCS για την καλύτερη συνεργασία μεταξύ των δημόσιων και ιδιωτικών φορέων έχει δημιουργήσει ένα δημόσιο-ιδιωτικό φόρουμ (Polish Abuse Forum) για την ανταλλαγή γνώσεων και πληροφοριών και για το συντονισμό των ενεργειών με στόχο την οικοδόμηση ασφαλών υποδομών, συμπεριλαμβανομένων αυτών του τομέα των ΤΠΕ. Αυτή η πρωτοβουλία είναι μια ενδιαφέρουσα προσπάθεια να συμπεριληφθούν οι ιδιωτικοί φορείς στην προστασία του πολωνικού κυβερνοχώρου [80] [518].

22.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Το Πολωνικό Κέντρο Ασφαλούς Διαδικτύου (PSIC) [530][531] ιδρύθηκε το 2005 στο πλαίσιο του προγράμματος Safer Internet της Ευρωπαϊκής Επιτροπής. Το Κέντρο διοικείται από το Ίδρυμα Fundacja dzieci Niczyje (FDN) και από το Ερευνητικό και Ακαδημαϊκό Δίκτυο Υπολογιστών (NASK). Το Κέντρο αναλαμβάνει μια σειρά από ολοκληρωμένες προσπάθειες που στοχεύουν στη βελτίωση της ασφάλειας των παιδιών και των νέων ανθρώπων που χρησιμοποιούν το Διαδίκτυο και τις νέες τεχνολογίες. Το πολωνικό Κέντρο Ασφαλούς Διαδικτύου υλοποιεί τρία έργα :Το Saferinternet.pl ένα έργο ολοκληρωμένων δραστηριοτήτων ευαισθητοποίησης με στόχο την προώθηση της ασφαλέστερης χρήσης του διαδικτύου και των νέων τεχνολογιών από τα παιδιά και τους νέους, το Helpline.org.pl βάσει του οποίου προσφέρεται υποστήριξη και συμβουλές στους νέους χρήστες του Διαδικτύου, τους γονείς και τους επαγγελματίες που αντιμετωπίζουν απειλές που σχετίζονται με τη χρήση του Διαδικτύου και των κινητών τηλεφώνων και το Dyżurnet.pl ως γραμμή επικοινωνίας όπου μπορούν να αναφερθούν ιστότοποι με παράνομο περιεχόμενο. Το NASK και το CERT Polska διατηρούν επίσης ένα πολύ σημαντικό δικτυακό τόπο ευαισθητοποίησης για ειδικούς πληροφορικής και οικιακούς χρήστες. Οι πληροφορίες στην ιστοσελίδα περιλαμβάνουν λεπτομέρειες σχετικά με τις νέες απειλές, τα τρωτά σημεία , τα συμβάντα, προληπτική

ενημέρωση, καθώς και προειδοποίηση σχετικά με τις πιθανές επιθέσεις. Το SECURE [532] είναι ένα ετήσιο συνέδριο αφιερωμένο εξ ολοκλήρου στην ασφάλεια πληροφορικής και απευθύνεται στους διαχειριστές, στα μέλη της ομάδας ασφαλείας και στους επαγγελματίες του χώρου. Το διεθνές συνέδριο Cryptography and Security Systems [533] πραγματοποιείται κάθε χρόνο στην Πολωνία με σκοπό να παρουσιάσει τις δραστηριότητες έρευνας και ανάπτυξης που σχετίζονται με όλες τις πτυχές της κρυπτογραφίας και της ασφάλειας του δικτύου.

22.5 Διεθνής Συνεργασία

Η Πολωνία συνεργάζεται με τις υπόλοιπες χώρες της Ε.Ε. σε θέματα Κυβερνοασφάλειας μέσω της Υπηρεσίας Εσωτερικής Ασφάλειας που είναι και ο κύριος εκπρόσωπος της χώρας στον οργανισμό ENISA [215]. Κατά τη διάρκεια του 2010 και του 2012 η Πολωνία έλαβε μέρος στην πανευρωπαϊκή άσκηση Cyber Europe [534]. Η Υπηρεσία Εσωτερικής Ασφάλειας έχει επίσης υπογράψει συμφωνία με το NATO σχετικά με τη συνεργασία τους στον τομέα του κυβερνοχώρου [535]. Η συνεργασία θα επιτρέψει την αμοιβαία ανταλλαγή γνώσεων και πληροφοριών, προκειμένου να βελτιωθεί η αποτελεσματικότητα της πρόληψης των επιθέσεων στον κυβερνοχώρο. Η πολωνική πλευρά συμμετέχει επίσης στην άσκηση Cyber Coalition 2011 [529][536]. Επιπλέον, η Πολωνία είναι μέλος της διεθνούς συμμαχίας IMPACT και από τον Νοέμβριο του 2011 είναι επίσημο μέλος του NATO CCDCOE [537]. Τέλος η CERT POLSKA και η OPL CERT είναι μέλη του FIRST [32] του TERENA TF-CSIRT και του CEENET [529].

Κεφάλαιο 23ο

Πορτογαλία

23.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Μέχρι σήμερα η Πορτογαλία δεν έχει δημοσιεύσει επίσημη Εθνική Στρατηγική Κυβερνοασφάλειας. Ωστόσο, μπορεί κανείς να παρατηρήσει δράσεις και πολιτικές που μπορούν να θεωρηθούν ως πρώιμο στάδιο ανάπτυξης μιας εθνικής στρατηγικής. Η στρατηγική ασφάλειας των πληροφοριών προκύπτει έμμεσα από το Τεχνολογικό Σχέδιο της Πορτογαλίας (Portugal's Technological Plan) σχετικά με τη ηλεκτρονική διακυβέρνηση της χώρας [538]. Το σχέδιο είναι μια ευρύτερη προσπάθεια για την προώθηση της ανάπτυξης της Κοινωνίας της Πληροφορίας στην Πορτογαλία.

23.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [539]

Ο Νόμος 41/2004, της 18ης Αυγούστου μεταφέρει στο εθνικό δίκαιο την οδηγία 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών, εκτός από το άρθρο 13 το οποίο αφορά τις αυτόκλητες επικοινωνίες. Η νομοθεσία αυτή ισχύει για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο πλαίσιο των διαθέσιμων στο κοινό υπηρεσιών, ηλεκτρονικών επικοινωνιών και δικτύων, ενώ παράλληλα συμπληρώνει τις διατάξεις του Ν. 67/98 της 26ης Οκτωβρίου (Νόμος για την προστασία των προσωπικών δεδομένων).

Νομοθεσία για το ηλεκτρονικό εμπόριο [539]

Το νομοθετικό διάταγμα για το ηλεκτρονικό εμπόριο ν. 7/2004 της 7ης Ιανουαρίου μεταφέρει στο εθνικό δίκαιο την οδηγία της ΕΕ για το ηλεκτρονικό εμπόριο (Οδηγία 2000/31/ΕΚ). Το Διάταγμα διέπει τις αυτόκλητες επικοινωνίες για σκοπούς απευθείας εμπορικής προώθησης και προβλέπει μέτρα προστασίας ενάντια στην εισβολή στην ιδιωτική ζωή. Προβλέπει την υποχρέωση των παρόχων να αποκτούν τη συγκατάθεση του παραλήπτη για την αποστολή μηνυμάτων για σκοπούς άμεσης εμπορίας, καθώς και

την υποχρέωση να διατηρούν ενημερωμένο κατάλογο των προσώπων που έχουν εκφράσει την επιθυμία τους να μη λαμβάνουν τέτοιες διαφημίσεις. Επίσης σύμφωνα με το νομοθετικό διάταγμα Ν 62/2009 η Γενική Διεύθυνση Καταναλωτών (DGC) πρέπει να διατηρεί μονίμως ενημερωμένη εθνική λίστα των προσώπων που έχουν εκφράσει την επιθυμία τους να μη λαμβάνουν διαφημίσεις.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [540]

Ο Πρόεδρος της Πορτογαλίας ενέκρινε στις 15 Σεπτεμβρίου 2009 το νόμο για το έγκλημα στον κυβερνοχώρο (N. 109/2009) ο οποίος μεταφέρει στο εθνικό δίκαιο την οδηγία 2005/222/JAI του Ευρωπαϊκού Συμβουλίου της 24ης Φεβρουαρίου 2009, που αναφέρεται στις επιθέσεις κατά των πληροφοριακών συστημάτων. Η Πορτογαλία έχει μια μακρά παράδοση στη θέσπιση της προστασίας του εγκλήματος πληροφορικής καθώς έχει θεσπίσει νομικό πλαίσιο για εγκληματικές ενέργειες που αφορούν τους υπολογιστές από το 1991 (Νόμος 109/91 της 17ης Αυγούστου 1991). Τα αδικήματα σχετικά με το κυβερνοέγκλημα περιγράφονται στα άρθρα:

Άρθρο 2 Παράνομη Πρόσβαση.

Άρθρο 3 Παράνομη υποκλοπή.

Άρθρο 4 Παρεμβολή δεδομένων.

Άρθρο 5 Παρεμβολή συστήματος.

Άρθρο 6 Κακή χρήση ηλεκτρονικών συσκευών.

Άρθρο 7 Πλαστογραφία με χρήση Η/Υ.

Άρθρο 8 Απάτη με χρήση Η/Υ.

23.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς [541]

Η Εθνική Υπηρεσία Ασφαλείας (GNS) [542] διευθύνεται από την Εθνική Αρχή Ασφαλείας η οποία είναι υπεύθυνη για την τεχνική επίβλεψη των διαδικασιών διαχείρισης της ασφάλειας των εθνικών πληροφοριών. Προεδρεύει της επιτροπής για την ασφάλεια στον κυβερνοχώρο στα πλαίσια της οποίας αναμένεται να δημιουργηθεί το μελλοντικό κέντρο Κυβερνοασφάλειας. Επίσης έχει αναλάβει το καθήκον της σύνταξης της Εθνικής Στρατηγικής Κυβερνοασφάλειας της Πορτογαλίας. Η Εθνική Υπηρεσία Επικοινωνιών (ANACOM) [543] είναι ο ρυθμιστής, του τομέα των επικοινωνιών στην Πορτογαλία. Η αρχή είναι υπεύθυνη για τη διασφάλιση της

συμμόρφωσης με το Νόμο για τις Ηλεκτρονικές Επικοινωνίες. Η Δικαστική Αστυνομία (PJ) [544] είναι το κύριο όργανο σε θέματα εγκλήματος στον κυβερνοχώρο. Η αποστολή της είναι να βοηθήσει τις δικαστικές αρχές στην πρόληψη, την ανίχνευση και τη διερεύνηση των κυβερνοεγκλημάτων. Ο δημόσιος οργανισμός για την Κοινωνία της Πληροφορίας UMIC [545] έχει ως αποστολή τον συντονισμό των πολιτικών. Επίσης είναι υπεύθυνος για την ασφάλεια και την προστασία της ιδιωτικότητας όσον αφορά τη χρήση του διαδικτύου και των ΤΠΕ.

Τέλος η Εθνική Επιτροπή Προστασίας Δεδομένων (CNPD) [546] είναι ένα ανεξάρτητο όργανο, με την εξουσία να επιβλέπει και να παρακολουθεί τη συμμόρφωση με τους νόμους και τους κανονισμούς στον τομέα της προστασίας των προσωπικών δεδομένων.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CERT.PT [547] είναι η εθνική CERT. Προτεραιότητές της είναι η προσφορά τεχνικής υποστήριξης στους χρήστες των υπολογιστών για την επίλυση περιστατικών ασφάλειας, η παροχή συμβουλών σχετικά με τις βέλτιστες πρακτικές, καθώς και ο συντονισμός των ενεργειών με τα ενδιαφερόμενα μέρη. Επίσης είναι υπεύθυνη για την παροχή πληροφοριών σχετικά με τις ευπάθειες και τις εν εξελίξει κακόβουλες δραστηριότητες, να ενεργεί με στόχο την ελαχιστοποίηση των επιπτώσεων των περιστατικών σε Εθνικό επίπεδο, να προωθεί τη δημιουργία νέων CERTs στην Πορτογαλία, και να συμβάλλει στην ενημέρωση και την ευαισθητοποίηση των χρηστών υπολογιστών στα θέματα ασφάλειας. Η CSIRT.FEUP [548] είναι η ομάδα του Πανεπιστήμιου του Πόρτο. Το πεδίο δράσης της αφορά τους χρήστες του δικτύου του πανεπιστημίου. Η DGS-IRT [549] δημιουργήθηκε από μια ομάδα ερευνητών από το CERT-IPN και το Πανεπιστήμιο της Κοΐμπρα. Μετά από πέντε χρόνια δραστηριότητας, μετατράπηκε σε ιδιωτική εταιρεία**.** Η CSIRTPT [550] του τηλεπικοινωνιακού παρόχου Portugal Telecom έχει ως αποστολή να συμβάλλει στην εθνική προσπάθεια στον κυβερνοχώρο εντός του Εθνικού Δικτύου CSIRTs. Ανταποκρίνεται κυρίως σε περιστατικά ασφάλειας των υπολογιστών, στο πλαίσιο των δικτύων και των υπηρεσιών που λειτουργούν με ευθύνη της Portugal Telecom. Επίσης συνεργάζεται για την αντιμετώπιση περιστατικών με την CERT.PT.

Ιδιωτικοί φορείς

Η ANETIE [551] είναι μια ένωση που δημιουργήθηκε με στόχο την προώθηση της σταθερής ανάπτυξης του κλάδου της πληροφορικής. Σήμερα συγκεντρώνει τις περισσότερες από τις εθνικές εταιρείες που δραστηριοποιούνται στους κλάδους των

ηλεκτρονικών, λογισμικού, επικοινωνιών και πληροφοριών. Από τα στρατηγικά ζητήματα της ANETIE είναι η καινοτομία, τα διπλώματα ευρεσιτεχνίας και η άμυνα απέναντι στο hacking. Στοχεύει στη συντονισμένη χρήση πόρων και μέσων - τεχνικών, ανθρώπινων και οικονομικών - προκειμένου να οδηγήσει, σε συνεργασία με τους ευρωπαϊκούς και διεθνείς ομολόγους της καταπολέμηση του hacking και της ηλεκτρονικής πειρατείας και στην υπεράσπιση της βιομηχανικής ιδιοκτησίας [552].

Η APRITEL [553] είναι η ένωση των εταιρειών τηλεπικοινωνιών που δραστηριοποιούνται στην Πορτογαλία. Στις αρμοδιότητές της περιλαμβάνεται η προώθηση ενός νομικού και κανονιστικού περιβάλλοντος στον τομέα των ηλεκτρονικών επικοινωνιών.

Ακαδημαϊκοί φορείς

Το FNSC [554] είναι το δίκτυο έρευνας των πανεπιστημίων της Πορτογαλίας. Στα καθήκοντά συγκαταλέγεται η λειτουργία της CERT.PT. Το Πανεπιστήμιο της Λισαβώνας διεξάγει μεταπτυχιακό πρόγραμμα στην ασφάλεια της πληροφορικής. Με το πανεπιστήμιο συνεργάζονται αρκετές εταιρείες του χώρου με σκοπό την έρευνα. Η Portugal Telecom έχει δημιουργήσει ένα εργαστήριο με σκοπό την πρακτική εκπαίδευση σε θέματα ασφάλειας.

Συνεργασία μεταξύ φορέων

Συνολικά οι μηχανισμοί ανταλλαγής πληροφοριών δεν είναι ακόμη πολύ ώριμοι στην Πορτογαλία. Ο κύριος οργανισμός που εργάζεται προς αυτή την κατεύθυνση είναι η Εθνική Αρχή Επικοινωνιών. Ωστόσο, τα τελευταία χρόνια έχει δημιουργηθεί ένα φόρουμ για τη συνεργασία και το συντονισμό μεταξύ των ομάδων CSIRT της Πορτογαλίας, το οποίο έχει ως στόχους να δημιουργήσει ένα περιβάλλον συνεργασίας και αμοιβαίας βοήθειας για την αντιμετώπιση περιστατικών, την ανταλλαγή ορθών πρακτικών ασφάλειας, και την ανάπτυξη δεικτών και εθνικών στατιστικών στοιχείων σχετικά με συμβάντα ασφάλειας. Το δίκτυο αποτελείται από δέκα φορείς CSIRT των τηλεπικοινωνιών, την εθνική άμυνα, τον τραπεζικό κλάδο και την ακαδημαϊκή κοινότητα[555]. Μεταξύ του δημόσιου και του ιδιωτικού τομέα δεν υπάρχει ιδιαίτερα αναπτυγμένη συνεργασία. Μοναδική εξαίρεση είναι η συνεργασία μεταξύ του CERT.PT και των ISP , σχετικά με την αναφορά παράνομων δραστηριοτήτων [556].

23.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Στην Πορτογαλία μέτρα ευαισθητοποίησης και ενημέρωσης λαμβάνονται τόσο από τον δημόσιο τομέα όσο και από ιδιωτικές επιχειρήσεις, ακαδημαϊκούς φορείς και ΜΚΟ. Υπάρχουν αρκετές ενημερωτικές ιστοσελίδες που παρέχουν ενημέρωση σχετικά με τα spam ή / και τα κακόβουλα προγράμματα, συμπεριλαμβανομένων και συμβουλών για την καλύτερη αντιμετώπισή τους. Ενημερώσεις σε θέματα ασφάλειας πληροφοριών δημοσιεύονται επίσης στους δικτυακούς τόπους των πορτογαλικών τραπεζών και καλύπτουν θέματα που σχετίζονται με ενημερώσεις ασφαλείας, χρήση κωδικών πρόσβασης, τους κανόνες που αφορούν την παροχή προσωπικών, εμπιστευτικών και ευαίσθητων πληροφορίων μέσω ηλεκτρονικού ταχυδρομείου ή με οποιοδήποτε άλλο μέσο κλπ. Επιπρόσθετα μια σειρά από πρωτοβουλίες έχουν αναληφθεί στην Πορτογαλία όσον αφορά την ευαισθητοποίηση σχετικά με την ασφάλεια στο διαδίκτυο, όπως η "Internet Segura [557]" (ασφαλές διαδίκτυο) η οποία είναι μια κοινοπραξία φορέων (UMIC, Υπουργείο Παιδείας, FCCN, Microsoft Πορτογαλίας) με σκοπό την ευαισθητοποίηση σχετικά με την ασφάλεια του web και έχει τέσσερις βασικούς στρατηγικούς στόχους την καταπολέμηση του παράνομου περιεχομένου, την ελαχιστοποίηση των επιπτώσεων του παράνομου και επιβλαβούς περιεχομένου για τους πολίτες, την προώθηση της ασφαλούς χρήσης του διαδικτύου και την αύξηση της ευαισθητοποίησης σχετικά με τους κινδύνους από τη χρήση του διαδικτύου. Διοργανώνει τακτικά δραστηριότητες με τη μορφή των συνόδων ευαισθητοποίησης, σεμινάρια, διαλέξεις και, επίσης, προωθεί και υποστηρίζει συγκεκριμένες εκστρατείες (ετήσιες εθνικές εκστρατείες σε σχολεία και άλλα δίκτυα διάδοσης) όπως της ημέρας για ασφαλέστερη χρήση του διαδικτύου και η παγκόσμια ημέρα τηλεπικοινωνιών και Κοινωνίας της Πληροφορίας. Επίσης προωθεί δραστηριότητες ευαισθητοποίησης στα σχολεία και την εκπαιδευτική κοινότητα [558].

Στην Πορτογαλία πραγματοποιήθηκε το 2012 η εθνική άσκηση κυβερνοάμυνας COMPOR 2012 [28].

23.5 Διεθνής Συνεργασία

Η Πορτογαλία συνεργάζεται με ευρωπαϊκούς και διεθνείς οργανισμούς σε θέματα που αφορούν την ασφάλεια των υπολογιστών όπως ο ENISA, και η Αρχή Διαχείρισης Κυβερνοάμυνας του ΝΑΤΟ. Κύριοι εκπρόσωποι της χώρας είναι η Εθνική Υπηρεσία Ασφαλείας και η Εθνική Υπηρεσία Επικοινωνιών (ANACOM) [215]. Η CERT.PT

παρακολούθησε για Τρίτη συνεχόμενη χρονιά την άσκηση Cyber Coalition 2013 το μεγαλύτερο τεστ ετοιμότητας κατά των απειλών στον κυβερνοχώρο στα πλαίσια του NATO[559][560]. Επίσης η CERT.PT και η η ANACOM συμμετέχουν από το 2010 στην ευρωπαϊκή άσκηση Cyber Europe.[561][562]. Επιπλέον η CERT.PT είναι μέλος του διεθνούς φόρουμ FIRST [32].

Κεφάλαιο 24ο

Ρουμανία

24.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Με το Ψήφισμα. 271/2013 τον Μάιο του 2013 εγκρίθηκε η Στρατηγική για την Ασφάλεια στον Κυβερνοχώρο της Ρουμανίας [563], ένα εθνικό σχέδιο δράσης για την υλοποίηση ενός εθνικού συστήματος ασφάλειας στον κυβερνοχώρο. Η Στρατηγική θέτει ως στόχους την προσαρμογή των κανονιστικών και θεσμικών πλαισίων λαμβάνοντας υπ' οψιν τις απειλές κυβερνοχώρο, την εξασφάλιση της ανθεκτικότητας των υποδομών στον κυβερνοχώρο, την ανάπτυξη της γνώσης, της πρόληψης και της ικανότητας εξουδετέρωσης των τρωτών σημείων, των κινδύνων και των απειλών για την ασφάλεια στον κυβερνοχώρο της Ρουμανίας. Επίσης στοχεύει στην προώθηση και την ανάπτυξη της συνεργασίας μεταξύ του δημόσιου και του ιδιωτικού τομέα σε εθνικό και διεθνή επίπεδο, τη ανάπτυξη ευαισθητοποίησης στον πληθυσμό για τα τρωτά σημεία, τους κινδύνους και τις απειλές στον κυβερνοχώρο. Τέλος έχει ως στόχο την ενεργό συμμετοχή σε πρωτοβουλίες των διεθνών οργανισμών στους οποίους η Ρουμανία θα έχει ρόλο στον καθορισμό και στη θέσπιση μιας σειράς μέτρων που θα αποσκοπούν στην αύξηση του επιπέδου εμπιστοσύνης στον κυβερνοχώρο.

24.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [564]

Ο νόμος 677/2001 θεσπίστηκε για την προστασία των ατόμων όσον αφορά την επεξεργασία προσωπικών δεδομένων και την ελεύθερη κυκλοφορία των δεδομένων. Συμπληρώθηκε από τις πρόσφατες προσθήκες του νόμου (244/23.03.2005 OJ.) που επικυρώνει τη Σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, και τη διασυνοριακή ροή δεδομένων. Επιπλέον, η Εθνική Εποπτική Αρχή για την επεξεργασία δεδομένων προσωπικού χαρακτήρα ιδρύθηκε το 2005 με τον Νόμο. 102/2005 (O.J. αριθ. 391 / 09.05.2005). Όλα τα αρχεία προστασίας δεδομένων που τηρούνται έχουν παραδοθεί στην Αρχή, η οποία

εποπτεύει και ελέγχει τη νομιμότητα της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σύμφωνα με το Νόμο 677/2001.

