Πανεπιστήμιο Πειραιώς

Σχολή Τεχνολογιών Πληροφορικής και Επικοινωνιών

Τμήμα Ψηφιακών Συστημάτων

Πρόγραμμα Μεταπτυχιακών Σπουδών

Ασφάλεια Ψηφιακών Συστημάτων

Μεταπτυχιακή Διατριβή με θέμα:

Ανάπτυξη εκπαιδευτικού υλικού σε θέματα Κυβερνοασφάλειας (Cybersecurity), με έμφαση σε Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (Operators of Essential Services) της NIS Directive 2016/1148 (N.4577/2018)

Επιβλέπων Καθηγητής: Στέφανος Γκρίτζαλης

Πανδώρα Τσιλίκη tsilikipan@gmail.com ΜΤΕ2032

Πειραιάς

19/12/2022

Περίληψη

Στόχος της παρούσας Μεταπτυχιακής Διατριβής είναι η Ανάπτυξη εκπαιδευτικού υλικού σε θέματα Κυβερνοασφάλειας (Cybersecurity), με έμφαση σε Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (Operators of Essential Services) της NIS Directive 2016/1148 (Ν.4577/2018). Για τον σκοπό αυτό πραγματοποιήθηκε εις βάθος μελέτη των σχετικών προτύπων ISO/IEC σε σχέση με την Κυβερνοασφάλεια καθώς και της ισχύουσας ελληνικής νομοθεσίας και των σχετικών Οδηγιών της Ευρωπαϊκής Ένωσης τόσο των υπό έκδοση αλλά και των προτάσεων που έχουν κατατεθεί.

Συγκεκριμένα δόθηκε έμφαση στο ISO/IEC 27032:2012 σχετικά με την Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κατευθυντήριες γραμμές για την ασφάλεια στον κυβερνοχώρο, στο ISO/IEC 27100:2020 σχετικά με την Τεχνολογία πληροφοριών – Κυβερνοασφάλεια – Επισκόπηση και έννοιες και στο ISO/IEC 27110:2021 σχετικά με Τεχνολογία πληροφοριών, κυβερνοασφάλεια και προστασία ιδιωτικότητας – Οδηγίες ανάπτυξης προτύπου ιδιωτικότητας. Επιπλέον, λήφθηκαν υπ’ όψη οι απαιτήσεις του νόμου υπ’ αριθμών 4577 της 3ης Δεκεμβρίου του 2018 με τον οποίο πραγματοποιήθηκε ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις. Τέλος, πραγματοποιήθηκε ενδελεχής μελέτη της υπό έκδοση Οδηγίας του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου η οποία αναμένεται να αναβαθμίσει τις απατήσεις 2016/1148/ΕΕ και αντίστοιχα να ενσωματωθεί στις εθνικές διατάξεις των μελών της Κοιτνότητας.

Περιεχόμενα

1 Αντικείμενο

Το παρόν Διεθνές Πρότυπο παρέχει καθοδήγηση για τη βελτίωση της κατάστασης της Κυβερνοασφάλειας, επισημαίνοντας τις μοναδικές πτυχές αυτής της δραστηριότητας και τις εξαρτήσεις της από άλλους τομείς της ασφάλειας, ειδικότερα:

- την ασφάλεια πληροφοριών,

- την ασφάλεια δικτύων,

- την ασφάλεια του διαδικτύου, και

- την προστασία των υποδομών πληροφοριών ζωτικής σημασίας (critical information infrastructure protection, CIIP).

Καλύπτει τις βασικές πρακτικές ασφάλειας των ενδιαφερόμενων μερών στον Κυβερνοχώρο. Το παρόν διεθνές πρότυπο παρέχει:

- μια επισκόπηση της ασφάλειας στον κυβερνοχώρο,

- εξήγηση της σχέσης μεταξύ της Κυβερνοασφάλειας και άλλων τύπων ασφάλειας,

- ορισμό των ενδιαφερομένων μερών και περιγραφή των ρόλων τους στην Κυβερνοασφάλεια,

- καθοδήγηση για την αντιμετώπιση συνήθισμένων ζητημάτων Κυβερνοασφάλειας, και

- ένα πρότυπο που επιτρέπει στα ενδιαφερόμενα μέρη να συνεργάζονται για την επίλυση ζητημάτων Κυβερνοασφάλειας.

2. Εφαρμογή

2.1 Κοινό στο οποίο απευθύνεται

Το παρόν Διεθνές Πρότυπο έχει εφαρμογή στους παρόχους υπηρεσιών στον Κυβερνοχώρο. Το κοινό, ωστόσο, περιλαμβάνει τους καταναλωτές που χρησιμοποιούν αυτές τις υπηρεσίες. Όταν οι οργανισμοί παρέχουν υπηρεσίες στον Κυβερνοχώρο σε ανθρώπους για οικιακή χρήση ή για χρήση σε άλλους οργανισμούς, μπορεί να χρειαστεί να προετοιμάσουν καθοδήγηση με βάση το παρόν Διεθνές Πρότυπο η οποία να περιέχει πρόσθετες επεξηγήσεις ή παραδείγματα επαρκή που θα επιτρέψουν στον αναγνώστη να την κατανοήσει και να ενεργήσει σύμφωνα με αυτήν.

2.2 Περιορισμοί

Το παρόν διεθνές πρότυπο δεν αφορά:

- Την Κυβερνοασφάλεια,

- Το κυβερνοέγκλημα,

- Την προστασία των υποδομών πληροφοριών ζωτικής σημασίας,

- Την Ασφάλεια στο Διαδίκτυο, και

- Το έγκλημα που σχετίζεται με το Διαδίκτυο.

Αναγνωρίζεται ότι υπάρχουν σχέσεις μεταξύ των προαναφερθέντων τομέων και της Κυβερνοασφάλειας. Ωστόσο, είναι πέρα από το πεδίο εφαρμογής του παρόντος Διεθνούς Προτύπου να εξετάσει αυτές τις σχέσεις και τον διαμοιρασμό μέτρων μεταξύ αυτών των τομέων.

Είναι σημαντικό να σημειωθεί ότι η έννοια του κυβερνοεγκλήματος, αν και αναφέρεται, δεν εξετάζεται. Το παρόν Διεθνές Πρότυπο δεν παρέχει καθοδήγηση σχετικά με νομικές πτυχές του Κυβερνοχώρου ή τους κανονισμούς για την Κυβερνοασφάλεια.

Η καθοδήγηση στο παρόν Διεθνές Πρότυπο περιορίζεται στην κατανόηση του Κυβερνοχώρου στο Διαδίκτυο, συμπεριλαμβανομένων των τερματικών. Ωστόσο, δεν εξετάζεται η επέκταση του Κυβερνοχώρου σε άλλες μορφές μέσω μέσων επικοινωνίας και πλατφορμών, ούτε οι πτυχές της φυσικής ασφάλειας αυτών.

ΠΑΡΑΔΕΙΓΜΑ 1 Δεν εξετάζεται η προστασία των στοιχείων υποδομής, όπως οι φορείς επικοινωνίας, που υποστηρίζουν τον Κυβερνοχώρο.

ΠΑΡΑΔΕΙΓΜΑ 2 Δεν εξετάζεται η φυσική ασφάλεια των κινητών τηλεφώνων που συνδέονται στον Κυβερνοχώρο για τη λήψη ή/και τον χειρισμό περιεχομένου.

ΠΑΡΑΔΕΙΓΜΑ 3 Δεν εξετάζονται οι λειτουργίες ανταλλαγής μηνυμάτων κειμένου και φωνητικής συνομιλίας που παρέχονται για κινητά τηλέφωνα.

3 Κανονιστικές αναφορές

Τα ακόλουθα αναφερόμενα έγγραφα είναι απαραίτητα για την εφαρμογή του παρόντος εγγράφου. Για αναφορές με ημερομηνία, ισχύει μόνο η αναφερόμενη έκδοση. Για παραπομπές χωρίς ημερομηνία, ισχύει η τελευταία έκδοση του εγγράφου στο οποίο γίνεται παραπομπή (συμπεριλαμβανομένων τυχόν τροποποιήσεων).

ISO/IEC 27000, Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Συστήματα διαχείρισης ασφάλειας πληροφοριών - Επισκόπηση και λεξιλόγιο

4. Όροι και ορισμοί

Για τους σκοπούς του παρόντος εγγράφου, ισχύουν οι όροι και ορισμοί που δίνονται στο ISO/IEC 27000, και στα ακόλουθα.

4.1 λογισμικό διαφημίσεων (adware)

εφαρμογή που προωθεί διαφημίσεις στους χρήστες ή/και συλλέγει τη διαδικτυακή συμπεριφορά των χρηστών

ΣΗΜΕΙΩΣΗ Η εφαρμογή μπορεί να εγκατασταθεί εν γνώσει ή εν αγνοία, με ή χωρίς τη συγκατάθεση του χρήστη ή να επιβληθεί στον χρήστη μέσω των όρων αδειοδότησης άλλου λογισμικού.

4.2 εφαρμογή (application)

λύση ΤΠ, που περιλαμβάνει λογισμικό εφαρμογών, δεδομένα εφαρμογών και διαδικασίες, σχεδιασμένη να βοηθά τους χρήστες ενός οργανισμού να εκτελούν συγκεκριμένες εργασίες ή να χειρίζονται συγκεκριμένους τύπους προβλημάτων ΤΠ αυτοματοποιώντας μια επιχειρησιακή διαδικασία ή λειτουργία

[ISO/IEC 27034-1:2011]

4.3 πάροχος υπηρεσιών εφαρμογών (application service provider)

φορέας εκμετάλλευσης που παρέχει φιλοξενούμενη λύση λογισμικού η οποία προσφέρει υπηρεσίες εφαρμογών και περιλαμβάνει μοντέλα παροχής μέσω διαδικτύου ή πελάτη-εξυπηρετητή.

ΠΑΡΑΔΕΙΓΜΑ Διαχειριστές διαδικτυακών παιχνιδιών, πάροχοι εφαρμογών γραφείου και πάροχοι διαδικτυακής αποθήκευσης.

4.4 υπηρεσίες εφαρμογών (application services)

λογισμικό με λειτουργίες που παρέχονται κατά παραγγελία σε συνδρομητές μέσω ενός διαδικτυακού μοντέλου που περιλαμβάνει διαδικτυακές εφαρμογές ή εφαρμογές πελάτη-εξυπηρετητή

4.5 λογισμικό εφαρμογής (application software)

λογισμικό που έχει σχεδιαστεί για να βοηθά τους χρήστες να εκτελούν συγκεκριμένες εργασίες ή να χειρίζονται συγκεκριμένους τύπους προβλημάτων, σε διαφοροποίηση με το λογισμικό που ελέγχει τον ίδιο τον υπολογιστή

[ISO/IEC 18019]

4.6 περιουσιακό στοιχείο (asset)

οτιδήποτε έχει αξία για ένα άτομο, έναν οργανισμό ή μια κυβέρνηση

ΣΗΜΕΙΩΣΗ Προσαρμόστηκε από το ISO/IEC 27000 για να υπάρξει πρόβλεψη για τα άτομα και για τον διαχωρισμό των κυβερνήσεων από τους οργανισμούς (4.37).

4.7 άβαταρ (avatar)

αναπαράσταση ενός προσώπου που συμμετέχει στον κυβερνοχώρο

ΣΗΜΕΙΩΣΗ 1 Ένα άβαταρ μπορεί επίσης να αναφέρεται ως το alter ego ενός ατόμου.

ΣΗΜΕΙΩΣΗ 2 Ένα άβαταρ μπορεί επίσης να θεωρηθεί ως "αντικείμενο" που αντιπροσωπεύει την ενσάρκωση του χρήστη.

4.8 επίθεση (attack)

απόπειρα καταστροφής, έκθεσης, μεταβολής, απενεργοποίησης, κλοπής ή απόπειρα μη εξουσιοδοτημένης πρόσβασης ή μη εξουσιοδοτημένης χρήσης ενός περιουσιακού στοιχείου

[ISO/IEC 27000:2009]

4.9 δυνατότητα επίθεσης (attack potential)

η εκτιμώμενη προοπτική επιτυχίας μιας επίθεσης, σε περίπτωση που η επίθεση εξαπολυθεί, η οποία εκφράζεται με βάση την εμπειρογνωμοσύνη, τους πόρους και τα κίνητρα του επιτιθέμενου

[ISO/IEC 15408-1:2005]

4.10 συντελεστής επίθεσης (attack vector)

πορεία ή μέσο με το οποίο ένας επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε έναν υπολογιστή ή εξυπηρετητή δικτύου προκειμένου να προκαλέσει ένα κακόβουλο αποτέλεσμα

4.11 συνδυασμένη επίθεση (blended attack)

επίθεση που επιδιώκει να μεγιστοποιήσει τη σοβαρότητα της ζημίας και την ταχύτητα της μετάδοσης συνδυάζοντας πολλαπλές μεθόδους επίθεσης

4.12 ρομπότ (bot / robot)

αυτοματοποιημένο πρόγραμμα λογισμικού που χρησιμοποιείται για την εκτέλεση συγκεκριμένων εργασιών

ΣΗΜΕΙΩΣΗ 1 Η λέξη χρησιμοποιείται συχνά για την περιγραφή προγραμμάτων, που συνήθως εκτελούνται σε έναν εξυπηρετητή, τα οποία αυτοματοποιούν εργασίες όπως η προώθηση ή η ταξινόμηση ηλεκτρονικού ταχυδρομείου.

ΣΗΜΕΙΩΣΗ 2 Ως ρομπότ επίσης περιγράφεται ένα πρόγραμμα που λειτουργεί ως μέσο για έναν χρήστη ή για ένα άλλο πρόγραμμα ή που προσομοιώνει μια ανθρώπινη δραστηριότητα. Στο Διαδίκτυο, τα πιο διαδεδομένα ρομπότ είναι τα προγράμματα, που ονομάζονται επίσης αράχνες ή ερπετά, τα οποία έχουν πρόσβαση σε ιστότοπους και συγκεντρώνουν το περιεχόμενό τους για τα ευρετήρια των μηχανών αναζήτησης.

4.13 ρομποτικό δίκτυο (botnet)

λογισμικό απομακρυσμένου ελέγχου, συγκεκριμένα ένα σύνολο κακόβουλων μηχανών, που λειτουργούν αυτόνομα ή αυτόματα σε παραβιασμένους υπολογιστές

4.14 cookie

Δυνατότητα <ελέγχου πρόσβασης> ή στοιχείο σε ένα σύστημα ελέγχου πρόσβασης

4.15 cookie

<IPSec> δεδομένα που ανταλλάσσονται από το ISAKMP (Internet Security Association and Key Management Protocol) για την αποτροπή ορισμένων επιθέσεων άρνησης παροχής υπηρεσιών κατά τη δημιουργία μιας σύνδεσης ασφαλείας

4.16 cookie

<Πρωτόκολλο Μεταφοράς Υπερκειμένου (HyperText Transfer Protocol, HTTP)> δεδομένα που ανταλλάσσονται μεταξύ ενός εξυπηρετητή Πρωτοκόλλου Μεταφοράς Υπερκειμένου και ενός προγράμματος περιήγησης για την αποθήκευση πληροφοριών κατάστασης στην πλευρά του πελάτη και την ανάκτησή τους αργότερα για χρήση από τον εξυπηρετητή.

ΣΗΜΕΙΩΣΗ Ένας φυλλομετρητής μπορεί να είναι πελάτης ή εξυπηρετητής.

4.17 μέτρο / αντίμετρο (control / countermeasure)

μέσο διαχείρισης κινδύνου, συμπεριλαμβανομένων πολιτικών, διαδικασιών, κατευθυντήριων γραμμών, πρακτικών ή δομών του οργανισμού, τα οποία μπορεί να είναι διοικητικής, τεχνικής, διαχειριστικής ή νομικής φύσης

[ISO/IEC 27000:2009]

ΣΗΜΕΙΩΣΗ Ο οδηγός ISO 73:2009 ορίζει το μέτρο ως απλά ένα μέσο που τροποποιεί τον κίνδυνο.

4.18 Κυβερνοέγκλημα (Cybercrime)

εγκληματική δραστηριότητα κατά την οποία υπηρεσίες ή εφαρμογές στον Κυβερνοχώρο χρησιμοποιούνται για ή αποτελούν στόχο ενός εγκλήματος, ή κατά τις οποίες ο Κυβερνοχώρος είναι η πηγή, το εργαλείο, ο στόχος ή ο τόπος ενός εγκλήματος

4.19 Κυβερνοασφάλεια (Cybersafety)

κατάσταση όπου εξασφαλίζεται προστασία από φυσικές, κοινωνικές, πνευματικές, οικονομικές, πολιτικές, συναισθηματικές, επαγγελματικές, ψυχολογικές, εκπαιδευτικές ή άλλες μορφές ή συνέπειες αποτυχίας, ζημίας, σφάλματος, ατυχήματος, βλάβης ή οποιουδήποτε άλλου γεγονότος στον Κυβερνοχώρο, το οποίο θα μπορούσε να θεωρηθεί μη επιθυμητό.

ΣΗΜΕΙΩΣΗ 1 Αυτό μπορεί να λάβει τη μορφή της προστασίας από το συμβάν ή από την έκθεση σε κάτι που προκαλεί απώλειες στην υγεία ή οικονομικές απώλειες. Μπορεί να περιλαμβάνει την προστασία ανθρώπων ή περιουσιακών στοιχείων.

ΣΗΜΕΙΩΣΗ 2 Η ασφάλεια γενικά ορίζεται επίσης ως η κατάσταση βεβαιότητας ότι δε θα προκληθούν δυσμενείς επιπτώσεις από κάποιον παράγοντα υπό συγκεκριμένες συνθήκες.

4.20 Κυβερνοασφάλεια / Ασφάλεια στον κυβερνοχώρο (Cybersecurity /Cyberspace security)

διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών στον κυβερνοχώρο

ΣΗΜΕΙΩΣΗ 1 Επιπλέον, μπορεί να εμπλέκονται και άλλες ιδιότητες, όπως η αυθεντικότητα, η λογοδοσία, η μη άρνηση και η αξιοπιστία.

ΣΗΜΕΙΩΣΗ 2 Προσαρμοσμένη από τον ορισμό για την ασφάλεια πληροφοριών στο ISO/IEC 27000:2009.

4.21 ο Κυβερνοχώρος (the Cyberspace)

πολύπλοκο περιβάλλον που προκύπτει από την αλληλεπίδραση ανθρώπων, λογισμικού και υπηρεσιών στο Διαδίκτυο μέσω συσκευών τεχνολογίας και δικτύων που συνδέονται με αυτό, το οποίο δεν υπάρχει σε κάποια φυσική μορφή.

4.22 υπηρεσίες εφαρμογών στον Κυβερνοχώρο (Cyberspace application services)

υπηρεσίες εφαρμογών (4.4) που παρέχονται μέσω του κυβερνοχώρου

4.23 κυβερνοκαταπατητής (cyber-squatter)

άτομα ή οργανισμοί που καταχωρούν και διατηρούν Ενιαίους Εντοπιστές Πόρων (Uniform Resource Locators, URLs) που μοιάζουν με αναφορές ή ονόματα άλλων οργανισμών στον πραγματικό κόσμο ή στον κυβερνοχώρο.

4.24 παραπλανητικό λογισμικό (deceptive software)

λογισμικό το οποίο εκτελεί δραστηριότητες στον υπολογιστή ενός χρήστη χωρίς προηγουμένως να ενημερώνει τον χρήστη για το τι ακριβώς θα κάνει το λογισμικό στον υπολογιστή του ή χωρίς να ζητά τη συγκατάθεση του χρήστη για τις ενέργειες αυτές

ΠΑΡΑΔΕΙΓΜΑ 1 Ένα πρόγραμμα που καταλαμβάνει τις ρυθμίσεις του χρήστη

ΠΑΡΑΔΕΙΓΜΑ 2 Ένα πρόγραμμα που προκαλεί συνεχείς εμφανιζόμενες διαφημίσεις οι οποίες δεν μπορούν εύκολα να σταματήσουν από τον χρήστη.

ΠΑΡΑΔΕΙΓΜΑ 3 Λογισμικό διαφημίσεων και λογισμικό κατασκοπείας.

4.25 παραβίαση (hacking)

η σκόπιμη πρόσβαση ενός συστήματος υπολογιστή χωρίς την άδεια του χρήστη ή του ιδιοκτήτη

4.26 ακτιβισμός που υλοποιείται με τεχνικές παραβίασης (hactivism)

παραβίαση για πολιτικούς ή κοινωνικούς σκοπούς

4.27 περιουσιακό στοιχείο πληροφοριών (information asset)

γνώση ή δεδομένα που έχουν αξία για το άτομο ή τον οργανισμό

ΣΗΜΕΙΩΣΗ Προσαρμοσμένο από το ISO/IEC 27000:2009.

4.28 διαδίκτυο / δίκτυο διαδικτύου (internet / internetwork)

συλλογή διασυνδεδεμένων δικτύων

ΣΗΜΕΙΩΣΗ 1 Προσαρμοσμένο από το ISO/IEC 27033-1:2009

ΣΗΜΕΙΩΣΗ 2 Σε αυτό το πλαίσιο, θα πρέπει να γίνεται αναφορά σε "ένα διαδίκτυο". Υπάρχει διαφορά μεταξύ του ορισμού του "διαδίκτυο" και του ορισμού "το διαδίκτυο".

4.29 το Διαδίκτυο (the internet)

παγκόσμιο σύστημα διασυνδεδεμένων δικτύων στον δημόσιο τομέα

[ISO/IEC 27033-1:2009]

ΣΗΜΕΙΩΣΗ Υπάρχει διαφορά μεταξύ του ορισμού του " ένα διαδίκτυο" και του ορισμού " το διαδίκτυο".

4.30 Διαδικτυακό έγκλημα (Internet crime)

εγκληματική δραστηριότητα κατά την οποία υπηρεσίες ή εφαρμογές του Διαδικτύου χρησιμοποιούνται για ένα έγκλημα ή αποτελούν τον στόχο ενός εγκλήματος, ή κατά την οποία το Διαδίκτυο είναι η πηγή, το εργαλείο, ο στόχος ή ο τόπος ενός εγκλήματος

4.31 ασφάλεια στο Διαδίκτυο (Internet safety)

κατάσταση προστατευμένη από φυσικές, κοινωνικές, πνευματικές, οικονομικές, πολιτικές, συναισθηματικές, επαγγελματικές, ψυχολογικές, εκπαιδευτικές ή άλλες μορφές ή συνέπειες αποτυχίας, ζημίας, σφάλματος, ατυχήματος, βλάβης ή οποιουδήποτε άλλου γεγονότος στο Διαδίκτυο που θα μπορούσε να θεωρηθεί ανεπιθύμητο.

4.32 ασφάλεια Διαδικτύου (Internet security)

διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών στο Διαδίκτυο

4.33 υπηρεσίες Διαδικτύου (Internet services)

υπηρεσίες που παρέχονται σε έναν χρήστη για να του επιτραπεί η πρόσβαση στο Διαδίκτυο μέσω μιας εκχωρημένης διεύθυνσης διαδικτυακού πρωτοκόλλου, οι οποίες συνήθως περιλαμβάνουν υπηρεσίες ελέγχου ταυτότητας, εξουσιοδότησης και ονομάτων τομέων

4.34 Πάροχος υπηρεσιών διαδικτύου (Internet service provider)

οργανισμός που παρέχει υπηρεσίες Διαδικτύου σε έναν χρήστη και επιτρέπει στους πελάτες του την πρόσβαση στο Διαδίκτυο

ΣΗΜΕΙΩΣΗ Αναφέρεται επίσης μερικές φορές ως πάροχος πρόσβασης στο Διαδίκτυο.

4.35 κακόβουλο λογισμικό (malware)

λογισμικό σχεδιασμένο με κακόβουλη πρόθεση που περιέχει χαρακτηριστικά ή δυνατότητες που μπορούν δυνητικά να προκαλέσουν βλάβη άμεσα ή έμμεσα στον χρήστη ή/και στο σύστημα του υπολογιστή του χρήστη

ΠΑΡΑΔΕΙΓΜΑΤΑ Ιοί, σκουλήκια (worms), δούρειοι ίπποι (trojans).

4.36 κακόβουλο περιεχόμενο (malicious contents)

εφαρμογές, έγγραφα, αρχεία, δεδομένα ή άλλοι πόροι που έχουν ενσωματωμένα κακόβουλα στοιχεία και λειτουργίες συγκαλυμμένα ή κρυμμένα σε αυτά

4.37 οργανισμός (organization)

ομάδα ατόμων και εγκαταστάσεων με μια ρύθμιση αρμοδιοτήτων, εξουσιών και σχέσεων

[ISO 9000:2005]

ΣΗΜΕΙΩΣΗ 1 Στο πλαίσιο του παρόντος Διεθνούς Προτύπου, το άτομο διαχωρίζεται από τον οργανισμό.

ΣΗΜΕΙΩΣΗ 2 Γενικά, μια κυβέρνηση είναι επίσης ένας οργανισμός. Στο πλαίσιο του παρόντος Διεθνούς Προτύπου, οι κυβερνήσεις μπορούν να θεωρηθούν χωριστά από άλλους οργανισμούς για λόγους σαφήνειας.

4.38 ηλεκτρονικό ψάρεμα (phishing)

η δόλια διαδικασία απόπειρας απόκτησης ιδιωτικών ή εμπιστευτικών πληροφοριών με τη μεταμφίεση ως αξιόπιστη οντότητα σε μια ηλεκτρονική επικοινωνία

ΣΗΜΕΙΩΣΗ Το ηλεκτρονικό ψάρεμα μπορεί να επιτευχθεί με τη χρήση κοινωνικής μηχανικής ή τεχνικών εξαπάτησης.

4.39 φυσικό περιουσιακό στοιχείο (physical asset)

περιουσιακό στοιχείο που έχει απτή ή υλική ύπαρξη

ΣΗΜΕΙΩΣΗ Τα φυσικά περιουσιακά στοιχεία αναφέρονται συνήθως σε μετρητά, εξοπλισμό, αποθέματα και ακίνητα που ανήκουν στο άτομο ή στον οργανισμό. Το λογισμικό θεωρείται άυλο περιουσιακό στοιχείο ή μη φυσικό περιουσιακό στοιχείο.

4.40 δυνητικά ανεπιθύμητο λογισμικό (potentially unwanted software)

παραπλανητικό λογισμικό, συμπεριλαμβανομένου του κακόβουλου και μη κακόβουλου λογισμικού, που παρουσιάζει τα χαρακτηριστικά του παραπλανητικού λογισμικού

4.41 απάτη (scam)

εξαπάτηση ή κόλπο με στόχο την εμπιστοσύνη

4.42 ανεπιθύμητο μήνυμα (spam)

κατάχρηση των συστημάτων ηλεκτρονικών μηνυμάτων για την άνευ διακρίσεων αποστολή ανεπιθύμητων μαζικών μηνυμάτων

ΣΗΜΕΙΩΣΗ Αν και η πιο ευρέως αναγνωρισμένη μορφή ανεπιθύμητων μηνυμάτων είναι μέσω ηλεκτρονικού ταχυδρομείου, ο όρος εφαρμόζεται σε παρόμοιες καταχρήσεις σε άλλα μέσα: μέσω άμεσων μηνυμάτων, σε ομάδες ειδήσεων δικτύου Usenet, σε μηχανές αναζήτησης στο διαδίκτυο, σε ιστολόγια, σε wiki, σε μηνύματα κινητής τηλεφωνίας, σε φόρουμ στο Διαδίκτυο και άχρηστες μεταδόσεις τηλεομοιοτυπίας.

4.43 λογισμικό κατασκοπείας (spyware)

παραπλανητικό λογισμικό που συλλέγει ιδιωτικές ή εμπιστευτικές πληροφορίες από τον χρήστη του υπολογιστή

ΣΗΜΕΙΩΣΗ Οι πληροφορίες μπορεί να περιλαμβάνουν θέματα όπως ιστοσελίδες που επισκέπτονται συχνότερα ή πιο ευαίσθητες πληροφορίες όπως κωδικούς πρόσβασης.

4.44 ενδιαφερόμενος (stakeholder)

<διαχείριση κινδύνων> πρόσωπο ή οργανισμός που μπορεί να επηρεάσει, να επηρεαστεί ή να θεωρήσει ότι επηρεάζεται από μια απόφαση ή δραστηριότητα

[ISO Guide 73:2009]

4.45 ενδιαφερόμενος (stakeholder)

<σύστημα> άτομο ή οργανισμός που έχει δικαίωμα, μερίδιο, αξίωση ή συμφέρον σε ένα σύστημα ή στην κατοχή χαρακτηριστικών που ανταποκρίνονται στις ανάγκες και τις προσδοκίες του

[ISO/IEC 12207:2008]

4.46 απειλή (threat)

δυνητική αιτία ενός ανεπιθύμητου συμβάντος, το οποίο μπορεί να οδηγήσει σε βλάβη ενός συστήματος, ενός ατόμου ή ενός οργανισμού

ΣΗΜΕΙΩΣΗ Προσαρμοσμένο από το ISO/IEC 27000:2009.

4.47 δούρειος ίππος (trojan / trojan horse)

κακόβουλο λογισμικό που φαίνεται να εκτελεί μια επιθυμητή λειτουργία

4.48 ανεπιθύμητο ηλεκτρονικό μήνυμα (unsolicited email)

ηλεκτρονικό μήνυμα που δεν είναι ευπρόσδεκτο, ή δε ζητήθηκε ή δεν προσκλήθηκε

4.49 εικονικό περιουσιακό στοιχείο (virtual asset)

αναπαράσταση ενός περιουσιακού στοιχείου στον Κυβερνοχώρο

ΣΗΜΕΙΩΣΗ Σε αυτό το πλαίσιο, ως νόμισμα μπορεί να οριστεί είτε ένα μέσο ανταλλαγής είτε μια ιδιότητα που έχει αξία σε ένα συγκεκριμένο περιβάλλον, όπως ένα βιντεοπαιχνίδι ή μια άσκηση προσομοίωσης χρηματοοικονομικών συναλλαγών.

4.50 εικονικό νόμισμα (virtual currency)

νομισματικά εικονικά περιουσιακά στοιχεία

4.51 εικονικός κόσμος (virtual world)

προσομοιωμένο περιβάλλον στο οποίο έχουν πρόσβαση πολλαπλοί χρήστες μέσω διαδικτυακής διεπαφής

ΣΗΜΕΙΩΣΗ 1 Τα προσομοιωμένα περιβάλλοντα είναι συχνά διαδραστικά.

ΣΗΜΕΙΩΣΗ 2 Ο φυσικός κόσμος στον οποίο ζουν οι άνθρωποι, και τα σχετικά χαρακτηριστικά, θα αναφέρεται ως "πραγματικός κόσμος" για να διαφοροποιείται από τον εικονικό κόσμο.

4.52 ευπάθεια (vulnerability)

αδυναμία ενός περιουσιακού στοιχείου ή αντιμέτρου που μπορεί να χρησιμοποιηθεί από μια απειλή

[ISO/IEC 27000:2009]

4.53 ζόμπι / υπολογιστής ζόμπι / τηλεχειριζόμενη μηχανή (zombie / zombie computer / drone)

υπολογιστής που περιέχει κρυφό λογισμικό που επιτρέπει τον τηλεχειρισμό του μηχανήματος, συνήθως για την πραγματοποίηση επίθεσης σε άλλον υπολογιστή

ΣΗΜΕΙΩΣΗ Γενικά, ένας παραβιασμένος υπολογιστής είναι μόνο ένας από τους πολλούς σε ένα δίκτυο ρομπότ και θα χρησιμοποιηθεί για την εκτέλεση κακόβουλων δραστηριοτήτων υπό απομακρυσμένη καθοδήγηση.

5 Συντομογραφίες

Οι ακόλουθες συντομογραφίες χρησιμοποιούνται στο παρόν Διεθνές Πρότυπο.

ΑΣ (AS)	Αυτόνομο Σύστημα (Autonomous System)
ΣΠ (AP)	Σημείο Πρόσβασης (Access Point)
ΕΜΥ (CBT)	Εκπαίδευση Μέσω Υπολογιστή (Computer Based Training)
ΟΑΕΑΥ (CERT)	Ομάδα Αντιμετώπισης Εκτάκτων Αναγκών Υπολογιστών (Computer Emergency Response Team)
ΟΑΠΥ (CIRT)	Ομάδα Αντιμετώπισης Περιστατικών Υπολογιστών (Computer Incident Response Team)
ΟΑΠΑΥ (CSIRT)	Ομάδα Αντιμετώπισης Περιστατικών Ασφάλειας Υπολογιστών (Computer Security Incident Response Team)
ΠΥΠΖΣ (CIIP)	Προστασία Υποδομών Πληροφοριών Ζωτικής Σημασίας (Critical Information Infrastructure Protection)
ΑΕ (DoS)	Άρνηση Εξυπηρέτησης (Denial-of-Service)
ΔΑΕ (DDoS)	Διαδεδομένη Άρνηση Εξυπηρέτησης (Distributed Denial-of-Service)
ΣΑΕΒΕΚΥ (HBIDS)	Σύστημα Ανίχνευσης Εισβολών με Βάση Έναν Κεντρικό Υπολογιστή (Host-based Intrusion Detection System)
ΑΠΕ (IAP)	Ανεξάρτητος Πάροχος Εφαρμογών (Independent Application Provider)
ΠΕΜΔ (ICMP)	Πρωτόκολλο Ελέγχου Μηνυμάτων Διαδικτύου (Internet Control Message Protocol)
ΤΠΕ (ICT)	Τεχνολογία Πληροφοριών και Επικοινωνιών (Information and Communications Technology)
ΣΑΕ (IDS)	Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System)
ΠΔ (IP)	Πρωτόκολλο Διαδικτύου (Internet Protocol)
ΟΠΠ (IPO)	Οργανισμός Παροχής Πληροφοριών (Information Providing Organization)
ΣΠΕ (IPS)	Σύστημα Πρόληψης Εισβολών (Intrusion Prevention System)
ΟΛΠ (IRO)	Οργανισμός Λήψης Πληροφοριών (Information Receiving Organization)
ΠΥΔ (ISP)	Πάροχος Υπηρεσιών Διαδικτύου (Internet Service Provider)
ΑΠΛ (ISV)	Ανεξάρτητος Πάροχος Λογισμικού (Independent Software Vendor)
ΤΠ (IT)	Τεχνολογία Πληροφοριών (Information Technology)

ΔΠΡΠΠ (MMORPG)	Διαδικτυακό Παιχνίδι Ρόλων με Πολλούς Παίκτες (Massively Multiplayer Online Role-Playing Game)
ΣΕ (NDA)	Συμφωνία Εμπιστευτικότητας (Non-Disclosure Agreement)
ΚΖΑΛ (SDLC)	Κύκλος Ζωής Ανάπτυξης Λογισμικού (Software Development Life-cycle)
ΑΣΥ (SSID)	Αναγνωριστικό Συνόλου Υπηρεσίας (Service Set Identifier)
ΠΕΜ (TCP)	Πρωτόκολλο Ελέγχου Μεταφοράς (Transmission Control Protocol)
ΠΔΧ (UDP)	Πρωτόκολλο Δεδομένων Χρήστη (User Datagram Protocol)
ΕΑΠ (URI)	Ενιαίο Αναγνωριστικό Πόρων (Uniform Resource Identifier)
ΕΕΠ (URL)	Ενιαίος Εντοπιστής Πόρων (Uniform Resource Locator)

6. Επισκόπηση

6.1 Εισαγωγή

Η ασφάλεια στο Διαδίκτυο και στον Κυβερνοχώρο αποτελεί αντικείμενο αυξανόμενης ανησυχίας. Οι ενδιαφερόμενοι έχουν καθιερώσει την παρουσία τους στον Κυβερνοχώρο μέσω δικτυακών τόπων και τώρα προσπαθούν να αξιοποιήσουν περαιτέρω τον εικονικό κόσμο που παρέχει ο Κυβερνοχώρος. ΠΑΡΑΔΕΙΓΜΑ Αυξανόμενος αριθμός ατόμων ξοδεύει όλο και περισσότερο χρόνο με τα εικονικά τους άβαταρ στα ΔΠΡΠΠ.

Ενώ ορισμένα άτομα είναι προσεκτικά στη διαχείριση της διαδικτυακής τους ταυτότητας, οι περισσότεροι άνθρωποι ανεβάζουν λεπτομέρειες του προσωπικού τους προφίλ για να τις μοιραστούν με άλλους. Τα προφίλ σε πολλούς ιστότοπους, ιδίως σε ιστότοπους κοινωνικής δικτύωσης και χώρους συνομιλίας, μπορούν να μεταφορτωθούν και να αποθηκευτούν από άλλα μέρη. Αυτό μπορεί να οδηγήσει στη δημιουργία ενός ψηφιακού φακέλου προσωπικών δεδομένων που μπορεί να χρησιμοποιηθεί καταχρηστικά, να αποκαλυφθεί σε άλλα μέρη ή να χρησιμοποιηθεί για τη συλλογή δευτερογενών δεδομένων. Ενώ η ακρίβεια και η ακεραιότητα αυτών των δεδομένων είναι αμφισβητήσιμες, δημιουργούν δεσμούς με άτομα και οργανισμούς που συχνά δεν μπορούν να διαγραφούν πλήρως. Οι εξελίξεις αυτές στους τομείς της επικοινωνίας, της ψυχαγωγίας, των μεταφορών, των αγορών, των χρηματοοικονομικών, των ασφαλίσεων και της υγείας δημιουργούν νέους κινδύνους για τους ενδιαφερόμενους στον Κυβερνοχώρο. Έτσι, οι κίνδυνοι μπορεί να συνδέονται με την απώλεια της ιδιωτικότητας.

Η σύγκλιση των τεχνολογιών πληροφορικής και επικοινωνιών, η ευκολία εισόδου στον κυβερνοχώρο και η μείωση του προσωπικού χώρου μεταξύ των ατόμων προσελκύουν την προσοχή μεμονωμένων κακοποιών και εγκληματικών οργανώσεων. Αυτές οι οντότητες χρησιμοποιούν υφιστάμενους μηχανισμούς, όπως το ηλεκτρονικό ψάρεμα, τα ανεπιθύμητα μηνύματα και λογισμικά κατασκοπείας, καθώς και αναπτυσσόμενες νεότερες τεχνικές επίθεσης, για να εκμεταλλευτούν οποιεσδήποτε αδυναμίες μπορούν να ανακαλύψουν στον Κυβερνοχώρο. Τα τελευταία χρόνια, οι επιθέσεις ασφαλείας στον Κυβερνοχώρο έχουν εξελιχθεί από παραβιάσεις για προσωπική φήμη σε οργανωμένο έγκλημα ή

έγκλημα στον Κυβερνοχώρο. Μια πληθώρα εργαλείων και διαδικασιών που προηγουμένως παρατηρούνταν σε μεμονωμένα περιστατικά Κυβερνοασφάλειας χρησιμοποιούνται πλέον μαζί σε συνδυασμένες επιθέσεις, συχνά με εκτεταμένους κακόβουλους στόχους. Οι στόχοι αυτοί κυμαίνονται από προσωπικές επιθέσεις, κλοπή ταυτότητας, οικονομικές απάτες ή κλοπές, έως πολιτικό ακτιβισμό. Ειδικευμένα φόρουμ για την ανάδειξη πιθανών ζητημάτων ασφάλειας έχουν επίσης εξυπηρετήσει για την προβολή τεχνικών επιθέσεων και ευκαιριών εγκληματικότητας.

Οι πολλαπλοί τύποι επιχειρηματικών συναλλαγών που πραγματοποιούνται στον κυβερνοχώρο γίνονται στόχος των συνδικάτων Κυβερνοεγκλήματος. Οι κίνδυνοι που εγκυμονούνται είναι εγγενώς πολύπλοκοι, καθώς οι επιχειρηματικές συναλλαγές κυμαίνονται από υπηρεσίες μεταξύ επιχειρήσεων, μεταξύ επιχειρήσεων και καταναλωτών έως υπηρεσίες μεταξύ καταναλωτών και καταναλωτών. Έννοιες όπως το τι συνιστά συναλλαγή ή συμφωνία εξαρτώνται από την ερμηνεία του νόμου και από το πώς κάθε μέρος της σχέσης διαχειρίζεται την ευθύνη του. Συχνά, το ζήτημα της χρήσης των δεδομένων που συλλέγονται κατά τη διάρκεια της συναλλαγής ή της σχέσης δεν αντιμετωπίζεται επαρκώς. Αυτό μπορεί τελικά να οδηγήσει σε προβλήματα ασφάλειας, όπως η διαρροή πληροφοριών.

Οι νομικές και τεχνικές προκλήσεις που προκύπτουν από αυτά τα ζητήματα Κυβερνοασφάλειας είναι εκτεταμένες και παγκόσμιας εμβέλειας. Οι προκλήσεις μπορούν να αντιμετωπιστούν μόνο αν η τεχνική κοινότητα για την ασφάλεια των πληροφοριών, η νομική κοινότητα, τα έθνη και η κοινότητα των εθνών ενωθούν μέσω μιας συντονισμένης στρατηγικής. Η στρατηγική αυτή θα πρέπει να λαμβάνει υπόψη το ρόλο κάθε ενδιαφερόμενου και τις υφιστάμενες πρωτοβουλίες, μέσα σε ένα πλαίσιο διεθνούς συνεργασίας.

ΠΑΡΑΔΕΙΓΜΑ Ένα παράδειγμα πρόκλησης προκύπτει από το γεγονός ότι ο κυβερνοχώρος παρέχει εικονική ανωνυμία και κάλυψη της επίθεσης, καθιστώντας τον εντοπισμό δύσκολο. Αυτό καθιστά όλο και πιο δύσκολο για τα άτομα και τους οργανισμούς να δημιουργήσουν εμπιστοσύνη και να πραγματοποιήσουν συναλλαγές, καθώς και για τις υπηρεσίες επιβολής του νόμου να επιβάλουν σχετικές πολιτικές. Ακόμη και αν η πηγή της επίθεσης μπορεί να προσδιοριστεί, διασυνοριακά νομικά ζητήματα συχνά εμποδίζουν την περαιτέρω πρόοδο για οποιαδήποτε έρευνα ή νομικό επαναπατρισμό.

Η τρέχουσα πρόοδος για την αντιμετώπιση αυτών των προκλήσεων παρεμποδίζεται από πολλά ζητήματα, ενώ τα ζητήματα Κυβερνοασφάλειας αυξάνονται και συνεχίζουν να εξελίσσονται.

Αν και υπάρχει πληθώρα απειλών για την Κυβερνοασφάλεια, αλλά και πολλοί, αν και όχι τυποποιημένοι, τρόποι αντιμετώπισής τους, το παρόν Διεθνές Πρότυπο επικεντρώνεται στα ακόλουθα βασικά ζητήματα:

- επιθέσεις από κακόβουλο και δυνητικά ανεπιθύμητο λογισμικό,

- επιθέσεις κοινωνικής μηχανικής και

- ανταλλαγή πληροφοριών και συντονισμός.

Επιπλέον, ορισμένα εργαλεία Κυβερνοασφάλειας θα συζητηθούν εν συντομία στο παρόν Διεθνές Πρότυπο. Αυτά τα εργαλεία και οι τομείς σχετίζονται στενά με την πρόληψη, την ανίχνευση, την αντιμετώπιση και τη διερεύνηση του Κυβερνοεγκλήματος. Περισσότερες λεπτομέρειες διατίθενται στο παράρτημα Α.

6.2 Η φύση του Κυβερνοχώρου

Ο κυβερνοχώρος μπορεί να περιγραφεί ως ένα εικονικό περιβάλλον, το οποίο δεν υπάρχει σε καμία φυσική μορφή, αλλά μάλλον ως ένα σύνθετο περιβάλλον ή χώρος που προκύπτει από την εμφάνιση του Διαδικτύου, καθώς και των ανθρώπων, των οργανισμών και των δραστηριοτήτων σε κάθε είδους τεχνολογικές συσκευές και δίκτυα που συνδέονται με αυτό. Η ασφάλεια του κυβερνοχώρου, ή κυβερνοασφάλεια, αφορά την ασφάλεια αυτού του εικονικού κόσμου.

Πολλοί εικονικοί κόσμοι διαθέτουν ένα εικονικό νόμισμα, όπως αυτό που χρησιμοποιείται για την αγορά αντικειμένων εντός ενός παιχνιδιού. Το εικονικό νόμισμα, ακόμη και τα αντικείμενα του παιχνιδιού, έχουν μια σχετική αξία στον πραγματικό κόσμο. Αυτά τα εικονικά αντικείμενα ανταλλάσσονται συχνά με πραγματικό νόμισμα σε διαδικτυακούς ιστότοπους δημοπρασιών και ορισμένα παιχνίδια διαθέτουν ακόμη και επίσημο κανάλι με δημοσιευμένες ισοτιμίες εικονικού ή πραγματικού νομίσματος για τη νομισματοποίηση των εικονικών αντικειμένων. Συχνά αυτά τα κανάλια νομισματοποίησης είναι που καθιστούν αυτούς τους εικονικούς κόσμους στόχο για επιθέσεις, συνήθως μέσω phishing ή άλλων τεχνικών για την κλοπή πληροφοριών λογαριασμών.

6.3 Η φύση της Κυβερνοασφάλειας

Οι ενδιαφερόμενοι στον Κυβερνοχώρο πρέπει να διαδραματίσουν ενεργό ρόλο, πέρα από την προστασία των δικών τους περιουσιακών στοιχείων, προκειμένου να επικρατήσει η χρησιμότητα του Κυβερνοχώρου. Οι εφαρμογές στον Κυβερνοχώρο επεκτείνονται πέρα από τα μοντέλα επιχειρήσεων προς καταναλωτές και καταναλωτών προς καταναλωτές, σε μια μορφή αλληλεπιδράσεων και συναλλαγών πολλών προς πολλούς. Οι απαιτήσεις επεκτείνονται για τα άτομα και τους οργανισμούς που πρέπει να είναι προετοιμασμένοι να αντιμετωπίσουν τους αναδυόμενους κινδύνους και τις προκλήσεις ασφαλείας για την αποτελεσματική πρόληψη και αντιμετώπιση της κακής χρήσης και της εγκληματικής εκμετάλλευσης.

Η Κυβερνοασφάλεια αφορά τις ενέργειες στις οποίες πρέπει να προβούν οι ενδιαφερόμενοι φορείς για την εγκαθίδρυση και τη διατήρηση της ασφάλειας στον Κυβερνοχώρο.

Η Κυβερνοασφάλεια βασίζεται στην ασφάλεια των πληροφοριών, την ασφάλεια των εφαρμογών, την ασφάλεια των δικτύων και την ασφάλεια του Διαδικτύου ως θεμελιώδη δομικά στοιχεία. Η ασφάλεια στον κυβερνοχώρο είναι μία από τις δραστηριότητες που είναι απαραίτητες για την ΠΥΠΖΣ, και, ταυτόχρονα, η επαρκής προστασία των υπηρεσιών υποδομής ζωτικής σημασίας συμβάλλει στις βασικές ανάγκες ασφάλειας (δηλ. ασφάλεια, αξιοπιστία και διαθεσιμότητα των υποδομών ζωτικής σημασίας) για την επίτευξη των στόχων της Κυβερνοασφάλειας.

Ωστόσο, η Κυβερνοασφάλεια δεν είναι συνώνυμη με την ασφάλεια του Διαδικτύου, την ασφάλεια δικτύων, την ασφάλεια εφαρμογών, την ασφάλεια πληροφοριών ή την ΠΥΠΖΣ. Έχει ένα μοναδικό πεδίο εφαρμογής που απαιτεί από τα ενδιαφερόμενα μέρη να διαδραματίσουν ενεργό ρόλο προκειμένου να διατηρηθεί, αν όχι να βελτιωθεί, η χρησιμότητα και η αξιοπιστία του Κυβερνοχώρου. Το παρόν Διεθνές Πρότυπο διαφοροποιεί την Κυβερνοασφάλεια από τους άλλους τομείς της ασφάλειας ως εξής:

- Η ασφάλεια των πληροφοριών αφορά την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών γενικά, ώστε να εξυπηρετούνται οι ανάγκες του αντίστοιχου χρήστη των πληροφοριών.

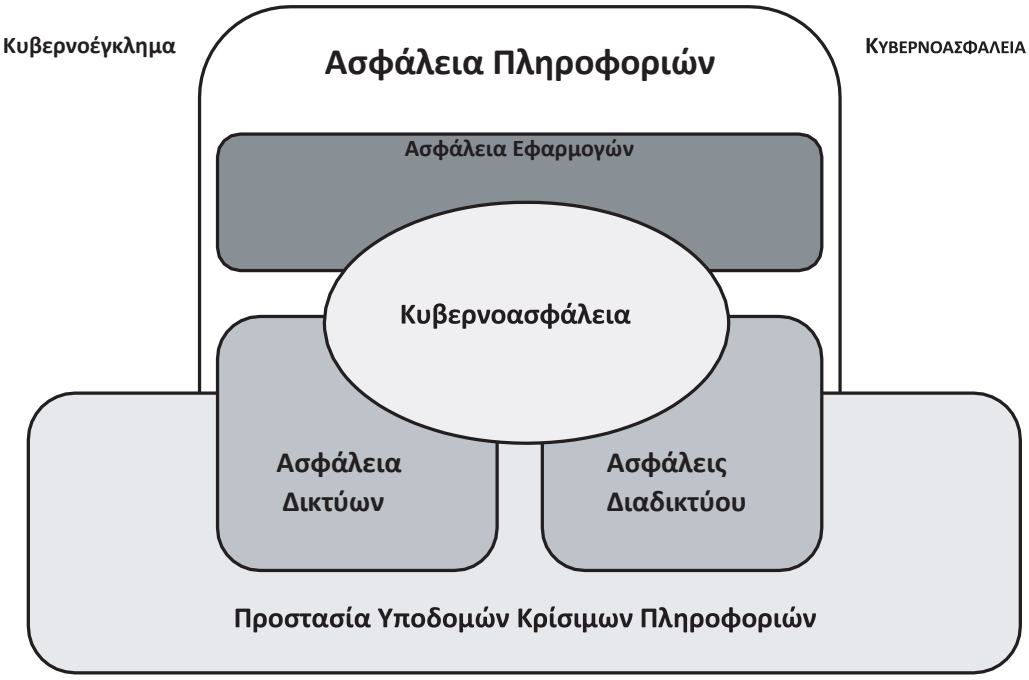
- Η ασφάλεια εφαρμογών είναι μια διαδικασία που πραγματοποιείται για την εφαρμογή μηχανισμών ελέγχου και μετρήσεων στις εφαρμογές ενός οργανισμού, προκειμένου να γίνεται διαχείριση του κινδύνου από τη χρήση τους. Οι έλεγχοι και οι μετρήσεις μπορούν να εφαρμοστούν στην ίδια την εφαρμογή (στις διαδικασίες, τα στοιχεία, το λογισμικό και τα αποτελέσματά της), στα δεδομένα της (δεδομένα παραμετροποίησης, δεδομένα χρήστη, δεδομένα οργανισμού) και σε όλη την τεχνολογία, τις διαδικασίες και τους παράγοντες που εμπλέκονται στον κύκλο ζωής της εφαρμογής.

- Η ασφάλεια δικτύων αφορά τον σχεδιασμό, την υλοποίηση και τη λειτουργία δικτύων για την επίτευξη των σκοπών της ασφάλειας των πληροφοριών σε δίκτυα εντός οργανισμών, μεταξύ οργανισμών και μεταξύ οργανισμών και χρηστών.

- Η ασφάλεια του Διαδικτύου αφορά την προστασία των υπηρεσιών που σχετίζονται με το Διαδίκτυο και των συναφών συστημάτων και δικτύων ΤΠΕ ως επέκταση της ασφάλειας δικτύων σε οργανισμούς και στο σπίτι, για την επίτευξη του σκοπού της ασφάλειας. Η ασφάλεια του Διαδικτύου εξασφαλίζει επίσης τη διαθεσιμότητα και την αξιοπιστία των υπηρεσιών του Διαδικτύου.