Νομοθεσία ηλεκτρονικού εμπορίου [564]

Ο νόμος 365/2002 εγκρίθηκε τον Ιούνιο του 2002 και τροποποιήθηκε τον Μάιο του 2006 και μεταφέρει τις βασικές διατάξεις της οδηγίας 2000/31/ΕΚ για το ηλεκτρονικό εμπόριο. Καθορίζει το ηλεκτρονικό εμπόριο και άλλες βασικές έννοιες, όπως την αποστολή ηλεκτρονικών μηνυμάτων ή την ανταλλαγή δεδομένων μέσω του Διαδικτύου. Τα βασικά του σημεία είναι η ελεύθερη κυκλοφορία των υπηρεσιών της κοινωνίας της πληροφορίας, οι συμβάσεις που συνάπτονται με ηλεκτρονικά μέσα, και οι εμπορικές επικοινωνίες με ηλεκτρονικά μέσα. Επιπλέον, ορίζει αυστηρές ποινές για την κατοχή εξοπλισμού για την παραποίηση των ηλεκτρονικών μέσων πληρωμής.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [564]

Η Ρουμανία ήταν η πρώτη χώρα στην Ευρώπη που μετέφερε στην εθνική νομοθεσία το κανονιστικό πλαίσιο της Ευρωπαϊκής Ένωσης για τις ηλεκτρονικές επικοινωνίες. Τον Ιανουάριο του 2002, η κυβέρνηση ενέκρινε το διάταγμα σχετικά με την πρόσβαση στα δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς εγκαταστάσεις, καθώς και τη διασύνδεσή τους (αρ. 34/2002). Οι διατάξεις του οργανώνονται γύρω από τον καθορισμό νέων εννοιών που σχετίζονται με τις ηλεκτρονικές επικοινωνίες, τα δικαιώματα και τις υποχρεώσεις των φορέων εκμετάλλευσης, των εξουσιών της εθνικής ρυθμιστικής αρχής και της δυνατότητας να επιβάλει συγκεκριμένες υποχρεώσεις σε φορείς εκμετάλλευσης με σημαντική ισχύ στην αγορά.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Η Ρουμανία επικύρωσε τη σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο στις 12 Μαΐου του 2004 αφού πρώτα εναρμόνισε την εθνική της νομοθεσία ψηφίζοντας το 2003 τον νόμο για την καταπολέμηση της διαφθοράς [565]. Αυτός περιλαμβάνει τα εξής άρθρα:

Άρθρο 42 Παράνομη πρόσβαση.

Άρθρο 43 Παράνομη υποκλοπή.

Άρθρο 44 Παράνομη αλλοίωση, διαγραφή ή τη φθορά των ηλεκτρονικών δεδομένων, Μη εξουσιοδοτημένη μεταφορά δεδομένων.

Άρθρο 45 Παρεμβολή σε δεδομένα, παρεμβολή σε σύστημα.

24.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Υπουργείο Συγκοινωνιών και Κοινωνίας της Πληροφορίας [566] είναι υπεύθυνο για τον καθορισμό των πολιτικών αναδιάρθρωσης, το συντονισμό της διαδικασίας ιδιωτικοποίησης στον τομέα των ΤΠΕ, τη χρηματοδότηση των κυριότερων έργων μετάβασης της ρουμανικής κοινωνίας σε μια κοινωνία της πληροφορίας και την προώθηση της ανάπτυξης του διαδικτύου. Επιπλέον, είναι αρμόδιο για την εναρμόνιση της ειδικής νομοθεσίας με αυτή της Ευρωπαϊκής Ένωσης και για το συντονισμό της εφαρμογής των πολιτικών και των στρατηγικών. Στη Ρουμανική Υπηρεσία Πληροφοριών (SRI) [567] έχει ανατεθεί η αποστολή της πρόληψης και της αντιμετώπισης των κυβερνοεπιθέσεων κατά κρίσιμων υποδομών του κράτους όπως οι τηλεπικοινωνίες ή το διαδίκτυο, ή είναι ουσιαστικής σημασίας για τη λειτουργία των άλλων κρίσιμων υποδομών (π.χ. αεροπορικές, σιδηροδρομικές ή οδικές μεταφορές υποδομών, ενέργειας, φυσικού αερίου, πετρελαίου ή συστήματα υδροδότησης , ιατρικές υπηρεσίες, χρηματοπιστωτικό και τραπεζικό σύστημα, κ.λπ.). Μετά τον χαρακτηρισμό της ως εθνική αρχή κυβερνοάμυνας από το Ανώτατο Συμβούλιο Εθνικής Άμυνας, η SRI δημιούργησε μια εξειδικευμένη δομή, το Εθνικό Κέντρο Κυβερνοάμυνας. Το Υπουργείο Άμυνας [568] έχει τμήματα σχετικά με τον τομέα της Ασφάλειας των Πληροφοριών και των Ηλεκτρονικών. Η Υπηρεσία για το Έγκλημα στον Κυβερνοχώρο [569] είναι μια εξειδικευμένη δομή της Ρουμανικής Αστυνομίας, που έχει την αρμοδιότητα να αποτρέπει και να έρευνα το έγκλημα στον κυβερνοχώρο. Η Υπηρεσία λειτουργεί 24/7, για να διασφαλίζει τη διεθνή συνεργασία και τη λήψη επειγόντων μέτρων σε περιπτώσεις ηλεκτρονικού εγκλήματος, μαζί με την Υπηρεσία Καταπολέμησης του Οργανωμένου εγκλήματος και της Τρομοκρατίας DIICOT [570]. Η Ειδική Υπηρεσία Τηλεπικοινωνιών [571] είναι η κεντρική εξειδικευμένη υπηρεσία, η οποία οργανώνει και συντονίζει τις δραστηριότητες στον τομέα των τηλεπικοινωνιών ειδικά για τις ρουμανικές δημόσιες αρχές και άλλους χρήστες όπως προβλέπεται από το νόμο. Το ίδρυμα έχει στρατιωτική οργάνωση και αποτελεί μέρος του εθνικού συστήματος άμυνας. Οι ειδικές τηλεπικοινωνίες περιλαμβάνουν μεταδόσεις και εκπομπές σημάτων, κείμενα, εικόνες, ήχους ή πληροφορίες οποιασδήποτε φύσεως , που μεταδίδονται μέσω καλωδίου, ραδιοκυμάτων, οπτικών συστημάτων ή άλλων ηλεκτρομαγνητικών συστημάτων. Η Εθνική Εποπτική Αρχή για την Επεξεργασία

Δεδομένων Προσωπικού Χαρακτήρα [572] είναι μια δημόσια αρχή, αυτόνομη και ανεξάρτητη από οποιαδήποτε αρχή της δημόσιας διοίκησης, καθώς και από οποιοδήποτε φυσικό ή νομικό πρόσωπο από τον ιδιωτικό τομέα. Η Αρχή έχει θέσει ως στόχο την προστασία των θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων και ειδικότερα το δικαίωμα της στενής, οικογενειακής και ιδιωτικής ζωής, σε σχέση με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών. Το τμήμα Επικοινωνιών και Πληροφορικής του Υπουργείου Εσωτερικών [573] είναι μια εξειδικευμένη μονάδα που οργανώνει, συντονίζει και ελέγχει το έργο των υπηρεσιών των επικοινωνιών και της πληροφορικής. Στο υπουργείο Εσωτερικών λειτουργεί επίσης Τμήμα Προστασίας Υποδομών Ζωτικής Σημασίας.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CERT-RO [574] είναι το εθνικό σημείο επαφής για τη διασφάλιση της ανάπτυξης και της διάδοσης των δημόσιων πολιτικών για την πρόληψη και την αντιμετώπιση περιστατικών ασφάλειας των υποδομών στον κυβερνοχώρο. Η CERT-RO υποστηρίζεται από μια συντονιστική επιτροπή που αποτελείται από εκπροσώπους: του Υπουργείου Συγκοινωνιών και Κοινωνίας της Πληροφορίας, Υπουργείου Άμυνας, Υπουργείου Εσωτερικών, της Υπηρεσίας Πληροφοριών της Ρουμανίας, της Ειδικής Τηλεπικοινωνιακής Υπηρεσίας και άλλων δημόσιων αρχών. Η CORIS-STS [575] είναι ο φορέας που έχει οριστεί για την πρόληψη και την αντιμετώπιση περιστατικών ασφάλειας που σχετίζονται με τα πληροφοριακά συστήματα των δημόσιων αρχών του ρουμανικού κράτους. Η RoCSIRT [576] είναι η Ομάδα του ερευνητικού δικτύου AARNIEC / RoEduNet. Παρέχει υποστήριξη σε όλα τα συνδεδεμένα ιδρύματα (ερευνητικά κέντρα, πανεπιστήμια, γυμνάσια, δημοτικά σχολεία, κλπ). Επιπλέον μπορεί να παρέχει υπηρεσίες σε άλλες οντότητες εντός της Ρουμανίας.

Ιδιωτικοί φορείς

Η Εθνική Ένωση Παρόχων Υπηρεσιών Διαδικτύου στη Ρουμανία (ANISP) [577] έχει εκπονήσει θέσεις για τα πιο σημαντικά θέματα που αφορούν την ανάπτυξη και τη λειτουργία του τομέα των ηλεκτρονικών επικοινωνιών, όπως η ανάπτυξη του νέου κανονιστικού πλαισίου στον τομέα των ηλεκτρονικών επικοινωνιών σε επίπεδο Ε.Ε. η προστασία των δεδομένων, η διατήρηση δεδομένων ; το έγκλημα στον κυβερνοχώρο και το ασφαλές διαδίκτυο. Ο Σύνδεσμος Πληροφορικής και Επικοινωνιών [578] Οργανώνει και αναπτύσσει την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των

μελών του, για την ανάπτυξη και τη συζήτηση των στρατηγικών προσανατολισμών και των νομοθετικών πρωτοβουλιών.

Ακαδημαϊκοί φορείς

Η Στρατιωτική Τεχνική Ακαδημία [579] μέσω του Τμήματος Ηλεκτρονικής και Συστημάτων Πληροφορικής παρέχει εκπαίδευση και διεξάγει έρευνα σε θέματα που αφορούν την ασφάλεια της πληροφορικής και των επικοινωνιών. Το Εθνικό Ίδρυμα Ερευνών Επικοινωνιών [580] διεξάγει έρευνα στην ασφάλεια δικτύων και το Εθνικό Ινστιτούτο Έρευνας και Ανάπτυξης στην Πληροφορική [581] που είναι το πιο σημαντικό ερευνητικό ινστιτούτο στην ανάπτυξη και την καινοτομία στους τομείς της πληροφορικής και των επικοινωνιών στη Ρουμανία, διαθέτει τμήμα που ασχολείται με την ασφάλεια των υπολογιστών.

Συνεργασία μεταξύ φορέων

Ολα τα περιστατικά ασφάλειας στον κυβερνοχώρο, πρέπει να αναφέρονται / συλλέγονται σύμφωνα με το Σύστημα Έγκαιρης Προειδοποίησης το οποίο διαχειρίζεται η CERT-RO σε συνεργασία με άλλα ιδρύματα της Ρουμανίας που έχουν ευθύνη για την ασφάλεια στον κυβερνοχώρο, όπως η Ρουμανική Υπηρεσία Πληροφοριών και η Ειδική Υπηρεσία Τηλεπικοινωνιών [582].

24.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Το έργο Sigur.Info [581] αποτελεί μέρος του κοινοτικού προγράμματος για την προώθηση της χρήσης του διαδικτύου και των νέων τεχνολογιών με μεγαλύτερη ασφάλεια. Το Sigur.Info περιλαμβάνει δραστηριότητες ευαισθητοποίησης και προώθησης ενός ασφαλέστερου διαδικτύου, μια γραμμή συμβουλών (Helpline) για επιζήμια προβλήματα του διαδικτύου και μια γραμμή αναφοράς (hotline) για την καταγγελία παράνομου περιεχομένου στις ιστοσελίδες της Ρουμανίας. Με το secure.info.org συνεργάζονται οι μεγάλοι πάροχοι τηλεπικοινωνιών και πληροφορικής της Ρουμανίας. Η CERT-RO παρέχει επίσης στην ιστοσελίδα της ειδοποιήσεις σχετικές με θέματα ασφάλειας των υπολογιστών, ενώ παράλληλα διοργανώνει αρκετές εκδηλώσεις όπως το ετήσιο συνέδριο του Εθνικού Κέντρου για την αντιμετώπιση περιστατικών Cyber Security [583] και το ετήσιο forum Προστασίας Προσωπικών Δεδομένων [584]. Επίσης έχει μια διεύθυνση e-mail, που χρησιμεύει ως one-stop-shop για το κοινό που θέλει να αναφέρει παράνομη online δραστηριότητα [585].

24.5 Διεθνής Συνεργασία

Η Ρουμανία συνεργάζεται με τις υπόλοιπες χώρες της Ευρωπαϊκής Ένωσης στα πλαίσια οργανισμών όπως ο ENISA και η Europol. Κύριοι φορείς συνεργασίας είναι το Υπουργείο Συγκοινωνιών και Κοινωνίας της Πληροφορίας και η CERT-RO. Η Ρουμανία συμμετέχει στη Ευρωπαϊκή άσκηση Cyber Europe,καθώς και σε άλλες δραστηριότητες που διοργανώνονται από τον ENISA [586][587]. Παράλληλα η CERT-RO έχει συνάψει συμφωνίες συνεργασίας με αντίστοιχα CERT της Ουγγαρίας και της Κίνας και παρέχει βοήθεια στη Βοσνία-Ερζεγοβίνη στη δημιουργία του δικού της CERT[23]. Επίσης είναι διαπιστευμένο μέλος TI, και μέλος του FIRST ενώ η RoCSIRT είναι μέλος του δικτύου CEENET [79][24b]. Ακόμη η Ρουμανία στα πλαίσια του NATO συμμετέχει στις συμμαχικές δραστηριότητες όπως η άσκηση Cyber Coalition [587][589]. Τέλος η Ρουμανία είναι μέλος του οργανισμού IMPACT [33].

Κεφάλαιο 25ο

Σλοβακία

25.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Ο σκοπός της Εθνικής Στρατηγικής για την Ασφάλεια Πληροφοριών [590] είναι η θέσπιση ενός πλαισίου ασφάλειας των πληροφοριών στη Σλοβακική Δημοκρατία. Η Στρατηγική θέτει τρεις στόχους:

- Την Πρόληψη, με σκοπό να επιτευχθεί η κατάλληλη προστασία του ψηφιακού χώρου της Σλοβακίας και να ελαχιστοποιηθεί η εμφάνιση των περιστατικών ασφαλείας.
- Την Ετοιμότητα, μέσω της ανάπτυξης ικανοτήτων αποτελεσματικής αντιμετώπισης περιστατικών ασφάλειας, προκειμένου να ελαχιστοποιηθούν οι επιπτώσεις τους και να καταστεί δυνατή η έγκαιρη ανάκτηση των κατεστραμμένων συστημάτων
- Το Βιώσιμο επίπεδο ασφάλειας πληροφοριών με την κατασκευή, συντήρηση και ανάπτυξη της τεχνογνωσίας που απαιτείται για την προστασία του ψηφιακού χώρου της Σλοβακίας.

Η στρατηγική καθορίζει σημεία εκκίνησης, κατανέμει τις αρμοδιότητες και προτείνει τους στόχους, τις προτεραιότητες και τα μέτρα που πρέπει να ληφθούν προκειμένου να επιτευχθεί ο συνολικός σκοπός. Η στρατηγική περιλαμβάνει επίσης μια βασική περιγραφή των επιμέρους εργασιών με στόχο την εξασφάλιση της προστασίας του συνόλου του ψηφιακού χώρο , με την εξαίρεση των διαβαθμισμένων πληροφοριών που εμπίπτουν στην αρμοδιότητα της Σλοβακικής Εθνικής Αρχής Ασφάλειας. Πρόκειται, ειδικότερα για μέτρα για την αποφυγή της διαρροής πληροφοριών και της μη εξουσιοδοτημένης χρήσης, τη παραβίαση της ακεραιότητας των δεδομένων, τη παραβίαση του δικαιώματος των πολιτών στην προστασία των προσωπικών δεδομένων, μέτρα για την προστασία από τη φθορά και την κατάχρηση των συστημάτων πληροφόρησης και επικοινωνίας, καθώς και μέτρα για την εφαρμογή των ισχυόντων νόμων της Σλοβακίας και της ΕΕ

25.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [591]

Ο νόμος περί Ασφάλειας Πληροφοριών εγκρίθηκε από την κυβέρνηση με το ψήφισμα αριθ. 136/2010. Ο κύριος σκοπός του είναι να προσδιοριστεί τη βασική δομή και το ουσιαστικό επίκεντρο της ασφάλειας των πληροφοριών, εξασφαλίζοντας ικανοποιητικό επίπεδο προστασίας σε όλο το χώρο στη Σλοβακίας.

Ο νόμος αριθ. 428/2002 περί προστασίας προσωπικών δεδομένων εφαρμόζει τις αρχές που καθορίζονται στην οδηγία προστασίας δεδομένων της ΕΕ (95/46/ΕΚ). Σύμφωνα με το νόμο, τα άτομα μπορούν να έχουν πρόσβαση στις προσωπικές πληροφορίες που κατέχουν οι δημόσιοι και ιδιωτικοί φορείς. Ο νόμος επιβάλλεται από το Γραφείο για την Προστασία Προσωπικών Δεδομένων.

Νομοθεσία ηλεκτρονικού εμπορίου [591]

Ο νόμος για το ηλεκτρονικό εμπόριο τέθηκε σε ισχύ την 1η Φεβρουαρίου του 2004 ρυθμίζει τις σχέσεις μεταξύ των φορέων παροχής υπηρεσιών της κοινωνίας της πληροφορίας και των δικαιούχων που μπορεί να προκύψουν όταν η επικοινωνία λαμβάνει χώρα εξ αποστάσεως.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [591]

Ο νόμος περί ηλεκτρονικών επικοινωνιών, τέθηκε σε ισχύ την 1η Ιανουαρίου 2004, για να μεταφέρει στη Σλοβακία το Κανονιστικό Πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Το 2005 η Σλοβακία τροποποίησε τον Ποινικό Κώδικα [592][593], ώστε να είναι συμβατός με τη σύμβαση του Συμβουλίου της Ευρώπης στην οποία προσχώρησε το 2007. Στο άρθρο 247 προβλέπονται τα αδικήματα σχετικά με το έγκλημα στον κυβερνοχώρο:

Άρθρο 247 Παράνομη προσπέλαση, παρεμβολή σε δεδομένα, παρεμβολή σε σύστημα, παράνομη υποκλοπή, κακή χρήση ηλεκτρονικών συσκευών, απάτη με Η/Υ, πλαστογραφία με Η/Υ.

25.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Η Εθνική Αρχή Ασφαλείας (NBU) [594] είναι ο επίσημος οργανισμός για την προστασία των διαβαθμισμένων πληροφοριών, τις υπηρεσίες κρυπτογράφησης και ηλεκτρονικής υπογραφής. Οι ρόλοι της περιλαμβάνουν, μεταξύ άλλων: έκδοση αδειών ασφαλείας για τον χειρισμό διαβαθμισμένων πληροφοριών (για φυσικά πρόσωπα, και νομικά πρόσωπα), φορέας πιστοποίησης για τα τεχνικά συστήματα διασφάλισης και για τις ηλεκτρονικές υπογραφές, κεντρικά γραφεία κρυπτογράφησης, αρχή πιστοποίησης ρίζας και διαπίστευση των αρχών πιστοποίησης. Είναι επίσης η Εθνική Αρχή Κυβερνοάμυνας και σε αυτόν τον ρόλο είναι υπεύθυνη για τη διατομεακή ομάδα εργασίας που συγκροτήθηκε για τον συντονισμό με το NATO σε δραστηριότητες που σχετίζονται με την κυβερνοάμυνα στη Σλοβακία. Η κοινωνία της πληροφορίας ανήκει στις περιοχές που εποπτεύονται από το Υπουργείο Οικονομικών[595], το οποίο είναι υπεύθυνο για την ασφάλεια των μη διαβαθμισμένων συστημάτων. Οι αρμοδιότητες του υπουργείου περιλαμβάνουν την ευθύνη για την προστασία των κρίσιμων υποδομών στον τομέα της πληροφορικής και των τεχνολογιών επικοινωνίας, την προετοιμασία των εγγράφων στρατηγικής, τα πρότυπα, τις προτάσεις, τις απόψεις και άλλα έγγραφα για τα πληροφοριακά συστήματα της δημόσιας διοίκησης και την ασφάλειά τους. Επίσης αναλύει και αξιολογεί την κατάσταση της ασφάλειας της δημόσιας διοίκησης. Τέλος αντιπροσωπεύει τη δημόσια διοίκηση σε φορείς της Ευρωπαϊκής Ένωσης σε θέματα σχετικά με την ασφάλεια των πληροφοριών. Στο Υπουργείο Οικονομικών υπάγεται επίσης η Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Υπολογιστών (CSIRT.SK). Το Υπουργείο Εσωτερικών [596] μέσω του τμήματος πολιτικής άμυνας έχει αναλάβει καθήκοντα που σχετίζονται με την προετοιμασία των στρατηγικών, το συντονισμό και τον έλεγχο στους τομείς της διαχείρισης κρίσεων και την προστασία των κρίσιμων υποδομών. Στις δομές του Αστυνομικού Σώματος [597] υπάρχει το Ινστιτούτο Εγκληματολογικών Επιστημών, Τμήμα Ανάλυσης Δεδομένων το οποίο ασχολείται με ιατροδικαστικές έρευνες των συστημάτων πληροφορικής και επικοινωνιών διαθέτοντας εμπειρογνώμονες κυβερνοεγκλημάτων. Το Υπουργείο Άμυνας [598] εκπροσωπεί την Σλοβακία στο NATO και στο CCDCoE με δικούς στου εμπειρογνώμονες. Το Γραφείο για την Προστασία Προσωπικών Δεδομένων της Δημοκρατίας της Σλοβακίας [599] είναι μια ανεξάρτητη κρατική αρχή, που εποπτεύει την προστασία των προσωπικών δεδομένων και συμβάλλει στην προστασία των

θεμελιωδών δικαιωμάτων και ελευθεριών των φυσικών προσώπων όσον αφορά την επεξεργασία των προσωπικών τους δεδομένων.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CSIRT.SK [600] είναι η εθνική ομάδα, τα βασικά καθήκοντα της οποίας περιλαμβάνουν αντιμετώπιση των περιστατικών ασφάλειας, σε συνεργασία με τους ιδιοκτήτες και τους πάροχους των εθνικών υποδομών ζωτικής σημασίας και των τηλεπικοινωνιών, ευαισθητοποίηση στον τομέα της ασφάλειας των πληροφοριών, συνεργασία με τους ξένους ομολόγους και οργανώσεις και εκπροσώπηση της Σλοβακίας στον τομέα της ασφάλειας των πληροφοριών σε διεθνές επίπεδο. Η CSIRT.SK, είναι επιφορτισμένη με την παροχή υπηρεσιών, κυρίως για την κυβέρνηση προκειμένου να ανταποκριθεί σε περιστατικά ασφάλειας πληροφορικής που αφορούν εθνικές κρίσιμες υποδομές, καθώς και σε υπηρεσίες της δημόσιας διοίκησης.

Ιδιωτικοί φορείς

Υπάρχουν δύο επαγγελματικές κοινότητες που επικεντρώνονται στην ασφάλεια των πληροφοριών ή σχετίζονται με το συγκεκριμένο τομέα.

Η Σλοβακική ένωση για την ασφάλεια των πληροφοριών (SASIB)[601] και ο Σύλλογος Πληροφορικής της Σλοβακίας (ITAS) [602]. Ο στόχος της SASIB είναι η ανάπτυξη της γνώσης και της συνειδητοποίησης της νομοθεσίας για την ασφάλεια και η εξειδίκευση των μελών της στην ασφάλεια των πληροφοριών και την προστασία λογισμικού. Η ITAS είναι μια ένωση που εκπροσωπεί τις τοπικές και διεθνείς εταιρείες πληροφορικής που δραστηριοποιούνται στον τομέα των ΤΠΕ στη Σλοβακία.

Ακαδημαϊκοί φορείς

Το Τμήμα Επιστήμης Υπολογιστών του Πανεπιστημίου Comenius της Μπρατισλάβα[603], προσφέρει μαθήματα και διεξάγει έρευνα σχετικά με την Ασφάλεια της πληροφορικής και την κρυπτογραφία.

Συνεργασία μεταξύ φορέων

Η Εθνική Αρχή Ασφαλείας, αναγνωρίζεται μεταξύ των ενδιαφερομένων στη Σλοβακική Δημοκρατία ως φορέας εθνικής ασφάλειας υπεύθυνος για την περιοχή των διαβαθμισμένων πληροφοριών. Για μη διαβαθμισμένες πληροφορίες, το Υπουργείο Οικονομικών είναι ο κύριος υπεύθυνος. Ένα συμβουλευτικό και συντονιστικό συμβούλιο έχει συσταθεί από το Υπουργείο Οικονομικών της Σλοβακικής Δημοκρατίας για τη διευκόλυνση της αμοιβαίας επικοινωνίας. Η CSIRT.SK ανταποκρίνεται στα περιστατικά ασφάλειας πληροφοριών στη Σλοβακική Δημοκρατία,

σε συνεργασία με τους ιδιοκτήτες και τους παρόχους των εθνικών υποδομών ζωτικής σημασίας, τους φορείς τηλεπικοινωνιών, και άλλους δημόσιους φορείς (αστυνομία, δικαστικό σώμα), και συνεργάζεται με τους διεθνείς ομολόγους και οργανισμούς στον τομέα της ασφάλειας των πληροφοριών σε διεθνές επίπεδο.

25.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Το πρόγραμμα της Ε.Ε. για ασφαλέστερη χρήση του διαδικτύου είναι επίσης ενεργό στη Σλοβακία με το όνομα www.zodpovedne.sk. Το έργο επικεντρώνεται στην ασφαλή και υπεύθυνη χρήση του Διαδικτύου, κινητών τηλεφώνων και άλλων νέων τεχνολογιών και επιδιώκει να διαδώσει συμβουλές και βοήθεια. κυρίως σε νέους και παιδιά. Στα πλαίσια του έργου λειτουργεί η γραμμή υποστήριξης Pomoc.sk, για συμμετοχή σε διεθνή καθώς και ένα εθνικού κέντρο για την καταγγελία παράνομου περιεχομένου και δραστηριοτήτων με την ονομασία Stopline.sk. Η SASIB συμβάλλει επίσης στην αύξηση της ευαισθητοποίησης και της τεχνογνωσίας των μελών της, στον τομέα της ασφάλειας των πληροφοριών και λογισμικού προστασίας. Η δραστηριότητά της συμπληρώνεται από την ετήσια διοργάνωση του συνεδρίου τοπικού χαρακτήρα «Ασφάλειας πληροφοριών» με την υποστήριξη της εταιρείας προϊόντων και υπηρεσιών ασφάλειας υπολογιστών ESET [601]. Το 2011 η CSIRT.SK οργάνωσε την πρώτη εθνική άσκηση σε κρίσιμες πληροφορίες στην προστασία των υποδομών (SISE 2011) [28]. Εκτός από το Υπουργείο Οικονομικών και τη CSIRT.SK συμμετείχαν επίσης το Υπουργείο Εσωτερικών, το Γραφείο της κυβέρνησης της Σλοβακίας και η Ρυθμιστική Αρχή Τηλεπικοινωνιών.

25.5 Διεθνής Συνεργασία

Το Υπουργείο Οικονομικών, το Υπουργείο Εσωτερικών και η CSIRT.SK αντιπροσωπεύουν τη Σλοβακία στους αντίστοιχους διεθνείς οργανισμούς συνήθως μέσα από τις δομές της ΕΕ και του ΝΑΤΟ. Οι ειδικοί κυβερνοάμυνας του ΥΕΘΑ συμμετείχαν ενεργά στις Ασκήσεις Κυβερνοάμυνας (CDX NATO).[604], Lock Shields [605] και Cyber Coalition [606]. Επίσης η Σλοβακία είναι μέλος του CCDCoE. Η Σλοβακία συμμετέχει επίσης στην άσκηση Cyber Europe και στην άσκηση μεταξύ Ε.Ε. και Η.Π.Α Cyber Atlantic [607]. Τέλος η Σλοβακία συμμετέχει στον οργανισμό IMPACT [33].

Κεφάλαιο 26ο

Σλοβενία

26.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Σλοβενία δεν έχει δημοσιεύσει κάποια στρατηγική ή πολιτική σχετικά με την προστασία του κυβερνοχώρου της. Στο παρελθόν έχει εκδώσει στρατηγικές [608] σχετικά με την ανάπτυξη της ηλεκτρονικής διακυβέρνησης, στις οποίες, ενώ γίνεται αναφορά στην προστασία των δεδομένων και των υποδομών, δεν περιγράφεται κάποιος σχεδιασμός ή μέτρα τα οποία θα πρέπει να ληφθούν.

26.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [609]

Ο νόμος περί προστασίας δεδομένων προσωπικού χαρακτήρα, εκδόθηκε τον Ιούλιο του 2004 και τέθηκε σε ισχύ την 1η Ιανουαρίου 2005. Μεταφέρει την οδηγία 95/46/ΕΚ της ΕΕ σχετικά με την προστασία των δεδομένων στο σλοβενικό δίκαιο. Ο κύριος στόχος του νόμου είναι να αποτρέψει την παράνομη παραβίαση της ιδιωτικής ζωής και να διασφαλίσει την προστασία των προσωπικών δεδομένων.

Νομοθεσία ηλεκτρονικού εμπορίου [609]

Τέθηκε σε ισχύ στις 22 Αυγούστου 2000 και ρυθμίζει τη δημιουργία, τη χρήση, τα δικαιώματα και τις υποχρεώσεις των εταιρειών και των ατόμων, καθώς και την αξιοπιστία και την προστασία της ψηφιακής υπογραφής. Η Εθνική Αρχή Ασφαλείας είναι ο κεντρικός κρατικός φορέας διαχείρισης των ηλεκτρονικών υπογραφών.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [609]

Ο νόμος περί ηλεκτρονικών επικοινωνιών τέθηκε σε ισχύ την 1η Μαΐου 2004 και αποσκοπεί στην καθιέρωση αποτελεσματικού ανταγωνισμού στην αγορά ηλεκτρονικών επικοινωνιών, τη διαχείριση της χρήσης του φάσματος ραδιοσυχνοτήτων, τη διασφάλιση καθολικών υπηρεσιών και την προστασία των δικαιωμάτων των χρηστών. Ο νόμος αυτός καλύπτει όλα τα σχετικά θέματα που

περιέχονται στις οδηγίες της ΕΕ που αποτελούν το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [610]

Ο Ποινικός Κώδικας της Σλοβενίας περιλαμβάνει άρθρα σχετικά με εγκλήματα στον κυβερνοχώρο της Σλοβενίας:

Άρθρο 154-2 Παράνομη Πρόσβαση σε Η/Υ.

Άρθρο 225-1 Παράνομη υποκλοπή.

Άρθρο 225-2 Παράνομη Πρόσβαση σε πληροφοριακό σύστημα, Παρεμβολή σε δεδομένα, παρεμβολή σε σύστημα, Παράνομη τροποποίηση δεδομένων.

Άρθρο 242-1 Παράνομη Πρόσβαση σε πληροφοριακό σύστημα, Παρεμβολή σε δεδομένα, παρεμβολή σε σύστημα, Παράνομη τροποποίηση δεδομένων.

26.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Υπουργείο Παιδείας, Επιστημών και Αθλητισμού μέσω της Γενικής Διεύθυνσης της Κοινωνίας της Πληροφορίας [611] συντονίζει την εφαρμογή του προγράμματος για την ανάπτυξη της κοινωνίας της πληροφορίας. Έργα της είναι η νομοθεσία στον τομέα των ηλεκτρονικών, το Ακαδημαϊκό και Ερευνητικό Δίκτυο της Σλοβενίας (ARNES) και η τήρηση μητρώου των αρχών πιστοποίησης. Επίσης είναι υπεύθυνη για την υλοποίηση των υπαρχουσών στρατηγικών αλλά και για τη σχεδίαση νέων. Είναι ο κύριος φορέας συνεργασίας στις ΤΠΕ εντός Σλοβενίας και η κύρια επαφή συνεργασίας με διεθνείς εταίρους. Η διεύθυνση προωθεί την ασφαλή χρήση του Διαδικτύου και την ασφάλεια των πληροφοριών μέσω του Κέντρο Ασφαλούς Διαδικτύου SAFE.SI και της Σλοβενικής CERT. Το Υπουργείο Δημόσιας Διοίκησης, [612] είναι υπεύθυνο για την ηλεκτρονική διακυβέρνηση της χώρας. Η Υπηρεσία Δικτύων και Υπηρεσιών (AKOS) [613] είναι ένα ανεξάρτητο όργανο που ρυθμίζει και εποπτεύει την αγορά ηλεκτρονικών επικοινωνιών, διαχειρίζεται και επιβλέπει το φάσμα των ραδιοσυχνοτήτων στη Δημοκρατία της Σλοβενίας. Το Κυβερνητικό γραφείο για την προστασία των διαβαθμισμένων πληροφοριών [614] είναι αρμόδιο για την εφαρμογή των μέτρων ασφαλείας για την προστασία των διαβαθμισμένων πληροφοριών, που υποβάλλονται σε επεξεργασία, αποθηκεύονται και διαβιβάζονται σε ηλεκτρονικά συστήματα. Ο Επίτροπος Πληροφοριών [615] εποπτεύει την προστασία των προσωπικών δεδομένων και την πρόσβαση στις δημόσιες πληροφορίες. Τέλος, η

Εθνική Υπηρεσία Ερευνών [616] είναι μια εξειδικευμένη μονάδα ποινικής έρευνας σε εθνικό επίπεδο για την ανίχνευση και τη διερεύνηση σοβαρών ποινικών αδικημάτων, συμπεριλαμβανομένων των εγκλημάτων του κυβερνοχώρου.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η SI-CERT [617][618] είναι το εθνικό κέντρο απόκρισης για την αντιμετώπιση περιστατικών στον τομέα της ασφάλειας των ηλεκτρονικών δικτύων και των πληροφοριών. Εκτελεί υπηρεσίες συντονισμού σε περιστατικά, παρέχει τεχνικές συμβουλές σε εισβολές, και άλλες καταχρήσεις, και εκδίδει προειδοποιήσεις για τους διαχειριστές δικτύων και το ευρύ κοινό σχετικά με τις τρέχουσες απειλές για τα ηλεκτρονικά δίκτυα. Το SI-CERT διεκπεραιώνει το εθνικό πρόγραμμα ευαισθητοποίησης «Ασφάλεια στο Διαδίκτυο» και λαμβάνει μέρος στο πρόγραμμα SAFE-SI. Η SI-CERT λειτουργεί εντός του Ακαδημαϊκού και Ερευνητικού Δικτύου της Σλοβενίας (ARNES).

Ιδιωτικοί φορείς

Το Εμπορικό Επιμελητήριο [619] εκπροσωπεί τα συμφέροντα των επιχειρήσεων στις σχέσεις τους με την κυβέρνηση και τα συνδικάτα. Μέλος του επιμελητηρίου είναι και η Ένωση Παρόχων διαδικτύου. Επίσης στο επιμελητήριο λειτουργεί τμήμα για τη διαχείριση της ασφάλειας των πληροφοριών [620]. Το τμήμα προωθεί λύσεις ασφαλείας για της επιχειρήσεις δίνοντας έμφαση στο πρότυπο ISO 27001:2005.

Ακαδημαϊκοί φορείς

Το Ακαδημαϊκό και Ερευνητικό Δίκτυο της Σλοβενίας (Arnes) [621] παρέχει υπηρεσίες δικτύου σε οργανισμούς έρευνας, εκπαίδευσης και πολιτισμού. Το κέντρο υποστηρίζει τη SI-CERT καθώς και το πρόγραμμα ευαισθητοποίησης SAFE.SI.

Το Κέντρο Μεθοδολογίας και Πληροφορικής του Πανεπιστημίου της Λιουμπλιάνας υποστηρίζει το πρόγραμμα « Χρήση του διαδικτύου στη Σλοβενία» (RIS) [622]. Στα πλαίσια του έργου οργανώνονται δράσεις ευαισθητοποίησης για την ασφαλή χρήση του διαδικτύου.

Συνεργασία φορέων

Στην αντιμετώπιση περιστατικών η SI-CERT προσδιορίζει την αρχική αιτία του συμβάντος διευκολύνει την επικοινωνία με άλλους δικτυακούς τόπους που μπορεί να εμπλέκονται κάνοντας αναφορές σε άλλες CSIRTs και συνθέτοντας ανακοινώσεις προς τους χρήστες, κατά περίπτωση.

26.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Το Έργο Ασφάλεια στο Διαδίκτυο [623] υλοποιείται από τη SI-CERT και χρηματοδοτείται εξ ολοκλήρου από το Υπουργείο Παιδείας, Επιστημών και Αθλητισμού. Οι δραστηριότητές του στοχεύουν στην ευαισθητοποίηση των Σλοβένων χρηστών του διαδικτύου σχετικά με τις διάφορες απειλές που αντιμετωπίζουν στο διαδίκτυο, στην ενημέρωση σχετικά με την ασφαλή χρήση του online banking και των online αγορών, και στην ενημέρωση για την προστασία της προσωπικής ταυτότητας. Το Κέντρο για ασφαλέστερη χρήση του διαδικτύου SAFE.SI [624][625] που χρηματοδοτείται από την Ευρωπαϊκή Επιτροπή και το Υπουργείο Παιδείας, Επιστημών και αθλητισμού είναι ένα σημείο ευαισθητοποίησης σχετικά με την ασφαλή χρήση του διαδικτύου και των νέων τεχνολογιών, με μια μεγάλη βάση πληροφορίων, συμβουλών, φυλλαδίων, βίντεο, και άλλων υλικών σε θέματα ασφαλούς χρήσης του διαδικτύου και κινητών τηλεφώνων. Το κέντρο παρέχει μια τηλεφωνική γραμμή συμβουλών καθώς και έναν ιστότοπο αναφοράς επιβλαβούς περιεχομένου. Το εμπορικό επιμελητήριο διοργανώνει εκδηλώσεις και δράσεις ενημέρωσης με σκοπό την ενίσχυση της θέσης των επιχειρήσεων όσον αφορά την ασφάλεια των πληροφοριών[626]. Τέλος το έργο VarnostNaSpletu.si [627] του Ινστιτούτου Νέων Επιχειρηματιών σε συνεργασία με το πρόγραμμα «Χρήση του διαδικτύου στη Σλοβενία», στοχεύει στην ευαισθητοποίηση και στην εκπαίδευση των χρηστών του διαδικτύου. Η ιστοσελίδα δημοσιεύει εβδομαδιαία νέα σχετικά με την ασφάλεια της πληροφορικής.

26.5 Διεθνής Συνεργασία

Το Υπουργείο Οικονομικών, η Εθνική Αρχή Ασφαλείας και η SI-CERT αντιπροσωπεύουν την Σλοβενία στους αντίστοιχους διεθνείς οργανισμούς συνήθως μέσα από τις δομές της ΕΕ και του NATO. Η SI-CERT είναι μέλος του FIRST, διαπιστευμένο μέλος TI και το σημείο επαφής για τη συνεργασία με τον ENISA[628]. Το 2012 συμμετείχε στην άσκηση Cyber Europe [629][630]. Η Σλοβενία συμμετέχει επίσης στον οργανισμό IMPACT και ως μέλος του NATO συμμετέχει στην άσκηση κυβερνοάμυνας Cyber Coalition[630] [631].

Κεφάλαιο 27ο

Σουηδία

27.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η κυβέρνηση ανέθεσε στον MSB (Οργανισμός για την πολιτική προστασία και την ετοιμότητα) να συντάξει ένα εθνικό σχέδιο δράσης για την ασφάλεια των πληροφοριών[632]. Το σχέδιο δημοσιεύτηκε το 2008 και επικαιροποιήθηκε το 2010. Το σχέδιο δημιουργήθηκε σε συνεργασία με μια σειρά από άλλες αρχές και φορείς και αποτελείται από δέκα κύρια σημεία-στόχους:

1. Ανάπτυξη της θέσης της Σουηδίας στην Ευρωπαϊκή Ένωση και σε διεθνές πλαίσιο.
2. Δημιουργία εμπιστοσύνης, αξιοπιστίας, ασφάλειας και αυξημένης προστασίας της ακεραιότητας.
3. Ενθάρρυνση για την αυξημένη χρήση της πληροφορικής.
4. Πρόληψη και αύξηση της ικανότητας αντιμετώπισης διαταραχών στα συστήματα επικοινωνιών.
5. Ενίσχυση των υπηρεσιών πληροφοριών και των υπηρεσιών ασφάλειας και βελτίωση της ανταλλαγής πληροφοριών.
6. Ενίσχυση του τομέα της εθνικής ασφάλειας.
7. Αξιοποίηση των δυνατοτήτων της κοινωνίας.
8. Εστίαση σε ζωτικές κοινωνικές λειτουργίες.
9. Αυξημένη συνειδητοποίηση των κινδύνων ασφάλειας
10. Διασφάλιση των απαραίτητων πόρων για της αρμόδιες αρχές.

Για την επίτευξη των στόχων η στρατηγική προτείνει συγκεκριμένα μέτρα και κατευθύνσεις και καθορίζει τις αρμόδιες αρχές για την υλοποίηση τους.

27.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [633]

Ο νόμος περί προσωπικών δεδομένων θεσπίστηκε για να μεταφέρει στη σουηδική την οδηγίας περί προστασίας δεδομένων της ΕΕ 95/46/ΕΚ. Ο νόμος απαριθμεί ορισμένες βασικές απαιτήσεις σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα. Οι απαιτήσεις αυτές περιλαμβάνουν, μεταξύ άλλων, ότι τα προσωπικά δεδομένα μπορούν να τύχουν επεξεργασίας μόνο για συγκεκριμένο, ρητά και δικαιολογημένο σκοπό και αν το πρόσωπο που έχει καταχωρηθεί δίνει τη συγκατάθεσή του / της. Εξαιρέσεις σε αυτόν τον κανόνα περιλαμβάνουν την άσκηση δημόσιας εξουσίας, ή την εκπλήρωση της νομικής υποχρέωσης από τον υπεύθυνο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα.

Νομοθεσία ηλεκτρονικού εμπορίου [633]

Η πράξη μεταφέρει την οδηγία της ΕΕ 2000/31/ΕΚ σχετικά με ορισμένες νομικές πτυχές των υπηρεσιών της κοινωνίας της πληροφορίας, ιδίως του ηλεκτρονικού εμπορίου («οδηγία για το ηλεκτρονικό εμπόριο»). Καθορίζει τις υποχρεώσεις των παρόχων υπηρεσιών και ρυθμίζει την επεξεργασία των πληροφοριών του διαδίκτυο.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [633]

Σκοπός του νόμου είναι να παρέχει στους πολίτες και τις δημόσιες αρχές πρόσβαση σε ασφαλείς και αποτελεσματικές ηλεκτρονικές επικοινωνίες. Επίσης να διασφαλιστεί ότι οι ηλεκτρονικές επικοινωνίες είναι στη διάθεση των πολιτών σε όλες τις περιοχές της Σουηδίας.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Ο Σουηδικός Ποινικός Κώδικας περιγράφει τα αδικήματα τα οποία σχετίζονται με το έγκλημα στον κυβερνοχώρο:[634]

Κεφάλαιο 8, Τμήμα 8: Παρεμβολή σε δεδομένα, παρεμβολή σε σύστημα

Κεφάλαιο 4, Τμήμα 9γ: Παράνομη προσπέλαση, Παράνομη υποκλοπή, Παράνομη τροποποίηση δεδομένων

27.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το SAMFI [635] είναι ένα δίκτυο συνεργασίας των αρχών με συγκεκριμένες κοινωνικές ευθύνες για την ασφάλεια των πληροφοριών, όπως προσδιορίζονται από τη κυβέρνηση. Οι αρχές που συμμετέχουν στο δίκτυο είναι:

Ο Σουηδικός Οργανισμός Απρόοπτων Γεγονότων (MSB) [636] αναπτύσσει την προστασία του ατόμου και την ικανότητα της κοινωνίας για την πρόληψη και την αντιμετώπιση καταστάσεων έκτακτης ανάγκης και καταστροφών. Επιπλέον, παρέχει συμβουλές και υποστήριξη σε άλλες αρχές, δήμους, περιφερειακά συμβούλια και οργανισμούς του ιδιωτικού τομέα. Επίσης κάνει προτάσεις προς την κυβέρνηση που μπορούν να οδηγήσουν στην ανάγκη για λήψη μέτρων και είναι υπεύθυνος για τη διαχείριση της εθνικής στρατηγικής και των σχεδίων δράσης για την ασφάλεια των πληροφοριών. Ο MSB έχει το δικαίωμα να εκδίδει κανονισμούς για τις κυβερνητικές αρχές. Το έργο του MSB για θέματα που σχετίζονται με την ασφάλεια σε βιομηχανικά συστήματα πληροφόρησης και ελέγχου διεξάγεται στο πλαίσιο ενός τριετούς προγράμματος. Ο στόχος του προγράμματος είναι να δημιουργήσει δυνατότητες πρόληψης και αντιμετώπισης των κινδύνων και των απειλών κατά των πληροφοριακών συστημάτων ιδιαίτερα αυτών των υποδομών ζωτικής σημασίας. Τέλος, ο MSB αποφασίζει ποιες πολιτικές αρχές και άλλες ζωτικές κοινωνικές υπηρεσίες θα πρέπει να χρησιμοποιούν υπηρεσίες κρυπτογράφησης για να καταστεί δυνατή η ασφαλής διατομεακή συνεργασία. Το δίκτυο SAMFI και το CERT.SE λειτουργούν με πόρους του MSB. Ο Οργανισμός Ταχυδρομείων και Τηλεπικοινωνιών (PTS) [637] είναι ένας ανεξάρτητος οργανισμός για την ασφάλεια των επικοινωνιών στο πλαίσιο του νόμου περί Ηλεκτρονικών Επικοινωνιών. Παρακολουθεί τις υπηρεσίες ηλεκτρονικών επικοινωνιών και των ταχυδρομικών υπηρεσιών στη Σουηδία και λειτουργεί ως αρχή για τη ρύθμιση της ασφάλειας στις ηλεκτρονικές επικοινωνίες (τηλεπικοινωνίες, διαδίκτυο και το ραδιόφωνο) και στη χρήση των ηλεκτρονικών υπογραφών. Η Εθνική Υπηρεσία Άμυνας Ραδιοσυχνοτήτων (FRA) [638] παρέχει υπηρεσίες στην κυβέρνηση, τις Σουηδικές Ένοπλες Δυνάμεις και άλλες επιλεγμένες κυβερνητικές αρχές και κρατικές εταιρείες. Η FRA είναι μια πολιτική αρχή που υπάγεται στο Υπουργείο Άμυνας, έχει υψηλή τεχνογνωσία στον τομέα της ασφάλειας των πληροφοριών και βοηθά στον εντοπισμό των παραγόντων που σχετίζονται με απειλές σε κρίσιμα συστήματα, εφαρμόζει λύσεις ασφαλείας και παρέχει τεχνική στήριξη. Η Υπηρεσία Ασφαλείας της Σουηδίας (SAPO) [639] προλαμβάνει και ανιχνεύει εγκλήματα κατά της εθνικής ασφάλειας, καταπολεμά την τρομοκρατία και προστατεύει την κεντρική κυβέρνηση. Οι δραστηριότητές της περιλαμβάνουν την προστασία της Σουηδίας στον κυβερνοχώρο. Ο Φορέα Πιστοποίησης Ασφάλειας Πληροφορικής (CSEC) [640] της Διοίκηση Αμυντικού Υλικού (FMV) είναι υπεύθυνος για ένα σύστημα αξιολόγησης και

πιστοποίησης των προϊόντων ασφαλείας. Η Στρατιωτική Υπηρεσία Πληροφοριών και Ασφάλειας (MUST) [641] συγκεντρώνει και αναλύει πληροφορίες σχετικές με την ασφάλεια, συμπεριλαμβανομένων των απειλών κατά των πληροφοριακών συστημάτων.