- Η ΠΥΠΖΣ ασχολείται με την προστασία των συστημάτων που παρέχονται ή λειτουργούν από παρόχους κρίσιμων υποδομών, όπως οι υπηρεσίες ενέργειας, τηλεπικοινωνιών και ύδρευσης. Η ΠΥΠΖΣ διασφαλίζει ότι τα εν λόγω συστήματα και δίκτυα προστατεύονται και είναι ανθεκτικά έναντι κινδύνων ασφάλειας πληροφοριών, κινδύνων ασφάλειας δικτύων, κινδύνων ασφάλειας του Διαδικτύου, καθώς και κινδύνων κυβερνοασφάλειας.

Στην εικόνα 1 συνοψίζεται η σχέση μεταξύ της Κυβερνοασφάλειας και άλλων τομέων ασφάλειας. Η σχέση μεταξύ αυτών των τομέων ασφάλειας και της Κυβερνοασφάλειας είναι πολύπλοκη. Ορισμένες από τις κρίσιμες υπηρεσίες υποδομής, όπως για παράδειγμα το νερό και οι μεταφορές, δε χρειάζεται να επηρεάζουν άμεσα ή σημαντικά την κατάσταση της Κυβερνοασφάλειας. Ωστόσο, η έλλειψη Κυβερνοασφάλειας μπορεί να έχει αρνητικό αντίκτυπο στη διαθεσιμότητα των κρίσιμων συστημάτων πληροφοριακής υποδομής που παρέχονται από τους παρόχους κρίσιμων υποδομών.



Σχήμα 1 - σχέση μεταξύ της Κυβερνοασφάλειας και άλλων τομέων ασφάλειας

Από την άλλη πλευρά, η διαθεσιμότητα και η αξιοπιστία του Κυβερνοχώρου εξαρτάται από πολλές απόψεις από τη διαθεσιμότητα και την αξιοπιστία συναφών υπηρεσιών υποδομής ζωτικής σημασίας, όπως η υποδομή τηλεπικοινωνιακών δικτύων. Η ασφάλεια του Κυβερνοχώρου συνδέεται επίσης στενά με την ασφάλεια του Διαδικτύου, των εταιρικών/οικιακών δικτύων και της ασφάλειας των πληροφοριών γενικότερα. Θα πρέπει να σημειωθεί ότι οι τομείς ασφάλειας που προσδιορίζονται στην παρούσα ενότητα έχουν τους δικούς τους στόχους και το δικό τους πεδίο εστίασης. Για την αντιμετώπιση των θεμάτων Κυβερνοασφάλειας, επομένως, απαιτείται ουσιαστική επικοινωνία και συντονισμός μεταξύ διαφορετικών ιδιωτικών και δημόσιων φορέων από διαφορετικές χώρες και οργανισμούς. Οι υπηρεσίες υποδομής ζωτικής σημασίας θεωρούνται από ορισμένες κυβερνήσεις ως υπηρεσίες που σχετίζονται με την εθνική ασφάλεια και, ως εκ τούτου, δεν μπορούν να συζητηθούν ή να κοινοποιηθούν ανοιχτά. Επιπλέον, η γνώση των αδυναμιών των κρίσιμων υποδομών, εάν δε χρησιμοποιηθεί κατάλληλα, μπορεί να έχει άμεσες επιπτώσεις στην εθνική ασφάλεια. Συνεπώς, ένα βασικό πλαίσιο για την ανταλλαγή πληροφοριών και τον συντονισμό θεμάτων ή περιστατικών είναι απαραίτητο για να γεφυρωθούν τα κενά και να παρασχεθεί επαρκής ασφάλεια στους ενδιαφερόμενους στον Κυβερνοχώρο.

6.4 Γενικό μοντέλο

6.4.1 Εισαγωγή

Σε αυτήν την ενότητα παρουσιάζεται ένα γενικό μοντέλο που χρησιμοποιείται σε αυτό το Διεθνές Πρότυπο. Αυτή η ενότητα προϋποθέτει κάποια γνώση της ασφάλειας και δεν προτίθεται να λειτουργήσει ως εγχειρίδιο σε αυτόν τον τομέα.

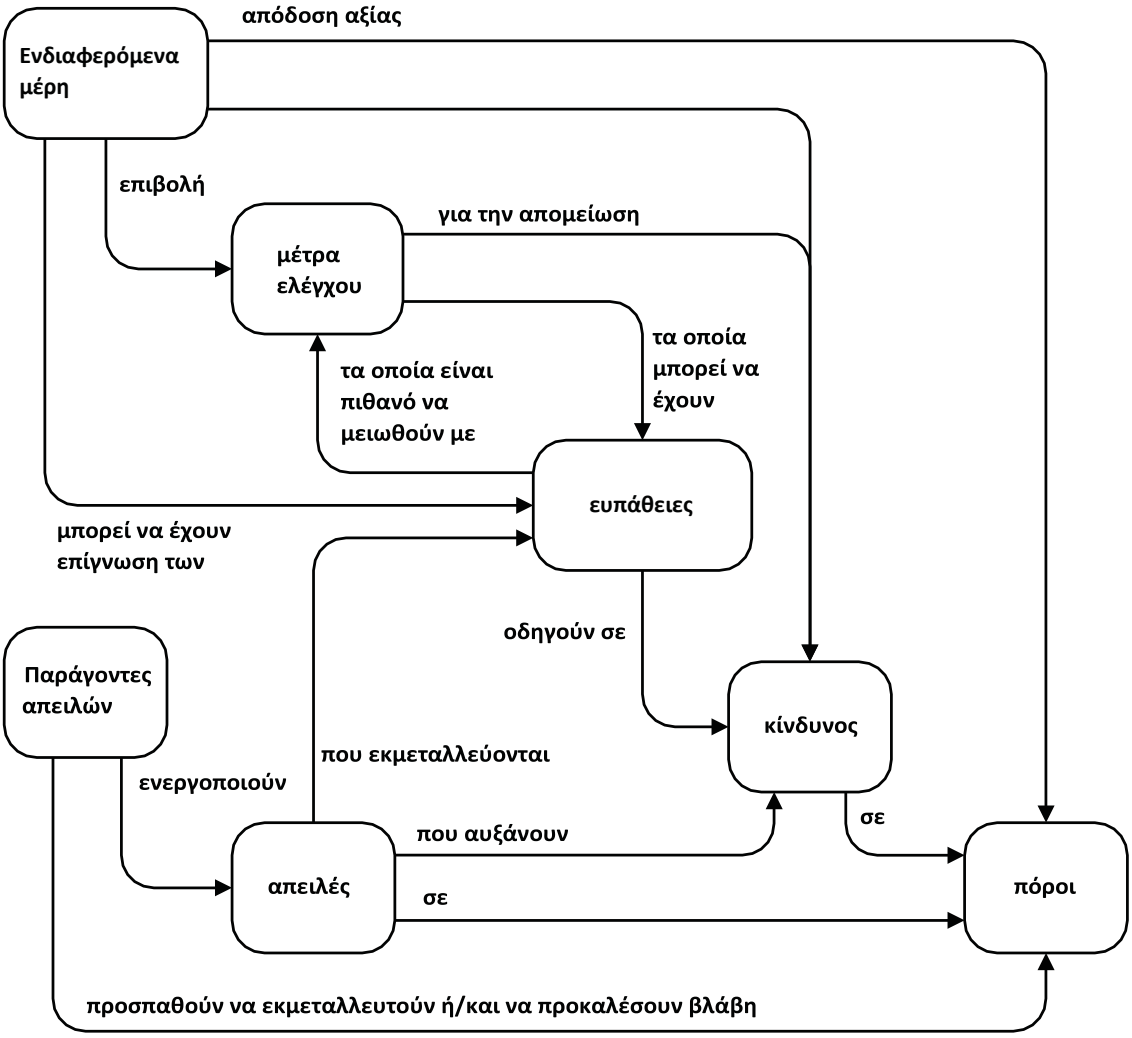
Σε αυτό το Διεθνές Πρότυπο αναλύεται η ασφάλεια με τη χρήση ενός συνόλου εννοιών και ορολογίας ασφάλειας. Η κατανόηση αυτών των εννοιών και της ορολογίας αποτελεί προϋπόθεση για την αποτελεσματική χρήση του Διεθνούς Προτύπου. Ωστόσο, οι ίδιες οι έννοιες είναι αρκετά γενικές και δεν

αποσκοπούν στο να περιορίσουν την κατηγορία των προβλημάτων ασφάλειας ΤΠ στα οποία έχει εφαρμογή αυτό το Διεθνές Πρότυπο.

6.4.2 Γενικό πλαίσιο ασφαλείας

Η ασφάλεια αφορά την προστασία των περιουσιακών στοιχείων από απειλές, όπου οι απειλές διακρίνονται ως το ενδεχόμενο κατάχρησης των προστατευόμενων περιουσιακών στοιχείων. Πρέπει να εξετάζονται όλες οι κατηγορίες απειλών, αλλά στον τομέα της ασφάλειας μεγαλύτερη προσοχή δίνεται στις απειλές που σχετίζονται με κακόβουλες ή άλλες ανθρώπινες δραστηριότητες. Στο σχήμα 2 απεικονίζονται αυτές οι έννοιες και οι σχέσεις υψηλού επιπέδου.

ΣΗΜΕΙΩΣΗ Το σχήμα 2 προέρχεται από το ISO/IEC 15408-1:2005, Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κριτήρια αξιολόγησης της ασφάλειας ΤΠ - Μέρος 1: Εισαγωγή και γενικό μοντέλο.



Σχήμα 2 - Έννοιες και σχέσεις ασφάλειας

Η διαφύλαξη των περιουσιακών στοιχείων ενδιαφέροντος αποτελεί ευθύνη των ενδιαφερομένων μερών που αποδίδουν αξία στα εν λόγω περιουσιακά στοιχεία. Οι πραγματικοί ή οι εικαζόμενοι παράγοντες απειλής μπορεί επίσης να αποδίδουν αξία στα περιουσιακά στοιχεία και να επιδιώκουν την κατάχρηση

των περιουσιακών στοιχείων κατά τρόπο αντίθετο προς τα συμφέροντα των ενδιαφερόμενων μερών. Τα ενδιαφερόμενα μέρη θα εκλάβουν τέτοιες απειλές ως πιθανή υποβάθμιση των περιουσιακών στοιχείων, με αποτέλεσμα να μειωθεί η αξία των περιουσιακών στοιχείων για τα ενδιαφερόμενα μέρη. Η συγκεκριμένη υποβάθμιση ασφάλειας συνήθως περιλαμβάνει, μεταξύ άλλων, την επιζήμια αποκάλυψη του περιουσιακού στοιχείου σε μη εξουσιοδοτημένους παραλήπτες (απώλεια εμπιστευτικότητας), τη ζημία του περιουσιακού στοιχείου μέσω μη εξουσιοδοτημένης τροποποίησης (απώλεια ακεραιότητας) ή τη μη εξουσιοδοτημένη απώλεια πρόσβασης στο περιουσιακό στοιχείο (απώλεια διαθεσιμότητας).

Τα ενδιαφερόμενα μέρη αξιολογούν τους κινδύνους λαμβάνοντας υπόψη τις απειλές που αφορούν τα περιουσιακά τους στοιχεία. Η ανάλυση αυτή μπορεί να βοηθήσει στην επιλογή των ελέγχων για την αντιμετώπιση των κινδύνων και τη μείωσή τους σε αποδεκτό επίπεδο.

Μέτρα επιβάλλονται για τη μείωση των ευπαθειών ή των επιπτώσεων και για την ικανοποίηση των απαιτήσεων ασφάλειας των ενδιαφερομένων μερών (είτε άμεσα είτε έμμεσα, παρέχοντας οδηγίες σε άλλα μέρη). Μετά την επιβολή των ελέγχων μπορεί να παραμείνουν εναπομένουσες ευπάθειες. Οι εν λόγω ευπάθειες μπορούν να αξιοποιηθούν από παράγοντες απειλής που αντιπροσωπεύουν ένα εναπομένον επίπεδο κινδύνου για τα περιουσιακά στοιχεία. Τα ενδιαφερόμενα μέρη θα προσπαθήσουν να ελαχιστοποιήσουν αυτόν τον κίνδυνο ορίζοντας άλλους περιορισμούς.

Οι ενδιαφερόμενοι θα πρέπει να είναι βέβαιοι ότι τα μέτρα είναι επαρκή για την αντιμετώπιση των απειλών κατά των περιουσιακών στοιχείων προτού επιτρέψουν την έκθεση των περιουσιακών στοιχείων στις προσδιορισμένες απειλές. Οι ενδιαφερόμενοι ενδέχεται να μην έχουν οι ίδιοι την ικανότητα να κρίνουν όλες τις πτυχές των μέτρων ελέγχου και, ως εκ τούτου, ενδέχεται να ζητήσουν την αξιολόγηση των μέτρων από εξωτερικούς οργανισμούς.

6.5 Προσέγγιση

Ένας αποτελεσματικός τρόπος αντιμετώπισης των κινδύνων κυβερνοασφάλειας περιλαμβάνει συνδυασμό πολλαπλών στρατηγικών, λαμβάνοντας υπόψη τα διάφορα ενδιαφερόμενα μέρη. Οι στρατηγικές αυτές περιλαμβάνουν:

- τις βέλτιστες πρακτικές του κλάδου, με τη συνεργασία όλων των ενδιαφερομένων μερών για τον εντοπισμό και την αντιμετώπιση ζητημάτων και κινδύνων Κυβερνοασφάλειας,

- ευρεία εκπαίδευση των καταναλωτών και των εργαζομένων, παρέχοντας μια αξιόπιστη πηγή για τον εντοπισμό και την αντιμετώπιση συγκεκριμένων κινδύνων Κυβερνοασφάλειας εντός του οργανισμού καθώς και στον Κυβερνοχώρο, και

- καινοτόμες τεχνολογικές λύσεις που συμβάλλουν στην προστασία των καταναλωτών από τις γνωστές Κυβερνοεπιθέσεις, ώστε να παραμένουν ενήμεροι και να είναι προετοιμασμένοι για τις νέες επιθέσεις.

Το εγχειρίδιο επικεντρώνεται στην παροχή βέλτιστων πρακτικών του κλάδου και στην ευρεία εκπαίδευση των καταναλωτών και των εργαζομένων, ώστε να βοηθήσει τους ενδιαφερόμενους στον Κυβερνοχώρο να διαδραματίσουν ενεργό ρόλο στην αντιμετώπιση των προκλήσεων Κυβερνοασφάλειας. Περιλαμβάνει οδηγίες για:

- ρόλους,

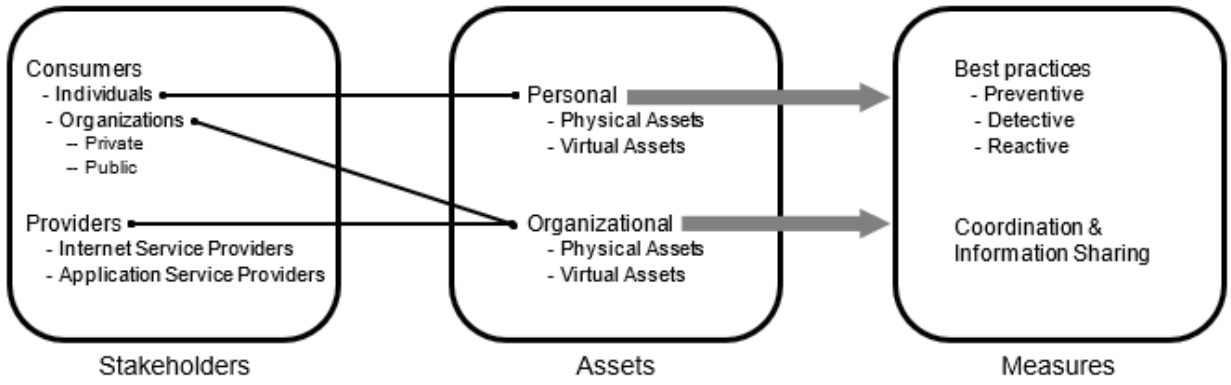
- πολιτικές,

- μεθόδους,

- διαδικασίες και

- σχετικούς τεχνικούς ελέγχους.

Το Σχήμα 3 παρέχεται μια επισκόπηση των σημαντικότερων σημείων της προσέγγισης που υιοθετείται σε αυτό το Διεθνές Πρότυπο. Αυτό το Διεθνές Πρότυπο δεν προορίζεται για άμεση χρήση για την παροχή ευρείας εκπαίδευσης των καταναλωτών. Αντίθετα, προορίζεται για χρήση από παρόχους υπηρεσιών στον Κυβερνοχώρο, καθώς και από οργανισμούς που παρέχουν εκπαίδευση στους καταναλωτές σχετικά με τον Κυβερνοχώρο, για την προετοιμασία υλικού για ευρεία εκπαίδευση των καταναλωτών.



Σχήμα 3 – Επισκόπηση της προσέγγισης

7. Ενδιαφερόμενα μέρη στον Κυβερνοχώρο

7.1 Επισκόπηση

Ο Κυβερνοχώρος δεν ανήκει σε κανέναν. Όλοι μπορούν να συμμετάσχουν και έχουν μερίδιο σε αυτόν.

Για τους σκοπούς αυτού του Διεθνούς Προτύπου, οι ενδιαφερόμενοι στον Κυβερνοχώρο κατηγοριοποιούνται στις ακόλουθες ομάδες:

- καταναλωτές, συμπεριλαμβανομένων

    - ιδιωτών, και

    - ιδιωτικών και δημόσιων οργανισμών,

- πάροχοι, συμπεριλαμβανομένων ενδεικτικά αλλά όχι περιοριστικά

    - παρόχων υπηρεσιών διαδικτύου- και

    - παρόχων υπηρεσιών εφαρμογών.

7.2 Καταναλωτές

Όπως περιγράφεται στο Σχήμα 3, ως καταναλωτές νοούνται οι μεμονωμένοι χρήστες καθώς και οι ιδιωτικοί και δημόσιοι οργανισμοί. Οι ιδιωτικοί οργανισμοί περιλαμβάνουν μικρές και μεσαίες

επιχειρήσεις (ΜΜΕ), καθώς και μεγάλες επιχειρήσεις. Η κυβέρνηση και άλλοι δημόσιοι οργανισμοί αναφέρονται συλλογικά ως δημόσιοι οργανισμοί. Ένα άτομο ή ένας οργανισμός γίνεται καταναλωτής όταν έχει πρόσβαση στον Κυβερνοχώρο ή σε οποιεσδήποτε υπηρεσίες που είναι διαθέσιμες στον Κυβερνοχώρο.

Ένας καταναλωτής μπορεί επίσης να είναι πάροχος εάν με τη σειρά του παρέχει μια υπηρεσία στον Κυβερνοχώρο ή επιτρέπει σε άλλον καταναλωτή να έχει πρόσβαση στον Κυβερνοχώρο. Ένας καταναλωτής μιας υπηρεσίας του εικονικού κόσμου μπορεί να γίνει πάροχος καθιστώντας διαθέσιμα εικονικά προϊόντα και υπηρεσίες σε άλλους καταναλωτές.

7.3 Πάροχοι

Οι πάροχοι αφορούν τους παρόχους υπηρεσιών στον Κυβερνοχώρο, καθώς και τους παρόχους υπηρεσιών Διαδικτύου που επιτρέπουν στους καταναλωτές να έχουν πρόσβαση στον Κυβερνοχώρο και στις διάφορες υπηρεσίες που είναι διαθέσιμες στον Κυβερνοχώρο.

Οι πάροχοι θα μπορούσαν επίσης να κατανοηθούν ως μεταφορείς ή χονδρέμποροι, έναντι των διανομέων και των λιανεμπόρων υπηρεσιών πρόσβασης. Η διάκριση αυτή είναι σημαντική από την άποψη της ασφάλειας και, ιδίως, της επιβολής του νόμου, διότι, σε περίπτωση που ο διανομέας ή ο λιανέμπορος δεν είναι σε θέση να παράσχει επαρκή ασφάλεια ή νόμιμη πρόσβαση, οι υπηρεσίες υποστήριξης συχνά επιστρέφουν στον μεταφορέα ή τον χονδρέμπορο. Η κατανόηση της φύσης ενός συγκεκριμένου παρόχου υπηρεσιών αποτελεί χρήσιμο στοιχείο στη διαχείριση κινδύνων στον Κυβερνοχώρο.

Οι πάροχοι υπηρεσιών εφαρμογών καθιστούν τις υπηρεσίες διαθέσιμες στους καταναλωτές μέσω του λογισμικού τους. Οι υπηρεσίες αυτές λαμβάνουν πολλές μορφές και περιλαμβάνουν συνδυασμούς της ακόλουθης μη εξαντλητικής λίστας:

- επεξεργασία εγγράφων, αποθήκευση, διανομή,

- διαδικτυακά εικονικά περιβάλλοντα για ψυχαγωγία, επικοινωνία και αλληλεπίδραση με άλλους χρήστες,

- διαδικτυακά αποθετήρια ψηφιακών μέσων με υπηρεσίες συγκέντρωσης, ευρετηρίου, αναζήτησης, βιτρίνας, καταλόγου, καλαθιού αγορών και πληρωμών- και

- λειτουργίες διαχείρισης επιχειρησιακών πόρων, όπως ανθρώπινου δυναμικού, οικονομικών και μισθοδοσίας, διαχείρισης εφοδιαστικής αλυσίδας, πελατειακών σχέσεων, τιμολόγησης.

8 Περιουσιακά στοιχεία στον κυβερνοχώρο

8.1 Επισκόπηση

Ένα περιουσιακό στοιχείο είναι οτιδήποτε έχει αξία για ένα άτομο ή έναν οργανισμό. Υπάρχουν πολλά είδη περιουσιακών στοιχείων, συμπεριλαμβανομένων αλλά χωρίς να περιορίζονται σε αυτά των:

α) πληροφοριών,

β) λογισμικού, όπως ένα πρόγραμμα υπολογιστή,

γ) φυσικών, όπως ένας υπολογιστής,

δ) υπηρεσιών,

ε) ανθρώπων, των προσόντων, των δεξιοτήτων και της εμπειρίας τους, και

στ) άυλων αγαθών, όπως η φήμη και η εικόνα.

ΣΗΜΕΙΩΣΗ 1 Συχνά, τα περιουσιακά στοιχεία θεωρούνται για απλούστευση μόνο οι πληροφορίες ή οι πόροι.

ΣΗΜΕΙΩΣΗ 2 Σύμφωνα με το ISO/IEC 15408-1:2005, ως περιουσιακά στοιχεία ορίζονται οι πληροφορίες ή οι πόροι που πρέπει να προστατεύονται από τους ελέγχους ενός ΣΑ (στόχος αξιολόγησης).

ΣΗΜΕΙΩΣΗ 3 Το ISO/IEC 19770-1 αναπτύχθηκε για να επιτρέψει σε έναν οργανισμό να αποδείξει ότι εκτελεί τη Διαχείριση Περιουσιακών Στοιχείων Λογισμικού (Software Asset Management - SAM) σε επίπεδο επαρκές για την ικανοποίηση των απαιτήσεων εταιρικής διακυβέρνησης και για την εξασφάλιση αποτελεσματικής υποστήριξης της συνολικής διαχείρισης υπηρεσιών πληροφορικής. Το ISO/IEC 19770 προορίζεται να ευθυγραμμιστεί στενά με το ISO/IEC 20000 και να το υποστηρίξει.

ΣΗΜΕΙΩΣΗ 4 Το ISO/IEC 20000-1 προωθεί την υιοθέτηση μιας ολοκληρωμένης προσέγγισης διαδικασιών κατά την καθιέρωση, εφαρμογή, λειτουργία, παρακολούθηση, μέτρηση, αναθεώρηση και βελτίωση ενός Συστήματος Διαχείρισης Υπηρεσιών (ΣΔΥ) για τον σχεδιασμό και την παροχή υπηρεσιών που ανταποκρίνονται στις επιχειρησιακές ανάγκες και τις απαιτήσεις των πελατών.

Για τους σκοπούς του παρόντος Διεθνούς Προτύπου, τα περιουσιακά στοιχεία στον Κυβερνοχώρο κατατάσσονται στις ακόλουθες κατηγορίες:

- προσωπικά, και

- του οργανισμού.

Και για τις δύο κατηγορίες, ένα περιουσιακό στοιχείο μπορεί επίσης να ταξινομηθεί περαιτέρω ως εξής

- ένα φυσικό περιουσιακό στοιχείο, του οποίου η μορφή υπάρχει στον πραγματικό κόσμο, ή

- εικονικό περιουσιακό στοιχείο, το οποίο υπάρχει μόνο στον Κυβερνοχώρο και δεν μπορεί να το δει ή να το αγγίξει κανείς στον πραγματικό κόσμο.

8.2 Προσωπικά περιουσιακά στοιχεία

Ένα από τα βασικά εικονικά περιουσιακά στοιχεία είναι η διαδικτυακή ταυτότητα ενός μεμονωμένου καταναλωτή και τα διαδικτυακά του διαπιστευτήρια. Η διαδικτυακή ταυτότητα θεωρείται περιουσιακό στοιχείο, δεδομένου ότι αποτελεί το βασικό αναγνωριστικό για κάθε μεμονωμένο καταναλωτή στον Κυβερνοχώρο.

Άλλα μεμονωμένα εικονικά περιουσιακά στοιχεία των καταναλωτών περιλαμβάνουν αναφορές σε εικονικούς κόσμους. Στους εικονικούς κόσμους, τα μέλη χρησιμοποιούν συχνά εικονικά άβαταρ για να τους αναπαριστούν ή να ενεργούν για λογαριασμό τους. Συχνά χρησιμοποιείται ένα εικονικό νόμισμα για εικονικές συναλλαγές. Αυτά τα άβαταρ και τα νομίσματα μπορούν να θεωρηθούν ως περιουσιακά στοιχεία που ανήκουν σε έναν μεμονωμένο καταναλωτή.

ΠΑΡΑΔΕΙΓΜΑ Ορισμένες τράπεζες λειτουργούν σε εικονικούς κόσμους και αναγνωρίζουν τα χρήματα του εικονικού κόσμου ως επίσημο νόμισμα.

Το υλικό και το λογισμικό πληροφορικής, καθώς και οι προσωπικές ψηφιακές συσκευές ή τα τερματικά που επιτρέπουν στον καταναλωτή να συνδέεται και να επικοινωνεί στον Κυβερνοχώρο, θεωρούνται επίσης περιουσιακά στοιχεία στο πλαίσιο του παρόντος Διεθνούς Προτύπου.