Το Εθνικό Γραφείο Ερευνών (NBI) της Σουηδικής Αστυνομίας [642] καταπολεμά σοβαρές μορφές οργανωμένου εγκλήματος, συμπεριλαμβανομένων των εγκλημάτων στον κυβερνοχώρο τόσο σε εθνικό όσο και σε διεθνές επίπεδο. Η Επιθεώρηση Δεδομένων [643] εποπτεύει την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CERT SE [644] είναι η Εθνική CERT της Σουηδίας, και είναι υπεύθυνη για τις κυβερνητικές αρχές, τις περιφερειακές αρχές, τους Δήμους τις Επιχειρήσεις και τις Εταιρείες. Επιπλέον η CERT-SE είναι η Κυβερνητική CERT της Σουηδίας και έχει πρόσθετες ευθύνες μέσα στο Κυβερνητικό σώμα. Η LiU IRT [645] είναι Ομάδα που χειρίζεται θέματα ασφαλείας του Πανεπιστήμιου του Linköping. Η SIST [646] (SNIC IT Security Team) συντονίζει και στηρίζει το προσωπικό ασφαλείας πληροφορικής στο πλαίσιο της SNIC (Σουηδική Εθνική Υποδομή Πληροφορικής) Η TS-CERT [647] ανήκει στον τηλεπικοινωνιακό πάροχου Teliasonera, η Handelsbanken SIRT στην τράπεζα Handelsbanken και η Swedbank CERT στην τράπεζα Swedbank.

Ιδιωτικοί φορείς

Η Ένωση Σουηδικών βιομηχανιών πληροφορικής και τηλεπικοινωνιών [648] προωθεί την αυξημένη χρήση της πληροφορικής στη Σουηδία και παρέχει ζωτική υποστήριξη στην ανάπτυξη των μελών της. Η SIG security [649] είναι μια ένωση επαγγελματιών που εργάζονται στον τομέα της πληροφορικής και της ασφάλειας των πληροφοριών.

Ακαδημαϊκοί φορείς

Το Πανεπιστήμιο της Στοκχόλμης [650] με το τμήμα Επιστήμης Υπολογιστών διεξάγει έρευνα σχετικά με την ασφάλεια του κυβερνοχώρου με στόχο την ασφάλεια και την προστασία της ιδιωτικής ζωής και τη συνολική αύξηση της ανθεκτικότητας και της αξιοπιστίας του χώρου. Το Πανεπιστήμιου του Linköping [651] διεξάγει έρευνα στην ασφάλεια της πληροφορικής και διατηρεί την δική του ομάδα CERT. Το Σουηδικό Ινστιτούτο Επιστήμης Υπολογιστών (SICS) [652] είναι ένας ερευνητικός οργανισμός με έμφαση στην εφαρμοσμένη επιστήμη των υπολογιστών και διεξάγει έρευνα σχετικά με την ασφάλεια των συστημάτων και την προστασία των προσωπικών δεδομένων.

Συνεργασία μεταξύ φορέων

Εκπρόσωποι από τις αρχές που συμμετέχουν στο δίκτυο SAMFI συνεδριάζουν περίπου 6 φορές το χρόνο για να συζητήσουν τις τρέχουσες εργασίες και τα θέματα στον τομέα της ασφάλειας των πληροφοριών. Μέσα από την ανταλλαγή πληροφοριών και τη συνεργασία τους οι αρχές αλληλοϋποστηρίζονται στο έργο τους για την ασφάλεια των πληροφοριών. Μέσω του SAMFI, οι αρχές σχηματίζουν ομάδες εργασίας για να εργαστούν σε τρέχοντα θέματα.

27.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Από το 2004 σουηδικό Συμβούλιο των ΜΜΕ ίδρυσε το κέντρο της Σουηδίας για ασφαλέστερη χρήση του διαδικτύου [653] ως κέντρο ευαισθητοποίησης. Δημοσιεύει πληροφοριακό υλικό και λειτουργεί γραμμή υποστήριξης μέσω τηλεφώνου, email και chat υπηρεσιών. Ο δικτυακός τόπος φιλοξενεί επίσης ένα φόρουμ υποστήριξης peer-to-peer. Το συνέδριο Nordic IT security πραγματοποιείται σε ετήσια βάση και συγκεντρώνει εταιρίες , επαγγελματίες και εμπειρογνώμονες του χώρου. Στη Σουηδία έχουν διοργανωθεί από το MSB οι ασκήσεις κυβερνοάμυνας NISÖ 2010 [654] και Telö 11 [655] NISÖ 2012 [656] με μεγάλη συμμέτοχή από τον δημόσιο και ιδιωτικό τομέα.

27.5 Διεθνής Συνεργασία

Η Σουηδία μέσω της συνεργασίας Nordic εργάζεται μαζί με τις υπόλοιπες σκανδιναβικές χώρες για κοινή άμυνα στον κυβερνοχώρο. Μέσω του δικτύου NORDUnet τα CERT των σκανδιναβικών χωρών ανταλλάσσουν πληροφορίες κοινού ενδιαφέροντος [80][657]. Επιπλέον, ως μέλος της Ε.Ε. η Σουηδία συνεργάζεται με τα υπόλοιπα μέλη για την προστασία του κυβερνοχώρου. Ο MSB συμμετείχε το 2010 και το 2012 στην κοινή ευρωπαϊκή άσκηση Cyber Europe [658]. Συμμετοχή είχε ακόμη στην άσκηση Cyber Storm που διοργανώνεται από τις Η.Π.Α. [253]. Όσον αφορά τη συνεργασία των ομάδων CERT, η CERT-SE είναι μέλος της ομάδας Ευρωπαϊκών κυβερνητικών CERT [31]. Οι CERT-SE, TS-CERT, SUNet CERT, είναι μέλη του διεθνούς φόρουμ συνεργασίας FIRST[32].

Κεφάλαιο 28ο

Τσεχία

28.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας

Η Στρατηγική της Τσεχικής Δημοκρατίας στον τομέα της κυβερνητικής ασφάλειας για το 2012–2015[659] αναπτύχθηκε από την κυβέρνηση της Τσεχικής Δημοκρατίας λόγω της παγκόσμια αύξησης των απειλών στον κυβερνοχώρο. Η στρατηγική πηγάζει από προσπάθειες κυβερνητικών φορέων για αύξηση του επίπεδου της κυβερνητικής ασφάλειας. Η στρατηγική προβλέπει δράσεις για την ενίσχυση της κυβερνητικής ασφάλειας στα κρατικά όργανα, στις κρίσιμες υποδομές, στον εμπορικό τομέα καθώς και στους πολίτες. Επίσης καθορίζει τους στόχους και τα συμφέροντα της Τσεχικής Δημοκρατίας για τη δημιουργία μιας αξιόπιστης κοινωνίας της πληροφορίας. Οι βασικές αρχές της στρατηγικής της κυβερνητικής ασφάλειας είναι η διασύνδεση και η ενίσχυση της συνεργασίας όλων των τμημάτων της κοινωνίας, η ατομική ευθύνη, η διυπουργική συνεργασία, η διεθνής συνεργασία και η επάρκεια των εγκεκριμένων μέτρων. Για την υλοποίηση της στρατηγικής ορίζονται συγκεκριμένοι στόχοι και μέτρα όπως η δημιουργία νομοθετικού πλαισίου, η καθιέρωση Εθνικού CERT, η προστασία των υποδομών πληροφοριών ζωτικής σημασίας η ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων της δημόσιας διοίκησης, η αποτελεσματικότητα της καταπολέμησης της εγκληματικότητας στον κυβερνοχώρο, ο συντονισμός των δραστηριοτήτων, η αύξηση του επιπέδου ευαισθητοποίησης η ανταπόκριση στις κυβερνοεπιθέσεις.

28.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [660]

Η Πράξη Προστασίας Δεδομένων (No.101/2000) εγκρίθηκε τον Απρίλιο του 2000 με σκοπό την προστασία του δικαιώματος των πολιτών στην ιδιωτικότητα. Καθορίζει τα δικαιώματα και τις υποχρεώσεις όσον αφορά την επεξεργασία δεδομένων προσωπικού χαρακτήρα και επιπλέον καθορίζει τις προϋποθέσεις υπό τις οποίες τα προσωπικά

δεδομένα μπορούν να μεταφερθούν σε άλλες χώρες. Επίσης, επιτρέπει στα άτομα να έχουν πρόσβαση και δικαίωμα διόρθωσης των προσωπικών στοιχείων που βρίσκονται στην κατοχή δημόσιων και ιδιωτικών φορέων.

Νομοθεσία ηλεκτρονικού εμπορίου[660]

Ο νόμος περί ορισμένων υπηρεσιών της κοινωνίας της πληροφορίας (αριθ. 480/2004 Coll.) εγκρίθηκε στις 7 Σεπτεμβρίου 2004 και τέθηκε σε ισχύ τον ίδιο μήνα με σκοπό να συμβάλει στην ανάπτυξη του ηλεκτρονικού εμπορίου.

Νομοθεσία για τις ηλεκτρονικές επικοινωνίες [660]

Ο νόμος περί ορισμένων υπηρεσιών της κοινωνίας της πληροφορίας (αριθ. 480/2004 Coll.) εγκρίθηκε από το Κοινοβούλιο στις 22 Φεβρουαρίου 2005 και τέθηκε σε ισχύ την 1η Μαΐου 2005. Ο νόμος μεταφέρει το κανονιστικό πλαίσιο της ΕΕ για τις ηλεκτρονικές επικοινωνίες στο εθνικό δίκαιο.

Νομοθεσία για το έγκλημα στον κυβερνοχώρο

Η πρόταση για την τροποποίηση της νομοθεσίας για να είναι σύμφωνη με τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο ολοκληρώθηκε στις 5 Φεβρουαρίου 2005. Οι ακόλουθες ισχύουσες διατάξεις του Ποινικού Κώδικα, αφορούν αυτού του είδους τα εγκλήματα:

Ποινικός Κώδικας [661]

Άρθρο 257α Παράνομη πρόσβαση, παρεμβολή σε δεδομένα, παρεμβολή συστήματος.

Άρθρο 239 Παράνομη υποκλοπή.

Άρθρο 250 Απάτη με Η/Υ.

28.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Τον Οκτώβριο του 2011, η κυβέρνηση της Τσεχίας με το ψήφισμα αριθ. 781 του συντάγματος όρισε την Εθνική Υπηρεσία Ασφαλείας [662] υπεύθυνη για την ασφάλεια στον κυβερνοχώρο. Το Εθνικό Κέντρο Κυβερνοασφάλειας (NCKB) [663] συστάθηκε βάση του ίδιου ψηφίσματος ως μονάδα της Εθνικής Αρχής Ασφάλειας. Ο ρόλος του κέντρου είναι να συντονίζει τη συνεργασία σε εθνικό και διεθνές επίπεδο για την αποτροπή των επιθέσεων στον κυβερνοχώρο, καθώς και το σχεδιασμό και την έγκριση μέτρων για την αντιμετώπιση συμβάντων. Το Γραφείο Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (OPPD) [664] είναι ένας ανεξάρτητος οργανισμός που

επιβλέπει τη συμμόρφωση με το νόμο κατά την επεξεργασία δεδομένων προσωπικού χαρακτήρα, διατηρεί ένα μητρώο επεξεργασίας δεδομένων προσωπικού χαρακτήρα και δέχεται υποδείξεις και παράπονα των πολιτών σε περιπτώσεις παράβασης του νόμου. Το Υπουργείο Εσωτερικών [665] είναι αρμόδιο για θέματα της δημόσιας διοίκησης, της εσωτερικής ασφάλειας, της προστασίας των συνόρων, για τη διαχείριση κρίσεων και την ηλεκτρονική διακυβέρνηση στην Τσεχική Δημοκρατία. Η Υπηρεσία Ασφάλειας Πληροφοριών (BIS) [666] είναι μια μυστική υπηρεσία της Τσεχικής Δημοκρατίας που δραστηριοποιείται και στον τομέα της ασφάλειας των πληροφοριακών συστημάτων και επικοινωνιών. Βασικός στόχος της είναι να μειωθεί η ευπάθεια των συστημάτων ηλεκτρονικών επικοινωνιών, η αποτροπή πιθανών επεισοδίων, και ο εντοπισμός των δυνητικά επιτιθέμενων - και τα κίνητρά τους. Οι αρμοδιότητες της καθορίζονται από την «Εθνική Στρατηγική για την Ασφάλεια Πληροφοριών». Η Αστυνομία της Τσεχικής Δημοκρατίας [667] μέσω του Τμήματος Ηλεκτρονικού Εγκλήματος είναι υπεύθυνη για την παρακολούθηση και διερεύνηση των εγκληματικών δραστηριοτήτων σε σχέση την πληροφορική. Τα καθήκοντά του τμήματος περιλαμβάνουν την εξέταση στοιχείων στο διαδίκτυο, καθώς και την υποστήριξη άλλων υπηρεσιών.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13][668]

Η CSIRT.CZ [669] είναι η Εθνική CSIRT της Τσεχικής Δημοκρατίας και έχει ως στόχους τη παροχή υπηρεσιών ασφάλειας όπως αντιμετώπιση περιστατικών ασφάλειας, εκπαίδευση και προληπτικές υπηρεσίες στον τομέα της ασφάλειας. Είναι υπεύθυνη για το σύνολο της Τσεχικής Δημοκρατίας. Η GOVCERT.CZ [670] είναι η κυβερνητική CERT και λειτουργεί υπό το Εθνικό Κέντρο Κυβερνοασφάλειας. Η CESNET [671] είναι η ομάδα του συλλόγου των πανεπιστήμιων και των ακαδημιών της Τσεχικής Δημοκρατίας. Η CSIRT-MU[672] είναι μια ομάδα ασφαλείας του Masaryk University. Ασχολείται όχι μόνο με λύσεις σε προβλήματα ασφάλειας, αλλά και με την ανίχνευση τέτοιων περιστατικών στο δίκτυο υπολογιστών του πανεπιστημίου καθώς και με την ευαισθητοποίηση των χρηστών. Η ACTIVE24-CSIRT[673] είναι η ομάδα της ACTIVE 24,εταιρείας web hosting στην Τσεχική Δημοκρατία. Η SEZNAM.CZ-CSIRT [674] είναι μια ιδιωτική CERT που προσφέρει τις υπηρεσίες εντός της Τσεχικής Δημοκρατίας και τέλος η CZ.NIC-CSIRT είναι η ομάδα της CZ.NIC, μιας ένωσης συμφερόντων νομικών προσώπων, που ιδρύθηκε το 1998 από τους κορυφαίους παρόχους υπηρεσιών διαδικτύου.

Ιδιωτικοί φορείς

Η CZ.NIC Association [675] είναι η Ένωση των κορυφαίων πάροχων υπηρεσιών διαδικτύου αριθμώντας 79 μέλη. Ο Σύλλογος για την Πληροφορική και τις Τηλεπικοινωνίες [676] είναι μια επαγγελματική ένωση των εταιρειών της πληροφορικής και των ηλεκτρονικών επικοινωνιών, η οποία αποσκοπεί στην ευαισθητοποίηση για τη σημασία και τη χρήση της σύγχρονης τεχνολογίας των πληροφορικής στην κοινωνία, συμπεριλαμβανομένης της δημιουργίας των βέλτιστων συνθηκών για την ανάπτυξη των δημόσιων δικτύων ηλεκτρονικών επικοινωνιών στην Τσεχική Δημοκρατία. Ο Network Security Monitoring Cluster (NSM Cluster) είναι ένας συνεργατικός βιομηχανικός όμιλος με επίκεντρο την ασφάλεια των δικτύων και την ασφάλεια στον τομέα των ΤΠΕ.

Ακαδημαϊκοί φορείς

Ο CESNET [671] είναι ένας σύλλογος των πανεπιστημίων και των ακαδημιών της Τσεχικής Δημοκρατίας. Ο κύριος στόχος του είναι η έρευνα και η ανάπτυξη των τεχνολογιών της πληροφορικής και των επικοινωνιών. Το Ινστιτούτο Πληροφορικής του Masaryk University [677] έχει αναλάβει να δημιουργήσει ένα κέντρο αριστείας για την κατάρτιση και την εκπαίδευση σχετικά με την πρόληψη και την καταστολή του εγκλήματος στον κυβερνοχώρο. Το Czech Technical University in Prague [678] διεξάγει μεταπτυχιακό πρόγραμμα σχετικά με την ασφάλεια των υπολογιστών και συνεργάζεται στην έρευνα με τη Cisco [679].

Συνεργασία μεταξύ φορέων

Σύμφωνα με την απόφαση της κυβέρνησης της Τσεχικής Δημοκρατίας 781 της 19ης Οκτωβρίου 2011, η αρχή που είναι υπεύθυνη για τον τομέα της κυβερνητικής ασφάλειας είναι η εθνική αρχή ασφαλείας. Είναι υπεύθυνη για την πιστοποίηση των πληροφοριακών συστημάτων, για την έγκριση των σχεδίων ασφάλειας, των συστημάτων επικοινωνιών και για το χειρισμό διαβαθμισμένων πληροφοριών. Επίσης το Συμβούλιο Κυβερνοασφάλειας στο οποίο προεδρεύει ο υπουργός εσωτερικών διαδραματίζει καίριο ρόλο στον διυπουργικό συντονισμό. Σύμφωνα με το καταστατικό του, το Συμβούλιο συγκροτεί ομάδες εργασίας που αποτελούνται από εμπειρογνώμονες του τομέα. Οι ομάδες εργασίας θα ασχολούνται με συγκεκριμένα ζητήματα της κυβερνητικής ασφάλειας. Το CSIRT.CZ, συντονίζει την αντιμετώπιση περιστατικών ασφαλείας στα δίκτυα υπολογιστών της Τσεχικής Δημοκρατίας. Η CSIRT.CZ

συνεργάζεται με άλλους οργανισμούς, όπως το CERT-CESNET και CZNIC-CSIRT που την βοηθούν στην επίτευξη των στόχων της.

28.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Η ιστοσελίδα www.saferinternet.cz του Εθνικού Κέντρου Κυβερνοασφάλειας λειτουργεί από το 2009 και είναι μια προσπάθεια που υποστηρίζεται από την Ευρωπαϊκή Επιτροπή στο πλαίσιο του προγράμματος Safer Internet. Επίσης το Εθνικό Κέντρο Κυβερνοασφάλειας σε συνεργασία με τους εταίρους του, διοργανώνει συνέδρια, σεμινάρια, και διαλέξεις, επικεντρωμένα στην ασφαλέστερη χρήση του Διαδικτύου και την πρόληψη του εγκλήματος στον κυβερνοχώρο. Ακόμη παρέχει επικαιροποιημένες πληροφορίες σχετικά με τις εξελίξεις στον τομέα της τεχνολογίας και των κινδύνων που εμφανίζονται. Στην Τσέχική Δημοκρατία διεξάγονται επίσης σε ετήσια βάση μια σειρά από συνέδρια που αφορούν την ασφάλεια στον κυβερνοχώρο. Η CYTER [680] διάσκεψη για το έγκλημα στον κυβερνοχώρο και την τρομοκρατία, καλύπτει ευρύ φάσμα θεμάτων της τρομοκρατίας και του εγκλήματος στον κυβερνοχώρο. Το IT Security Workshop [681] έχει ως στόχο την εκπαίδευση των επαγγελματιών που ασχολούνται με την ασφάλεια της πληροφορικής στην αντιμετώπιση των κινδύνων. Τέλος η διεθνής διάσκεψη για την ασφάλεια πληροφορικής Information Security Summit [682] που πραγματοποιείται στην Πράγα έχει ως στόχο την ανάπτυξη των ΤΠΕ και τη διαχείριση της ασφάλειας τους.

28.5 Διεθνής Συνεργασία

Η Τσέχικη Δημοκρατία, μέσω των δραστηριοτήτων του Εθνικού Κέντρου Κυβερνοασφάλειας αλλά και άλλων αρμόδιων αρχών εκπροσωπείται στην Ευρωπαϊκή Ένωση, τον ENISA[215] και άλλους διεθνείς οργανισμούς. Η εθνική CERT συμμετείχε στην πανευρωπαϊκή άσκηση, Cyber Europe [28] και στην άσκηση μεταξύ ΕΕ-ΗΠΑ CYBER ATLANTIC 2011 [683]. Η Τσεχική Δημοκρατία υπέγραψε Μνημόνιο Κατανόησης για συνεργασία στην ασφάλεια του κυβερνοχώρου με το NATO στις 14 Μαρτίου 2012 [684]. Η υπογραφή του μνημονίου θα επιτρέψει την καλύτερη συμμετοχή στις δραστηριότητες του NATO, καθώς και τον αποτελεσματικό συντονισμό των εθνικών και Συμμαχικών φορέων σε περίπτωση μείζονος συμβάντος

στον κυβερνοχώρο. Τέλος η Κροατία είναι μέλος της Ένωσης Δικτύωσης Κεντρικής και Ανατολικής Ευρώπης (CEENet) [79] και η CSIRT.CZ είναι διαπιστευμένο μέλος TI[685].

Κεφάλαιο 29ο

Φινλανδία

29.1 Εθνική Στρατηγική και πολιτικές Κυβερνοασφάλειας [686]

Η πρώτη Εθνική Στρατηγική Κυβερνοασφάλειας στη Φινλανδία εγκρίθηκε το 2003. Τον Δεκέμβριο του 2008 η φινλανδική κυβέρνηση ενέκρινε το δεύτερο ψήφισμά για την Εθνική Στρατηγική Κυβερνοασφάλειας και τον Ιανουάριο του 2013 ψηφίστηκε η τελευταία Εθνική Στρατηγική Ασφάλειας Πληροφορικής [687]. Σύμφωνα με αυτή το όραμα της Φινλανδίας για την Κυβερνοασφάλεια είναι να μπορεί να εξασφαλίσει τις ζωτικές λειτουργίες του κυβερνοχώρου σε όλες τις καταστάσεις, οι πολίτες, οι αρχές και οι επιχειρήσεις να μπορούν να χρησιμοποιούν ένα ασφαλή κυβερνοχώρο και μέχρι το 2016 η Φινλανδία να είναι μια παγκόσμια πρωτοπόρος στον κυβερνοχώρο ως προς την ετοιμότητα έναντι των απειλών. Η στρατηγική ορίζει δέκα στόχους για την Φινλανδία:

1.Τη δημιουργία ενός αποτελεσματικού μοντέλου συνεργασίας μεταξύ των αρχών και των άλλων φορέων με σκοπό την προώθηση της εθνικής ασφάλειας στον κυβερνοχώρο.

2.Τη βελτίωση της ευαισθητοποίησης και της επίγνωσης της κατάστασης της ασφάλειας στον κυβερνοχώρο μεταξύ των βασικών παραγόντων που συμμετέχουν στην κάλυψη των ζωτικών λειτουργιών της κοινωνίας,

3. Τη διατήρηση και την βελτίωση των ικανοτήτων των επιχειρήσεων και οργανισμών ζωτικής σημασίας για τις ζωτικές λειτουργίες της κοινωνίας όσον αφορά την ανίχνευση και την απώθησης των απειλών στον κυβερνοχώρο

4. Τη βεβαίωση ότι η αστυνομία έχει επαρκείς δυνατότητες για την πρόληψη και την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο,

5. Τη δημιουργία μιας ολοκληρωμένης άμυνας στον κυβερνοχώρο από τις φινλανδικές δυνάμεις άμυνας,

6. Την ενίσχυση της εθνικής ασφάλειας στον κυβερνοχώρο μέσα από την ενεργή και αποτελεσματική συμμετοχή στις δραστηριότητες των διεθνών οργανισμών,

7. Τη βελτίωση της τεχνογνωσίας στον κυβερνοχώρο και την ευαισθητοποίηση όλων των κοινωνικών φορέων,

8 Τη διασφάλιση των προϋποθέσεων για την εφαρμογή αποτελεσματικών μέτρων ασφαλείας κυβερνοχώρο μέσω της εθνικής νομοθεσίας,
9. Τον καθορισμό των αρμοδιοτήτων στις αρχές και στους φορείς της επιχειρηματικής κοινότητας που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.
10.Την παρακολούθηση της υλοποίησης και της ολοκλήρωσης της Στρατηγικής.

29.2 Νομοθετικό Πλαίσιο

Νομοθεσία προστασίας της ιδιωτικότητας / Προστασία Προσωπικών Δεδομένων [688]

Ο νόμος περί προσωπικών δεδομένων, τέθηκε σε ισχύ την 1η Ιουνίου 1999 και αντικατέστησε τη πράξη του 1988, που ήταν ο πρώτος νόμος σχετικά με την προστασία των δεδομένων στη Φινλανδία, με σκοπό την προστασία των προσωπικών δεδομένων σε όλα τα στάδια της επεξεργασίας τους. Οι βασικές αρχές της προστασίας της ιδιωτικής ζωής παρέμειναν αμετάβλητες στη συνταγματική μεταρρύθμιση για την εφαρμογή της οδηγίας για την προστασία των δεδομένων της ΕΕ (95/46/ΕΚ).

Νομοθεσία ηλεκτρονικού εμπορίου [688]

Ο νόμος σχετικά με την παροχή των υπηρεσιών της κοινωνίας της πληροφορίας (512/2011) τέθηκε σε ισχύ την 1η Ιουνίου 2011. Τα κύρια ζητήματα που αφορούν την ελευθερία παροχής υπηρεσιών της κοινωνίας της πληροφορίας, τις απαιτήσεις πληροφόρησης για τους παρόχους υπηρεσιών, τις ηλεκτρονικές παραγγελίες και τις ηλεκτρονικές συμβάσεις, καθώς και τις σχετικές υποχρεώσεις. Ο νόμος μεταφέρει στο εθνικό δίκαιο την οδηγία της ΕΕ για το ηλεκτρονικό εμπόριο (2000/31/ΕΚ).

Νομοθεσία για το έγκλημα στον κυβερνοχώρο [689]

Ο ποινικός Κώδικας της Φιλανδίας προβλέπει αδικήματα που σχετίζονται με την ασφάλεια του κυβερνοχώρου. Συγκεκριμένα:
Άρθρο 38-3 Υποκλοπή μηνύματος.
Άρθρο 38-5 Παρεμβολή στις επικοινωνίες.
Άρθρο 38-7α Παρεμβολή συστήματος Η/Υ.
Άρθρο 38-8 Παράνομη πρόσβαση σε Η/Υ.

29.3 Αρχές και Οργανισμοί

Δημόσιοι φορείς

Το Υπουργείο Μεταφορών και Επικοινωνιών [690] είναι αρμόδιο για τη νομοθεσία και την ανάπτυξη στρατηγικών για την ασφάλεια των πληροφοριών σε δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών. Η ασφάλεια των πληροφοριών αναφέρεται στα διοικητικά και τεχνικά μέτρα που διασφαλίζουν την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών και τη διαθεσιμότητα των συστημάτων. Η Φινλανδική Ρυθμιστική Αρχή Επικοινωνιών (FICORA) [691] είναι ένας κυβερνητικός οργανισμός που υπάγεται στο Υπουργείο Μεταφορών και Επικοινωνιών και ενεργεί ως εθνική αρχή για την ασφάλεια των πληροφοριών. Το Εθνικό Κέντρο Κυβερνοασφάλειας (NCSC) ιδρύθηκε εντός του FICORA την 1η Ιανουαρίου 2014. Το Κέντρο Κυβερνοασφάλειας είναι αρμόδιο για την παρακολούθηση των κινδύνων για την ασφάλεια του κυβερνοχώρου για συλλογή πληροφοριών, για την επεξεργασία τους και για την επικοινωνία με άλλους εταίρους. Το Υπουργείο Οικονομικών [692] έχει τη συνολική ευθύνη για την καθοδήγηση και την ανάπτυξη της ασφάλειας των πληροφοριών στην κυβέρνηση της Φινλανδίας. Καθορίζει τις κατευθυντήριες γραμμές για την ανάπτυξη της ασφάλειας των πληροφοριών, τη διαχείριση του κινδύνου και των διοικητικών μεταρρυθμίσεων. Το Υπουργείο Οικονομικών έχει συστήσει το κυβερνητικό συμβούλιο Διαχείρισης Ασφάλειας Πληροφοριών (VAHTI) για ζητήματα που σχετίζονται με τη συνεργασία και την ανάπτυξη της ασφάλειας των πληροφοριών στην κεντρική κυβέρνηση. Ο Εθνικός Οργανισμός έκτακτης ανάγκης (NESA) [693] έχει ως στόχο να εξασφαλιστεί η συνέχεια της παραγωγής και των υποδομών ζωτικής σημασίας για την κοινωνία κάτω από όλες τις συνθήκες με τέτοιο τρόπο ώστε οι συνθήκες διαβίωσης του πληθυσμού και οι κρίσιμες λειτουργίες της κοινωνίας να εξασφαλιστούν σε περιπτώσεις έκτακτης ανάγκης, Κρίσιμες υπηρεσίες υποδομής για τις οποίες έχει ευθύνη ο οργανισμός περιλαμβάνουν τα ηλεκτρονικά συστήματα δεδομένων και επικοινωνιών. Το Γραφείο του Συνηγόρου του Πολίτη Προστασίας Δεδομένων [694] είναι μια ανεξάρτητη αρχή που παρέχει καθοδήγηση και συμβουλές για όλα τα θέματα που σχετίζονται με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και τον έλεγχο της τήρησης του νόμου.

Ομάδες Αντιμετώπισης Εκτάκτων Περιστατικών Κυβερνοασφάλειας [13]

Η CERT-FI [695] είναι η φινλανδική εθνική CERT, έργο της οποίας είναι η προώθηση της ασφάλειας στην κοινωνία της πληροφορίας, με την πρόληψη και την επίλυση των περιστατικών ασφάλειας και τη διάδοση πληροφοριών σχετικά με τις απειλές για την

ασφάλεια των πληροφοριών. Από την 1η Ιανουαρίου 2014 τα καθήκοντα του FICORA στους τομείς της αντιμετώπισης περιστατικών (CERT-FI) και διασφάλισης πληροφοριών (NCSA-FI) έχουν ενσωματωθεί στο νέο κέντρο κυβερνοασφάλειας NCSC-FI. Η Funet CERT [696] είναι η CERT του ερευνητικού δικτύου της Φινλανδίας Funet. Η Ericsson PSIRT είναι η ομάδα της εταιρείας Ericsson ενώ η Nokia NIRT της εταιρείας Nokia. Τέλος η F-Secure Security Response είναι η ομάδα της εταιρείας παραγωγής προϊόντων ασφάλειας υπολογιστών F-Secure.

Ιδιωτικοί φορείς

Η Φινλανδική Ομοσπονδία Επικοινωνιών και Τηλεπληροφορικής, (FiCom) [697] είναι ένας οργανισμός συνεργασίας για τις ΤΠΕ στη βιομηχανία στη Φινλανδία. Μαζί με τις επιχειρήσεις των ΤΠΕ, αναπτύσσει την αξιοπιστία των δικτύων δεδομένων και συμβάλλει στην ετοιμότητα των ΤΠΕ σε καταστάσεις έκτακτης ανάγκης. Η F-Secure Corporation [698] είναι μια από τις μεγαλύτερες εταιρείες λογισμικού διεθνώς η οποία αναπτύσσει προϊόντα για την ασφάλεια του υπολογιστή και έχει έδρα το Ελσίνκι.

Ακαδημαϊκοί φορείς

Το Πανεπιστήμιο του Turku [699] διεξάγει έρευνα για την ασφάλεια πληροφοριών μέσω του Τμήματος Τεχνολογίας Πληροφορικής και Πληροφοριακών Συστημάτων. Η έρευνα αφορά την κρυπτογραφία και την ασφάλεια των δεδομένων, την ασφάλεια δικτυακών συστημάτων και τη διαχείριση της επιχειρησιακής συνέχειας. Το Oulu University [700] μέσω της Ομάδας Ασφαλούς Προγραμματισμού μελέτα, την ανάπτυξη μεθόδων για την υλοποίηση λογισμικού, ώστε να αποτρέπονται και να εξαλείφονται τα τρωτά σημεία. Η Αστυνομική Ακαδημία της Φινλανδίας [701] είναι ένα εκπαιδευτικό ίδρυμα, που υπάγεται στο Υπουργείο Εσωτερικών και την εθνικής αστυνομία το οποίο πραγματοποιεί έρευνα και εκπαιδεύει τους μελλοντικούς αστυνομικούς σε τεχνικές αντιμετώπισης του κυβερνοεγκλήματος. Το Πανεπιστήμιο του Ελσίνκι [702] πραγματοποιεί επίσης έρευνα και διδασκαλία σε θέματα που αφορούν το χώρο της Ασφάλειας Πληροφοριών.

Συνεργασία μεταξύ φορέων

Το NCSC-FI συλλέγει και συσχετίζει τις πληροφορίες από μια ποικιλία πηγών. Οι φινλανδικοί πάροχοι τηλεπικοινωνιακών υπηρεσιών είναι υποχρεωμένοι από το νόμο να αναφέρουν περιστατικά ασφάλειας των πληροφοριών στο NCSC-FI. Σύμφωνα με το νόμο, πρέπει επίσης να αναφέρονται οι απειλές για την ασφάλεια των πληροφοριών. Το NCSC-FI ζητάει επίσης εθελοντικές αναφορές από όλους τους άλλους οργανισμούς

του δημόσιου και του ιδιωτικού τομέα, καθώς και από ιδιώτες. Το κέντρο είναι δικτυωμένο σε μεγάλο βαθμό και έρχεται σε επαφή σε καθημερινή βάση με οργανώσεις του ιδιωτικού τομέα και των διαφόρων κυβερνητικών οργανισμών στη Φινλανδία και στο εξωτερικό. Το CERT-FI συνεργάζεται με εθνικές και διεθνείς CERT και με εκπροσώπους του εμπορίου και της βιομηχανίας, καθώς και με τη δημόσια διοίκηση.

29.4 Δράσεις Εκπαίδευσης & Ευαισθητοποίησης

Το Φινλανδικό Κέντρο Safer Internet (FISIC) (σχέδιο 2012-2014) [703] είναι το εθνικό πρόγραμμα ευαισθητοποίησης. Κύριος στόχος του κέντρου είναι η ευαισθητοποίηση και η οργάνωση εκστρατειών και ενημερωτικών συναντήσεων για τα παιδιά και τους νέους, τους γονείς, τους κηδεμόνες, τους κοινωνικούς λειτουργούς και εκπαιδευτικούς. Μια υπηρεσία hotline είναι μέρος του Κέντρου και παρέχεται από τον οργανισμό Save the Children ο οποίος συνεργάζεται με την αστυνομία. Επίσης το Κέντρο είναι υπεύθυνο για την οργάνωση της εκστρατείας «εβδομάδα Ασφαλέστερου Διαδικτύου» κάθε Φεβρουάριο. Η Εκστρατεία διοργανώνεται σε μια ευρεία συνεργασία με τη βιομηχανία, την κοινωνία των πολιτών και τα κυβερνητικά όργανα [704]. Το HAVARO, είναι ένα σύστημα έγκαιρης προειδοποίησης και ανίχνευσης που δημιούργησε ο FICORA σε συνεργασία με τον NESA [705]. Στο σύστημα μπορούν να ενταχθούν εθελοντικά και εταιρίες του ιδιωτικού τομέα. Το σύστημα προειδοποιεί τους συμμετέχοντες όταν εντοπισθεί μια απειλή. Το Συνέδριο t2 infosec [706] είναι ένα ετήσιο συνέδριο που πραγματοποιείται στο Ελσίνκι και εστιάζει την έρευνα για την ασφάλεια πληροφοριών. Τέλος στην Φιλανδία πραγματοποιούνται οι εθνικές ασκήσεις κυβερνοάμυνας FiCom και TIETO [28].

29.5 Διεθνής Συνεργασία

Η FUNET CERT αντιπροσωπεύει τη Φιλανδία στο δίκτυο NORDUnet [686] για τη συνεργασία στων σκανδιναβικών χωρών και ην κοινή άμυνα στον κυβερνοχώρο. Ο FICORA συνεργάζεται επίσης στενά με εταίρους σε παγκόσμιο και ευρωπαϊκό επίπεδο. Στη Φινλανδία, οι δράσεις που αφορούν τον ENISA εμπίπτουν στο διοικητικό κλάδο του Υπουργείου Μεταφορών και Επικοινωνιών [215. Το Υπουργείο Οικονομικών λαμβάνει επίσης ενεργό μέρος στη διεθνή συνεργασία στον τομέα της ασφάλειας των πληροφοριών με την ΕΕ, και τον ENISA. Η Φινλανδία αν και δεν είναι χώρα μέλος του

ΝΑΤΟ αποφάσισε να συμμετάσχει ως Εταίρος στο CCDCOE. και θα στείλει Φινλανδούς εμπειρογνώμονες να εργαστούν στο κέντρο από το 2014 [707]. Το CERT-FI συνεργάζεται στενά με τα ευρωπαϊκά κυβερνητικά [31] ειδικά σε σχέση με την ανάλυση κακόβουλου λογισμικού και είναι διαπιστευμένο μέλος TI. Τέλος οι τέσσερις από τις πέντε CERT της Φιλανδίας είναι μέλη του FIRST [32].

Κεφάλαιο 30ο

Συμπεράσματα

30.1 Συγκριτική Ανάλυση

Έχοντας ολοκληρώσει τη μελέτη της κάθε χώρας της Ε.Ε βάση των κριτηρίων που θεσπίστηκαν, μπορούν να εξαχθούν χρήσιμα συμπεράσματα τόσο για τη γενικότερη κατάσταση της κυβερνοασφάλειας στην Ε.Ε όσο και για κάθε μέλος ξεχωριστά. Παρατηρείται ότι όλα τα μέλη έχουν υλοποιήσει προγράμματα και δράσεις με σκοπό την επίτευξη ενός ικανοποιητικού επιπέδου κυβερνοασφάλειας. Αυτό οφείλεται κυρίως στην πολιτική της Ε.Ε. για την υλοποίηση του δικού της οράματος και στρατηγικής με σκοπό τη δημιουργία ενός ασφαλούς κυβερνοχώρου για τους πολίτες της. Μέσω της έκδοσης οδηγιών και πολιτικών που καλούνται οι χώρες να υιοθετήσουν αλλά και με τη χρηματοδότηση αρκετών προγραμμάτων έχει βελτιωθεί σημαντικά το επίπεδο της Κυβερνοασφάλειας. Ωστόσο παρά την κεντρική καθοδήγηση της Ε.Ε. κάθε κράτος ξεχωριστά ανάλογα με τις δικές του δομές και οργάνωση έχει πραγματοποιήσει δικές του πολιτικές και πρακτικές με αποτέλεσμα να υπάρχει διακύμανση μεταξύ των χωρών-μελών. Αυτό επιβεβαιώνεται μέσω της σύγκρισης όλων των κρατών μελών με τα ίδια κριτήρια που χρησιμοποιήθηκαν για την ανάλυση τους ξεχωριστά Αρχικά, εξετάζοντας το κριτήριο της εθνικής στρατηγικής και των πολιτικών Κυβερνοασφάλειας παρατηρούμε ότι ενώ ήδη από το 2008 η Εσθονία ήταν η πρώτη χώρα που δημοσίευσε εθνική στρατηγική, ενέργεια που ακολούθησαν τον επόμενο χρόνο η Γερμανία και το Ηνωμένο Βασίλειο, μέχρι σήμερα υπάρχουν έντεκα χώρες που δεν έχουν εκδώσει τη δική τους στρατηγική. Αξίζει να σημειωθεί ότι τα περισσότερα κράτη της κεντρικής και βορειοδυτικής Ευρώπης, έχουν υιοθετήσει αντίστοιχη στρατηγική. Εξαίρεση αποτελούν η Δανία, η Ιρλανδία και το Βέλγιο το οποίο ενώ έχει δημοσιεύσει ένα προσχέδιο, εκκρεμεί η έγκρισή του από το κοινοβούλιο. Αντίθετα παρατηρείται μεγάλη υστέρηση στις χώρες τις Νότιας Ευρώπης και των Βαλκανίων. Συγκεκριμένα με εξαίρεση, την Κύπρο και την πρόσφατη δημοσίευση της ισπανικής στρατηγικής το Δεκέμβριο του 2013, η Πορτογαλία, η Ιταλία, η Ελλάδα και η Μάλτα δεν έχουν προχωρήσει σε αντίστοιχη ενέργεια. Στο χώρο των Βαλκανίων, η

Ρουμανία και η Ουγγαρία δημοσίευσαν εθνική στρατηγική την άνοιξη του 2013 ενώ υπολείπονται η Ελλάδα, η Κροατία, η Βουλγαρία και η Σλοβενία.

Σχετικά με το Νομοθετικό Πλαίσιο παρατηρούμε ότι το σύνολο των χωρών έχουν ενσωματώσει στο εθνικό τους δίκαιο τις σχετικές οδηγίες της Ε.Ε. που αφορούν την προστασία των δεδομένων και της ιδιωτικότητας, τις ηλεκτρονικές επικοινωνίες και το ηλεκτρονικό εμπόριο. Επίσης όλα τα μέλη έχουν θεσπίσει νομοθεσία σχετικά με το έγκλημα στο κυβερνοχώρο. Ωστόσο, μόλις δεκατέσσερα από τα εικοσιοχτώ έχουν επικυρώσει τη σύμβαση για το κυβερνοέγκλημα του Συμβουλίου της Ευρώπης. Μελετώντας το κριτήριο της ύπαρξης φορέων για την υποστήριξη της Κυβερνοασφάλειας παρατηρείται ότι όλες οι χώρες της Ε.Ε. διαθέτουν αντίστοιχες υπηρεσίες όπως Προστασίας Προσωπικών Δεδομένων, Προστασίας Πληροφοριών και Υποδομών Ζωτικής Σημασίας και Ρυθμιστικές Αρχές Επικοινωνιών. Επίσης όλες διαθέτουν Μονάδες Αστυνομίας για την καταπολέμηση του κυβερνοεγκλήματος. Σε αρκετές χώρες επίσης, κυρίως μελών του ΝΑΤΟ, λειτουργούν μονάδες κυβερνοασφάλειας στις ένοπλες δυνάμεις. Το σημείο στο οποίο παρουσιάζεται μεγάλη διαφοροποίηση μεταξύ των κρατών είναι αυτό των ομάδων CERT. Καταρχάς η ύπαρξη μιας εθνικής ομάδας είναι υποχρέωση των μελών σύμφωνα με τη δράση 38 [708] για την υλοποίηση της ψηφιακής ατζέντας. Ωστόσο, η Ιρλανδία ενώ έχει θεσμοθετήσει τη δημιουργία εθνικής CERT δεν έχει προχωρήσει ακόμα στην υλοποίηση. Επίσης οι εθνικές CERT της Κύπρου και της Ιταλίας δεν είναι ακόμα πλήρως επιχειρησιακές. Αξίζει να σημειωθεί ότι από τις επιχειρησιακές Εθνικές CERT αυτές της Ελλάδας και του Ηνωμένου Βασιλείου είναι οι μόνες που δεν είναι διαπιστευμένα μέλη TI. Σημαντική είναι επίσης η διαφοροποίηση μεταξύ των μελών, όσον αφορά τον αριθμό των ομάδων CERT. Έτσι παρατηρούμε ότι χώρες όπως η Γερμανία, το Ηνωμένο Βασίλειο, η Γαλλία, η Ισπανία και η Ολλανδία έχουν διψήφιο αριθμό ομάδων οι οποίες δραστηριοποιούνται σε ένα ευρύ φάσμα τομέων. Μία άλλη παρατήρηση σχετικά με τις εθνικές CERT αφορά το πλαίσιο λειτουργίας τους, καθώς στις πιο προηγμένες χώρες λειτουργούν εντός ενός εθνικού κέντρου κυβερνοασφάλειας. Παραδείγματα αυτών των χωρών είναι η Γαλλία, η Γερμανία, το Ηνωμένο Βασίλειο η Εσθονία και η Ολλανδία. Αντίθετα, σε εννέα χώρες, εκ των οποίων οι οχτώ είναι στις χώρες που δεν έχουν στρατηγική κυβερνοασφάλειας, λειτουργούν εντός κάποιου πανεπιστημίου. Η Ελλάδα μαζί με την Ουγγαρία είναι οι δύο μόνες χώρες των οποίων οι εθνικές ομάδες λειτουργούν στα πλαίσια των μυστικών υπηρεσιών. Επίσης η εθνική CERT της

Ελλάδας είναι η μοναδική στην Ευρώπη η οποία στην ιστοσελίδα της περιλαμβάνει μόνο στοιχεία επικοινωνίας για αναφορά περιστατικών και προειδοποιήσεις, συμβουλές, νέα, και εργαλεία σχετικά με την κυβερνοασφάλεια, πρακτική που δεν συμβάλλει στην πρόληψη των περιστατικών κυβερνοασφάλειας.

Διαφοροποίηση μεταξύ των χωρών παρατηρείται επίσης και στη συνεργασία μεταξύ των φορέων. Κατ' αρχάς, οι χώρες που διαθέτουν εθνική στρατηγική πλεονεκτούν καθώς έχουν καθορίσει τις αρμοδιότητες και τη συνεργασία μεταξύ των φορέων. Επιπλέον οι περισσότερες από αυτές τις χώρες όπως το Ηνωμένο Βασίλειο, η Γερμανία, η Ολλανδία και η Σουηδία έχουν ιδρύσει κέντρα Κυβερνοασφάλειας τα οποία έχουν δημιουργήσει δομές και διαδικασίες συνεργασίας.

Όπως έχει ειπωθεί, για την επίτευξη Κυβερνοασφάλειας είναι απαραίτητη η συνεργασία μεταξύ ιδιωτικού και δημοσίου τομέα. Αυτό είναι ένα ζήτημα όπου τα περισσότερα κράτη αντιμετωπίζουν αρκετές δυσκολίες. Το Ηνωμένο Βασίλειο, η Γερμανία και το Λουξεμβούργο έχουν δημιουργήσει μέσω των κέντρων κυβερνοασφάλειας πλατφόρμες συνεργασίας με τον ιδιωτικό τομέα. Θετική είναι επίσης η ίδρυση κέντρων αριστείας κυβερνοασφάλειας σε εννιά χώρες, μεταξύ των οποίων και η Ελλάδα, ύστερα από χρηματοδότηση της Ευρωπαϊκής Επιτροπής. Τα κέντρα συμβάλλουν στη συνεργασία μεταξύ του δημόσιου και ιδιωτικού τομέα καθώς και με την ακαδημαϊκή κοινότητα.