8.3 Περιουσιακά στοιχεία του οργανισμού

Μια βασική πτυχή του Κυβερνοχώρου είναι η υποδομή που τα καθιστά όλα αυτά δυνατά. Αυτή η υποδομή είναι μια συνδυασμένη διασύνδεση δικτύων, εξυπηρετητών και εφαρμογών που ανήκουν σε πολλούς παρόχους υπηρεσιών. Ωστόσο, η αξιοπιστία και η διαθεσιμότητα αυτής της υποδομής είναι ζωτικής σημασίας για τη διασφάλιση ότι οι υπηρεσίες και οι εφαρμογές του Κυβερνοχώρου είναι διαθέσιμες σε οποιονδήποτε στον Κυβερνοχώρο. Ενώ οποιαδήποτε υποδομή που επιτρέπει σε οποιονδήποτε καταναλωτή να συνδεθεί στον Κυβερνοχώρο ή επιτρέπει σε οποιονδήποτε καταναλωτή να έχει πρόσβαση σε υπηρεσίες στον Κυβερνοχώρο, θεωρείται φυσικό περιουσιακό στοιχείο που πρέπει να αντιμετωπιστεί στο παρόν Διεθνές Πρότυπο, ενδέχεται να υπάρχουν επικαλύψεις με μέτρα ασφαλείας που προτείνονται, για παράδειγμα, ΠΥΠΖΣ, ασφάλειας Διαδικτύου και ασφάλειας δικτύων. Ωστόσο, το παρόν Διεθνές Πρότυπο επικεντρώνεται στη διασφάλιση ότι τα θέματα ασφάλειας που ενδέχεται να επηρεάσουν αυτά τα οργανωτικά περιουσιακά στοιχεία αντιμετωπίζονται κατάλληλα, χωρίς να δίνεται υπερβολική έμφαση σε άλλα θέματα που δεν εμπίπτουν στο πεδίο εφαρμογής του παρόντος Διεθνούς Προτύπου.

Εκτός από τα φυσικά περιουσιακά στοιχεία, τα εικονικά περιουσιακά στοιχεία του οργανισμού αποκτούν ολοένα και μεγαλύτερη αξία. Το διαδικτυακό εμπορικό σήμα και άλλες αναπαραστάσεις του οργανισμού στον Κυβερνοχώρο προσδιορίζουν μοναδικά τον οργανισμό στον Κυβερνοχώρο και είναι εξίσου σημαντικά με τα τούβλα και τα κονιάματα του εν λόγω οργανισμού.

ΠΑΡΑΔΕΙΓΜΑ 1 Η διεύθυνση του Ενιαίου Εντοπιστή Πόρων και οι πληροφορίες του ιστότοπου ενός οργανισμού αποτελούν περιουσιακά στοιχεία.

ΠΑΡΑΔΕΙΓΜΑ 2 Χώρες έχουν δημιουργήσει ακόμη και πρεσβείες σε έναν μεγάλο εικονικό κόσμο για την προστασία της εκπροσώπησης της χώρας.

Άλλα περιουσιακά στοιχεία του οργανισμού που εκτίθενται μέσω ευπαθειών στον Κυβερνοχώρο περιλαμβάνουν πνευματική ιδιοκτησία (φόρμουλες, ιδιόκτητες διαδικασίες, διπλώματα ευρεσιτεχνίας, ερευνητικά αποτελέσματα) και επιχειρηματικά σχέδια και στρατηγικές (τακτικές προώθησης και μάρκετινγκ προϊόντων, πληροφορίες για τον ανταγωνισμό, οικονομικές πληροφορίες και δεδομένα αναφορών).

9 Απειλές κατά της ασφάλειας του Κυβερνοχώρου

9.1 Απειλές

9.1.1 Επισκόπηση

Οι απειλές που υπάρχουν στον Κυβερνοχώρο συζητούνται σε σχέση με τα περιουσιακά στοιχεία στον Κυβερνοχώρο. Οι απειλές στον Κυβερνοχώρο μπορούν να χωριστούν σε δύο βασικούς τομείς:

- απειλές για τα προσωπικά περιουσιακά στοιχεία,

- απειλές σε περιουσιακά στοιχεία οργανισμών.

9.1.2 Απειλές σε προσωπικά περιουσιακά στοιχεία

Οι απειλές για τα προσωπικά περιουσιακά στοιχεία περιστρέφονται κυρίως γύρω από ζητήματα ταυτότητας, που δημιουργούνται από τη διαρροή ή την κλοπή προσωπικών πληροφοριών.

ΠΑΡΑΔΕΙΓΜΑ 1 Οι πληροφορίες διαπίστευσης μπορούν να πωληθούν στη μαύρη αγορά, γεγονός που μπορεί να διευκολύνει την κλοπή ταυτότητας στο διαδίκτυο.

Εάν η διαδικτυακή ταυτότητα ενός ατόμου κλαπεί ή παραποιηθεί, το εν λόγω άτομο μπορεί να στερηθεί την πρόσβαση σε σημαντικές υπηρεσίες και εφαρμογές. Σε πιο σοβαρά σενάρια, οι συνέπειες μπορεί να κυμαίνονται από οικονομικά έως και περιστατικά εθνικού επιπέδου.

Η μη εξουσιοδοτημένη πρόσβαση στις οικονομικές πληροφορίες ενός ατόμου ανοίγει επίσης την πιθανότητα κλοπής των χρημάτων του ατόμου και απάτης.

Μια άλλη απειλή είναι η πιθανότητα το τερματικό σημείο να μετατραπεί σε ζόμπι ή ρομπότ. Οι προσωπικές υπολογιστικές συσκευές μπορούν να παραβιαστούν και να γίνουν έτσι μέρος ενός μεγαλύτερου δικτύου ρομπότ.

Εκτός από τα παραπάνω, άλλα εικονικά περιουσιακά στοιχεία που βρίσκονται στο στόχαστρο είναι τα προσωπικά περιουσιακά στοιχεία σε εικονικούς κόσμους και διαδικτυακά παιχνίδια. Τα περιουσιακά στοιχεία σε έναν εικονικό κόσμο ή στον κόσμο των διαδικτυακών παιχνιδιών υπόκεινται επίσης σε επιθέσεις και εκμετάλλευση.

ΠΑΡΑΔΕΙΓΜΑ 2 Τα στοιχεία των άβαταρ και τα εικονικά νομίσματα, τα οποία, σε ορισμένες περιπτώσεις, μπορούν να ανιχνευθούν και να επαναφερθούν στον πραγματικό κόσμο, θα ήταν οι πρωταρχικοί στόχοι.

Εικονική κλοπή και εικονική ληστεία είναι μερικοί από τους νέους όρους που επινοήθηκαν για αυτόν τον τύπο επίθεσης. Η ασφάλεια, σε αυτή την περίπτωση, εξαρτάται από το πόση πληροφορία του πραγματικού κόσμου είναι προσβάσιμη, καθώς και από το πλαίσιο ασφαλείας του ίδιου του εικονικού κόσμου, όπως ορίζεται και εφαρμόζεται από τον διαχειριστή του.

Καθώς οι κανόνες και οι κανονισμοί για την προστασία των πραγματικών φυσικών περιουσιακών στοιχείων, σε σχέση με τον Κυβερνοχώρο, βρίσκονται ακόμη υπό διαμόρφωση, εκείνοι που αφορούν τα εικονικά περιουσιακά στοιχεία είναι σχεδόν ανύπαρκτοι. Οι συμμετέχοντες στην αναζήτηση πρέπει να είναι ιδιαίτερα προσεκτικοί και επιφυλακτικοί για να εξασφαλίσουν την κατάλληλη προστασία των εικονικών περιουσιακών στοιχείων τους.

9.1.3 Απειλές για τα περιουσιακά στοιχεία του οργανισμού

Η διαδικτυακή παρουσία και η διαδικτυακή επιχειρηματική δραστηριότητα των οργανισμών συχνά μπαίνουν στο στόχαστρο κακοποιών, των οποίων η πρόθεση είναι κάτι περισσότερο από απλή φάρσα.

ΠΑΡΑΔΕΙΓΜΑ 1 Τα οργανωμένα συνδικάτα ηλεκτρονικού εγκλήματος συχνά απειλούν οργανισμούς ότι οι ιστότοποί τους θα καταστραφούν ή ότι θα τους προκαλέσουν δυσφήμηση μέσω ενεργειών όπως η αλλοίωση ιστότοπων.

ΠΑΡΑΔΕΙΓΜΑ 2 Εάν η διεύθυνση του Ενιαίου Εντοπιστή Πόρων ενός οργανισμού καταχωρηθεί ή κλαπεί από διαδικτυακούς καταπατητές και πωληθεί σε οργανισμούς που δε σχετίζονται με τον πραγματικό οργανισμό, η διαδικτυακή εμπιστοσύνη που αποδίδεται στον οργανισμό που έχει πέσει θύμα μπορεί να εκπέσει.

Σε περίπτωση επιτυχούς επίθεσης, προσωπικές πληροφορίες εργαζομένων, πελατών, συνεργατών ή προμηθευτών θα μπορούσαν να αποκαλυφθούν και να οδηγήσουν σε κυρώσεις σε βάρος των

οργανισμών, εάν διαπιστωνόταν ότι η διαχείρισή τους ή η προστασία τους ήταν ανεπαρκής, συμβάλλοντας στην απώλεια.

Οι κανονισμοί υποβολής οικονομικών στοιχείων θα μπορούσαν επίσης να παραβιαστούν εάν τα αποτελέσματα του οργανισμού δημοσιοποιηθούν με μη εξουσιοδοτημένο τρόπο.

Οι κυβερνήσεις κατέχουν πληροφορίες για θέματα εθνικής ασφάλειας, στρατηγικής, στρατού, πληροφοριών, μεταξύ πολλών άλλων στοιχείων που αφορούν την κυβέρνηση και το κράτος, αλλά και ένα ευρύ φάσμα πληροφοριών για άτομα, οργανισμούς και την κοινωνία στο σύνολό της.

Σε μεγαλύτερη κλίμακα, η υποδομή που υποστηρίζει το Διαδίκτυο, και συνεπώς τον Κυβερνοχώρο, μπορεί επίσης να αποτελέσει στόχο. Αν και αυτό δε θα επηρεάσει μόνιμα τη λειτουργία του Κυβερνοχώρου, θα επηρεάσει την αξιοπιστία και τη διαθεσιμότητα της υποδομής, η οποία συμβάλλει στην ασφάλεια του Κυβερνοχώρου.

Σε εθνικό ή διεθνές επίπεδο, ο Κυβερνοχώρος είναι μια γκρίζα ζώνη στην οποία ευδοκιμεί η τρομοκρατία. Ένας από τους λόγους είναι η ευκολία επικοινωνίας που παρέχει ο Κυβερνοχώρος. Λόγω της φύσης του Κυβερνοχώρου, και συγκεκριμένα των προκλήσεων στον καθορισμό ορίων και συνόρων, είναι δύσκολο να ρυθμιστεί και να ελεγχθεί ο τρόπος με τον οποίο μπορεί να χρησιμοποιηθεί.

Οι τρομοκρατικές ομάδες μπορούν είτε να αγοράζουν νόμιμα τις εφαρμογές, τις υπηρεσίες και τους πόρους που διευκολύνουν τον σκοπό τους, είτε να καταφεύγουν σε παράνομα μέσα εξασφάλισης αυτών των πόρων για να αποφύγουν την ανίχνευση και τον εντοπισμό. Αυτό μπορεί να περιλαμβάνει την απόκτηση μαζικών υπολογιστικών πόρων μέσω δικτύων ρομπότ.

9.2 Παράγοντες απειλών

Παράγοντας απειλής είναι ένα άτομο ή μια ομάδα ατόμων που έχουν οποιοδήποτε ρόλο στην εκτέλεση ή την υποστήριξη μιας επίθεσης.

Η εμπεριστατωμένη κατανόηση των κινήτρων τους (θρησκευτικά, πολιτικά, οικονομικά κ.λπ.), των δυνατοτήτων τους (γνώση, χρηματοδότηση, μέγεθος κ.λπ.) και των προθέσεών τους (διασκέδαση, έγκλημα, κατασκοπεία κ.λπ.) είναι ζωτικής σημασίας για την αξιολόγηση των ευπαθειών και των κινδύνων, καθώς και για την ανάπτυξη και την εφαρμογή μέτρων ελέγχου.

9.3 Ευπάθειες

Μια ευπάθεια είναι μια αδυναμία ενός περιουσιακού στοιχείου ή ενός μέτρου ελέγχου που μπορεί να αξιοποιηθεί από μια απειλή. Στο πλαίσιο ενός πληροφοριακού συστήματος, το ISO/IEC TR 19791:2006 ορίζει επίσης την ευπάθεια ως σφάλμα, αδυναμία ή ιδιότητα του σχεδιασμού ή της υλοποίησης ενός πληροφοριακού συστήματος (συμπεριλαμβανομένων των ελέγχων ασφαλείας του) ή του περιβάλλοντός του, η οποία θα μπορούσε να αξιοποιηθεί εκούσια ή ακούσια για να επηρεάσει αρνητικά τα περιουσιακά στοιχεία ή τις λειτουργίες ενός οργανισμού.

Η αξιολόγηση των τρωτών σημείων πρέπει να είναι ένα συνεχές έργο. Καθώς τα συστήματα λαμβάνουν επιδιορθώσεις, ενημερώσεις ή προστίθενται νέα στοιχεία, ενδέχεται να παρουσιαστούν νέες ευπάθειες. Οι ενδιαφερόμενοι φορείς απαιτούν ενδελεχή γνώση και κατανόηση του εν λόγω περιουσιακού στοιχείου ή ελέγχου, καθώς και των απειλών, των παραγόντων απειλής και των κινδύνων που εμπλέκονται, προκειμένου να πραγματοποιηθεί μια ολοκληρωμένη αξιολόγηση.

ΣΗΜΕΙΩΣΗ Το ISO/IEC 27005 παρέχει κατευθυντήριες γραμμές για τον εντοπισμό ευπαθειών.

Ένας κατάλογος γνωστών ευπαθειών θα πρέπει να τηρείται με το αυστηρότερο πρωτόκολλο πρόσβασης και κατά προτίμηση χωριστά, φυσικά και λογικά, από το περιουσιακό στοιχείο ή τον έλεγχο στον οποίο εφαρμόζεται. Σε περίπτωση παραβίασης της πρόσβασης και παραβίασης του καταλόγου των ευπαθειών, ο κατάλογος των ευπαθειών θα είναι ένα από τα πιο αποτελεσματικά εργαλεία στο οπλοστάσιο ενός παράγοντα απειλής που θα χρησιμοποιήσει για να διαπράξει μια επίθεση.

Πρέπει να αναζητούνται λύσεις για τις ευπάθειες, να εφαρμόζονται και, όταν η λύση δεν είναι δυνατή ή εφικτή, να εφαρμόζονται μέτρα ελέγχου. Η προσέγγιση αυτή πρέπει να εφαρμόζεται κατά προτεραιότητα, ώστε να αντιμετωπίζονται πρώτα οι ευπάθειες που ενέχουν υψηλότερο κίνδυνο. Οι διαδικασίες αποκάλυψης ευπαθειών θα μπορούσαν να καθοριστούν στο πλαίσιο της ανταλλαγής πληροφοριών και του συντονισμού της παραγράφου 13 του παρόντος Διεθνούς Προτύπου.

ΣΗΜΕΙΩΣΗ Ένα μελλοντικό διεθνές πρότυπο, το ISO/IEC 29147, θα παρέχει καθοδήγηση σχετικά με την αποκάλυψη ευπαθειών.

9.4 Μηχανισμοί επίθεσης

9.4.1 Εισαγωγή

Πολλές από τις επιθέσεις στον Κυβερνοχώρο πραγματοποιούνται με τη χρήση κακόβουλου λογισμικού, όπως λογισμικό κατασκοπείας, σκουλήκια και ιοί. Οι πληροφορίες συλλέγονται συχνά μέσω τεχνικών ηλεκτρονικού ψαρέματος. Μια επίθεση μπορεί να εκδηλωθεί ως μεμονωμένη επίθεση ή να πραγματοποιηθεί ως μέρος συνδυασμένης επίθεσης. Οι επιθέσεις αυτές μπορούν να διαδοθούν, για παράδειγμα, μέσω ύποπτων ιστότοπων, μη αναγνωρισμένων λήψεων, ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, απομακρυσμένης αξιοποίησης και μολυσμένων αφαιρούμενων μέσων.

Οι επιθέσεις μπορεί να προέρχονται από δύο μεγάλες κατηγορίες:

- επιθέσεις από το εσωτερικό του ιδιωτικού δικτύου και

- επιθέσεις από το εξωτερικό του ιδιωτικού δικτύου.

Υπάρχουν όμως περιπτώσεις που οι επιθέσεις είναι συνδυασμός επιθέσεων τόσο εντός όσο και εκτός ιδιωτικού δικτύου. Άλλοι μηχανισμοί που αυξάνονται σε χρήση και πολυπλοκότητα, για την πραγματοποίηση επιθέσεων, είναι αυτοί που βασίζονται σε ιστότοπους κοινωνικής δικτύωσης και η χρήση μολυσμένων αρχείων σε νόμιμους ιστότοπους.

Τα άτομα τείνουν να εμπιστεύονται αυθόρμητα τα μηνύματα και το περιεχόμενο που λαμβάνουν από επαφές που έχουν γίνει προηγουμένως αποδεκτές στο προφίλ τους στους ιστότοπους κοινωνικής δικτύωσης. Μόλις ένας επιτιθέμενος, μέσω υποκλοπής ταυτότητας, μπορέσει να μεταμφιεστεί σε νόμιμη επαφή, ο επιτιθέμενος μπορεί να εμπλέξει άλλους και ανοίγεται μια νέα οδός για την εξαπόλυση των διαφόρων τύπων επιθέσεων που συζητήθηκαν προηγουμένως.

Οι νόμιμοι ιστότοποι μπορούν επίσης να παραβιαστούν και να παραποιηθούν ορισμένα από τα αρχεία τους και να χρησιμοποιηθούν ως μέσο για τη διάπραξη επιθέσεων. Τα άτομα τείνουν να εμπιστεύονται αυθόρμητα τους ιστότοπους που επισκέπτονται συχνά, οι οποίοι συχνά είναι αποθηκευμένοι στους σελιδοδείκτες των προγραμμάτων περιήγησης στο Διαδίκτυο για μεγάλο χρονικό διάστημα, και ακόμη περισσότερο εκείνους που χρησιμοποιούν μηχανισμούς ασφαλείας όπως το SSL (Secure Sockets Layer). Ενώ η αυθεντικοποίηση των μερών και η ακεραιότητα των πληροφοριών που μεταδίδονται ή λαμβάνονται εξακολουθούν να ισχύουν, το SSL δεν κάνει διάκριση μεταξύ του αρχικού περιεχομένου και

του νέου αλλοιωμένου περιεχομένου, που έχει τοποθετηθεί από έναν επιτιθέμενο, εκθέτοντας έτσι τους χρήστες του εν λόγω δικτυακού τόπου σε επιθέσεις.

Παρά την υποτιθέμενη νόμιμη πηγή, όπως για παράδειγμα σε περιπτώσεις όπως η παραπάνω, τα άτομα πρέπει να λαμβάνουν τις προφυλάξεις που περιγράφονται στην παράγραφο 11 για την καλύτερη προστασία τους.

9.4.2 Επιθέσεις από το εσωτερικό του ιδιωτικού δικτύου

Οι επιθέσεις αυτές συνήθως εξαπολύονται εντός του ιδιωτικού δικτύου ενός οργανισμού, συνήθως του τοπικού δικτύου, και μπορούν να ξεκινήσουν από υπαλλήλους ή από κάποιον που αποκτά πρόσβαση σε υπολογιστή ή δίκτυο εντός των εγκαταστάσεων ενός οργανισμού ή ενός ατόμου.

ΠΑΡΑΔΕΙΓΜΑ 1 Μια πιθανή περίπτωση είναι ότι οι διαχειριστές του συστήματος μπορεί να εκμεταλλευτούν τα προνόμια πρόσβασης στο σύστημα που κατέχουν, όπως η πρόσβαση στις πληροφορίες των κωδικών πρόσβασης των χρηστών, και να τα χρησιμοποιήσουν για να ξεκινήσουν μια επίθεση. Από την άλλη πλευρά, οι ίδιοι οι διαχειριστές του συστήματος μπορούν να γίνουν ο αρχικός στόχος μιας επίθεσης, ως μέσο για να αποκτήσει ο επιτιθέμενος πρόσθετες πληροφορίες (ονόματα χρηστών, κωδικούς πρόσβασης κ.λπ.), προτού προχωρήσει στον ή στους αρχικά επιδιωκόμενους στόχους του.

Ο επιτιθέμενος μπορεί να χρησιμοποιήσει μηχανισμούς όπως το λογισμικό εντοπισμού πακέτων για να αποκτήσει κωδικούς πρόσβασης ή άλλες πληροφορίες ταυτότητας. Εναλλακτικά, ο επιτιθέμενος μπορεί να μεταμφιεστεί σε εξουσιοδοτημένη οντότητα και να ενεργήσει ως ενδιάμεσος στην επικοινωνία για να υποκλέψει πληροφορίες ταυτότητας.

ΠΑΡΑΔΕΙΓΜΑ 2 Ένα παράδειγμα είναι η χρήση παραπλανητικών σημείων πρόσβασης (ΣΠ) για την κλοπή ταυτοτήτων. Σε αυτή την περίπτωση, ο επιτιθέμενος μπορεί να βρίσκεται σε ένα αεροδρόμιο, μια καφετέρια ή άλλους δημόσιους χώρους που προσφέρουν δωρεάν ασύρματη πρόσβαση στο Διαδίκτυο. Σε ορισμένες περιπτώσεις, ο επιτιθέμενος μπορεί ακόμη και να μεταμφιεστεί ως ο νόμιμος ιδιοκτήτης του ασύρματου σημείου πρόσβασης στον χώρο, χρησιμοποιώντας το Αναγνωριστικό Συνόλου Υπηρεσίας (ΑΣΥ) του χώρου. Εάν ένας χρήστης αποκτήσει πρόσβαση σε αυτό το παραπλανητικό ΣΠ, ο επιτιθέμενος μπορεί να ενεργήσει ως ενδιάμεσος στην επικοινωνία και να αποκτήσει πολύτιμες πληροφορίες κωδικών πρόσβασης ή/και ταυτότητας από τον χρήστη, για παράδειγμα, πληροφορίες και κωδικό πρόσβασης τραπεζικού λογαριασμού, κωδικό πρόσβασης λογαριασμού ηλεκτρονικού ταχυδρομείου κ.λπ.

ΠΑΡΑΔΕΙΓΜΑ 3 Συχνά, είναι αρκετό να είναι κανείς κοντά σε ένα μη προστατευμένο δίκτυο ασύρματης σύνδεσης, όπως π.χ. να κάθεται σε ένα αυτοκίνητο έξω από ένα σπίτι, για να μπορέσει να υποκλέψει πληροφορίες από το δίκτυο.

Εκτός από τις επιθέσεις που εξαπολύουν οι φυσικοί επιτιθέμενοι, οι μολυσμένοι με κακόβουλο λογισμικό υπολογιστές εξαπολύουν επίσης διάφορες επιθέσεις στους συμμετέχοντες υπολογιστές εντός του ιδιωτικού δικτύου.

ΠΑΡΑΔΕΙΓΜΑ 4 Πολλά κακόβουλα προγράμματα στέλνουν συχνά πακέτα σάρωσης στο ιδιωτικό δίκτυο για να βρουν τους συμμετέχοντες υπολογιστές και στη συνέχεια προσπαθούν να εκμεταλλευτούν τους υπολογιστές που ανακαλύπτονται.

ΠΑΡΑΔΕΙΓΜΑ 5 Κάποιο κακόβουλο λογισμικό χρησιμοποιεί τη προνομιακή λειτουργία μιας διασύνδεσης δικτύου του μολυσμένου υπολογιστή του για να παρακολουθεί την κυκλοφορία που ρέει μέσω του ιδιωτικού δικτύου.

ΠΑΡΑΔΕΙΓΜΑ 6 Τα προγράμματα καταγραφής πλήκτρων είναι εφαρμογές υλικού ή λογισμικού που καταγράφουν όλα τα πλήκτρα που πατιούνται στο σύστημα-στόχο. Αυτό μπορεί να γίνει κρυφά για την παρακολούθηση των ενεργειών ενός χρήστη. Τα προγράμματα καταγραφής πλήκτρων χρησιμοποιούνται συχνά για την καταγραφή πληροφοριών αυθεντικοποίησης από σελίδες σύνδεσης εφαρμογών.

9.4.3 Επιθέσεις εκτός του ιδιωτικού δικτύου (π.χ. από το Διαδίκτυο)

Υπάρχουν πολλές διαφορετικές επιθέσεις που μπορούν να εξαπολυθούν από το εξωτερικό ενός ιδιωτικού δικτύου, συμπεριλαμβανομένου του Διαδικτύου.

Αν και η αρχική επίθεση θα στοχεύει πάντα ένα σύστημα στο οποίο υπάρχει δυνατότητα πρόσβασης από το εξωτερικό του δικτύου (π.χ. δρομολογητής, διακομιστής, τείχος προστασίας, ιστότοπος κ.λπ.), οι επιτιθέμενοι μπορεί επίσης να επιδιώκουν να εκμεταλλευτούν περιουσιακά στοιχεία που βρίσκονται εντός του ιδιωτικού δικτύου.

Οι παλιές μέθοδοι επίθεσης βελτιώνονται και νέες αναπτύσσονται σε συνεχή βάση. Οι επιτιθέμενοι είναι όλο και πιο εξελιγμένοι και συνήθως συνδυάζουν διαφορετικές τεχνικές και μηχανισμούς επίθεσης για να μεγιστοποιήσουν την επιτυχία τους, γεγονός που καθιστά την ανίχνευση και την πρόληψη των επιθέσεων ακόμη πιο δύσκολη.