Εξετάζοντας το κριτήριο των δράσεων ευαισθητοποίησης και εκπαίδευσης παρατηρούμε ότι κύριο μέσο αποτελεί το πρόγραμμα της Ευρωπαϊκής Επιτροπής για το ασφαλές διαδίκτυο. Το πρόγραμμα το έχουν υλοποιήσει όλα τα μέλη εκτός από την Κροατία. Ωστόσο, το πρόγραμμα απευθύνεται κυρίως στην ευαισθητοποίηση και την εκπαίδευση των νέων, των γονέων και των εκπαιδευτικών, ενώ λίγες είναι οι χώρες όπως η Γερμανία, το Ηνωμένο Βασίλειο και το Λουξεμβούργο που έχουν υλοποιήσει αντίστοιχα εθνικά προγράμματα με σκοπό την ευαισθητοποίηση και την εκπαίδευση του προσωπικού των μικρών και μεσαίων επιχειρήσεων. Αξιοσημείωτο είναι το εθελοντικό πρόγραμμα ευαισθητοποίησης μέσω των WARP's στο Ηνωμένο Βασίλειο. Επίσης, η πλειοψηφία των χωρών της Ευρώπης, μεταξύ των οποίων και η Ελλάδα, διεξάγει εθνικές ασκήσεις κυβερνοάμυνας.

Τέλος, μελετώντας το κριτήριο της διεθνούς συνεργασίας παρατηρούμε ότι οι διεθνείς οργανισμοί όπως ο ENISA και το ΝΑΤΟ έχουν κύριο ρόλο στη συνεργασία μεταξύ των χωρών κυρίως με την διεξαγωγή κοινών ασκήσεων στις οποίες συμμετέχει και η

Ελλάδα.

Η Βουλγαρία, η Κύπρος, η Μάλτα και το Λουξεμβούργο δεν έχουν μέχρι σήμερα συμμετοχή σε κάποια διεθνή άσκηση. Επιπλέον, διεθνή φόρουμ όπως το FIRST, το Ceenet και το ECG συμβάλλουν στη συνεργασία μεταξύ των ομάδων CERT. Όπως παρατηρείται, οι ελληνικές CERT δεν έχουν ιδιαίτερη συμμετοχή στα διεθνή φόρουμ. Τέλος, εκτός από τους διεθνείς οργανισμούς, αρκετές χώρες έχουν συνάψει μεταξύ τους συνεργασίες. Αυτές είναι κυρίως μεταξύ χωρών της ίδιας γεωγραφικής περιοχής όπως η συνεργασία των σκανδιναβικών χωρών, της Γερμανίας με την Αυστρία και την Ελβετία και των χωρών BENELUX.

Λαμβάνοντας υπόψη όλα τα παραπάνω διαπιστώνεται ότι η Γερμανία, η Γαλλία, το Ηνωμένο Βασίλειο, η Ολλανδία και η Ισπανία ανήκουν στις πιο προηγμένες χώρες στον τομέα της κυβερνοασφάλειας εντός της Ε.Ε. Σε πολύ καλό επίπεδο βρίσκονται επίσης οι χώρες τις βαλτικής καθώς και οι σκανδιναβικές χώρες. Αντίθετα οι χώρες του νότου και των Βαλκανίων διαφαίνεται ότι υστερούν έναντι των υπολοίπων με ουραγό την Κροατία. Η Ελλάδα έχει κάνει σημαντικά βήματα υιοθετώντας το σύνολο σχεδόν το ευρωπαϊκών δράσεων και οδηγιών. Ωστόσο, λόγω της έλλειψης εθνικής στρατηγικής και κατ' επέκταση γενικότερου συντονισμού και συνεργασίας και λόγω του μικρού αριθμού και τις περιορισμένης δράσης των CERT τόσο σε εθνικό όσο και σε διεθνές επίπεδο, δύσκολα μπορεί να καταταγεί πάνω από τον ευρωπαϊκό μέσο όρο. Στον πίνακα 30.1 φαίνονται αναλυτικά οι δράσεις που έχει υλοποιήσει κάθε χώρα-μέλος ανά τομέα σύγκρισης.

Χώρα																													
Στρατιγικές																													
Στρατηγική Κυβερνοασφάλειας	x 2013			x 2011	x 2011			x 2008	x 2011		x 2013			x 2012		x 2011	x 2011		x 2013		x 2013		x 2011	x 2008		x 2012	x 2011	x 2013
Ψηφιακή Στρατηγική	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Νομοθετικό Πλαίσιο																													
Υιοθέτηση Ευρωπαϊκής νομοθεσίας	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Νομοθεσία κατά των κυβερνοεγκλημάτων	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Κύρωση σύμβασης Συμβούλιου της Ευρώπης			x	x		x		x				x	x	x	x			x	x			x	x	x			x		x

Χώρα																													
Δημόσιοι φορείς																													
Κέντρο Κυβερνοασφάλειας	x			x	x	x		x	x		x			x	x			x	x			x				x	x
Υπηρεσία δίωξης ηλεκτρονικού εγκλήματος	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Υπηρεσία προστασίας προσωπικών δεδομένων	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Συνεργασία με ιδιωτικό τομέα		x			x	x			x	x	x						x	x	x		x							x	
CERT																													
Αρ. CERT	5	3	1	11	25	6	4	1	22	4	15	8	3	1	1	4	5	1	16	3	4	4	3	1	1	7	7	5	
Μέλη FIRST	3	1	0	6	19	5	1	1	15	0	10	0	3	0	1	3	0	0	8	1	2	1	0	0	1	3	0	4	
Εθνική CERT	x	x	x	x	x	x	x	x	x		x		x		x	x	x	x	x	x	x	x	x	x	x		x	x	
TI διαπιστευμένα / πιστοποιημένα	2 / 0	2 / 0	1 / 0	5 / 0	12 / 1	3 / 0	2 / 1	1 / 0	3 / 0	1 / 0	8 / 0	2 / 0	2 / 0	0 / 0	1 / 0	3 / 0	4 / 0	1 / 0	4 / 2	1 / 0	1 / 0	4 / 0	1 / 0	1 / 0	1 / 0	6 / 2	4 / 0	3 / 0	
Συμμετοχή σε ECG	x			x	x	x			x		x								x							x		x	
Συμμετοχή σε Ceenet			x					x								x				x			x	x	x		x		

Συμπεράσματα

Χώρα																													
CERT ανά κοινωνικοοικονομικό τομέα	x			x	x				x		x	x							x			x				x	x	x
Ακαδημαϊκοί φορείς																													
Προγράμματα εκπαίδευσης στην ασφάλεια των ΤΠΕ	x	x	x	x	x	x	x	x	x	x	x	x	x				x	x	x	x	x	x	x	x		x	x	x
Έρευνα στην ασφάλεια των ΤΠΕ	x	x	x	x	x	x	x	x	x	x	x	x	x				x		x	x	x	x	x	x		x	x	x
Δράσεις Εκπαίδευσης & Ευαισθητοποίησης																													
Εθνικό-Ευρωπαϊκό Πρόγραμμα Ευαισθητοποίησης	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Άλλα εθνικά προγράμματα		x			x	x			x	x	x								x		x							x
Ύπαρξη γραμμής επικοινωνίας	x	x	x	x	x	x	x	x	x	x	x	x		x	x	x	x	x		x	x	x	x	x	x	x	x	x	x
Υποστήριξη από αρχές επιβολής του νόμου	x			x	x	x	x	x	x	x	x	x			x	x	x	x		x	x	x	x		x	x		x
Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων	x			x	x				x	x	x						x		x		x							x

Χώρα																													
Διεξαγωγή εθνικών ασκήσεων	x	x	x	x	x	x	x	x	x	x	x	x			x	x		x	x	x	x		x		x		x		x
Διεθνής Συνεργασία																													
Μέλος ENISA	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
Μέλος NATO		x	x	x	x	x	x	x	x		x	x	x		x	x	x		x	x	x	x	x	x	x		x		
Μέλος ITU/IMPACT	x		x								x	x	x	x		x		x			x		x	x	x		x		
Μέλος CCDCoE					x			x			x	x			x	x			x	x	x			x			x	x	
Μέλος 2Centre Network		x	x	x			x	x	x	x	x												x						
Διακρατικές συμφωνίες	x	x	x	x	x	x		x	x								x		x	x			x			x		x	
Διεθνείς Ασκήσεις	x	x		x	x	x	x	x	x	x	x	x	x		x	x			x	x	x	x	x	x	x	x	x	x	

X= Υλοποιημένη δράση

Πίνακας 30.1 Συγκριτικός Πίνακας Χωρών-μελών Ε.Ε.

30.2 Προτάσεις για την Ελλάδα

Έχοντας εντοπίσει τις βέλτιστες πρακτικές και δράσεις που εφαρμόζουν οι πρωτοπόρες χώρες, παρουσιάζονται συγκεκριμένες προτάσεις για την Ελλάδα με σκοπό τη βελτίωση της κυβερνοασφάλειας.

Στον τομέα της εθνικής στρατηγικής και πολιτικών κυβερνοασφάλειας προέχει η επίσπευση ανάπτυξης και ολοκλήρωσης της εθνικής στρατηγικής. Ακολουθώντας το παράδειγμα της Γερμανίας η στρατηγική μπορεί να είναι τμήμα ευρύτερου συνόλου στρατηγικών με ιεραρχική δομή (Εθνική Στρατηγική Ασφαλείας - Εθνική Στρατηγική Προστασίας Κρίσιμων Υποδομών - Εθνική Στρατηγική Κυβερνοασφάλειας). Σχετικά με το περιεχόμενό της, ως στρατηγική-πρότυπο θεωρείται αυτή της Ολλανδίας, η οποία δεν περιγράφει μόνο τη βασική φιλοσοφία, τις δράσεις και τις πρακτικές αλλά εξειδικεύει ποιοι φορείς πρέπει να λάβουν συγκεκριμένα μέτρα μέσα σε ορισμένο χρονικό διάστημα.

Επίσης ο υπεύθυνος οργανισμός για την Κυβερνοασφάλεια της χώρας, ανάλογα με τις εξελίξεις, θα πρέπει να δημοσιεύει τακτικά σχετικές πολιτικές και κανονισμούς όπως συμβαίνει στα πρότυπα της Εσθονίας και της Γερμανίας.

Αναφορικά με το Νομοθετικό πλαίσιο πρέπει να εξεταστεί η κύρωση και η εφαρμογή της σύμβασης του Συμβουλίου της Ευρώπης, την οποία η Ελλάδα έχει υπογράψει από το 2001. Επίσης το Κέντρο Αριστείας Κυβερνοεγκλήματος μέσω των συνεργασιών με τις νομικές σχολές μπορεί να συμβάλλει με προτάσεις νόμων και κανονισμών στην παρακολούθηση των τεχνολογικών εξελίξεων.

Σχετικά με τις Αρχές και τους Οργανισμούς και την υποκατηγορία των δημόσιων φορέων, προτείνεται η δημιουργία ενός κέντρου κυβερνοασφάλειας το οποίο θα συντονίζει τη συνεργασία με τους υπόλοιπους φορείς και θα αναπτύσσει πολιτικές και δράσεις. Σύμφωνα με τα διεθνή πρότυπα, το κέντρο πρέπει να υπάγεται σε υπηρεσία προστασίας ζωτικών υποδομών. Επίσης, ακολουθώντας τα παραδείγματα της Γερμανίας και του Ηνωμένου Βασιλείου, το κέντρο αναπτύσσει πλατφόρμες συνεργασίας τόσο με τον δημόσιο όσο και με τον ιδιωτικό τομέα.

Στην υποκατηγορία των Cert’s πρώτα απ’ όλα θα πρέπει να υπάρξει ενθάρρυνση δημιουργίας περισσότερων οι οποίες—θα αφορούν κάθε φάσμα της ελληνικής κοινωνίας και οικονομίας, όπως για παράδειγμα ο χρηματοπιστωτικός τομέας, η βιομηχανία και οι ένοπλες δυνάμεις. Επίσης όλες οι Cert εκτός ότι πρέπει να επιδιώξουν

να γίνουν διαπιστευμένα μέλη ΤΙ, πρέπει να προωθήσουν και τη διεθνή συνεργασία, είτε συμμετέχοντας ως μέλη διεθνών οργανισμών (π.χ. FIRST, ECG) είτε με τη σύναψη επιμέρους διμερών συνεργασιών. Σε όλες αυτές τις δραστηριότητες πρωταγωνιστικό ρόλο θα έχει η εθνική CERT η οποία θα αναλάβει πιο ενεργό ρόλο, μέσω πρωτοβουλιών ενημέρωσης ευαισθητοποίησης και παροχής βοήθειας με σκοπό όχι μόνο την αντιμετώπιση αλλά και την πρόληψη των περιστατικών κυβερνοασφάλειας. Για την καλύτερη εφαρμογή όλων των παραπάνω πρέπει να εξεταστεί η λειτουργία της εθνικής CERT στα πλαίσια ενός κέντρου κυβερνοασφάλειας, όπως συμβαίνει στην πλειοψηφία των χωρών της Ευρώπης, ενώ η ΕΥΠ μπορεί να αναλάβει την λειτουργία της κυβερνητικής CERT. Αντίστοιχο είναι το παράδειγμα του Ηνωμένου Βασιλείου.

Στην υποκατηγορία της ακαδημαϊκής κοινότητας προτείνεται η συνεργασία με το Ελληνικό Κέντρο Αριστείας Κυβερνοεγκλήματος. ακολουθώντας τις αντίστοιχες επιτυχημένες περιπτώσεις του Ηνωμένου Βασίλειου, της Ιρλανδίας και του Βελγίου. Στην κατηγορία των δράσεων εκπαίδευσης και ευαισθητοποίησης προτείνεται η συνέχιση και εντατικοποίηση των είδη επιτυχημένων προγραμμάτων που αφορούν τους πολίτες καθώς και η δημιουργία προγραμμάτων που θα αφορούν τις μικρές και μεγάλες επιχειρήσεις. Επιπλέον, εκτός από την συνέχιση της άσκησης Πανόπτης οι διεξαγωγή συχνότερων ασκήσεων μικρότερης κλίμακας αυξάνει το επίπεδο ετοιμότητας και αυξάνει την εμπειρία για την αντιμετώπιση περιστατικών κυβερνοασφάλειας όλων των συμμετεχόντων φορέων. Επίσης προτείνεται η υιοθέτηση του επιτυχημένου στο Ηνωμένο Βασίλειο. μέτρου των WARP’s όπου με χαμηλό κόστος εθελοντικές ομάδες μπορούν να συμβάλουν σε μεγάλο βαθμό στη βελτίωση της κυβερνοασφάλειας.

Κλείνοντας, στον τομέα της διεθνούς συνεργασίας η Ελλάδα πρέπει να εξετάσει τη συμμετοχή της σε περισσότερους διεθνείς οργανισμούς όπως η ITU/IMPACT και το CCDCoE αλλά και τη συμμετοχή της σε περισσότερες διεθνείς ασκήσεις. Τέλος στα πρότυπα των σκανδιναβικών και βαλτικών χωρών, προτείνεται η συνεργασία με τις χώρες των Βαλκανίων τόσο μέσω επιμέρους συμφωνιών και ανταλλαγής πληροφοριών όσο και με την διεξαγωγή διακρατικών ασκήσεων κυβερνοάμυνας.

Πηγές

[1] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport
[2] https://www.ccdcoe.org/369.html
[3] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[4] https://www.bka.gv.at/DocView.axd?CobId=50999
[5] http://www.epractice.eu/en/document/288170
[6] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Austria%20_30%20May%2007_En.pdf
[7] https://www.onlinesicherheit.gv.at/73239.html
[8] www.bka.gv.at
[9] www.bka.at
[10] www.bmi.gv.at
[11] www.dsk.gv.at
[12] www.a-sit.at
[13] http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map
[14] http://daeimplementation.eu/indicator.php?id_country=1&action_n=38
[15] www.cert.at
[16] www.govcert.gv.at
[17] http://www.r-it.at
[18] http://cert.aco.net/
[19] http://www.wien.gv.at
[20] www.it-safe.at
[21] www.itsecurityexperts.at
[22] http://www.sba-research.org/
[23] http://www.iaik.tugraz.at/content/about_iaik/

[24] www.jku.at/content
[25] http://daeimplementation.eu/indicator.php?id_country=1&action_n=40
[26] https://www.sicherheitshandbuch.gv.at/
[27] http://idc-cema.com/eng/events/56341-idc-it-security-roadshow-2014
[28] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012/at_download/fullReport
[29] http://daeimplementation.eu/indicator.php?id_country=1&action_n=39
[30] http://www.a-sit.at/de/internationales/index.php
[31] http://www.egc-group.org/links.html
[32] http://www.first.org/members/teams
[33] http://www.impact-alliance.org/home/index-countries.html
[34] http://www.lsec.be/upload_directories/documents/TowardsaBelgianStrategyonInformationSecurity_BISI_080908.pdf
[35] http://www.icss2013.eu/sites/default/files/Presentations/ICSS2013-BeirensL.pdf
[36] http://www.epractice.eu/en/document/288180
[37] http://www.rand.org/content/dam/rand/pubs/technical_reports/2006/RAND_TR337.pdf
[38] http://www.b-ccentre.be/links-2
[39 http://2centre.eu/coe/belgium/overview
[40]] www.polfed-fedpol.be
[41] http://www.fedict.belgium.be/
[42] http://www.belgium.be/nl/justitie/veiligheid/criminaliteit/computercriminaliteit/
[43] http://www.privacycommission.be/
[44] http://justitie.belgium.be/nl/overheidsdienst_justitie/organisatie/onafhankelijke_diensten_en_commissies/veiligheid_van_de_staat/
[45] https://www.cert.be
[46] http://daeimplementation.eu/indicator.php?id_country=2&action_n=38
[47] http://www.beltug.be/page/3/Who_is_BELTUG/
[48] http://www.clusib.be/wp/?lang=fr
[49] http://www.lsec.be/

[50] http://www.agoria.be/www.wsc/webextra/Prg/izContentWeb?sessionlid=3

[51] http://www.febelfin.be/

[52] http://www.iccbelgium.be/

[53] http://www.esat.kuleuven.be/cosic/

[54] http://daeimplementation.eu/indicator.php?id_country=2&action_n=41

[55] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012/at_download/fullReport

[56] http://daeimplementation.eu/indicator.php?id_country=2&action_n=39

[57] http://www.nato.int/cps/en/natolive/news_105205.htm

[58] http://ict.investinluxembourg.lu/ict/luxembourg-joins-forces-belgium-and-netherlands-towards-increased-cybersecurity

[59] https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&ved=0CDIQFjAA&url=http%3A%2F%2Fwww.anticorruption-bulgaria.org%2Fcomponent%2Fdocman%2Fdoc_download%2F24-national-strategy-for-counteracting-crime-english&ei=XtrKUuiyEIKl0wXz-YB4&usg=AFQjCNGYnczx6BI5rVMWnKCiRGZ8ZgSlqQ&bvm=bv.58187178,d.d2k

[60] http://www.epractice.eu/en/document/5303501

[61] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Bulgaria%20_9%20May%2007_En.pdf

[62] http://www.esmis.government.bg/en/page.php?c=1

[63] http://www.dksi.bg/en/

[64] http://www.cybercrime.bg/bg

[65] https://govcert.bg/EN/Pages/default.aspx

[66] http://daeimplementation.eu/indicator.php?id_country=3&action_n=38

[67] http://www.iseca.org/

[68[http://www.nlcv.bas.bg/

[69] http://www.fmi.uni-sofia.bg/

[70] http://www.tu-sofia.bg/index.html

[71] http://www.tu-varna.bg/

[72] http://www.academy.mvr.bg/
[73] http://2centre.eu/coe/bulgaria
[74] http://daeimplementation.eu/indicator.php?id_country=3&action_n=41
[75] http://www.safenet.bg/
[76] http://daeimplementation.eu/indicator.php?id_country=3&action_n=40
[77] http://bulgaria.usembassy.gov/event_11152013c.html
[78] http://www.gsnmagazine.com/node/27556
[79] http://www.ceenet.org/category/members/
[80] http://www.enisa.europa.eu/activities/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders/at_download/fullReport
[81] http://www.ambafrance-ca.org/IMG/pdf/Livre_blanc_Press_kit_english_version.pdf
[82] http://www.gouvernement.fr/sites/default/files/fichiers_joints/livre-blanc-sur-la-defense-et-la-securite-nationale_2013.pdf
[83] http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf
[84] http://www.epractice.eu/files/eGovernmentFrance.pdf
[85] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20France%20_26%20March%2007_En.pdf
[86] http://www.ssi.gouv.fr/en/the-anssi/
[87] http://www.ssi.gouv.fr/fr/anssi/formations/
[88] www.cnil.fr
[89] www.arcep.fr
[90] http://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Office-central-de-lutte-contre-la-criminalite-liee-aux-technologies-de-l-information-et-de-la-communication
[91] http://www.giteptics.fr/about/nous.html
[92] http://www.security-research-map.eu//index.php?file=show.php&ref=479
[93] http://2centre.eu/france
[94] www.renater.fr

[95] http://www.diplomatie.gouv.fr/en/french-foreign-policy-1/defence-security/cyber-security/
[96] http://www.economie.gouv.fr/hfds/communications-electroniques-defense-et-securite-des-systemes-dinformation
[97] http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006574476&cidTexte=LEGITEXT000006071307&dateTexte=20100809&oldAction=rechCodeArticle
[98] http://www.securite-informatique.gouv.fr/
[99] https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action
[100] https://www.signal-spam.fr/
[101] http://www.clusif.asso.fr/en/clusif/present/
[102] http://www.ossir.org/
[103] http://daeimplementation.eu/indicator.php?id_country=9&action_n=40
[104] http://www.internetsanscrainte.fr/
[105] http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/cyber-attaques-l-exercice-piranet-2012-met-l-etat-a-l-epreuve-d-une-crise.html
[106] http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/exercice-piranet-2010-l-etat-s-entraine-a-faire-face-a-une-attaque-de-grande.html
[107] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2010/BSI-ANSSI_050210.html
[108] http://www.dhs.gov/cyber-storm-securing-cyber-space
[109] http://daeimplementation.eu/indicator.php?id_country=9&action_n=39
[110] http://www.ssi.gouv.fr/fr/ssi/la-ssi-en-france/les-cert-francais.html
[111] http://www.bmi.bund.de/cae/servlet/contentblob/598732/publicationFile/34423/kritis_englisch.pdf
[112] http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
[113] http://www.epractice.eu/en/document/288243
[114] http://www.gesetze-im-internet.de/stgb/

[115]
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile
[116] http://www.bmi.bund.de/EN/Home/home_node.html
[117] https://www.bsi.bund.de/EN/Home/home_node.html
[118] http://www.bka.de/EN/Home/homepage__node.html?__nnn=true
[119] http://www.bmwi.de/DE/root.html
[120] http://www.bundesnetzagentur.de/cln_1912/DE/Home/home_node.html
[121] www.bsi.bund.de/cln_174/DE/Themen/CERTBund/certbund_node.html
[122] http://www.bitkom.org/en/Default.aspx
[123] www.eco.de
[124] www.itsmig.de
[125] www.internet-sicherheit.de
[126] www.is-its.org
[127] http://iaks-www.ira.uka.de
[128] www.sit.fraunhofer.de
[129] http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cyberabwehrzentrum/cyberabwehrzentrum_node.html
[122] http://www.dfn-cert.de/veranstaltungen.html
[123] https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html
[124] https://www.buerger-cert.de/
[125]
http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/Leitfaden_Schutz_kritischer_Infrastrukturen_en.pdf?__blob=publicationFile
[126] https://www.botfrei.de/en/ueber-das-projekt.html
[127] http://www.bmbf.de/en/73.php
[128] http://www.eco.de/?s=Anti%20Spam%20Summit
[129] http://daeimplementation.eu/indicator.php?id_country=10&action_n=39
[130] https://www.ccdcoe.org/423.html
[131] http://www.fmn.dk/eng/allabout/Documents/TheDanishDefenceAgrement2013-2017english-version.pdf
[132] http://www.epractice.eu/en/document/288207