Οι σαρωτές θυρών είναι ένα από τα παλαιότερα, και ακόμη πολύ αποτελεσματικά, εργαλεία που χρησιμοποιούν οι επιτιθέμενοι. Σαρώνουν όλες τις θύρες που είναι διαθέσιμες σε έναν εξυπηρετητή για να επιβεβαιώσουν ποιες θύρες είναι "ανοιχτές". Αυτό είναι συνήθως ένα από τα πρώτα βήματα που εκτελεί ένας υποψήφιος επιτιθέμενος στο σύστημα-στόχο.

Αυτές οι επιθέσεις μπορούν να εξελιχθούν σε διάφορες επιθέσεις Άρνησης Εξυπηρέτησης είτε στους εξυπηρετητές εφαρμογών είτε σε άλλο δικτυακό εξοπλισμό, εκμεταλλευόμενοι ευπάθειες σχεδιασμού πρωτοκόλλου ή εφαρμογής.

ΠΑΡΑΔΕΙΓΜΑ Με τη βοήθεια ενός δικτύου ρομπότ, μπορούν να εξαπολυθούν επιθέσεις Άρνησης Εξυπηρέτησης μεγάλης κλίμακας που μπορούν να καταστρέψουν την πρόσβαση μιας χώρας στον Κυβερνοχώρο.

Με τη διάδοση των εφαρμογών ομότιμης πρόσβασης, που χρησιμοποιούνται συνήθως για την ανταλλαγή αρχείων όπως ψηφιακή μουσική, βίντεο, φωτογραφίες κ.λπ., οι επιτιθέμενοι γίνονται όλο και πιο επιδέξιοι στο πώς να μεταμφιέζουν τους εαυτούς τους και τον κακόβουλο κώδικά τους χρησιμοποιώντας τα αρχεία που ανταλλάσσονται ως δούρειο ίππο για τις επιθέσεις τους.

Οι υπερχειλίσεις προσωρινής μνήμης (ή αλλιώς υπερβάσεις προσωρινής μνήμης) είναι μια άλλη δημοφιλής μέθοδος παραβίασης διακομιστών στο Διαδίκτυο. Εκμεταλλευόμενοι τρωτά σημεία κωδικοποίησης και στέλνοντας πολύ μεγαλύτερες από το αναμενόμενο σειρές χαρακτήρων, οι επιτιθέμενοι προκαλούν τη λειτουργία του διακομιστή εκτός του κανονικού (ελεγχόμενου) περιβάλλοντος, διευκολύνοντας έτσι την εισαγωγή/εκτέλεση κακόβουλου κώδικα.

Μια άλλη τεχνική είναι η παραπλανητική διεύθυνση ΠΔ, η οποία περιλαμβάνει την παραποίηση της διεύθυνσης ΠΔ που σχετίζεται με τον επιτιθέμενο χρησιμοποιώντας μηνύματα σε μια προσπάθεια να θεωρηθεί ως μια γνωστή, αξιόπιστη πηγή, αποκτώντας έτσι μη εξουσιοδοτημένη πρόσβαση σε συστήματα.

10 Ρόλοι των ενδιαφερομένων στην κυβερνοασφάλεια

10.1 Επισκόπηση

Για να βελτιωθεί η κατάσταση της Κυβερνοασφάλειας, οι ενδιαφερόμενοι στον Κυβερνοχώρο πρέπει να διαδραματίσουν ενεργό ρόλο στην αντίστοιχη χρήση και ανάπτυξη του Διαδικτύου. Αυτοί οι ρόλοι

μπορεί κατά καιρούς να επικαλύπτονται με τους ατομικούς και εταιρικούς τους ρόλους εντός των προσωπικών ή των δικτύων των οργανισμών τους. Ο όρος δίκτυο οργανισμού αναφέρεται στο συνδυασμό των ιδιωτικών δικτύων ενός οργανισμού (συνήθως ένα εσωτερικό δίκτυο), των εξωτερικών δικτύων και των δημόσια προβεβλημένων δικτύων. Για τους σκοπούς του παρόντος Διεθνούς Προτύπου, τα δημόσια προβαλλόμενα δίκτυα είναι εκείνα τα δίκτυα που εκτίθενται στο Διαδίκτυο, για παράδειγμα για τη φιλοξενία ενός δικτυακού τόπου. Εξαιτίας αυτής της αλληλοεπικάλυψης, οι ρόλοι αυτοί μπορεί να φαίνεται ότι έχουν ασήμαντο ή καθόλου άμεσο όφελος για το άτομο και τον οργανισμό. Είναι, ωστόσο, σημαντικοί για την ενίσχυση της Κυβερνοασφάλειας, όταν όλοι οι εμπλεκόμενοι ενεργούν ανάλογα.

10.2 Ρόλος των καταναλωτών

10.2.1 Εισαγωγή

Οι καταναλωτές μπορούν να βλέπουν ή να συλλέγουν πληροφορίες, καθώς και να παρέχουν ορισμένες συγκεκριμένες πληροφορίες εντός του χώρου μιας εφαρμογής του Κυβερνοχώρου, ή να καθιστούν τις πληροφορίες προσβάσιμες σε περιορισμένα μέλη ή ομάδες εντός του χώρου της εφαρμογής, ή στο ευρύ κοινό. Οι ενέργειες που αναλαμβάνουν οι καταναλωτές σε αυτούς τους ρόλους μπορεί να είναι παθητικές ή ενεργητικές και μπορούν να συμβάλουν άμεσα ή έμμεσα στην κατάσταση της Κυβερνοασφάλειας.

10.2.2 Ρόλος των ατόμων

Οι μεμονωμένοι καταναλωτές του Κυβερνοχώρου μπορούν να αναλάβουν διαφορετικούς ρόλους σε διαφορετικά πλαίσια και εφαρμογές.

Οι ρόλοι των καταναλωτών μπορεί να περιλαμβάνουν, μεταξύ άλλων, τα εξής:

- Γενικός χρήστης εφαρμογών του Κυβερνοχώρου ή γενικός χρήστης, όπως παίκτης διαδικτυακών παιχνιδιών, χρήστης άμεσων μηνυμάτων ή περιηγητής στον ιστό,

- Αγοραστής/πωλητής, που εμπλέκεται στην τοποθέτηση αγαθών και υπηρεσιών σε δικτυακούς τόπους δημοπρασιών και αγορών για ενδιαφερόμενους αγοραστές και το αντίστροφο,

- Μπλόγκερ και άλλοι συνεισφέροντες περιεχομένου (π.χ. συγγραφέας ενός άρθρου σε ένα δικτυακό τόπο), στους οποίους δημοσιεύονται πληροφορίες σε κείμενο και πολυμέσα (π.χ. βίντεο κλιπ) για κατανάλωση από το ευρύ κοινό ή από περιορισμένο κοινό,

- ΑΠΕ στο πλαίσιο μιας εφαρμογής (όπως ένα διαδικτυακό παιχνίδι), ή στον κυβερνοχώρο γενικά,

- Μέλος ενός οργανισμού (όπως υπάλληλος μιας εταιρείας, ή άλλη μορφή σύνδεσης με μια εταιρεία),

- Άλλοι ρόλοι. Είναι δυνατόν να ανατεθεί σε έναν χρήστη ένας ρόλος ακούσια ή χωρίς τη συγκατάθεσή του.

ΠΑΡΑΔΕΙΓΜΑ Όταν ένας χρήστης επισκέπτεται έναν ιστότοπο που απαιτεί εξουσιοδότηση και αποκτά ακούσια πρόσβαση, ο χρήστης μπορεί να χαρακτηριστεί ως εισβολέας.

Σε καθέναν από αυτούς τους ρόλους, τα άτομα μπορούν να βλέπουν ή να συλλέγουν πληροφορίες, καθώς και να παρέχουν ορισμένες συγκεκριμένες πληροφορίες εντός του χώρου μιας εφαρμογής του Κυβερνοχώρου, ή να καθιστούν τις πληροφορίες προσβάσιμες σε περιορισμένα μέλη ή ομάδες εντός του χώρου της εφαρμογής, ή στο ευρύ κοινό. Οι ενέργειες που αναλαμβάνουν τα άτομα σε αυτούς τους

ρόλους μπορεί να είναι παθητικές ή ενεργητικές και μπορούν να συμβάλουν άμεσα ή έμμεσα στην κατάσταση της Κυβερνοασφάλειας.

ΠΑΡΑΔΕΙΓΜΑ 1 Εάν ένας ΑΠΕ παρέχει μια εφαρμογή που περιέχει τρωτά σημεία ασφαλείας, αυτά τα τρωτά σημεία μπορούν να χρησιμοποιηθούν από κακοποιούς του κυβερνοχώρου ως δίαυλος για να προσεγγίσουν τους χρήστες της εφαρμογής.

ΠΑΡΑΔΕΙΓΜΑ 2 Οι μπλόγκερ ή άλλοι συντελεστές περιεχομένου μπορούν να λάβουν ένα αίτημα με τη μορφή αθώων ερωτήσεων σχετικά με το περιεχόμενό τους. Στην απάντησή τους, μπορεί να αποκαλύψουν ακούσια στο κοινό περισσότερες προσωπικές ή εταιρικές πληροφορίες από ό,τι επιθυμούν.

ΠΑΡΑΔΕΙΓΜΑ 3 Ένα άτομο, ενεργώντας ως αγοραστής ή πωλητής, μπορεί εν αγνοία του να συμμετέχει σε εγκληματικές συναλλαγές πώλησης κλεμμένων αγαθών ή δραστηριότητες ξεπλύματος χρημάτων.

Κατά συνέπεια, όπως και στον πραγματικό κόσμο, οι μεμονωμένοι καταναλωτές πρέπει να είναι προσεκτικοί σε κάθε ρόλο που διαδραματίζουν στον Κυβερνοχώρο.

10.2.3 Ρόλος των οργανισμών

Οι οργανισμοί χρησιμοποιούν συχνά τον Κυβερνοχώρο για να δημοσιοποιήσουν την εταιρεία και τις σχετικές πληροφορίες, καθώς και για να προωθήσουν στην αγορά σχετικά προϊόντα και υπηρεσίες. Οι οργανισμοί χρησιμοποιούν επίσης τον Κυβερνοχώρο ως μέρος του δικτύου τους για την παράδοση και τη λήψη ηλεκτρονικών μηνυμάτων (π.χ. μηνύματα ηλεκτρονικού ταχυδρομείου) και άλλων εγγράφων (π.χ. μεταφορά αρχείων).

Σύμφωνα με τις ίδιες αρχές που διέπουν την ιδιότητα του καλού εταιρικού πολίτη, οι οργανισμοί αυτοί θα πρέπει να επεκτείνουν τις εταιρικές τους ευθύνες στον Κυβερνοχώρο, διασφαλίζοντας προληπτικά ότι οι πρακτικές και οι ενέργειές τους στον Κυβερνοχώρο δεν εισάγουν περαιτέρω κινδύνους για την ασφάλεια στον Κυβερνοχώρο. Ορισμένα προληπτικά μέτρα περιλαμβάνουν:

- ορθή διαχείριση της ασφάλειας των πληροφοριών με την εφαρμογή και λειτουργία ενός αποτελεσματικού συστήματος διαχείρισης της ασφάλειας των πληροφοριών (ΣΔΑΠ) (Information Security Management System, ISMS),

ΣΗΜΕΙΩΣΗ 1 Το ISO/IEC 27001 παρέχει απαιτήσεις για συστήματα διαχείρισης ασφάλειας των πληροφοριών.

- κατάλληλη παρακολούθηση και αντιμετώπιση της ασφάλειας,

- ενσωμάτωση της ασφάλειας ως μέρος του κύκλου ζωής της ανάπτυξης λογισμικού (ΚΖΑΛ), όπου το επίπεδο ασφάλειας που ενσωματώνεται στα συστήματα πρέπει να καθορίζεται με βάση την κρισιμότητα των δεδομένων του οργανισμού,

- τακτική εκπαίδευση των χρηστών του οργανισμού σε θέματα ασφάλειας μέσω συνεχών ενημερώσεων τεχνολογίας και παρακολούθησης των τελευταίων τεχνολογικών εξελίξεων- και

- κατανόηση και χρήση των κατάλληλων διαύλων επικοινωνίας με τους προμηθευτές και τους παρόχους υπηρεσιών για θέματα ασφάλειας που ανακαλύπτονται κατά τη χρήση.

ΣΗΜΕΙΩΣΗ 2 Ένα μελλοντικό διεθνές πρότυπο, το ISO/IEC 29147, θα παρέχει κατευθυντήριες γραμμές σχετικά με την αποκάλυψη ευπαθειών.

ΣΗΜΕΙΩΣΗ 3 Το ISO/IEC 27031 παρέχει κατευθυντήριες γραμμές για την ετοιμότητα των ΤΠΕ για την επιχειρησιακή συνέχεια.

ΣΗΜΕΙΩΣΗ 4 Το ISO/IEC 27035 παρέχει κατευθυντήριες γραμμές για τη διαχείριση περιστατικών ασφάλειας πληροφοριών.

ΣΗΜΕΙΩΣΗ 5 Το ISO/IEC 27034-1 παρέχει κατευθυντήριες γραμμές για την ασφάλεια εφαρμογών.

Η κυβέρνηση, κυρίως οι υπηρεσίες επιβολής του νόμου και οι ρυθμιστικές αρχές, μπορεί να διαδραματίσει τους ακόλουθους σημαντικούς ρόλους:

- να συμβουλεύει τους οργανισμούς σχετικά με τους ρόλους και τις ευθύνες τους στον Κυβερνοχώρο,

- να ανταλλάσσει πληροφορίες με άλλους ενδιαφερόμενους φορείς σχετικά με τις τελευταίες τάσεις και εξελίξεις στην τεχνολογία,

- να ανταλλάσσει πληροφορίες με άλλους ενδιαφερόμενους φορείς σχετικά με τους τρέχοντες επικρατούντες κινδύνους ασφάλειας,

- να είναι αγωγός για τη λήψη οποιασδήποτε πληροφορίας, είτε στενής είτε ανοικτής, όσον αφορά τους κινδύνους ασφάλειας στον Κυβερνοχώρο- και

- να είναι ο κύριος συντονιστής για τη διάδοση πληροφοριών και την οργάνωση τυχόν απαιτούμενων πόρων, τόσο σε εθνικό όσο και σε εταιρικό επίπεδο, σε περιόδους κρίσης που προκύπτουν από μια μαζική επίθεση στον κυβερνοχώρο.

10.3 Ρόλοι των παρόχων

Οι οργανισμοί παροχής υπηρεσιών μπορούν να περιλαμβάνουν δύο κατηγορίες:

- Οι πάροχοι πρόσβασης των εργαζομένων και των συνεργατών στον Κυβερνοχώρο, και

- πάροχοι υπηρεσιών σε καταναλωτές του Κυβερνοχώρου, είτε σε μια κλειστή κοινότητα (για παράδειγμα, εγγεγραμμένους χρήστες), είτε στο ευρύ κοινό, μέσω της παροχής εφαρμογών στον Κυβερνοχώρο.

ΠΑΡΑΔΕΙΓΜΑ Παραδείγματα υπηρεσιών είναι οι διαδικτυακές αγορές συναλλαγών, οι υπηρεσίες πλατφόρμας συζητήσεων, οι υπηρεσίες πλατφόρμας ιστολογίων και οι υπηρεσίες κοινωνικής δικτύωσης.

Οι πάροχοι υπηρεσιών είναι επίσης οργανώσεις καταναλωτών. Ως εκ τούτου, αναμένεται να ακολουθούν τους ίδιους ρόλους και τις ίδιες ευθύνες με τις οργανώσεις καταναλωτών. Ως πάροχοι υπηρεσιών, έχουν πρόσθετες ευθύνες για τη διατήρηση ή ακόμη και την ενίσχυση της ασφάλειας του Κυβερνοχώρου:

- παρέχοντας ασφαλή προϊόντα και υπηρεσίες,

- παρέχοντας καθοδήγηση για την ασφάλεια και την προστασία των τελικών χρηστών- και

- παρέχοντας πληροφορίες ασφάλειας σε άλλους παρόχους και στους καταναλωτές σχετικά με τις τάσεις και τις παρατηρήσεις της κυκλοφορίας στα δίκτυα και τις υπηρεσίες τους.

11 Κατευθυντήριες γραμμές για τα ενδιαφερόμενα μέρη

11.1 Επισκόπηση

Η καθοδήγηση στην παρούσα παράγραφο επικεντρώνεται σε τρεις κύριους τομείς:

- καθοδήγηση για την ασφάλεια των καταναλωτών,

- εσωτερική διαχείριση κινδύνων ασφάλειας πληροφοριών ενός οργανισμού- και

- απαιτήσεις ασφάλειας που πρέπει να καθορίζουν οι πάροχοι για την εφαρμογή από τους καταναλωτές.

Οι συστάσεις διαρθρώνονται ως εξής:

α) μια εισαγωγή στην αξιολόγηση και την αντιμετώπιση του κινδύνου,

β) κατευθυντήριες γραμμές για τους καταναλωτές και

γ) κατευθυντήριες γραμμές για τους οργανισμούς, συμπεριλαμβανομένων των παρόχων υπηρεσιών:

- διαχείριση του κινδύνου ασφάλειας των πληροφοριών στην επιχείρηση και

- απαιτήσεις ασφάλειας για υπηρεσίες φιλοξενίας και άλλες υπηρεσίες εφαρμογών.

11.2 Εκτίμηση κινδύνου και αντιμετώπιση

Το ISO 31000, Διαχείριση κινδύνων - Αρχές και κατευθυντήριες γραμμές, παρέχει αρχές και γενικές κατευθυντήριες γραμμές για τη διαχείριση κινδύνων, ενώ το ISO/IEC 27005, Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Διαχείριση κινδύνων ασφάλειας πληροφοριών, παρέχει κατευθυντήριες γραμμές και διαδικασίες για τη διαχείριση κινδύνων ασφάλειας πληροφοριών σε έναν οργανισμό, υποστηρίζοντας ιδίως τις απαιτήσεις ενός ΣΔΑΠ σύμφωνα με το ISO/IEC 27001. Οι εν λόγω κατευθυντήριες γραμμές και διαδικασίες θεωρούνται επαρκείς για την αντιμετώπιση της διαχείρισης κινδύνων στο πλαίσιο του Κυβερνοχώρου.

Το ISO/IEC 27005:2011 δεν παρέχει καμία συγκεκριμένη μεθοδολογία για τη διαχείριση κινδύνων ασφάλειας πληροφοριών. Εναπόκειται στους καταναλωτές και τους παρόχους να καθορίσουν την προσέγγισή τους για τη διαχείριση κινδύνων. Ορισμένες υφιστάμενες μεθοδολογίες μπορούν να χρησιμοποιηθούν στο πλαίσιο που περιγράφεται στο ISO/IEC 27005 για την εφαρμογή των απαιτήσεων ενός ΣΔΑΠ.

Κατά τον καθορισμό μιας προσέγγισης για τη διαχείριση των κινδύνων πρέπει να λαμβάνονται υπόψη οι ακόλουθες πτυχές:

- Προσδιορισμός των κρίσιμων περιουσιακών στοιχείων: Η σύνδεση με τον Κυβερνοχώρο ή η χρήση του διευρύνει το πεδίο ορισμού των περιουσιακών στοιχείων. Δεδομένου ότι δεν είναι οικονομικά αποδοτικό να προστατευθούν όλα τα περιουσιακά στοιχεία, είναι σημαντικό να προσδιοριστούν τα κρίσιμα περιουσιακά στοιχεία, ώστε να ληφθεί ιδιαίτερη μέριμνα για την προστασία τους. Ο προσδιορισμός πρέπει να γίνεται από το επιχειρηματικό πλαίσιο, μέσω της εξέτασης του αντίκτυπου της απώλειας ή της υποβάθμισης ενός περιουσιακού στοιχείου στην επιχείρηση στο σύνολό της.

- Προσδιορισμός των κινδύνων: Τα ενδιαφερόμενα μέρη θα πρέπει να εξετάζουν και να αντιμετωπίζουν κατάλληλα τους πρόσθετους κινδύνους, απειλές και επιθέσεις που καθίστανται σημαντικοί κατά τη συμμετοχή στον Κυβερνοχώρο.

- Ευθύνη: Συμμετέχοντας στον Κυβερνοχώρο, ένας ενδιαφερόμενος θα πρέπει να αποδεχθεί την πρόσθετη ευθύνη έναντι άλλων ενδιαφερόμενων μερών. Αυτό περιλαμβάνει:

- Αναγνώριση: Αναγνώριση του πιθανού κινδύνου που μπορεί να εισάγει η συμμετοχή του ενδιαφερομένου στον Κυβερνοχώρο γενικά και ειδικά στα πληροφοριακά συστήματα άλλων ενδιαφερομένων.

- Αναφορά: Μπορεί να είναι απαραίτητο να συμπεριληφθούν ενδιαφερόμενοι εκτός του οργανισμού κατά τη διανομή αναφορών που σχετίζονται με κινδύνους, περιστατικά και απειλές.

- Ανταλλαγή πληροφοριών: Όπως και με την υποβολή εκθέσεων, ενδέχεται να είναι απαραίτητη η ανταλλαγή σχετικών πληροφοριών με άλλα ενδιαφερόμενα μέρη.

- Αξιολόγηση κινδύνων: Είναι απαραίτητο να προσδιοριστεί ο βαθμός στον οποίο οι ενέργειες και η παρουσία ενός ενδιαφερόμενου μέρους στον Κυβερνοχώρο αποτελεί ή συμβάλλει σε κίνδυνο για ένα άλλο ενδιαφερόμενο μέρος.

- Ρυθμιστικές/νομοθετικές διατάξεις: Με τη σύνδεση με τον Κυβερνοχώρο, τα νομικά και κανονιστικά όρια είναι δύσκολο να διακριθούν και ισχύουν περισσότερες, ενίοτε αντιφατικές, απαιτήσεις.

- Απόσυρση συστήματος ή υπηρεσίας: Όταν ένα σύστημα ή μια υπηρεσία δε χρειάζεται πλέον, θα πρέπει να αποσυρθεί με τρόπο που να διασφαλίζει ότι δεν επηρεάζονται οι σχετικές υπηρεσίες ή διεπαφές. Όλες οι πληροφορίες που σχετίζονται με την ασφάλεια πρέπει να ακυρώνονται ώστε να διασφαλίζεται ότι τα συστήματα με τα οποία διασυνδέονται ή σχετίζονται δεν τίθενται σε κίνδυνο.

- Συνέπεια: Η προσέγγιση για τη διαχείριση των κινδύνων εφαρμόζεται σε ολόκληρο τον κυβερνοχώρο. Στο πλαίσιο αυτής της προσέγγισης ή μεθοδολογίας, στους καταναλωτές και τους παρόχους του Κυβερνοχώρου ανατίθενται ευθύνες για συγκεκριμένες δραστηριότητες, όπως ο σχεδιασμός έκτακτης ανάγκης, η ανάκαμψη από καταστροφές και η ανάπτυξη και εφαρμογή προστατευτικών προγραμμάτων για τα συστήματα που βρίσκονται υπό τον έλεγχο ή/και την ιδιοκτησία τους.

Σε γενικές γραμμές, η μεθοδολογία διαχείρισης κινδύνων του ISO/IEC27005 καλύπτει ολόκληρο τον κύκλο ζωής ενός γενικού συστήματος, καθιστώντας την έτσι χρησιμοποιήσιμη για νέα συστήματα ασφαλείας καθώς και για υφιστάμενα συστήματα. Δεδομένου ότι ασχολείται με την αντιμετώπιση των συστημάτων, είναι εφαρμόσιμη σε όλα τα επιχειρηματικά μοντέλα. Οι διαδικασίες εντός του πλαισίου μπορούν να αντιμετωπίζουν τα δίκτυα και τις υπηρεσίες των παρόχων υπηρεσιών ως ένα ολοκληρωμένο σύστημα, αποτελούμενο από υποσυστήματα που παρέχουν δημόσιες υπηρεσίες και ιδιωτικά υποσυστήματα που υποστηρίζουν εσωτερικές υπηρεσίες, ή μπορεί να αντιμετωπίζει κάθε μία από τις επιμέρους υπηρεσίες (π.χ. φιλοξενία ιστοσελίδων) ξεχωριστά και να περιγράφει την παροχή τους με όρους ξεχωριστών αλληλοεπιδρώντων συστημάτων. Για λόγους απλότητας, μπορεί να είναι επωφελές να θεωρηθεί ότι όλα όσα απαιτούνται για την υποστήριξη των υπηρεσιών του παρόχου αποτελούν ένα μεγάλο σύστημα που μπορεί να αναλυθεί σε μικρότερα συστήματα, καθένα από τα οποία παρέχει μια εμπορεύσιμη υπηρεσία ή αποτελεί μέρος της υποδομής.

Σημαντικές πτυχές που πρέπει να θυμόμαστε όταν εξετάζουμε τους σκοπούς και τους στόχους της Κυβερνοασφάλειας είναι:

α) προστασία της συνολικής ασφάλειας του Κυβερνοχώρου,

β) σχεδιασμός για καταστάσεις έκτακτης ανάγκης και κρίσεων μέσω της συμμετοχής σε ασκήσεις και επικαιροποίηση των σχεδίων αντιμετώπισης και των σχεδίων για τη συνέχιση των επιχειρήσεων,

γ) εκπαίδευση των ενδιαφερομένων για την Κυβερνοασφάλεια και τις πρακτικές διαχείρισης κινδύνων,

δ) διασφάλιση της έγκαιρης, συναφούς και ακριβούς ανταλλαγής πληροφοριών σχετικά με απειλές μεταξύ των κοινοτήτων επιβολής του νόμου και των υπηρεσιών πληροφοριών και των βασικών φορέων λήψης αποφάσεων που σχετίζονται με τον Κυβερνοχώρο- και

ε) καθιέρωση αποτελεσματικών διατομεακών και διακρατικών μηχανισμών συντονισμού για την αντιμετώπιση κρίσιμων αλληλεξαρτήσεων, συμπεριλαμβανομένης της επίγνωσης της κατάστασης του συμβάντος και της διαχείρισης συμβάντων μεταξύ τομέων και φορέων.

Οι στόχοι και οι επιδιώξεις α) έως γ) απευθύνονται άμεσα στους παρόχους υπηρεσιών, οι οποίοι είναι υπεύθυνοι για τον εξοπλισμό και τις υπηρεσίες που βρίσκονται υπό τον έλεγχό τους. Για τους στόχους δ) και ε), οι πάροχοι υπηρεσιών συμμετέχουν ενεργά στις δραστηριότητες ανταλλαγής πληροφοριών και συντονισμού.

Οι συγκεκριμένοι στόχοι του παρόχου υπηρεσιών, όπως οι υπηρεσίες που πρέπει να παρέχονται, απορρέουν από το επιχειρηματικό πλαίσιο.

11.3 Κατευθυντήριες γραμμές για τους καταναλωτές

Το παρόν Διεθνές Πρότυπο δεν απευθύνεται ειδικά σε άτομα του Κυβερνοχώρου, αλλά επικεντρώνεται σε οργανισμούς που παρέχουν υπηρεσίες σε καταναλωτές, καθώς και σε οργανισμούς που απαιτούν από τους υπαλλήλους τους ή τους τελικούς χρήστες να ασκούν ασφαλή χρήση του Κυβερνοχώρου για την αποτελεσματική διαχείριση του κινδύνου Κυβερνοασφάλειας. Η καθοδήγηση σχετικά με τους ρόλους και την ασφάλεια των χρηστών στον Κυβερνοχώρο και τον τρόπο με τον οποίο θα μπορούσαν να επηρεάσουν θετικά την κατάσταση της Κυβερνοασφάλειας έχει ως στόχο να χρησιμεύσει ως οδηγός για τον σχεδιασμό και την ανάπτυξη περιεχομένου από τους οργανισμούς αυτούς, στο πλαίσιο της παροχής των υπηρεσιών τους και των προγραμμάτων ευαισθητοποίησης και κατάρτισης για την παροχή στους τελικούς χρήστες τους.

Όπως περιγράφεται στην παράγραφο 10.2, οι καταναλωτές μπορούν να βλέπουν ή να συλλέγουν πληροφορίες, καθώς και να παρέχουν ορισμένες συγκεκριμένες πληροφορίες εντός του χώρου μιας εφαρμογής του Κυβερνοχώρου, ή οι πληροφορίες να είναι ανοικτές σε περιορισμένα μέλη ή ομάδες εντός του χώρου της εφαρμογής, ή στο ευρύ κοινό. Οι ενέργειες που αναλαμβάνουν οι καταναλωτές σε αυτούς τους ρόλους μπορεί να είναι παθητικές ή ενεργητικές και μπορούν να συμβάλουν άμεσα ή έμμεσα στην κατάσταση της Κυβερνοασφάλειας.

Για παράδειγμα, ως ΑΠΕ, εάν η παρεχόμενη εφαρμογή περιέχει ευπάθειες ασφαλείας, αυτές θα μπορούσαν να οδηγήσουν σε εκμετάλλευση από κυβερνοεγκληματίες που τις εκμεταλλεύονται ως δίαυλο για να προσεγγίσουν αθώους χρήστες της εφαρμογής. Ως χρήστες ιστολογίων ή άλλων μορφών συνεισφοράς περιεχομένου, μπορεί να λάβουν ένα αίτημα με τη μορφή αθώων ερωτήσεων σχετικά με το περιεχόμενό τους, στο οποίο μπορεί να αποκαλύψουν ακούσια περισσότερες προσωπικές ή εταιρικές πληροφορίες στο κοινό από τις επιθυμητές. Ως αγοραστής ή πωλητής, ένας καταναλωτής μπορεί να συμμετάσχει εν αγνοία του σε εγκληματικές συναλλαγές πώλησης κλεμμένων αγαθών ή σε δραστηριότητες νομιμοποίησης εσόδων από παράνομες δραστηριότητες. Κατά συνέπεια, όπως και στον φυσικό κόσμο, οι καταναλωτές πρέπει να είναι προσεκτικοί σε κάθε ρόλο που διαδραματίζουν στον Κυβερνοχώρο.

Σε γενικές γραμμές, οι καταναλωτές θα πρέπει να λαμβάνουν υπόψη τους τις ακόλουθες οδηγίες:

α) Να μαθαίνουν και να κατανοούν την πολιτική ασφάλειας και προστασίας προσωπικών δεδομένων του συγκεκριμένου ιστότοπου και της εφαρμογής, όπως δημοσιεύεται από τον πάροχο του ιστότοπου.

β) Να μαθαίνουν και να κατανοούν τους σχετικούς κινδύνους ασφάλειας και προστασίας της ιδιωτικής ζωής και να καθορίζουν τους κατάλληλους εφαρμοστέους ελέγχους. Να συμμετέχουν σε σχετικά διαδικτυακά φόρουμ συζητήσεων ή να ρωτούν κάποιον που γνωρίζει για τον ιστότοπο ή την εφαρμογή πριν παράσχουν προσωπικές ή οργανωτικές πληροφορίες ή πριν συμμετάσχουν και συνεισφέρουν πληροφορίες στη συζήτηση.

γ) Να καθιερώσουν και να εφαρμόσουν μια προσωπική πολιτική απορρήτου για την προστασία της ταυτότητας, καθορίζοντας τις κατηγορίες των διαθέσιμων προσωπικών πληροφοριών και τις αρχές ανταλλαγής που αφορούν τις πληροφορίες αυτές.

δ) Να διαχειρίζονται τη διαδικτυακή ταυτότητα. Να χρησιμοποιούν διαφορετικά στοιχεία προσδιορισμού ταυτότητας για διαφορετικές διαδικτυακές εφαρμογές και να ελαχιστοποιούν την κοινοποίηση προσωπικών πληροφοριών σε κάθε ιστότοπο ή εφαρμογή που ζητά τέτοιες πληροφορίες. Να καταχωρούν την ηλεκτρονική τους ταυτότητα σε δημοφιλείς ιστότοπους κοινωνικής δικτύωσης, ακόμη και αν ο λογαριασμός παραμένει αδρανής.

ΠΑΡΑΔΕΙΓΜΑ Η ενιαία καθολική σύνδεση είναι μια μορφή διαδικτυακής διαχείρισης ταυτότητας.

ε) Να αναφέρουν ύποπτα γεγονότα ή συναντήσεις στις αρμόδιες αρχές (βλ. παράρτημα Β ως παράδειγμα δημοσίως διαθέσιμου καταλόγου επαφών).

στ) Ως αγοραστής ή πωλητής, διαβάζουν και κατανοούν την ασφάλεια του ιστότοπου και την πολιτική απορρήτου της διαδικτυακής αγοράς και λαμβάνουν μέτρα για την επαλήθευση της γνησιότητας των εμπλεκόμενων ενδιαφερομένων μερών. Να μην κοινοποιούν προσωπικά δεδομένα, συμπεριλαμβανομένων των τραπεζικών πληροφοριών, εκτός εάν έχει διαπιστωθεί πραγματικό ενδιαφέρον για πώληση ή αγορά. Να χρησιμοποιούν έναν αξιόπιστο μηχανισμό πληρωμών.

ζ) Ως ΑΠΕ, να εφαρμόζουν πρακτική ασφαλούς ανάπτυξης λογισμικού και να παρέχουν μια τιμή κατακερματισμού του κώδικα στο διαδίκτυο, ώστε τα ενδιαφερόμενα μέρη που λαμβάνουν τον κώδικα να μπορούν να επαληθεύσουν την τιμή, εάν είναι απαραίτητο, για να διασφαλίσουν την ακεραιότητα του κώδικα. Να παρέχουν τεκμηρίωση των πολιτικών και πρακτικών ασφάλειας και προστασίας της ιδιωτικής ζωής του κώδικα και να σέβονται την ιδιωτική ζωή των χρηστών του κώδικα.

η) Ως χρήστης ιστολογίου ή άλλου περιεχομένου (συμπεριλαμβανομένων των συντηρητών ιστοτόπων), να διασφαλίζουν ότι η ιδιωτικότητα των σχετικών ενδιαφερομένων μερών και οι ευαίσθητες πληροφορίες δεν αποκαλύπτονται μέσω των ιστολογίων ή των διαδικτυακών δημοσιεύσεων. Να ελέγχουν τα σχόλια και τις δημοσιεύσεις που λαμβάνονται στον ιστότοπο και να διασφαλίζουν ότι δεν περιέχουν κακόβουλο περιεχόμενο, όπως συνδέσμους προς ιστότοπους ηλεκτρονικού "ψαρέματος" ή κακόβουλες λήψεις.

θ) Ως μέλος ενός οργανισμού, ο μεμονωμένος καταναλωτής θα πρέπει να μάθει και να κατανοήσει την εταιρική πολιτική ασφάλειας πληροφοριών του οργανισμού και να διασφαλίσει ότι οι διαβαθμισμένες ή/και ευαίσθητες πληροφορίες δε δημοσιοποιούνται σκόπιμα ή τυχαία σε οποιονδήποτε ιστότοπο στον Κυβερνοχώρο, εκτός εάν έχει χορηγηθεί επίσημα προηγούμενη άδεια για την εν λόγω δημοσιοποίηση.

ι) Άλλοι ρόλοι. Όταν ένας καταναλωτής επισκέπτεται έναν ιστότοπο που απαιτεί εξουσιοδότηση και αποκτά πρόσβαση χωρίς πρόθεση, ο χρήστης μπορεί να χαρακτηριστεί ως εισβολέας. Πρέπει να εξέλθει αμέσως από τον ιστότοπο και να το αναφέρει στην αρμόδια αρχή, καθώς το γεγονός ότι ήταν δυνατή η απόκτηση πρόσβασης μπορεί να αποτελεί ένδειξη παραβίασης.

11.4 Κατευθυντήριες γραμμές για οργανισμούς και παρόχους υπηρεσιών

11.4.1 Επισκόπηση

Οι έλεγχοι για τη διαχείριση των κινδύνων Κυβερνοασφάλειας εξαρτώνται σημαντικά από την ωριμότητα των διαδικασιών διαχείρισης της ασφάλειας εντός των οργανισμών (συμπεριλαμβανομένων των παρόχων υπηρεσιών). Ενώ οι κατευθυντήριες γραμμές που προτείνονται εδώ είναι κυρίως στη διακριτική ευχέρεια των οργανισμών, συνιστάται στους παρόχους υπηρεσιών να αντιμετωπίζουν τις κατευθυντήριες γραμμές ως βασικά υποχρεωτικά μέτρα.

Οι κατευθυντήριες γραμμές της παρούσας παραγράφου μπορούν να συνοψιστούν ως εξής:

- Διαχείριση του κινδύνου ασφάλειας πληροφοριών στην επιχείρηση.

- Συμμόρφωση με τις απαιτήσεις ασφάλειας για τη φιλοξενία διαδικτυακών και άλλων υπηρεσιών εφαρμογών στον Κυβερνοχώρο.

- Παροχή οδηγιών ασφάλειας στους καταναλωτές.

11.4.2 Διαχείριση του κινδύνου ασφάλειας πληροφοριών στην επιχείρηση

11.4.2.1 Σύστημα διαχείρισης ασφάλειας πληροφοριών

Σε επίπεδο επιχείρησης, οι οργανισμοί που συνδέονται με τον Κυβερνοχώρο θα πρέπει να εφαρμόζουν ένα σύστημα διαχείρισης της ασφάλειας των πληροφοριών (ΣΔΑΠ) για τον εντοπισμό και τη διαχείριση του σχετικού κινδύνου ασφάλειας των πληροφοριών για την επιχείρηση. Η σειρά διεθνών προτύπων ISO/IEC 27000 για τα συστήματα διαχείρισης της ασφάλειας των πληροφοριών παρέχει την απαιτούμενη καθοδήγηση και τις βέλτιστες πρακτικές για την εφαρμογή ενός τέτοιου συστήματος.

Μια βασική σκέψη κατά την εφαρμογή ενός ΣΔΑΠ είναι να διασφαλιστεί ότι ο οργανισμός διαθέτει ένα σύστημα για τον συνεχή εντοπισμό, την αξιολόγηση, την αντιμετώπιση και τη διαχείριση των κινδύνων ασφάλειας των πληροφοριών που σχετίζονται με τις δραστηριότητές του, συμπεριλαμβανομένης της παροχής υπηρεσιών στο Διαδίκτυο, απευθείας σε τελικούς χρήστες ή συνδρομητές, εφόσον πρόκειται για πάροχο υπηρεσιών.

ΣΗΜΕΙΩΣΗ 1 Το ISO/IEC 27005, Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Διαχείριση κινδύνων ασφάλειας πληροφοριών, παρέχει κατευθυντήριες γραμμές για τη διαχείριση κινδύνων ασφάλειας πληροφοριών σε έναν οργανισμό, υποστηρίζοντας ιδίως τις απαιτήσεις ενός ΣΔΑΠ σύμφωνα με το ISO/IEC 27001.

ΣΗΜΕΙΩΣΗ 2 Το ISO 31000, Διαχείριση κινδύνων - Αρχές και κατευθυντήριες γραμμές, παρέχει αρχές και γενικές κατευθυντήριες γραμμές για τη διαχείριση κινδύνων.

Οι οργανισμοί μπορούν επίσης να εξετάσουν το ενδεχόμενο επίσημης πιστοποίησης της συμμόρφωσής τους με τις απαιτήσεις ενός ΣΔΑΠ, όπως κατά ISO/IEC 27001.

Στο πλαίσιο της εφαρμογής ενός ΣΔΑΔ, ένας οργανισμός θα πρέπει επίσης να δημιουργήσει μια ικανότητα παρακολούθησης και αντιμετώπισης περιστατικών ασφαλείας και να συντονίσει τις

δραστηριότητες αντιμετώπισης περιστατικών με εξωτερικούς οργανισμούς ΟΑΠΥ, ΟΑΕΑΥ ή ΟΑΠΑΥ στη χώρα. Η πρόβλεψη αντιμετώπισης περιστατικών και έκτακτης ανάγκης θα πρέπει να περιλαμβάνει την παρακολούθηση και την αξιολόγηση της κατάστασης ασφαλείας της χρήσης των υπηρεσιών του οργανισμού από τους τελικούς χρήστες και τους πελάτες και να παρέχει καθοδήγηση για να βοηθήσει τα ενδιαφερόμενα μέρη να ανταποκριθούν αποτελεσματικά σε περιστατικά ασφαλείας.

ΣΗΜΕΙΩΣΗ Το ISO/IEC 27035, Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Διαχείριση περιστατικών ασφάλειας πληροφοριών, παρέχει καθοδήγηση σχετικά με τη διαχείριση περιστατικών ασφάλειας πληροφοριών.

11.4.2.2 Παροχή ασφαλών προϊόντων

Ορισμένοι οργανισμοί (είτε εσωτερικά είτε μέσω εξωτερικού παρόχου) αναπτύσσουν και κυκλοφορούν τις δικές τους γραμμές εργαλείων για τα προγράμματα περιήγησης ιστού, προγράμματα κλήσης ή κώδικα για την παροχή υπηρεσιών προστιθέμενης αξίας στους τελικούς χρήστες ή για τη διευκόλυνση της εύκολης πρόσβασης στις υπηρεσίες ή τις εφαρμογές του οργανισμού. Σε τέτοιες περιπτώσεις, θα πρέπει να υπάρχει κατάλληλη συμφωνία τελικού χρήστη σε κατάλληλη διατύπωση, η οποία να περιλαμβάνει δηλώσεις σχετικά με την πολιτική προγραμματισμού του οργανισμού, την πολιτική απορρήτου και τα μέσα με τα οποία οι χρήστες μπορούν να αλλάξουν την αποδοχή τους αργότερα ή να κλιμακώσουν τυχόν ζητήματα που μπορεί να έχουν σχετικά με την πολιτική και τις πρακτικές. Όταν χρησιμοποιείται μια τέτοια συμφωνία, θα πρέπει να εφαρμόζεται έλεγχος διαχείρισης των εκδόσεων και ο οργανισμός θα πρέπει να διασφαλίζει ότι οι τελικοί χρήστες την υπογράφουν με συνέπεια.

Όταν υπάρχει μεγάλος βαθμός εξάρτησης από την ασφάλεια των προϊόντων λογισμικού, αυτά θα πρέπει να επικυρώνονται ανεξάρτητα σύμφωνα με το καθεστώς Κοινών Κριτηρίων, όπως περιγράφεται στο ISO/IEC 15408.

Οι οργανισμοί θα πρέπει να τεκμηριώνουν τη συμπεριφορά του κώδικα και να αξιολογούν κατά πόσον η συμπεριφορά μπορεί να εμπίπτει σε πιθανές περιοχές που θα μπορούσαν να θεωρηθούν ως λογισμικό κατασκοπείας ή παραπλανητικό λογισμικό. Στην τελευταία περίπτωση, θα πρέπει να προσλάβουν έναν κατάλληλα καταρτισμένο αξιολογητή για να εκτιμήσει κατά πόσον ο κώδικας εμπίπτει στα αντικειμενικά κριτήρια των παρόχων αντικατασκοπείας τα οποία ακολουθούν τις βέλτιστες πρακτικές, έτσι ώστε τα εργαλεία λογισμικού που παρέχει ο οργανισμός στους τελικούς χρήστες να μη χαρακτηρίζονται ως λογισμικό κατασκοπείας ή λογισμικό διαφημίσεων από τους προμηθευτές αντι-κατασκοπευτικού λογισμικού. Πολλοί προμηθευτές αντι-κατασκοπευτικού λογισμικού δημοσιεύουν τα κριτήρια με τα οποία αξιολογούν το λογισμικό.

Οι οργανισμοί θα πρέπει να εφαρμόσουν ψηφιακή υπογραφή του κώδικα για τα εκτελέσιμα προγράμματά τους, έτσι ώστε οι προμηθευτές αντι-κακόβουλου και αντι-κατασκοπευτικού λογισμικού να μπορούν εύκολα να προσδιορίσουν τον ιδιοκτήτη ενός αρχείου, και οι ΑΠΛ, οι οποίοι παράγουν συστηματικά λογισμικό που ακολουθεί τις βέλτιστες πρακτικές, να κατηγοριοποιούνται ως πιθανώς ασφαλείς ακόμη και πριν από την ανάλυση.

Σε περίπτωση που ένας οργανισμός ανακαλύψει χρήσιμες τεχνικές λογισμικού που θα μπορούσαν να βοηθήσουν στη μείωση του προβλήματος των κατασκοπευτικών προγραμμάτων ή των κακόβουλων προγραμμάτων, ο οργανισμός θα πρέπει να εξετάσει το ενδεχόμενο σύμπραξης και συνεργασίας με τον προμηθευτή για την ευρεία διάθεσή τους.

Προκειμένου να ικανοποιηθούν αυτές οι απαιτήσεις, η εκπαίδευση των προγραμματιστών σε θέματα ασφάλειας είναι πολύ σημαντική. Θα πρέπει να χρησιμοποιείται ένας ασφαλής κύκλος ζωής ανάπτυξης λογισμικού, όπου οι ευπάθειες του λογισμικού μπορούν να ελαχιστοποιηθούν, παρέχοντας έτσι ένα ασφαλέστερο προϊόν λογισμικού.

ΣΗΜΕΙΩΣΗ Το ISO/IEC 27034, Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Ασφάλεια εφαρμογών, παρέχει κατευθυντήριες γραμμές για τον ορισμό, την ανάπτυξη, την υλοποίηση, τη διαχείριση, την υποστήριξη και την απόσυρση μιας εφαρμογής.

11.4.2.3 Παρακολούθηση και απόκριση δικτύου

Η παρακολούθηση του δικτύου εφαρμόζεται συνήθως από τους οργανισμούς για να διασφαλιστεί η αξιοπιστία και η ποιότητα των υπηρεσιών του δικτύου τους. Ταυτόχρονα, η δυνατότητα αυτή μπορεί να αξιοποιηθεί για την αναζήτηση εξαιρετικών συνθηκών δικτυακής κίνησης και την ανίχνευση κακόβουλων δραστηριοτήτων που εμφανίζονται στο δίκτυο. Σε γενικές γραμμές, οι οργανισμοί θα πρέπει να εκτελούν τα εξής:

- Να κατανοήσουν την κυκλοφορία στο δίκτυο - τι είναι φυσιολογικό, τι δεν είναι φυσιολογικό.

- Να χρησιμοποιούν ένα εργαλείο διαχείρισης δικτύου για τον εντοπισμό αιχμών στην κυκλοφορία, "ασυνήθιστης" κυκλοφορίας/θυρών και να διασφαλίζουν ότι υπάρχουν διαθέσιμα εργαλεία για τον εντοπισμό και την αντιμετώπιση της αιτίας.

- Να ελέγχουν την ικανότητα απόκρισης προτού χρειαστούν για ένα πραγματικό συμβάν. Να βελτιώνουν τις τεχνικές, τις διαδικασίες και τα εργαλεία απόκρισης με βάση τα αποτελέσματα των τακτικών ασκήσεων.

- Να κατανοούν τα συστατικά στοιχεία σε ατομική βάση - εάν κάποιος που συνήθως είναι ανενεργός χρήστης αρχίζει ξαφνικά να καλύπτει το 100 τοις εκατό του διαθέσιμου εύρους ζώνης, μπορεί να είναι απαραίτητο να απομονωθεί ο παραβάτης χρήστης μέχρι να βρεθεί ο λόγος. Η απομόνωση του δικτύου μπορεί να αποτρέψει την εξάπλωση κακόβουλου λογισμικού, αν και ορισμένες υλοποιήσεις μπορεί να απαιτούν τη συγκατάθεση του χρήστη ή ενημερώσεις των όρων χρήσης.

- Να εξετάσουν το ενδεχόμενο παρακολούθησης της δραστηριότητας από σημεία πληροφοριών στο δίκτυο, όπως φίλτρα του Συστήματος Ονοματοδοσίας του Διαδικτύου και φίλτρα μηνυμάτων, τα οποία μπορούν επίσης να εντοπίσουν συσκευές που έχουν προσβληθεί από κακόβουλο λογισμικό, αλλά, για διάφορους λόγους, δεν εντοπίζονται από υπηρεσίες προστασίας από ιούς ή από ΣΑΕ.

ΠΑΡΑΔΕΙΓΜΑ Λόγω του όγκου των πληροφοριών στο δίκτυο, εργαλεία όπως τα ΣΑΕ και τα ΣΠΕ μπορούν να χρησιμοποιηθούν για την παρακολούθηση εξαιρέσεων που αξίζει να αναφερθούν.

11.4.2.4 Υποστήριξη και κλιμάκωση

Οι επιχειρήσεις, συμπεριλαμβανομένων των παρόχων υπηρεσιών και των κυβερνητικών οργανισμών, διαθέτουν συνήθως μια υπηρεσία υποστήριξης για να απαντούν στα ερωτήματα των πελατών και να παρέχουν τεχνική βοήθεια και υποστήριξη για την αντιμετώπιση των προβλημάτων των τελικών χρηστών. Με την αυξανόμενη εξάπλωση των κακόβουλων λογισμικών στο Διαδίκτυο, ένας οργανισμός παροχής υπηρεσιών μπορεί να λαμβάνει αναφορές σχετικά με μολύνσεις από κακόβουλο λογισμικό και λογισμικό κατασκοπείας και άλλα θέματα ασφάλειας στον Κυβερνοχώρο. Τέτοιες πληροφορίες είναι σημαντικές και χρήσιμες για τους σχετικούς προμηθευτές ώστε να αξιολογούν τον κίνδυνο και την κατάσταση στον τομέα των κακόβουλων λογισμικών και να παρέχουν ενημερώσεις των απαραίτητων

εργαλείων για να διασφαλίσουν ότι κάθε νέο κακόβουλο λογισμικό ή λογισμικό κατασκοπείας που εντοπίζεται μπορεί να αφαιρεθεί ή να απενεργοποιηθεί αποτελεσματικά. Στο πλαίσιο αυτό, ένας οργανισμός θα πρέπει να έρθει σε επαφή με τους προμηθευτές ασφάλειας και να υποβάλει σχετικές αναφορές και δείγματα κακόβουλου λογισμικού για παρακολούθηση - ιδίως εάν φαίνεται να υπάρχει έξαρση της εξάπλωσης. Οι περισσότεροι προμηθευτές διατηρούν μια λίστα ηλεκτρονικού ταχυδρομείου για τη λήψη τέτοιων αναφορών ή δειγμάτων για ανάλυση και παρακολούθηση. Για παράδειγμα, βλ. πίνακα Β.1 στο παράρτημα Β.

11.4.2.5 Ενημέρωση για τις τελευταίες εξελίξεις

Στο πλαίσιο της εφαρμογής ενός ΣΔΑΠ για τη διαχείριση του επιχειρηματικού κινδύνου ασφάλειας πληροφοριών, καθώς και για να διασφαλιστεί ότι οι οργανισμοί συνεχίζουν να παρακολουθούν τις βέλτιστες πρακτικές του κλάδου και να παρακολουθούν τις τελευταίες ευπάθειες και εκμεταλλεύσεις/επιθέσεις, οι οργανισμοί θα πρέπει να συμμετέχουν σε σχετικές ομάδες της κοινότητας ή του κλάδου για να μοιράζονται τις βέλτιστες πρακτικές τους και να μαθαίνουν από άλλους ομόλογους παρόχους.

11.4.3 Απαιτήσεις ασφάλειας για τη φιλοξενία διαδικτυακών και άλλων υπηρεσιών εφαρμογών στον κυβερνοχώρο

Οι περισσότεροι πάροχοι υπηρεσιών παρέχουν υπηρεσίες φιλοξενίας στο δίκτυο και το κέντρο δεδομένων τους ως μέρος των επιχειρηματικών τους υπηρεσιών. Οι υπηρεσίες αυτές, οι οποίες περιλαμβάνουν ιστότοπους και άλλες διαδικτυακές εφαρμογές, συχνά αναδιαμορφώνονται και επαναπωλούνται από τους συνδρομητές φιλοξενίας σε άλλους καταναλωτές, όπως μικρές επιχειρήσεις και τελικούς χρήστες. Σε περίπτωση που οι συνδρομητές φιλοξενίας δημιουργήσουν έναν μη ασφαλή εξυπηρετητή ή φιλοξενήσουν κακόβουλο περιεχόμενο στους ιστότοπους ή τις εφαρμογές τους, η ασφάλεια των καταναλωτών θα επηρεαστεί αρνητικά. Ως εκ τούτου, είναι σημαντικό οι υπηρεσίες, τουλάχιστον, να πληρούν τα πρότυπα βέλτιστων πρακτικών συμμορφούμενες με την πολιτική ή τους όρους των συμφωνιών.