[133] http://fe-ddis.dk/cfcs/Pages/cfcs.aspx

[134] https://www.pet.dk/Nyheder/2013/PET%20styrker%20indsatsen%20i%20forhold%20til%20cybertrusler%20og%20cybersikkerhed.aspx

[135] http://cphpost.dk/news/police-launching-new-cybercrime-centre.8388.html

[136] http://www.datatilsynet.dk

[137] https://www.cert.dk

[138] http://kundeservice.tdc.dk/erhverv/publish.php?id=8571

[139] http://fe-ddis.dk/cfcs/opgaver/govcert/Pages/default.aspx

[140] http://www.kmd.dk/

[141] http://secunia.com/

[142] http://itek.di.dk

[143] http://www.uni-c.dk/

[144] http://www.itu.dk/

[145] http://fe-ddis.dk/cfcs/omos/Pages/Politikogstrategi.aspx

[146] http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2008-CNH-143803

[147] http://www2.imm.dtu.dk/~robs/CIT-AWARE/project.pdf

[148] http://www.waset.org/conference/2013/06/copenhagen/ICCCS

[149] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

[150] http://daeimplementation.eu/indicator.php?id_country=6&action_n=39

[151] http://daeimplementation.eu/indicator.php?id_country=6&action_n=38

[152] https://www.enisa.europa.eu/activities/cert/background/coop/files/cert-cooperation-and-its-further-facilitation-by-relevant-stakeholders/at_download/fullReport

[153] http://www.epractice.eu/en/document/288251

[154] http://www.digitalplan.gov.gr/resource-api/dipla/contentObject/Strathgikh-gia-thn-PShfiakh-Anaptyxh/content

[155] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategy-3

[156] http://www.epractice.eu/en/document/288252

[157] http://www.ministryofjustice.gr/site/kodikes/Ευρετήριο/ΠΟΙΝΙΚΟΣΚΩΔΙΚΑΣ/tabid/432/language/el-GR/Default.aspx
[158] www.yme.gr
[159] http://www.ydmed.gov.gr/
[160] http://www.kemea.gr/
[161] http://www.cybercc.gr/
[162] http://www.nis.gr/
[163] http://daeimplementation.eu/indicator.php?id_country=11&action_n=38
[164] http://www.geetha.mil.gr
[165] http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=
[166] http://www.adae.gr/
[167] http://www.eett.gr/
[168] http://www.dpa.gr/
[169] http://www.nis.gr/portal/page/portal/NIS/NCERT
[170] http://www.forthcert.gr
[171] http://cert.grnet.gr
[172] http://www.cert.auth.gr
[173] http://www.sepe.gr/
[174] http://www.icsd.aegean.gr/group/index.php?group=L1
[175] http://www.cis.aueb.gr/
[176] http://ssl.ds.unipi.gr/el/
[177] http://www.forth.gr/
[178] http://www.saferinternet.gr
[179] http://daeimplementation.eu/indicator.php?id_country=11&action_n=41
[180] http://daeimplementation.eu/indicator.php?id_country=11&action_n=40
[181] http://www.cyberkid.gov.gr/
[182] http://www.geetha.mil.gr/index.asp?a_id=1716&nid=2786
[183] http://government.gov.gr/wp-content/uploads/2012/05/Παρουσίαση-δράσεων-Ηλεκτρονικής-Διακυβέρνησης.pdf

[184] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/enisa-s-2nd-international-conference-on-cyber-crisis-cooperation

[185] http://gr2014.eu/sites/default/files/cyber_0.pdf

[186] http://www.geetha.mil.gr/index.asp?a_id=1716&nid=1922

[187] http://www.geetha.mil.gr/index.asp?a_id=1713&nid=3062

[188] www.riso.ee

[189]http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Estonia_Cyber_security_Strategy.pdf

[190] http://www.epractice.eu/files/media/media_186.pdf

[191] http://www.riso.ee/en/node/4143

[192] http://www.epractice.eu/en/document/288252

[193] https://www.riigiteataja.ee/akt/184411

[194] www.mkm.ee

[195] www.siseministeerium.ee

[196] www.mod.gov.ee

[197] www.pol.ee

[198] www.dp.gov.ee

[199] www.valitsus.ee/en/government-office/functions-and-units

[200] www.ria.ee/kiik

[201] www.ria.ee

[202] www.cert.ee

[203] www.eits.ee

[204] www.itl.ee

[205] http://www.security-research-map.eu//index.php?file=show.php&ref=483

[206] www.itcollege.ee

[207] www.ut.ee

[208] https://www.ria.ee/programme/

[209] http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SI-2009-SIC-123916

[210] http://www.targaltinternetis.ee/

[211] http://daeimplementation.eu/indicator.php?id_country=7&action_n=40

[212] http://daeimplementation.eu/indicator.php?id_country=7&action_n=39
[213] https://www.ccdcoe.org/
[214] https://www.ccdcoe.org/353.html
[215] http://www.enisa.europa.eu/about-enisa/structure-organization/management-board/MBMemberAlternate.pdf
[216] http://www.mil.ee/en/news/7961/estonia-to-host-nato-cyber-defence-exercise
[217] https://www.ria.ee/france-and-estonia-sign-a-cooperation-agreeement/
[218] http://daeimplementation.eu/indicator.php?id_country=7&action_n=38
[219] http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf
[220] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/UK_Cyber_Security_Strategies.pdf
[221] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
[222] http://www.epractice.eu/en/document/288388
[223] http://www.legislation.gov.uk/ukpga/1990/18/contents
[224] http://www.legislation.gov.uk/ukpga/2006/48/contents
[225] https://www.gov.uk/government/organisations/department-for-business-innovation-skills
[226] https://www.gov.uk/government/organisations/home-office
[227] https://www.gov.uk/government/organisations/ministry-of-defence
[228] https://www.gov.uk/government/organisations/cabinet-office
[229] http://www.cpni.gov.uk/
[230] http://www.cesg.gov.uk/
[231] http://content.met.police.uk/Site/pceu
[232] https://www.gov.uk/government/organisations/national-fraud-authority/about
[233] http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit
[234] http://ico.org.uk/
[235] http://www.tscheme.org/about/index.html
[236] www.micaf.co.uk
[237] https://www.iisp.org

[238] http://www.rhul.ac.uk/isg/
[239] http://www.ed.ac.uk/schools-departments/informatics/research/sicsa
[240] https://www.ja.net
[241] http://sec.cs.ucl.ac.uk/ace_csr/
[242] https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace
[243] https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/establishing-a-cyber-security-information-sharing-partnership
[244] http://www.warp.gov.uk/
[245] https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/providing-cyber-security-advice-for-businesses-and-the-public
[246] https://www.gov.uk/government/publications/cyber-security-guiding-principles
[247] http://www.gchq.gov.uk/press_and_media/news_and_features/Documents/Cyber_Security-the_UKs_approach_to_exports.pdf
[248] https://www.gov.uk/government/speeches/foreign-secretary-opens-the-london-conference-on-cyberspace
[249] https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/setting-up-centres-of-doctoral-training
[250] http://daeimplementation.eu/indicator.php?id_country=27&action_n=39
[251] http://ccdcoe.org/398.html
[252] http://blogs.technet.com/b/security/archive/2011/05/26/white-house-affirms-us-and-uk-cybersecurity-cooperation.aspx
[253] https://www.dhs.gov/cyber-storm-securing-cyber-space
[254] http://www.informationweek.com/traffic-management/uk-india-sign-cybersecurity-pact/d/d-id/1108802?
[258] http://www.nisc.go.jp/active/kihon/pdf/InternationalStrategyonCybersecurityCooperation_e.pdf
[259] http://www.dcenr.gov.ie/NR/rdonlyres/54AF1E6E-1A0D-413F-8CEB-2442C03E09BD/0/NationalDigitalStrategyforIreland.pdf
[260] http://www.epractice.eu/en/document/288270

[261] http://www.dcenr.gov.ie

[262] https://www.dataprotection.ie

[263] http://www.garda.ie/Controller.aspx?Page=29

[264] http://www.heanet.ie/services/cert

[265] http://www.iriss.ie/iriss/

[266] http://www.top1000.ie/industries/technology-consumer

[267] http://www.ictireland.ie

[268] http://www.tif.ie/Sectors/TIF/TIF.nsf/vPages/Home?OpenDocument

[269] http://www.iisf.ie/

[270] http://www.ispai.ie/

[271] www.dcu.ie

[272] http://www.ucd.ie/cci/

[273] http://www.makeitsecure.org

[274] http://www.internetsafety.ie

[275] http://daeimplementation.eu/indicator.php?id_country=13&action_n=40

[276] http://www.iiea.com/cybersecurityconference

[277] http://www.iriss.ie/iriss/irisscon.htm

[278] http://www.cosac.net/

[279] http://www.enisa.europa.eu/media/news-items/future-role-of-enisa-amongst-irish-presidencys-key-priorities

[280] http://www.dcenr.gov.ie/Press+Releases/2013/First+EU+agreement+during+Irish+presidency+welcomed+by+Communications+Minister+Pat+Rabbitte.htm

[281] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ES_NCSS.pdf

[282] http://www.epractice.eu/en/document/288370

[283] https://www.ccn.cni.es/

[284] http://www.cni.es/

[285] http://www.inteco.es/

[286] http://www.cnpic-es.es/

[287] https://www.gdt.guardiacivil.es

[288] http://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html

[289] http://www.agpd.es/

[290] https://www.ccn-cert.cni.es

[291] http://cert.inteco.es/

[292] http://www.cesicat.cat/cert/

[293] http://www.csirtcv.gva.es/

[294] http://www.lacaixa.es/

[295] http://www.mapfre.com/

[296] http://escert.upc.edu

[297] http://www.rediris.es/cert/

[298] http://www.cesca.cat/en/communications/security/incident-response-team

[299] https://cert.s21sec.com

[300] https://cybersoc.deloitte.es/

[301] http://www.tb-security.com

[302] https://www.ismsforum.es/

[303] http://www.criptored.upm.es/

[304] https://www.nics.uma.es/

[305] http://cnec.icfs.uam.es/

[306] http://www.centrointernetsegura.es/

[307] http://www.osi.es/

[308] https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=3214%3Ael-ccn-cert-participa-en-el-segundo-ejercicio-paneuropeo-de-ciberseguridad-ciber-europe-2012&catid=62%3Acomunicados-ccn-cert&Itemid=86&lang=en

[309] http://daeimplementation.eu/indicator.php?id_country=25&action_n=39

[310] http://www.nato.int/cps/en/natolive/news_105205.htm

[311] https://www.ccn-cert.cni.es/index.php?option=com_content&view=article&id=2922%3Ael-ccn-cert-participa-en-el-primer-ejercicio-conjunto-de-ciberseguridad-entre-la-ue-y-eeuu&catid=62%3Acomunicados-ccn-cert&Itemid=86&lang=en

[312] http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2013-03-19&atto.codiceRedazionale=13A02504&elenco30giorni=true

[313] http://www.epractice.eu/en/document/288279
[314]
http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20Italy%20_26%20%20April%202008_pub.pdf
[315] http://www.isticom.it/
[316] http://www.ocsi.isticom.it/
[317] http://www.digitpa.gov.it/
[318] http://www.poliziadistato.it/articolo/view/23401/
[319] http://www.garanteprivacy.it/
[320] http://security.dsi.unimi.it/
[321] http://www.cert.garr.it/en/
[322] https://www.picert.it/english_intro/
[323] http://www.difesa.it/smd_/staff/reparti/ii/cert/Pagine/default.aspx
[324]
https://www.tuconti.telecomitalia.it/qYnTnGzSaHR0cDovL3BvcnRhbC50dWNvbnRpLnRlbGVjb21pdGFsaWEuaXQ6NzAwMS9wb3J0YWwvZHQ=8GkTRyAT
[325] http://www.enel.it/attivita/servizi_diversificati/informatica/cert/
[326] http://cert-rafvg.regione.fvg.it/
[327] http://cert.chiesacattolica.it/
[328] http://www.ict-ce.it/
[329] http://www.aipsi.org/
[330] http://www.clusit.it/
[331] http://security.dsi.unimi.it/
[332] http://www.sicurinrete.it/il-centro/
[333] http://www.telecomitalia.it/
[334]
http://www.sviluppoeconomico.gov.it/index.php?option=com_content&view=article&viewType=1&idarea1=593&idarea2=0&idarea3=0&idarea4=0&andor=AND&sectionid=0&andorcat=AND&partebassaType=0&idareaCalendario1=0&MvediT=1&showMenu=1&showCat=1&showArchiveNewsBotton=0&idmenu=2263&id=2023615
[335] http://daeimplementation.eu/indicator.php?id_country=14&action_n=39
[336] http://www.digitpa.gov.it/notizie/l-agenzia-l-italia-digitale-partecipa-cyber-europe-2012

[337] http://daeimplementation.eu/indicator.php?id_country=14&action_n=38

[338] http://www.ccdcoe.org/6.html

[339] http://narodne-novine.nn.hr/clanci/sluzbeni/298919.html

[340] http://www.epractice.eu/en/document/288433

[341] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20croatia%20_30%20May%2007_En.pdf

[342] http://narodne-novine.nn.hr/clanci/sluzbeni/339036.html

[343] http://www.uvns.hr/

[344] https://www.zsis.hr

[345] http://www.policija.hr/159.aspx

[346] http://www.cert.hr/

[347] http://www.poslovniforum.hr/

[348] http://security.lss.hr

[349] http://www.carnet.hr

[350] http://fsec.foi.hr/#topics

[351] http://www.enisa.europa.eu/media/news-items/visit-by-croatia-to-enisa-cyber-security-cooperation-with-a-new-eu-member-state

[352] http://www.carnet.hr/novosti/novosti?news_id=2953

[353] http://www.ocecpr.org.cy/media/documents/General/EC_Doc_StratigikiKevernoasfalias_GR_31-5-2013_CE.pdf

[354] http://www.epractice.eu/en/document/288189

[355] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20cyprus%20_1%20June%2007_En.pdf

[356] http://www.ocecpr.org.cy/nqcontent.cfm?a_id=1&tt=ocecpr&lang=gr

[357] http://www.mof.gov.cy/mof/dits/dits.nsf

[358] http://www.police.gov.cy/

[359] http://www.army.gov.cy/

[360] http://www.police.gov.cy/police/police.nsf/dmldept16_gr/dmldept16_gr?OpenDocument
[361] http://www.dataprotection.gov.cy/
[362] http://www.mcw.gov.cy/mcw/mcw.nsf
[363] http://www.mcw.gov.cy/mcw/dec/dec.nsf/
[364] http://www.moi.gov.cy/moi/cd/cd.nsf
[365] http://security.cynet.ac.cy/
[366] https://www.ccs.org.cy/
[367] http://www.cynet.ac.cy/
[368] www.cyberethics.info
[369] http://daeimplementation.eu/indicator.php?id_country=4&action_n=40
[370] http://www.epractice.eu/en/document/288288
[371] http://likumi.lv/doc.php?id=220962
[372] http://www.epractice.eu/en/document/288289
[373] http://legislationline.org/download/action/download/id/4795/file/Latvia_CC_am2013_en.pdf
[374] https://cert.lv/section/show/18
[375] http://www.sam.gov.lv
[376] https://cert.lv/section/show/50
[377] https://cert.lv/section/show/113
[378] https://defense.lv/2013/08/12/oficiali-nodibinata-kiberaizsardzibas-vieniba/
[379] http://www.dvi.gov.lv/en/
[380] http://www.cert.lv/
[381] http://www.likta.lv
[382] http://www.lia.lv
[383] http://daeimplementation.eu/indicator.php?id_country=15&action_n=41
[384] http://www.drossinternets.lv/page/74
[385] http://daeimplementation.eu/indicator.php?id_country=15&action_n=40
[386] https://www.esidross.lv
[387] https://cert.lv/resource/show/241
[388] http://daeimplementation.eu/indicator.php?id_country=15&action_n=39

[389] https://cert.lv/resource/show/142

[390] https://cert.lv/resource/show/410

[391] http://daeimplementation.eu/indicator.php?id_country=15&action_n=38

[392] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Lithuania_Cyber_Security_Strategy.pdf

[393] http://www.epractice.eu/en/document/5298132

[394] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Lithuania%20_30%20May%2007_En.pdf

[395] http://www.transp.lt

[396] http://www.is.lt

[397] http://www.rrt.lt

[398] https://www.ada.lt

[399] http://www.cyberpolice.lt/

[400] https://www.cert.lt

[401] http://daeimplementation.eu/indicator.php?id_country=16&action_n=38

[402] http://www.is.lt/en/svdpt-cert_117.html

[403] https://cert.litnet.lt/lt

[404] http://www.infobalt.lt

[405] http://www.rrt.lt/lt/verslui/tinklu-ir-informacijos-saugumas/draugiskas-internetas.html

[406] http://daeimplementation.eu/indicator.php?id_country=16&action_n=40

[407] http://www.rrt.lt/lt/verslui/tinklu-ir-informacijos-saugumas/esaugumas.html

[408] http://www.rrt.lt/lt/verslui/tinklu-ir-informacijos-saugumas/enisa_969/enisa_972.html

[409] http://www.ccdcoe.org/172.html

[410] http://www.mediacom.public.lu/cybersecurity/index.html

[411] http://www.mediacom.public.lu/cybersecurity/Strat__gieCybersecurity_122011.pdf

[412] http://www.epractice.eu/en/document/288307

[413] http://www.hcpn.public.lu/

[414] http://www.hcpn.public.lu/comites_nationaux/conatic/index.html

[415] http://www.hcpn.public.lu/comites_nationaux/conatel/index.html
[416] http://www.ccg.public.lu/
[417]http://www.fonction-publique.public.lu/fr/structure-organisationnelle/ctie/index.html
[418] http://www.cnpd.public.lu/
[419] http://www.police.public.lu/conseils_prevention/computer-internet/index.html
[420] http://www.smile.public.lu/
[421] http://www.circl.lu/
[422] http://daeimplementation.eu/indicator.php?id_country=17&action_n=38
[423] http://www.govcert.lu/
[424] http://www.malware.lu/
[425] http://www.restena.lu/csirt/
[426] http://www.csrrt.org/
[427] http://www.isoc.lu/
[428] http://www.apsi.lu/
[429] http://www.fedil.lu/fr/about-fedil/mission-et-action/
[430] https://clusil.lu
[431] http://wwwen.uni.lu/recherche/fstc/laboratory_of_algorithmics_cryptology_and_security_lacs
[432] http://wwwen.uni.lu/snt
[433] http://www.restena.lu/
[434] https://www.bee-secure.lu
[435] http://daeimplementation.eu/indicator.php?id_country=17&action_n=40
[436] https://www.cases.lu
[437] http://2013.hack.lu/
[438] http://ict.investinluxembourg.lu/ict/luxembourg-joins-forces-belgium-and-netherlands-towards-increased-cybersecurity
[439] https://www.mita.gov.mt/MediaCenter/PDFs/1_MITA%20Strategic%20Plan%202009-2012%20(web).pdf
[440] http://unpan1.un.org/intradoc/groups/public/documents/UNPAN/UNPAN034350.pdf

[441] https://mita.gov.mt/en/Pages/Digital%20Malta/Digital-Malta.aspx

[442] http://www.epractice.eu/en/document/288316

[443] http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8574

[444] https://mita.gov.mt

[445] http://www.mca.org.mt/

[446] http://www.police.gov.mt/mt-mt/cybercrimeunit.aspx

[447] http://idpc.gov.mt/

[448] http://ciipmalta.gov.mt

[449] http://ciipmalta.gov.mt/csirtmalta

[450] http://maltainfosec.org

[451] http://www.mcast.edu.mt

[452] http://ciipmalta.gov.mt/ourpartners?l=1

[453] https://www.mita.gov.mt/en/Security/SecurityAwareness/Pages/SecurityAwareness.aspx

[454] http://www.saferinternet.org/malta

[455] http://daeimplementation.eu/indicator.php?id_country=18&action_n=40

[456] http://besmartonline.org.mt/

[457] http://www.enisa.europa.eu/media/news-items/exercises-boost-cooperation

[458] https://www.enisa.europa.eu/media/news-items/dutch-cyber-security-strategy-2011

[459] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NCSS2Engelseversie.pdf

[460] http://www.epractice.eu/en/document/288325

[461] http://www.legislationline.org/documents/id/4693

[462] http://www.rijksoverheid.nl/ministeries/ez

[463] http://www.agentschaptelecom.nl/radiocommunications-agency

[464] http://www.rijksoverheid.nl/ministeries/bzk

[465] http://www.logius.nl/

[466] http://www.rijksoverheid.nl/ministeries/venj

[467] www.politie.nl

[468] http://www.defensie.nl/

[469] http://www.defensie.nl/_system/handlers/generaldownloadHandler.ashx?filename=/english/media/cyberbrochure_engels_tcm48-199915.pdf
[470] http://www.dutchdpa.nl/
[471] https://www.ncsc.nl/
[472] http://www.nederlandict.nl/
[473] http://www.sentinels.nl/
[474] http://www.safe-nl.org/
[475] http://www.tue.nl/
[476] www.ru.n
[477] http://www.digibewust.nl/
[478] http://daeimplementation.eu/indicator.php?id_country=19&action_n=40
[479] http://www.blackhat.com/
[480] http://conference.hitb.org/
[481] http://daeimplementation.eu/indicator.php?id_country=19&action_n=39
[482] https://www.ncsc.nl/organisatie/samenwerkingspartners/internationaal.html
[483] http://www.nato.int/cps/en/natolive/news_69805.htm
[484] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/HU_NCSS.pdf
[485] http://www.epractice.eu/en/document/288261
[486] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Hungary%20_7%20June%2007_En.pdf
[487] http://www.kormany.hu/hu/nemzeti-fejlesztesi-miniszterium/infokommunikacioert-felelos-allamtitkarsag/felelossegi-teruletek
[488] http://www.nbf.hu
[489] http://www.naih.hu/
[490] http://police.hu
[491] http://www.cert-hungary.hu
[492] http://daeimplementation.eu/indicator.php?id_country=12&action_n=38
[493] http://csirt.niif.hu/
[494] http://www.cert.hu/

[495] http://english.ivsz.hu

[496] http://www.inforum.org.hu/

[497] http://www.mte.hu

[498] http://www.niif.hu

[499] http://www.it2.bme.hu

[500] http://daeimplementation.eu/indicator.php?id_country=12&action_n=41

[501] http://daeimplementation.eu/indicator.php?id_country=12&action_n=40

[502] http://nws.niif.hu/nws2014/index_desktop.php

[503] http://daeimplementation.eu/indicator.php?id_country=12&action_n=39

[504] http://ccdcoe.org/188.html

[505] http://www.nato.int/cps/en/natolive/news_105205.htm

[506] http://www.cert-hungary.hu/node/156

[507] http://www.dhs.gov/xlibrary/assets/cyber-storm-3-media-fact-sheet.pdf

[508] http://www.cert-hungary.hu/en/node/92

[509] http://www.cert-hungary.hu/en/node/165

[510] http://www.cert-hungary.hu/en/node/53

[511] http://www.cert-hungary.hu/en/node/39

[512] http://daeimplementation.eu/indicator.php?id_country=12&action_n=38

[513] http://bip.msw.gov.pl/bip/programy/19057,dok.html

[514] http://www.epractice.eu/en/document/288334

[515] https://mac.gov.pl

[516] http://www.abw.gov.pl/

[517] http://rcb.gov.pl/

[518] http://www.en.uke.gov.pl/

[519] http://www.giodo.gov.pl/

[520] http://www.policja.pl/pol/kgp/biuro-sluzby-kryminaln/bsk-struktura-i-zadani/bsk-wydzial-wsparcia-z-1/8082,dok.html