Όταν χρησιμοποιούνται πολλαπλοί πάροχοι, θα πρέπει να αναλύεται η αλληλεπίδραση μεταξύ των παρόχων και οι αντίστοιχες συμφωνίες παροχής υπηρεσιών θα πρέπει να αντιμετωπίζουν κάθε κρίσιμη αλληλεπίδραση. Για παράδειγμα, οι ενημερώσεις ή οι διορθώσεις στα συστήματα ενός παρόχου θα πρέπει να συντονίζονται με άλλους παρόχους, εάν η ενημέρωση μπορεί να έχει ως αποτέλεσμα αρνητική αλληλεπίδραση.

Οι όροι των συμφωνιών θα πρέπει να καλύπτουν τουλάχιστον τα εξής:

α) Σαφείς ειδοποιήσεις, που περιγράφουν τις πρακτικές ασφάλειας και προστασίας της ιδιωτικής ζωής του διαδικτυακού ιστότοπου ή της εφαρμογής, τις πρακτικές συλλογής δεδομένων και τη συμπεριφορά οποιουδήποτε κώδικα που μπορεί να διανέμει και να εκτελεί ο διαδικτυακός ιστότοπος ή η εφαρμογή σε υπολογιστές τελικού χρήστη ή σε περιβάλλοντα περιήγησης ιστού.

β) Συγκατάθεση χρήστη, που διευκολύνει τη συμφωνία ή τη διαφωνία του χρήστη με τους όρους των υπηρεσιών που περιγράφονται στις ανακοινώσεις. Αυτό θα επιτρέψει στον χρήστη να αποφασίσει ελεύθερα και να καθορίσει αν δύναται να αποδεχτεί τους όρους των υπηρεσιών αντίστοιχα.

γ) Έλεγχος χρήστη, που διευκολύνει τους χρήστες να αλλάξουν τις ρυθμίσεις τους ή να τερματίσουν με άλλο τρόπο την αποδοχή τους οποιαδήποτε στιγμή στο μέλλον μετά την αρχική συμφωνία.

Οι όροι είναι σημαντικοί για να διασφαλιστεί ότι οι τελικοί χρήστες είναι ενήμεροι σχετικά με τη συμπεριφορά και τις πρακτικές του διαδικτυακού ιστότοπου ή της εφαρμογής, σε σχέση με το απόρρητο και την ασφάλεια των τελικών χρηστών. Οι όροι θα πρέπει να καταρτίζονται με τη βοήθεια επαγγελματία νομικού, ώστε να διασφαλίζεται ότι θα προστατεύουν επίσης τον πάροχο υπηρεσιών από ενδεχόμενες δικαστικές αγωγές των τελικών χρηστών, ως αποτέλεσμα συγκεκριμένων απωλειών ή ζημιών που προκλήθηκαν λόγω κακόβουλου περιεχομένου ή ασαφών πολιτικών και πρακτικών στον ιστότοπο.

Εκτός από τις διατάξεις περί προστασίας δεδομένων και προσωπικών δεδομένων στον διαδικτυακό ιστότοπο ή την εφαρμογή, οι πάροχοι υπηρεσιών θα πρέπει να απαιτούν από τους διαδικτυακούς ιστότοπους ή τις εφαρμογές που φιλοξενούνται στα δίκτυά τους να εφαρμόζουν ένα σύνολο ελέγχων ασφαλείας βέλτιστων πρακτικών σε επίπεδο εφαρμογής πριν να τεθούν σε λειτουργία. Αυτοί θα πρέπει να περιλαμβάνουν, μεταξύ άλλων, τα παραδείγματα που αναφέρονται στην παράγραφο 12.2.

Ως μέρος της υποδομής φιλοξενίας ενός παρόχου υπηρεσιών, οι εξυπηρετητές θα πρέπει να προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και από τη δυνατότητα φιλοξενίας κακόβουλου περιεχομένου. Βλέπε παράγραφο 12.3 για παραδείγματα ελέγχων.

Για να καταστεί δυνατή η επιβολή αυτών των ελέγχων ασφαλείας, ιδίως εκείνων που αφορούν την ασφάλεια του διαδικτυακού ιστότοπου και της εφαρμογής, οι πάροχοι υπηρεσιών θα πρέπει να εξετάσουν το ενδεχόμενο ενσωμάτωσης των εν λόγω διατάξεων στους όρους των συμφωνιών παροχής υπηρεσιών.

11.4.4 Οδηγίες ασφάλειας για τους καταναλωτές

Οι πάροχοι υπηρεσιών θα πρέπει να παρέχουν οδηγίες στους καταναλωτές για το πώς να παραμένουν ασφαλείς στο διαδίκτυο. Οι πάροχοι υπηρεσιών μπορούν είτε να δημιουργήσουν τις οδηγίες απευθείας, είτε να παραπέμψουν τους χρήστες σε διαθέσιμους ιστότοπους καθοδήγησης που θα μπορούσαν να παρέχουν το περιεχόμενο. Είναι κρίσιμης σημασίας η εκπαίδευση των τελικών χρηστών σχετικά με τον τρόπο με τον οποίο μπορούν να συμβάλουν σε ένα ασφαλές Διαδίκτυο με βάση τους πολλαπλούς ρόλους που μπορούν να διαδραματίσουν στον Κυβερνοχώρο, όπως περιγράφεται στην παράγραφο 7. Επιπλέον, οι τελικοί χρήστες θα πρέπει να συμβουλεύονται να λαμβάνουν απαραίτητους τεχνικούς ελέγχους ασφαλείας, στους οποίους οι πάροχοι υπηρεσιών θα μπορούσαν επίσης να διαδραματίσουν ενεργό ρόλο, όπως περιγράφεται στην παράγραφο 11.3. Παραδείγματα δραστηριοτήτων καθοδήγησης μπορεί να περιλαμβάνουν:

α) Περιοδικές (π.χ. μηνιαίες) ενημερωτικές επιστολές για την ασφάλεια, οι οποίες παρέχουν συμβουλές σχετικά με συγκεκριμένες τεχνικές ασφάλειας (π.χ. πώς να επιλέγετε έναν καλό κωδικό πρόσβασης)- ενημερώσεις σχετικά με τις τάσεις της ασφάλειας- και παροχή ειδοποιήσεων για διαδικτυακές εκπομπές ασφάλειας, άλλα βίντεο κατά παραγγελία, ηχητικές εκπομπές και πληροφορίες ασφάλειας που είναι διαθέσιμες από την διαδικτυακή πύλη του οργανισμού ή άλλους παρόχους περιεχομένου ασφάλειας.

β) Απευθείας μεταδόσεις εκπαιδευτικών βίντεο ή διαδικτυακών εκπομπών ασφαλείας κατά παραγγελία που καλύπτουν ποικίλα θέματα ασφαλείας για τη βελτίωση των πρακτικών και της ευαισθητοποίησης των τελικών χρηστών σε θέματα ασφαλείας.

γ) Ενσωμάτωση μιας στήλης ασφάλειας στα έντυπα ενημερωτικά δελτία του παρόχου υπηρεσιών τα οποία αποστέλλονται στις διευθύνσεις των κατοίκων ή των γραφείων των τελικών χρηστών για την επισήμανση βασικών γεγονότων ή περιεχομένων ασφαλείας.

δ) Ετήσια ή άλλα περιοδικά σεμινάρια ασφάλειας τελικών χρηστών ή περιοδικές εκθέσεις, ενδεχομένως σε συνεργασία με άλλους φορείς του κλάδου, προμηθευτές και κυβερνήσεις.

Οι πάροχοι υπηρεσιών που χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο ως τον κύριο τρόπο επικοινωνίας με τους τελικούς χρήστες θα πρέπει να το κάνουν με τρόπο που βοηθά τους τελικούς χρήστες να αντιστέκονται στις επιθέσεις κοινωνικής μηχανικής. Ειδικότερα, οι τελικοί χρήστες θα πρέπει να τους υπενθυμίζεται συστηματικά ότι τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου από τον πάροχο υπηρεσιών δεν θα ζητούν ποτέ

- προσωπικές πληροφορίες,

- ονόματα χρηστών,

- κωδικούς πρόσβασης και

- δε θα περιλαμβάνουν ποτέ συνδέσμους που σχετίζονται με την ασφάλεια και στους οποίους ο αναγνώστης θα πρέπει να επιλέξει να φορτώσει τον σύνδεσμο.

Όταν ένας πάροχος υπηρεσιών επιθυμεί ο χρήστης να μεταβεί στον ιστότοπό του για πληροφορίες, θα πρέπει να ενημερώνει τον χρήστη για τον τρόπο ασφαλούς σύνδεσης στην απαιτούμενη διεύθυνση του Ενιαίου Εντοπιστή Πόρων. Για παράδειγμα, μπορεί να ζητήσει από τον χρήστη να πληκτρολογήσει μια παρατιθέμενη διεύθυνση του Ενιαίου Εντοπιστή Πόρων στο πρόγραμμα περιήγησής του και να βεβαιωθεί ότι η παρατιθέμενη διεύθυνση του Ενιαίου Εντοπιστή Πόρων δεν περιέχει σύνδεσμο με δυνατότητα επιλογής φόρτωσης.

Στο πλαίσιο της εκπαίδευσης των χρηστών σε θέματα ασφάλειας και της καθοδήγησης κατά παραπλανητικού λογισμικού και λογισμικού κατασκοπείας, οι οργανισμοί και οι πάροχοι υπηρεσιών θα πρέπει να συμβουλεύουν τους τελικούς χρήστες τους σχετικά με τη χρήση κατάλληλων τεχνικών ελέγχων ασφαλείας για την προστασία των συστημάτων τους από γνωστά εκμεταλλεύσιμα συστήματα και επιθέσεις. Ως γενικός οδηγός, οι καταναλωτές θα πρέπει να ενθαρρύνονται να εφαρμόζουν τους ελέγχους της παραγράφου 12.4.

Στο παράρτημα Β παρατίθεται ενδεικτικός κατάλογος παραπομπών και διαδικτυακών πηγών που θα μπορούσαν να χρησιμοποιηθούν για την υποστήριξη της εφαρμογής των ανωτέρω συστάσεων.

12 Έλεγχοι Κυβερνοασφάλειας

12.1 Επισκόπηση

Αφού προσδιοριστούν οι κίνδυνοι για την ασφάλεια στον Κυβερνοχώρο και καταρτιστούν οι κατάλληλες κατευθυντήριες γραμμές, μπορούν να επιλεχθούν και να εφαρμοστούν οι έλεγχοι ασφάλειας στον Κυβερνοχώρο που μπορούν να διασφαλίσουν τις απαιτήσεις ασφάλειας. Η παρούσα ενότητα παρέχει

μια επισκόπηση των βασικών ελέγχων Κυβερνοασφάλειας που μπορούν να εφαρμοστούν για την υποστήριξη των κατευθυντήριων γραμμών που ορίζονται στο παρόν Διεθνές Πρότυπο.

12.2 Έλεγχοι σε επίπεδο εφαρμογής

Οι έλεγχοι σε επίπεδο εφαρμογής περιλαμβάνουν τα εξής:

α) Εμφάνιση σύντομων ανακοινώσεων, οι οποίες παρέχουν σαφείς, συνοπτικές περιλήψεις μιας σελίδας (με απλή γλώσσα) των βασικών διαδικτυακών πολιτικών της εταιρείας. Με αυτό, οι χρήστες είναι σε θέση να κάνουν πιο ενημερωμένες επιλογές σχετικά με την κοινοποίηση των πληροφοριών τους στο διαδίκτυο. Οι σύντομες ανακοινώσεις θα πρέπει να συμμορφώνονται με όλες τις κανονιστικές απαιτήσεις και να παρέχουν συνδέσμους προς τις πλήρεις νομικές δηλώσεις και άλλες σχετικές πληροφορίες, ώστε οι πελάτες που επιθυμούν περισσότερες λεπτομέρειες να μπορούν εύκολα να επιλέξουν να διαβάσουν τη μεγαλύτερη έκδοση. Με μια ενιαία ειδοποίηση, οι πελάτες μπορούν να έχουν μια πιο συνεκτική εμπειρία για όλες τις εταιρικές ιδιότητες, ενώ τα ίδια πρότυπα και οι ίδιες προσδοκίες απορρήτου θα επεκτείνονται σε πολλούς δικτυακούς τόπους.

β) Ασφαλής χειρισμός των συνεδριών για εφαρμογές ιστού- αυτό μπορεί να περιλαμβάνει διαδικτυακούς μηχανισμούς όπως τα cookies.

γ) Ασφαλής επιβεβαίωση και χειρισμός δεδομένων εισόδου για την αποτροπή κοινών επιθέσεων. Με βάση το γεγονός ότι οι δικτυακοί τόποι, οι οποίοι γενικά θεωρούνται αξιόπιστοι, χρησιμοποιούνται όλο και περισσότερο για τη διανομή κακόβουλου κώδικα, η επικύρωση εισόδου και εξόδου πρέπει να πραγματοποιείται τόσο από ενεργό όσο και από δυναμικό περιεχόμενο.

δ) Δημιουργία ιστοσελίδων με χρήση ασφαλούς κώδικα για την αποτροπή κοινών επιθέσεων.

ε) Αναθεώρηση και δοκιμή ασφάλειας του κώδικα από κατάλληλα καταρτισμένους φορείς.

στ) Η υπηρεσία του οργανισμού, είτε παρέχεται από τον οργανισμό είτε από μέρος που εκπροσωπεί τον οργανισμό, θα πρέπει να παρέχεται με τρόπο ώστε ο καταναλωτής να μπορεί να αυθεντικοποιήσει την υπηρεσία. Αυτό μπορεί να περιλαμβάνει τη χρήση από τον πάροχο ενός υπο-τομέα από το εμπορικό όνομα του τομέα του οργανισμού και ενδεχομένως τη χρήση διαπιστευτηρίων του πρωτοκόλλου Μεταφοράς Υπερκειμένου που είναι καταχωρημένα στον οργανισμό. Η υπηρεσία θα πρέπει να αποφεύγει τη χρήση παραπλανητικών μεθόδων όπου ο καταναλωτής μπορεί να δυσκολευτεί να προσδιορίσει με ποιον έχει να κάνει.

12.3 Προστασία εξυπηρετητή

Οι ακόλουθοι έλεγχοι μπορούν να χρησιμοποιηθούν για την προστασία των εξυπηρετητών από μη εξουσιοδοτημένη πρόσβαση και τη φιλοξενία κακόβουλου περιεχομένου σε εξυπηρετητές:

α) Διαμόρφωση εξυπηρετητών, συμπεριλαμβανομένων των υποκείμενων λειτουργικών συστημάτων, σύμφωνα με έναν βασικό οδηγό διαμόρφωσης ασφαλείας. Ο οδηγός αυτός θα πρέπει να περιλαμβάνει τον κατάλληλο ορισμό των χρηστών του εξυπηρετητή έναντι των διαχειριστών, την επιβολή ελέγχων πρόσβασης σε καταλόγους και αρχεία προγραμμάτων και συστήματος και την ενεργοποίηση των ιχνών ελέγχου, ιδίως για συμβάντα ασφαλείας και άλλα συμβάντα αποτυχίας στο σύστημα. Επιπλέον, συνιστάται η εγκατάσταση του βασικού συστήματος σε έναν εξυπηρετητή, προκειμένου να μειωθεί ο παράγοντας επιθέσεων.

β) Δημιουργία ενός συστήματος για τη δοκιμή και την ανάπτυξη ενημερώσεων ασφαλείας και διασφάλιση της έγκαιρης ενημέρωσης του λειτουργικού συστήματος και των εφαρμογών του εξυπηρετητή όταν διατίθενται νέες ενημερώσεις ασφαλείας.

γ) Παρακολούθηση των επιδόσεων ασφαλείας του εξυπηρετητή μέσω τακτικών αξιολογήσεων των ιχνών ελέγχου.

δ) Επανεξέταση της διαμόρφωσης της ασφάλειας.

ε) Εκτέλεση ελέγχων κατά κακόβουλου λογισμικού (όπως προστασία από ιούς και λογισμικό κατασκοπείας) στον εξυπηρετητή.

στ) Σάρωση όλου του περιεχομένου που φιλοξενείται και μεταφορτώνεται τακτικά με τη χρήση ενημερωμένων ελέγχων κατά του κακόβουλου λογισμικού. Αναγνώριση ότι ένα αρχείο μπορεί, για παράδειγμα, να είναι λογισμικό κατασκοπείας ή κακόβουλο λογισμικό ακόμη και αν δεν ανιχνεύεται από τους τρέχοντες ελέγχους λόγω των περιορισμών ανεπαρκούς πληροφόρησης.

ζ) Πραγματοποίηση τακτικών αξιολογήσεων τρωτότητας και δοκιμών ασφαλείας για τους διαδικτυακούς ιστότοπους και τις εφαρμογές, ώστε να διασφαλίζεται ότι η ασφάλειά τους διατηρείται επαρκώς.

η) Πραγματοποίηση τακτικών σαρώσεων για παραβιάσεις.

12.4 Έλεγχοι τελικού χρήστη

Ακολουθεί ένας μη ολοκληρωμένος κατάλογος ελέγχων που μπορούν να χρησιμοποιήσουν οι τελικοί χρήστες για να προστατεύσουν τα συστήματά τους από γνωστές επιθέσεις:

α) Χρήση υποστηριζόμενων λειτουργικών συστημάτων, με εγκατεστημένες τις πιο ενημερωμένες εκδόσεις ασφαλείας. Οι καταναλωτές οργανισμών έχουν την ευθύνη να γνωρίζουν και να ακολουθούν την πολιτική του οργανισμού σχετικά με τα υποστηριζόμενα λειτουργικά συστήματα. Οι μεμονωμένοι καταναλωτές πρέπει να γνωρίζουν και να εξετάζουν τη χρήση των συνιστώμενων από τον πάροχο λειτουργικών συστημάτων. Σε κάθε περίπτωση, το λειτουργικό σύστημα θα πρέπει να είναι επικαιροποιημένο όσον αφορά τις ενημερώσεις ασφαλείας.

β) Χρήση των πιο πρόσφατων υποστηριζόμενων εφαρμογών λογισμικού, με εγκατεστημένες τις τελευταίες ενημερώσεις. Οι εταιρικοί καταναλωτές έχουν την ευθύνη να γνωρίζουν και να ακολουθούν την πολιτική του οργανισμού όσον αφορά το υποστηριζόμενο λογισμικό εφαρμογών. Οι μεμονωμένοι καταναλωτές πρέπει να γνωρίζουν και να εξετάζουν τη χρήση του λογισμικού εφαρμογών που συνιστάται από τον πάροχο. Σε κάθε περίπτωση, το λογισμικό εφαρμογών θα πρέπει να είναι επικαιροποιημένο όσον αφορά τις ενημερώσεις ασφαλείας.

γ) Χρήση εργαλείων κατά των ιών και των λογισμικών κατασκοπείας. Εάν είναι εφικτό, ένας πάροχος υπηρεσιών, όπως ένας πάροχος υπηρεσιών διαδικτύου, θα πρέπει να εξετάσει το ενδεχόμενο συνεργασίας με αξιόπιστους προμηθευτές ασφάλειας για να προσφέρει στους τελικούς χρήστες αυτά τα εργαλεία ως μέρος του πακέτου συνδρομής της υπηρεσίας, έτσι ώστε οι έλεγχοι ασφαλείας να είναι διαθέσιμοι κατά την εγγραφή της συνδρομής ή κατά την ανανέωση. Οι καταναλωτές οργανισμών έχουν την ευθύνη να γνωρίζουν και να ακολουθούν την πολιτική Οι μεμονωμένοι καταναλωτές πρέπει να χρησιμοποιούν εργαλεία λογισμικού ασφαλείας. Θα πρέπει να απευθύνονται στον πάροχο για οποιοδήποτε συνιστώμενο, παρεχόμενο ή διακοπτόμενο λογισμικό ασφαλείας. Σε κάθε περίπτωση, το

λογισμικό ασφαλείας θα πρέπει να επικαιροποιείται όσον αφορά τις ενημερώσεις ασφαλείας και τις βάσεις δεδομένων υπογραφών.

δ) Εφαρμόστε τα κατάλληλα μέτρα προστασίας κατά των ιών και των λογισμικών κατασκοπείας. Τα συνήθη προγράμματα περιήγησης στο διαδίκτυο και οι γραμμές εργαλείων τους έχουν πλέον ενσωματωμένες δυνατότητες, όπως οι λειτουργίες αποκλεισμού αναδυόμενων παραθύρων, οι οποίες θα αποτρέπουν την εμφάνιση παραθύρων από κακόβουλους ιστότοπους που περιέχουν λογισμικό κατασκοπείας ή παραπλανητικό λογισμικό, το οποίο θα μπορούσε να εκμεταλλευτεί αδυναμίες του συστήματος ή του προγράμματος περιήγησης ή να χρησιμοποιήσει κοινωνική μηχανική για να εξαπατήσει τους χρήστες ώστε να τα κατεβάσουν και να τα εγκαταστήσουν στο σύστημά τους. Οι οργανισμοί θα πρέπει να καθιερώσουν μια πολιτική που να επιτρέπει τη χρήση τέτοιων εργαλείων. Οι οργανισμοί που παρέχουν υπηρεσίες θα πρέπει να συγκεντρώνουν έναν κατάλογο συνιστώμενων εργαλείων και η χρήση τους θα πρέπει να προωθείται στους τελικούς χρήστες, με καθοδήγηση σχετικά με την ενεργοποίησή τους και με τη χορήγηση εξουσιοδότησης για ιστότοπους που οι χρήστες θα ήθελαν να επιτρέψουν.

ε) Ενεργοποίηση των αποκλειστών συγγραφής εντολών. Ενεργοποίηση του αποκλεισμού συγγραφής εντολών ή μιας υψηλότερης ρύθμισης ασφάλειας ιστού για να διασφαλιστεί ότι εντολές μόνο από αξιόπιστες πηγές εκτελούνται σε έναν τοπικό υπολογιστή.

στ) Χρησιμοποιήστε φίλτρα ηλεκτρονικού ψαρέματος. Τα κοινά προγράμματα περιήγησης στον ιστό και οι γραμμές εργαλείων του προγράμματος περιήγησης συχνά ενσωματώνουν αυτή τη δυνατότητα, η οποία θα μπορούσε να καθορίσει εάν ένας ιστότοπος που επισκέπτεται ένας χρήστης βρίσκεται σε μια βάση δεδομένων γνωστών ιστότοπων ηλεκτρονικού ψαρέματος ή εάν περιέχει μοτίβα σεναρίων που είναι παρόμοια με αυτά που συναντώνται σε τυπικούς ιστότοπους ηλεκτρονικού ψαρέματος. Το πρόγραμμα περιήγησης θα παρέχει ειδοποιήσεις, συνήθως με τη μορφή χρωματικών επισημάνσεων, για να προειδοποιήσει τους χρήστες για τον πιθανό κίνδυνο. Οι οργανισμοί θα πρέπει να καθιερώσουν μια πολιτική για να επιτρέπουν τη χρήση ενός τέτοιου εργαλείου.

ζ) Χρήση άλλων διαθέσιμων χαρακτηριστικών ασφαλείας του προγράμματος περιήγησης ιστού. Κατά καιρούς, καθώς αναδύονται νέοι κίνδυνοι Κυβερνοασφάλειας, τα προγράμματα περιήγησης στον ιστό και οι πάροχοι γραμμών εργαλείων περιήγησης προσθέτουν νέες δυνατότητες ασφαλείας για την προστασία των χρηστών από τους κινδύνους. Οι τελικοί χρήστες θα πρέπει να ενημερώνονται για τις εξελίξεις αυτές μαθαίνοντας για τις εν λόγω ενημερώσεις που συνήθως διατίθενται από τους παρόχους των εργαλείων. Οι οργανισμοί και οι πάροχοι υπηρεσιών θα πρέπει ομοίως να επανεξετάζουν αυτές τις νέες δυνατότητες και να ενημερώνουν τις σχετικές πολιτικές και υπηρεσίες ώστε να εξυπηρετούν καλύτερα τις ανάγκες των οργανισμών και των πελατών τους και να αντιμετωπίζουν τους σχετικούς κινδύνους Κυβερνοασφάλειας.

η) Ενεργοποίηση προσωπικού τείχους προστασίας και ΣΑΕΒΕΚΥ. Τα προσωπικά τείχη προστασίας και τα ΣΑΕΒΕΚΥ είναι σημαντικά εργαλεία για τον έλεγχο των υπηρεσιών δικτύου που έχουν πρόσβαση στα συστήματα των χρηστών. Ορισμένα νεότερα λειτουργικά συστήματα διαθέτουν ενσωματωμένα προσωπικά τείχη προστασίας και ΣΑΕΒΕΚΥ. Ενώ είναι ενεργοποιημένα από προεπιλογή, οι χρήστες ή οι εφαρμογές ενδέχεται να τα απενεργοποιήσουν, με αποτέλεσμα ανεπιθύμητες εκθέσεις της ασφάλειας του δικτύου. Οι οργανισμοί θα πρέπει να υιοθετήσουν μια πολιτική σχετικά με τη χρήση προσωπικού τείχους προστασίας και ΣΑΕΒΕΚΥ και να αξιολογήσουν κατάλληλα εργαλεία ή προϊόντα για εφαρμογή, ώστε η χρήση τους να είναι ενεργοποιημένη από προεπιλογή για όλους τους υπαλλήλους. Οι πάροχοι

υπηρεσιών θα πρέπει να ενθαρρύνουν τη χρήση προσωπικού τείχους προστασίας και λειτουργιών ΣΑΕΒΕΚΥ ή/και να προτείνουν άλλα προϊόντα προσωπικού τείχους προστασίας και ΣΑΕΒΕΚΥ τρίτων που έχουν αξιολογηθεί και θεωρηθεί αξιόπιστα, και να εκπαιδεύουν και να βοηθούν τους χρήστες στην ενεργοποίηση της βασικής ασφάλειας δικτύου σε επίπεδο συστήματος τελικού χρήστη.