[521] http://www.cert.gov.pl/

[522] http://www.cert.pl/

[523] http://www.orange.pl/bezpieczenstwo_w_sieci.phtml

[524] http://cert.pionier.gov.pl/

[525] http://www.piit.org.pl/

[526] http://www.nask.pl/

[527] http://www.cyfronet.krakow.pl/
[528] http://www.cert.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html
[529] http://daeimplementation.eu/indicator.php?id_country=20&action_n=38
[530] http://www.saferinternet.pl/
[531] http://daeimplementation.eu/indicator.php?id_country=20&action_n=40
[532] http://www.secure.edu.pl/
[533] http://www.css.umcs.lublin.pl/
[534] http://www.enisa.europa.eu/media/press-releases/online-security-it2019s-in-your-interest-1st-european-cyber-security-month-coming-up-in-october
[535] http://www.abw.gov.pl/pl/aktualnosci/717,Porozumienie-ABW-i-NATO-w-sprawie-cyberobrony.html?search=2041620
[536] http://www.abw.gov.pl/pl/aktualnosci/709,Polska-NATO-wspolpraca-w-sferze-cyberbezpieczenstwa.html?search=2041620
[537] http://www.ccdcoe.org/295.html
[538] eGovernment in Portugal, Septemper 2011, version 15.0, European Commission/ http://www.epractice.eu/files/eGovernmentPortugal.pdf
[539] http://www.epractice.eu/en/document/288343
[540]http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/Cybercrime_Law_n_109_2009_Portugal.pdf
[541] http://www.cert.pt/index.php/recomendacoes/1732-quem-e-quem-na-ciberseguranca-nacional-mes-europeu-da-ciber-seguranca-2013
[542] http://www.gns.gov.pt/
[543] www.anacom.pt
[544] http://www.pj.pt/
[545] www.umic.pt
[546] www.cnpd.pt
[547] www.cert.pt
[548] http://csirt.fe.up.pt
[549] https://www.dognaedis.com/
[550] http://csirt.telecom.pt
[551] www.anetie.pt
[552] http://www.anetie.pt/website.aspx?p=190
[553] www.apritel.org

[554] www.fccn.pt

[555] http://cert.pt/index.php/noticias/1612-anunciados-resultados-de-forum-para-a-ciberseguranca

[556] http://cert.pt/index.php/servicos/coordenacao-de-incidentes

[557] http://www.internetsegura.net

[558] http://daeimplementation.eu/indicator.php?id_country=21&action_n=40

[559] http://cert.pt/index.php/noticias/1733-cert-pt-no-exercicio-cyber-coalition-2013-da-nato

[560] http://daeimplementation.eu/indicator.php?id_country=21&action_n=39

[561] http://cert.pt/index.php/noticias/1613-exercicio-de-ciberseguranca-cyber-europe-2010

[562] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012

[563] http://www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf

[564] http://www.epractice.eu/en/document/288406

[565] http://www.cybercrimelaw.net/Romania.html

[566] http://www.mcsi.ro/

[567] http://www.sri.ro/

[568] http://www.mapn.ro/

[569] http://www.efrauda.ro/

[570] http://www.diicot.ro/

[571] http://www.stsnet.ro/

[572] http://www.dataprotection.ro/

[573] http://www.mai.gov.ro/

[574] http://www.cert-ro.eu/

[575] https://corisweb.stsisp.ro

[576] https://en.csirt.ro/

[577] http://www.anisp.ro/

[578] http://www.atic.org.ro/

[579] http://www.mta.ro/

[580] http://www.inscc.ro/

[581] http://www.sigur.info/

[582] http://daeimplementation.eu/indicator.php?id_country=22&action_n=41

[583] http://www.cert-ro.eu/articol.php?idarticol=777
[584] http://www.cert-ro.eu/articol.php?idarticol=606
[585] http://daeimplementation.eu/indicator.php?id_country=22&action_n=41
[586] http://www.cert-ro.eu/evenimente.php
[587] http://daeimplementation.eu/indicator.php?id_country=22&action_n=39
[588] http://daeimplementation.eu/indicator.php?id_country=22&action_n=38
[589] http://www.nato.int/cps/en/natolive/news_82213.htm
[590] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/Slovakia_National_Strategy_for_ISEC.pdf
[591] http://www.epractice.eu/en/document/288352
[592] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Slovakia%20_30%20May%2007_En.pdf
[593] http://legislationline.org/documents/section/criminal-codes
[594] http://www.nbusr.sk/
[595] http://www.finance.gov.sk/
[596] http://www.minv.sk/
[597] http://www.minv.sk/?policia
[598] http://www.mod.gov.sk/
[599] http://www.dataprotection.gov.sk/
[600] https://www.csirt.gov.sk/
[601] http://ww.sasib.sk/
[602] http://itas.sk/
[603] http://new.dcs.fmph.uniba.sk/index.php/Aktualne
[604] http://www.mod.gov.sk/unikatne-cvicenie-preveri-slovenskych-vojenskych-it-specialistov-zaskisu/
[605] http://www.mod.gov.sk/cyber-defence-exercise-locked-shields-2012/
[606] http://www.nato.int/cps/en/SID-1548CA52-7F7E361B/natolive/news_105205.htm?selectedLocale=en
[607] http://daeimplementation.eu/indicator.php?id_country=23&action_n=39
[608] http://www.epractice.eu/en/document/288360
[609] http://www.epractice.eu/en/document/288361

[610] http://www.cybercrimelaw.net/Slovenia.html
[611] http://www.mizs.gov.si/si/delovna_podrocja/direktorat_za_informacijsko_druzbo/
[612] http://www.arhiv.mju.gov.si/en/areas_of_work/index.html
[613] http://www.akos-rs.si/
[614] http://www.uvtp.gov.si/
[615] https://www.ip-rs.si
[616] http://www.policija.si/eng/index.php/component/content/article/59-criminal-police-directorate/1073-national-bureau-of-investigation
[617] https://www.cert.si
[618] http://daeimplementation.eu/indicator.php?id_country=24&action_n=38
[619] http://www.gzs.si/
[620] http://www.gzs.si/slo/regije/zbornica_osrednjeslovenske_regije/o_zbornici/organiziranost/sekcija_za_upravljanje_varovanja_informacij
[621] http://www.arnes.si/
[622] http://www.ris.org/
[623] https://www.varninainternetu.si
[624] http://www.safe.si/
[625] http://daeimplementation.eu/indicator.php?id_country=24&action_n=40
[626] http://www.suvi.si/
[627] http://varnostnaspletu.si/
[628] http://daeimplementation.eu/indicator.php?id_country=24&action_n=38
[629] https://www.cert.si/vaja-cyber-europe-2012/
[630] http://daeimplementation.eu/indicator.php?id_country=24&action_n=39
[631] http://www.nato.int/cps/en/natolive/news_91115.htm?mode=pressrelease
[632] https://www.msb.se/Upload/Produkter_tjanster/Publikationer/KBM/Information%20Security%20in%20Sweden.pdf
[633] http://www.epractice.eu/en/document/288379
[634] http://legislationline.org/download/action/download/id/1700/file/4c405aed10fb48cc256dd3732d76.pdf

[635] http://rib.msb.se/Filer/pdf/26177.pdf
[636] https://www.msb.se
[637] http://www.pts.se/
[638] http://www.fra.se/
[639] http://www.sakerhetspolisen.se
[640] http://www.fmv.se/en/Our-activities/CSEC---The-Swedish-Certification-Body-for-IT-Security/
[641] http://www.forsvarsmakten.se/en/our-organisation/our-forces/intelligence-and-security-service/
[642] http://polisen.se/en/Languages/The-Swedish-Police/Direction-/National-Criminal-Police-/
[643] http://www.datainspektionen.se/
[644] https://www.cert.se
[645] http://www.liu.se/
[646] http://www.snic.vr.se/snic-committees/sist
[647] http://www.teliasonera.com/
[648] http://www.itotelekomforetagen.se/
[649] http://www.sigsecurity.org/
[650] http://dsv.su.se/en/research/research-areas/security
[651] http://www.lith.liu.se/
[652] https://www.sics.se
[653] http://www.statensmedierad.se/
[654] https://www.msb.se/RibData/Filer/pdf/25653.pdf
[655] http://www.pts.se/upload/Ovrigt/Internet/PTS_Telo11_ENG_webb.pdf
[656] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/presentations/roger-holfeldt-msb-sweden-the-national-cyber.pdf
[657] http://www.defensenews.com/article/20121102/DEFREG01/311020001/Cyber-Defense-Takes-Center-Stage-Nordic-Cooperation
[658] https://www.msb.se/Templates/Pages/NewsPage.aspx?id=9301&epslanguage=en
[659] http://www.govcert.cz/download/nodeid-1190/
[660] http://www.epractice.eu/en/document/288198

[661] http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567-LEG-country%20profile%20Czech%20Rep%20_30%20May%2007_En.pdf

[662] http://www.nbu.cz

[663] http://www.nbu.cz/cs/o-nas/organizacni-struktura/narodni-centrum-kyberneticke-bezpecnosti/

[664] www.uoou.cz

[665] www.mvcr.cz/egovernment.aspx

[666] http://www.bis.cz/informacni-systemy.html

[667] http://www.policie.cz

[668] http://www.csirt.cz/page/884/cooperation/

[669] http://www.csirt.cz/

[670] http://www.govcert.cz/

[671] http://www.cesnet.cz

[672] http://www.muni.cz/ics/services/csirt

[673] http://www.active24.cz/csirt/

[674] http://napoveda.seznam.cz/cz/csirt/en/

[675] http://www.nic.cz

[676] http://www.ictu.cz/

[677] https://www.muni.cz/ics/research/projects/23963?lang=cs

[678] http://www.fit.cvut.cz/en/prospective-students/master/computer-security

[679] http://newsroom.cisco.com/press-release-content?articleId=1267895

[680] https://cythres.fd.cvut.cz/

[681] http://www.itsw.cz/

[682] http://itevent.net/3rd-annual-cyber-security-summit/

[683] http://daeimplementation.eu/indicator.php?id_country=5&action_n=39

[684] http://www.mzv.cz/nato.brussels/en/news_articles_speeches/czech_republic_signed_mou_on_cyber.html

[685] http://www.csirt.cz/page/884/cooperation/

[686] http://daeimplementation.eu/dae_actions.php?action_n=38&id_country=1

[687] http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

[688] http://www.epractice.eu/en/document/288225

[689] http://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf

[690] http://www.lvm.fi

[691] https://www.viestintavirasto.fi

[692] http://www.ministryoffinance.fi

[693] http://www.nesa.fi

[694] http://www.tietosuoja.fi

[695] https://www.cert.fi/

[696] http://www.csc.fi

[697] http://www.ficom.fi

[698] http://www.f-secure.com

[699]
http://www.utu.fi/en/units/sci/units/it/research/informationsecurity/Pages/home.aspx

[700] https://www.ee.oulu.fi/research/ouspg/

[701] http://www.policecollege.fi/

[702] http://www.cs.helsinki.fi

[703] http://www.meku.fi/fisic

[704] http://daeimplementation.eu/indicator.php?id_country=8&action_n=40

[705] https://www.viestintavirasto.fi/en/ficora/news/2012/P_52.html

[706] http://t2.fi/

[707] http://www.ccdcoe.org/447.html

[708] http://daeimplementation.eu/dae_actions.php?action_n=38&id_country=1

[709]
http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=2/27/2008&CL=ENG

ΠΑΡΑΡΤΗΜΑΤΑ

Παράρτημα Α Πίνακας Ανάλυσης Πλεονεκτημάτων Μειονεκτημάτων

Μέλος Ε.Ε.	+	-
Αυστρία 	-Στρατηγική Κυβερνοασφάλειας - Σύνολο Στρατηγικών -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Cert's ανά κοινωνικοοικονομικό τομέα -Πρόγραμμα Ευαισθητοποίησης πολιτών -Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων	
Βέλγιο 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών - Κέντρο Αριστείας Κυβερνοεγκλήματος -Καλή Συνεργασία με ιδιωτικό τομέα	-Έλλειψη εθνικής στρατηγικής -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Βουλγαρία 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Πρόγραμμα Ευαισθητοποίησης πολιτών - Κέντρο Αριστείας Κυβερνοεγκλήματος	-Έλλειψη εθνικής στρατηγικής -Μη συμμετοχή σε διεθνείς ασκήσεις -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Γαλλία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Cert's ανά κοινωνικοοικονομικό τομέα -Ύπαρξη πολλών Cert's -Πρόγραμμα Ευαισθητοποίησης πολιτών -Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων - Κέντρο Αριστείας Κυβερνοεγκλήματος	
Γερμανία 	-Στρατηγική Κυβερνοασφάλειας - Σύνολο Στρατηγικών -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Cert's ανά κοινωνικοοικονομικό τομέα -Ύπαρξη πολλών Cert's -Πρόγραμμα Ευαισθητοποίησης πολιτών -Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων - Τεχνογνωσία ιδιωτικού τομέα - Καλή Συνεργασία με ιδιωτικό τομέα	

Μέλος Ε.Ε.	+	-
Δανία 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών -Καλή Συνεργασία με ιδιωτικό τομέα	-Έλλειψη εθνικής στρατηγικής -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Ελλάδα 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών - Κέντρο Αριστείας Κυβερνοεγκλήματος	-Έλλειψη εθνικής στρατηγικής -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων -Προτεραιότητα της εθνικής Cert είναι η αντιμετώπιση και όχι η πρόληψη -Μέτρια διεθνής συνεργασία
Εσθονία 	-Στρατηγική Κυβερνοασφάλειας - Σύνολο Στρατηγικών -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών - Κέντρο Αριστείας Κυβερνοεγκλήματος	-Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Ηνωμένο Βασίλειο 	-Στρατηγική Κυβερνοασφάλειας - Σύνολο Στρατηγικών -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Cert's ανά κοινωνικοοικονομικό τομέα -Ύπαρξη πολλών Cert's -Πρόγραμμα Ευαισθητοποίησης πολιτών -Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων - Κέντρο Αριστείας Κυβερνοεγκλήματος - WARP's - Τεχνογνωσία ιδιωτικού τομέα -Καλή Συνεργασία με ιδιωτικό τομέα	
Ιρλανδία 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών -Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων - Κέντρο Αριστείας Κυβερνοεγκλήματος - Τεχνογνωσία ιδιωτικού τομέα	-Έλλειψη εθνικής στρατηγικής - Μικρή κυβερνητική συμμετοχή. -Μη επιχειρησιακή εθνική Cert - Μη ικανοποιητική διεθνής συνεργασία

Μέλος Ε.Ε.	+	-
Ισπανία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Cert's ανά κοινωνικοοικονομικό τομέα -Ύπαρξη πολλών Cert's -Πρόγραμμα Ευαισθητοποίησης πολιτών -Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων - Κέντρο Αριστείας Κυβερνοεγκλήματος - Τεχνογνωσία ιδιωτικού τομέα -Καλή Συνεργασία με ιδιωτικό τομέα	
Ιταλία 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Cert's ανά κοινωνικοοικονομικό τομέα -Ύπαρξη πολλών Cert's -Πρόγραμμα Ευαισθητοποίησης πολιτών	-Έλλειψη εθνικής στρατηγικής -Μη επιχειρησιακή εθνική Cert -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Κροατία 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Συμμετοχή σε διεθνείς ασκήσεις	-Έλλειψη εθνικής στρατηγικής -Μη διεξαγωγή εθνικών ασκήσεων -Έλλειψη Προγράμματος Ευαισθητοποίησης πολιτών -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων - Μέτρια διεθνής συνεργασία
Κύπρος 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Πρόγραμμα Ευαισθητοποίησης πολιτών	-Μη διεξαγωγή εθνικών ασκήσεων -Μη συμμετοχή σε διεθνείς ασκήσεις -Μη επιχειρησιακή εθνική Cert -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων - Μη ικανοποιητική διεθνής συνεργασία - Ελλιπής ερευνητική δραστηριότητα
Λετονία 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών	-Έλλειψη εθνικής στρατηγικής -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Λιθουανία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών	-Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Λουξεμβούργο 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Πρόγραμμα Ευαισθητοποίησης πολιτών -Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων -Καλή Συνεργασία με ιδιωτικό τομέα	-Μη διεξαγωγή εθνικών ασκήσεων -Μη συμμετοχή σε διεθνείς ασκήσεις

Μέλος Ε.Ε.	+	-
Μάλτα 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Πρόγραμμα Ευαισθητοποίησης πολιτών -Καλή Συνεργασία με ιδιωτικό τομέα	-Έλλειψη εθνικής στρατηγικής -Μη διεξαγωγή εθνικών ασκήσεων -Μη συμμετοχή σε διεθνείς ασκήσεις -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων - Μη ικανοποιητική διεθνή συνεργασία - Ελλιπής ερευνητική δραστηριότητα
Ολλανδία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Ύπαρξη πολλών Cert's -Cert's ανά κοινωνικοοικονομικό τομέα -Πρόγραμμα Ευαισθητοποίησης πολιτών -Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων -Καλή Συνεργασία με ιδιωτικό τομέα	
Ουγγαρία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών	-Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Πολωνία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών -Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων -Καλή Συνεργασία με ιδιωτικό τομέα	-Μη διεξαγωγή εθνικών ασκήσεων
Πορτογαλία 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Cert's ανά κοινωνικοοικονομικό τομέα -Πρόγραμμα Ευαισθητοποίησης πολιτών	-Έλλειψη εθνικής στρατηγικής -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων - Μέτρια διεθνής συνεργασία
Ρουμανία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών - Κέντρο Αριστείας Κυβερνοεγκλήματος	-Μη διεξαγωγή εθνικών ασκήσεων -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Σλοβακία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών	-Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων

Μέλος Ε.Ε.	+	-
Σλοβενία 	-Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Συμμετοχή σε διεθνείς ασκήσεις -Πρόγραμμα Ευαισθητοποίησης πολιτών	-Έλλειψη εθνικής στρατηγικής -Μη διεξαγωγή εθνικών ασκήσεων - Μέτρια διεθνής συνεργασία Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Σουηδία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Cert's ανά κοινωνικοοικονομικό τομέα -Πρόγραμμα Ευαισθητοποίησης πολιτών	-Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων
Τσεχία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Συμμετοχή σε διεθνείς ασκήσεις -Cert's ανά κοινωνικοοικονομικό τομέα -Πρόγραμμα Ευαισθητοποίησης πολιτών	-Μη διεξαγωγή εθνικών ασκήσεων -Έλλειψη Προγράμματος Ευαισθητοποίησης Επιχειρήσεων - Μέτρια διεθνής συνεργασία
Φινλανδία 	-Στρατηγική Κυβερνοασφάλειας -Υιοθέτηση Ευρωπαϊκής νομοθεσίας -Διεξαγωγή εθνικών ασκήσεων -Συμμετοχή σε διεθνείς ασκήσεις -Cert's ανά κοινωνικοοικονομικό τομέα -Πρόγραμμα Ευαισθητοποίησης πολιτών -Πρόγραμμα Ευαισθητοποίησης Επιχειρήσεων - Τεχνογνωσία ιδιωτικού τομέα -Καλή Συνεργασία με ιδιωτικό τομέα	

Παράρτημα Β Πίνακας Ανάλυσης Δράσεων

Μέλος Ε.Ε.	**Στρατηγική Κυβερνοασφάλειας**	**Νομοθεσία κυβερνοεγκλήματος/ Κύρωση σύμβασης Συμβούλιου της Ευρώπης***	**Εθνικές Ασκήσεις**	**Διεθνείς Ασκήσεις**	**Μέλος ITU/IMPACT**	**Μέλος CCDCoE**	**Μέλος 2Centre Network**
	X	X/-	X	X	X	-	-
	-(draft)	X/-	X	X	-	-	X
	-	X/X	X	-	X	-	X
	X	X/X	X	X	-	-	X
	X	X/-	X	X	-	X	-
	-	X/X	X	X	-	-	-
	-	X/-	X	X	-	-	X
	X	X/X	X	X	-	X	X
	X	X/-	X	X	-	-	X
	-	X/-	X	X	-	-	X
	X	X/-	X	X	X	X	X
	-	X/-	X	X	X	X	-
	-	X/X	-	X	X	-	-
	X	X/X	-	-	X	-	-

Μέλος Ε.Ε.	Στρατηγική Κυβερνοασφάλειας	Νομοθεσία κυβερνοεγκλήματος/ Κύρωση σύμβασης Συμβούλιου της Ευρώπης*	Εθνικές Ασκήσεις	Διεθνείς Ασκήσεις	Μέλος ITU/IMPACT	Μέλος CCDCoE	Μέλος 2Centre Network
	-	X/X	X	X	-	X	-
	X	X/X	X	X	X	X	-
	X	X/-	-	-	-	-	-
	-	X/-	-	-	X	-	-
	X	X/X	X	X	-	X	-
	X	X/X	X	X	-	X	-
	X	X/-	-	X	X	X	-
	-	X/-	X	X	-	-	-
	X	X/X	-	X	X	-	X
	X	X/X	X	X	X	X	-
	-	X/X	-	X	X	-	-
	X	X/-	X	X	-	-	-
	X	X/-	-	X	X	X	-
	X	X/X	X	X	-	-	-

* Κατάσταση από: 27/2/2008 [709]

X = έχει υλοποιηθεί,

- = δεν έχει υλοποιηθεί

Παράρτημα Γ Πίνακας Ανάλυσης Cert's

Μέλος Ε.Ε.	Αρ. CERTS	Μέλη FIRST	ΤΙ διαπιστευμένα / πιστοποιημένα	Συμμετοχή σε ECG	Συμμετοχή σε Ceenet
	5	3	2/-	X	
	3	1	2/-		
	1	-	1/-		X
	11	6	5/-	X	
	25	19	12/1	X	
	6	5	3/-	X	
	4	1	2/1		
	1	1	1/-		X
	22	15	3/-	X	
	4	-	1/-		
	15	10	8/-	X	
	8	-	2/-		
	3	3	2/-		
	1	0	-/-		
	1	1	1/-		
	4	3	3/-		X

Μέλος Ε.Ε.	Αρ. CERTS	Μέλη FIRST	ΤΙ διαπιστευμένα / πιστοποιημένα	Συμμετοχή σε ECG	Συμμετοχή σε Ceenet
	5	0	4/-		
	1	0	1/-		
	16	8	4/2	X	
	3	1	1/-		X
	4	2	1/-		
	4	1	4/-		
	3	0	1/-		X
	1	0	1/-		X
	1	1	1/-		X
	7	3	6/2	X	
	7	0	4/-		X
	5	4	3/-	X	

X = έχει υλοποιηθεί,

- = δεν έχει υλοποιηθε

Παράρτημα Δ Πίνακας Ανάλυσης Προγραμμάτων Ευαισθητοποίησης

Μέλος Ε.Ε.	**Εθνικό Πρόγραμμα Ευαισθητοποίησης**	**Ύπαρξη γραμμής επικοινωνίας/Υποστήριξη από αρχές επιβολής του νόμου**
	X	X/X
	X	X/-
	X	X/-
	X	X/X
	X	X/X
	X	X/X
	X	X/X
	X	X/X
	X	X/X
	X	X/X
	X	X/X
	X	X/X
	-	-
	X	X/-
	X	X/X

Μέλος Ε.Ε.	**Εθνικό Πρόγραμμα Ευαισθητοποίησης**	**Ύπαρξη γραμμής επικοινωνίας/Υποστήριξη από αρχές επιβολής του νόμου**
	X	X/X
	X	X/X
	X	X/X
	X	-/-
	X	X/X
	X	X/X
	X	X/X
	X	X/X
	X	X/-
	X	X/X
	X	X/X
	X	X/-
	X	X/X

X = έχει υλοποιηθεί,

- = δεν έχει υλοποιηθε