θ) Ενεργοποίηση αυτοματοποιημένων ενημερώσεων. Ενώ οι παραπάνω τεχνικοί έλεγχοι ασφαλείας είναι ικανοί να αντιμετωπίσουν το μεγαλύτερο μέρος του κακόβουλου λογισμικού στα αντίστοιχα επίπεδα λειτουργίας τους, δεν είναι πολύ αποτελεσματικοί έναντι της εκμετάλλευσης των ευπαθειών που υπάρχουν στα λειτουργικά συστήματα και στα προϊόντα εφαρμογών. Για να αποτραπούν τέτοιες εκμεταλλεύσεις, η λειτουργία ενημέρωσης που διαθέτουν τα λειτουργικά συστήματα, καθώς και εκείνες που παρέχονται από εφαρμογές που εμπιστεύεται ο χρήστης (για παράδειγμα, αξιόπιστα αξιολογημένα προϊόντα προστασίας από προγράμματα κατασκοπείας και ιούς τρίτων κατασκευαστών), θα πρέπει να ενεργοποιούνται για την πραγματοποίηση αυτοματοποιημένων ενημερώσεων. Αυτό θα εξασφαλίσει ότι τα συστήματα θα ενημερώνονται με τις τελευταίες διορθώσεις ασφαλείας όποτε αυτές είναι διαθέσιμες, κλείνοντας το χρονικό κενό για την πραγματοποίηση εκμεταλλεύσεων.

12.5 Έλεγχοι κατά των επιθέσεων κοινωνικής μηχανικής

12.5.1 Επισκόπηση

Οι εγκληματίες του Κυβερνοχώρου καταφεύγουν όλο και περισσότερο σε τακτικές ψυχολογικής ή κοινωνικής μηχανικής προκειμένου να επιτύχουν.

ΠΑΡΑΔΕΙΓΜΑ 1 Η χρήση μηνυμάτων ηλεκτρονικού ταχυδρομείου με ΕΑΠ που κατευθύνουν ανυποψίαστους χρήστες σε ιστότοπους ηλεκτρονικού ψαρέματος.

ΠΑΡΑΔΕΙΓΜΑ 2 Μηνύματα απάτης που ζητούν από τους χρήστες να παράσχουν προσωπικά στοιχεία ταυτοποίησης ή πληροφορίες σχετικά με εταιρική πνευματική ιδιοκτησία.

Η εξάπλωση των ιστότοπων κοινωνικής δικτύωσης και των κοινοτήτων παρέχει νέα μέσα που καθιστούν ακόμη πιο πιστευτές τις μεθόδους εξαπάτησης και εκμετάλλευσης. Όλο και περισσότερο, οι επιθέσεις αυτές υπερβαίνουν επίσης την τεχνολογία, πέρα από τα συστήματα Η/Υ και την παραδοσιακή συνδεσιμότητα δικτύου, αξιοποιώντας κινητά τηλέφωνα, ασύρματα δίκτυα.

Με την παρούσα παράγραφο παρέχεται ένα πλαίσιο ελέγχων που εφαρμόζεται για τη διαχείριση και την ελαχιστοποίηση του κινδύνου Κυβερνοασφάλειας σε σχέση με τις επιθέσεις κοινωνικής μηχανικής. Η καθοδήγηση που παρέχεται με την παρούσα παράγραφο βασίζεται στην εκτίμηση ότι ο μόνος αποτελεσματικός τρόπος για τον μετριασμό της απειλής της κοινωνικής μηχανικής είναι ο συνδυασμός των εξής:

- τεχνολογιών ασφαλείας,

- πολιτικών ασφαλείας που θέτουν βασικούς κανόνες για την προσωπική συμπεριφορά, τόσο σε προσωπικό πλαίσιο, όσο και σε περιβάλλον εργασίας, και

- κατάλληλης εκπαίδευσης και κατάρτισης.

Συνεπώς, το πλαίσιο καλύπτει:

- πολιτικές,

- μεθόδους και διαδικασίες,

- ανθρώπους και οργανισμούς- και

- τους κατάλληλους τεχνικούς ελέγχους.

12.5.2 Πολιτικές

Σύμφωνα με τις κοινές πρακτικές για τη διαχείριση κινδύνων ασφάλειας πληροφοριών, θα πρέπει να καθορίζονται και να τεκμηριώνονται οι βασικές πολιτικές που διέπουν τη δημιουργία, τη συλλογή, την αποθήκευση, τη διαβίβαση, τον διαμοιρασμό, την επεξεργασία και τη γενική χρήση των πληροφοριών του οργανισμού και των προσωπικών πληροφοριών και της πνευματικής ιδιοκτησίας στο Διαδίκτυο και στον Κυβερνοχώρο. Ειδικότερα, αυτό αφορά εφαρμογές όπως άμεσης ανταλλαγής μηνυμάτων, ιστολογίων, κοινής χρήσης αρχείων μεταξύ ανθρώπων και κοινωνικής δικτύωσης, οι οποίες συνήθως δεν εμπίπτουν στο πεδίο εφαρμογής της ασφάλειας των δικτύων και των πληροφοριών των επιχειρήσεων.

Στο πλαίσιο των εταιρικών πολιτικών, θα πρέπει επίσης να περιλαμβάνονται δηλώσεις και κυρώσεις σχετικά με την κακή χρήση των εφαρμογών του Κυβερνοχώρου για την αποτροπή πρακτικών κακής χρήσης από υπαλλήλους και τρίτους στο εταιρικό δίκτυο ή στα συστήματα που έχουν πρόσβαση στον Κυβερνοχώρο.

Θα πρέπει να αναπτυχθούν και να ανακοινωθούν πολιτικές που προωθούν την ευαισθητοποίηση και την κατανόηση των κινδύνων της Κυβερνοασφάλειας και να ενθαρρύνουν, αν όχι να επιβάλλουν, την εκμάθηση και την ανάπτυξη δεξιοτήτων κατά των επιθέσεων της Κυβερνοασφάλειας, ιδίως των επιθέσεων κοινωνικής μηχανικής. Αυτό θα πρέπει να περιλαμβάνει απαιτήσεις για τακτική συμμετοχή σε τέτοιες ενημερώσεις και εκπαίδευση.

Με την προώθηση κατάλληλων πολιτικών και την ευαισθητοποίηση σχετικά με τους κινδύνους κοινωνικής μηχανικής, οι εργαζόμενοι δεν μπορούν πλέον να ισχυρίζονται ότι αγνοούν αυτούς τους κινδύνους και τις απαιτήσεις και ταυτόχρονα αναπτύσσουν κατανόηση των βέλτιστων πρακτικών και πολιτικών που αναμένονται από εξωτερικές εφαρμογές κοινωνικής δικτύωσης και άλλες εφαρμογές στον Κυβερνοχώρο, για παράδειγμα, τη συμφωνία με την πολιτική ασφάλειας του παρόχου υπηρεσιών.

12.5.3 Μέθοδοι και διαδικασίες

12.5.3.1 Κατηγοριοποίηση και διαβάθμιση των πληροφοριών

Για την υποστήριξη των πολιτικών που προωθούν την συνειδητοποίηση για και την προστασία των διαβαθμισμένων εταιρικών και των ευαίσθητων προσωπικών πληροφοριών, συμπεριλαμβανομένης της πνευματικής ιδιοκτησίας, θα πρέπει να εφαρμόζονται διαδικασίες διαβάθμισης και ταξινόμησης των πληροφοριών.

Για κάθε κατηγορία και διαβάθμιση των εμπλεκόμενων πληροφοριών, θα πρέπει να αναπτύσσονται και να τεκμηριώνονται ειδικοί έλεγχοι ασφαλείας για την προστασία από τυχαία έκθεση και από σκόπιμη μη εξουσιοδοτημένη πρόσβαση.

Οι χρήστες των οργανισμών θα μπορούν στη συνέχεια να διακρίνουν μεταξύ των διαφόρων κατηγοριών και διαβαθμίσεων των πληροφοριών που παράγουν, συλλέγουν και χειρίζονται. Οι χρήστες μπορούν στη συνέχεια να ασκήσουν την απαιτούμενη προσοχή και τα προστατευτικά μέτρα ελέγχου κατά τη χρήση του Κυβερνοχώρου.

Θα πρέπει επίσης να αναπτυχθούν και να δημοσιευθούν διαδικασίες σχετικά με τον τρόπο χειρισμού της πνευματικής ιδιοκτησίας της εταιρείας, των προσωπικών δεδομένων και άλλων εμπιστευτικών πληροφοριών.

12.5.3.2 Ευαισθητοποίηση και κατάρτιση

Η ευαισθητοποίηση σε θέματα ασφάλειας και η εκπαίδευση, συμπεριλαμβανομένης της τακτικής ενημέρωσης των σχετικών γνώσεων και της μάθησης, αποτελούν σημαντικό στοιχείο για την αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής.

Στο πλαίσιο του προγράμματος Κυβερνοασφάλειας ενός οργανισμού, οι εργαζόμενοι και οι συμβαλλόμενοι τρίτοι θα πρέπει να υποχρεούνται να υποβάλλονται σε έναν ελάχιστο αριθμό ωρών εκπαίδευσης ευαισθητοποίησης, προκειμένου να διασφαλιστεί ότι γνωρίζουν τους ρόλους και τις ευθύνες τους στον Κυβερνοχώρο, καθώς και τους τεχνικούς ελέγχους που πρέπει να εφαρμόζουν ως άτομα που χρησιμοποιούν τον Κυβερνοχώρο. Επιπλέον, στο πλαίσιο του προγράμματος για την αντιμετώπιση των επιθέσεων κοινωνικής μηχανικής, η εν λόγω εκπαίδευση ευαισθητοποίησης θα πρέπει να περιλαμβάνει περιεχόμενο όπως τα ακόλουθα:

α) Οι πιο πρόσφατες απειλές και μορφές επιθέσεων κοινωνικής μηχανικής, για παράδειγμα, πώς το ηλεκτρονικό ψάρεμα έχει εξελιχθεί από ψεύτικες ιστοσελίδες αποκλειστικά σε έναν συνδυασμό επιθέσεων.

β) Τον τρόπο με τον οποίο μπορούν να κλαπούν και να χειραγωγηθούν ατομικές και εταιρικές πληροφορίες μέσω επιθέσεων κοινωνικής μηχανικής, παρέχοντας κατανόηση για το πώς οι επιτιθέμενοι μπορούν να εκμεταλλευτούν την ανθρώπινη φύση, όπως η τάση συμμόρφωσης με αιτήματα που φαίνεται ότι διατυπώνονται με εξουσιοδότηση (ακόμη και αν αυτή μπορεί να μην είναι πραγματική), η φιλική συμπεριφορά, το να παριστάνουν το θύμα και το να ανταποδίδουν, δίνοντας πρώτα κάτι πολύτιμο ή βοηθητικό.

γ) Ποιες πληροφορίες πρέπει να προστατεύονται και πώς να προστατεύονται, σύμφωνα με την πολιτική ασφάλειας πληροφοριών.

δ) Πότε να αναφερθεί ή να κλιμακωθεί ένα ύποπτο συμβάν ή μια κακόβουλη εφαρμογή για να προσεγγιστούν οι αρχές ή ο οργανισμός αντιμετώπισης, καθώς και διαθέσιμες πληροφορίες σχετικά με αυτές τις επαφές. Για παράδειγμα, βλέπε παράρτημα Β.

Οι οργανισμοί που παρέχουν διαδικτυακές εφαρμογές και υπηρεσίες στον Κυβερνοχώρο θα πρέπει να παρέχουν στους συνδρομητές ή καταναλωτές ενημερωτικό υλικό που να καλύπτει τα παραπάνω περιεχόμενα στο πλαίσιο των εφαρμογών ή υπηρεσιών τους.

12.5.3.3 Δοκιμές ελέγχων

Οι εργαζόμενοι θα πρέπει να υπογράφουν βεβαίωση ότι αποδέχονται και κατανοούν το περιεχόμενο της πολιτικής ασφάλειας του οργανισμού. Στο πλαίσιο της διαδικασίας για τη βελτίωση της ευαισθητοποίησης και τη διασφάλιση της δέουσας προσοχής στον εν λόγω κίνδυνο, ένας οργανισμός θα πρέπει να εξετάζει το ενδεχόμενο διεξαγωγής περιοδικών δοκιμών για τον προσδιορισμό του επιπέδου ευαισθητοποίησης και συμμόρφωσης με τις σχετικές πολιτικές και πρακτικές. Οι εργαζόμενοι μπορούν να πραγματοποιήσουν μια γραπτή εξέταση ή να υποβληθούν σε ΕΜΥ για να διαπιστώσουν αν κατανοούν το περιεχόμενο της πολιτικής ασφάλειας του οργανισμού. Τέτοιες δοκιμές μπορεί να περιλαμβάνουν,

μεταξύ άλλων, τη δημιουργία στοχευμένων αλλά ελεγχόμενων ιστότοπων ηλεκτρονικού ψαρέματος, ανεπιθύμητων μηνυμάτων και μηνυμάτων απάτης με χρήση αληθοφανούς περιεχομένου κοινωνικής μηχανικής. Κατά τη διενέργεια τέτοιων δοκιμών, είναι σημαντικό να διασφαλίζεται ότι:

α) οι εξυπηρετητές δοκιμών και τα περιεχόμενα είναι όλα υπό τον έλεγχο και τη διοίκηση της ομάδας δοκιμών,

β) όπου είναι δυνατόν, χρησιμοποιούνται επαγγελματίες που έχουν προηγούμενη εμπειρία στην εκτέλεση μιας τέτοιας δοκιμής,

γ) οι χρήστες προετοιμάζονται για τέτοιου είδους δοκιμές μέσω των προγραμμάτων ευαισθητοποίησης και κατάρτισης- και

δ) όλα τα αποτελέσματα των δοκιμών παρουσιάζονται σε συγκεντρωτική μορφή, προκειμένου να προστατεύεται η ιδιωτική ζωή των ατόμων, καθώς το περιεχόμενο που παρουσιάζεται σε τέτοιες δοκιμές μπορεί να φέρει σε δύσκολη θέση τα άτομα και να προκαλέσει προβλήματα ιδιωτικής ζωής, εάν δε γίνει κατάλληλη διαχείριση.

ΣΗΜΕΙΩΣΗ: Πρέπει να λαμβάνονται υπόψη η δεοντολογία και η νομοθεσία κάθε χώρας.

12.5.4 Άνθρωποι και οργανισμός

Ενώ τα άτομα είναι οι πρωταρχικοί στόχοι των επιθέσεων κοινωνικής μηχανικής, ένας οργανισμός μπορεί επίσης να είναι το επιδιωκόμενο θύμα. Οι άνθρωποι, ωστόσο, παραμένουν το κύριο σημείο εισόδου για τις επιθέσεις κοινωνικής μηχανικής. Ως εκ τούτου, οι άνθρωποι πρέπει να είναι ενήμεροι για τους σχετικούς κινδύνους στον Κυβερνοχώρο και οι οργανισμοί πρέπει να θεσπίσουν σχετικές πολιτικές και να λάβουν προληπτικά μέτρα για τη χορηγία σχετικών προγραμμάτων ώστε να διασφαλίσουν την ευαισθητοποίηση και την ικανότητα των ανθρώπων.

Ως γενικός οδηγός, όλοι οι οργανισμοί (συμπεριλαμβανομένων των επιχειρήσεων, των παρόχων υπηρεσιών και της κυβέρνησης) θα πρέπει να ενθαρρύνουν τους καταναλωτές στον Κυβερνοχώρο να μάθουν και να κατανοήσουν τους κινδύνους κοινωνικής μηχανικής στον Κυβερνοχώρο, καθώς και τα βήματα που πρέπει να λάβουν για να προστατευθούν από πιθανές επιθέσεις.

12.5.5 Τεχνικά

Εκτός από την καθιέρωση πολιτικών και πρακτικών κατά των επιθέσεων κοινωνικής μηχανικής, θα πρέπει επίσης να εξεταστούν και, όπου είναι δυνατόν, να υιοθετηθούν τεχνικοί έλεγχοι για την ελαχιστοποίηση της έκθεσης και των δυνατοτήτων εκμετάλλευσης από τους κακοποιούς του κυβερνοχώρου.

Σε προσωπικό επίπεδο, οι χρήστες του Κυβερνοχώρου θα πρέπει να υιοθετήσουν τις οδηγίες που αναλύονται στην παράγραφο 11.3.

Οι οργανισμοί και οι πάροχοι υπηρεσιών θα πρέπει να αναλαμβάνουν τα σχετικά μέτρα που περιγράφονται στην παράγραφο 11.4.4 για να διευκολύνουν την υιοθέτηση και τη χρήση των τεχνικών μέτρων ασφάλειας από τους χρήστες.

Οι οργανισμοί και οι πάροχοι υπηρεσιών θα πρέπει επίσης να υιοθετήσουν τις οδηγίες που παρέχονται στην παράγραφο 11.4, οι οποίες είναι σημαντικές ως βασικά μέτρα ελέγχου κατά των επιθέσεων κοινωνικής μηχανικής στον Κυβερνοχώρο.

Επιπλέον, οι ακόλουθοι τεχνικοί έλεγχοι που είναι χρήσιμοι κατά συγκεκριμένων επιθέσεων κοινωνικής μηχανικής θα πρέπει να λαμβάνονται υπόψη:

α) Όταν σε διαδικτυακές εφαρμογές εμπλέκονται ευαίσθητες προσωπικές ή εταιρικές πληροφορίες, να εξετάζεται το ενδεχόμενο παροχής λύσεων ισχυρού ελέγχου ταυτότητας είτε ως μέρος του ελέγχου ταυτότητας σύνδεσης είτε/και κατά την εκτέλεση κρίσιμων συναλλαγών. Ο ισχυρός έλεγχος ταυτότητας αναφέρεται στη χρήση δύο ή περισσότερων πρόσθετων παραγόντων επαλήθευσης της ταυτότητας, πέραν της χρήσης του αναγνωριστικού χρήστη και του κωδικού πρόσβασης. Ο δεύτερος και οι πρόσθετοι παράγοντες μπορούν να παρέχονται με τη χρήση έξυπνων καρτών, βιομετρικών στοιχείων ή άλλων φορητών συσκευών ασφαλείας.

β) Για υπηρεσίες που βασίζονται στο διαδίκτυο, οι οργανισμοί θα πρέπει να εξετάζουν τη χρήση ενός "πιστοποιητικού υψηλής αξιοπιστίας" για την παροχή πρόσθετης αξιοπιστίας στους διαδικτυακούς χρήστες. Οι περισσότερες αρχές πιστοποίησης (ΑΠ) της αγοράς και οι φυλλομετρητές Διαδικτύου είναι σε θέση να υποστηρίξουν τη χρήση τέτοιων πιστοποιητικών, τα οποία μειώνουν την απειλή επιθέσεων ηλεκτρονικού ψαρέματος.

γ) Για να διασφαλιστεί η ασφάλεια των υπολογιστών των χρηστών που συνδέονται με τον ιστότοπο ή την εφαρμογή του οργανισμού ή του παρόχου υπηρεσιών στον Κυβερνοχώρο, θα πρέπει να εξεταστούν πρόσθετοι έλεγχοι για την εξασφάλιση ενός ελάχιστου επιπέδου ασφάλειας, όπως η εγκατάσταση των πιο πρόσφατων ενημερώσεων ασφαλείας. Η χρήση τέτοιων ελέγχων θα πρέπει να δημοσιεύεται στη Συμφωνία Υπηρεσιών Τελικού Χρήστη και/ή στην Πολιτική Απορρήτου και Ασφάλειας της Ιστοσελίδας, ανάλογα με την περίπτωση.

12.6 Ετοιμότητα Κυβερνοασφάλειας

Στο παράρτημα Α περιγράφονται πρόσθετα τεχνικά μέτρα ελέγχου που εφαρμόζονται για τη βελτίωση της ετοιμότητας Κυβερνοασφάλειας ενός οργανισμού στον τομέα της ανίχνευσης συμβάντων, της διερεύνησης και της αντιμετώπισης.

12.7 Άλλα μέτρα ελέγχου

Άλλα μέτρα ελέγχου μπορεί να περιλαμβάνουν ελέγχους που σχετίζονται με την ειδοποίηση και την απομόνωση συσκευών που εμπλέκονται σε ύποπτη δραστηριότητα, όπως προκύπτει από τη συσχέτιση συμβάντων από τον πάροχο υπηρεσιών ή/και από στοιχεία της επιχείρησης, όπως τους διακομιστές του συστήματος ονοματοδοσίας του διαδικτύου, τη ροή δικτύου των δρομολογητών, το φιλτράρισμα εξερχόμενων μηνυμάτων και τις ομότιμες επικοινωνίες.

13 Πλαίσιο ανταλλαγής πληροφοριών και συντονισμού

13.1 Γενικά

Τα περιστατικά Κυβερνοασφάλειας συχνά υπερβαίνουν τα εθνικά γεωγραφικά και οργανωτικά όρια και η ταχύτητα της ροής των πληροφοριών και των αλλαγών από το εξελισσόμενο περιστατικό συχνά δίνει

περιορισμένο χρόνο στα άτομα και τους οργανισμούς που αποκρίνονται να δράσουν. Θα πρέπει να δημιουργηθεί ένα σύστημα για την ανταλλαγή πληροφοριών και τον συντονισμό που θα συμβάλει στην προετοιμασία και την αντιμετώπιση συμβάντων και περιστατικών Κυβερνοασφάλειας. Αυτό είναι ένα σημαντικό βήμα που πρέπει να κάνουν οι οργανισμοί στο πλαίσιο των ελέγχων Κυβερνοασφάλειας. Ένα τέτοιο σύστημα ανταλλαγής και συντονισμού πληροφοριών θα πρέπει να είναι ασφαλές, αποτελεσματικό, αξιόπιστο και αποδοτικό.

Το σύστημα θα πρέπει να είναι ασφαλές ώστε να εξασφαλίζεται ότι οι πληροφορίες που ανταλλάσσονται, συμπεριλαμβανομένων των λεπτομερειών σχετικά με τον συντονισμό των δραστηριοτήτων, προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, ιδίως από τον δράστη του σχετικού περιστατικού. Η ασφάλεια των πληροφοριών που αφορούν συμβάντα Κυβερνοασφάλειας είναι επίσης απαραίτητη για να αποφευχθεί η παρερμηνεία και η πρόκληση αδικαιολόγητου πανικού ή συναγερμού στο κοινό. Ταυτόχρονα, η ακεραιότητα και η αυθεντικότητα των πληροφοριών είναι ζωτικής σημασίας για τη διασφάλιση της ακρίβειας και της αξιοπιστίας τους, ανεξάρτητα από το αν οι πληροφορίες αυτές μοιράζονται εντός μιας κλειστής ομάδας ή δημοσιοποιούνται. Το σύστημα θα πρέπει να είναι αποτελεσματικό και αποδοτικό, ώστε να εξυπηρετεί τον σκοπό του με ελάχιστους πόρους και εντός του απαιτούμενου χρόνου και χώρου.

Η παρούσα παράγραφος παρέχει ένα βασικό πλαίσιο για την εφαρμογή ενός συστήματος ανταλλαγής πληροφοριών και συντονισμού. Το πλαίσιο περιλαμβάνει τέσσερις τομείς προς εξέταση, δηλαδή πολιτικές, μεθόδους και διαδικασίες, ανθρώπους και τεχνικά στοιχεία.

ΣΗΜΕΙΩΣΗ Η ομάδα εργασίας 17 του Τομέα Τυποποίησης Τηλεπικοινωνιών της Διεθνούς Ένωσης Τηλεπικοινωνιών αναλαμβάνει εκτεταμένες εργασίες για την ανταλλαγή πληροφοριών σχετικά με την Κυβερνοασφάλεια. Για περισσότερες πληροφορίες, ανατρέξτε στον πίνακα Γ.17 - Ανταλλαγή πληροφοριών για την Κυβερνοασφάλεια.

13.2 Πολιτικές

13.2.1 Οργανισμοί που παρέχουν πληροφορίες και οργανισμοί που λαμβάνουν πληροφορίες

Για τους σκοπούς του παρόντος πλαισίου, εισάγονται δύο τύποι οργανισμών ανταλλαγής πληροφοριών:

- ΟΠΠ, και

- ΟΛΠ.

Ως ΟΠΠ, οι βασικές πολιτικές όσον αφορά την ταξινόμηση και την κατηγοριοποίηση των πληροφοριών, τη σοβαρότητα των συμβάντων και των περιστατικών, καθώς και τη μορφή της δυνατής ανταλλαγής θα πρέπει να καθορίζονται πριν από την εμφάνιση οποιουδήποτε περιστατικού Κυβερνοασφάλειας ή πριν από την πραγματοποίηση οποιασδήποτε ανταλλαγής (στην περίπτωση που ένας ΟΠΠ μετατρέπεται σε ΟΛΠ για να μοιραστεί τις ληφθείσες πληροφορίες με άλλες εξουσιοδοτημένες οντότητες στην αλυσίδα πληροφοριών).

Στο τέλος της παραλαβής, ο ΟΠΠ θα πρέπει να συμφωνήσει να επιβάλει προστασία της ασφάλειας και τις σχετικές διαδικασίες κατά τη λήψη πληροφοριών από τον ΟΛΠ, σύμφωνα με τη συμφωνία που έχει επιτευχθεί προηγουμένως και με βάση τη διαβάθμιση και την κατηγοριοποίηση των σχετικών πληροφοριών.

13.2.2 Διαβάθμιση και κατηγοριοποίηση των πληροφοριών

Οι ΟΠΠ θα πρέπει να καθορίσουν τις διάφορες κατηγορίες πληροφοριών που συλλέγουν, συγκεντρώνουν, φυλάσσουν και διανέμουν. Παραδείγματα κατηγοριών πληροφοριών μπορεί να περιλαμβάνουν συμβάντα ασφαλείας, απειλές ασφαλείας, τρωτά σημεία ασφαλείας, προφίλ υπόπτων/επιβεβαιωμένων δραστών, οργανωμένες ομάδες, πληροφορίες για τα θύματα και κατηγορίες προφίλ συστημάτων ΤΠΕ.

Κάθε κατηγορία θα πρέπει να αναλύεται περαιτέρω σε δύο ή περισσότερες ταξινομήσεις με βάση το περιεχόμενο των σχετικών πληροφοριών. Η ελάχιστη διαβάθμιση μπορεί να περιλαμβάνει την ευαίσθητη και την ελεύθερη. Εάν οι πληροφορίες περιέχουν προσωπικά δεδομένα, μπορούν επίσης να εφαρμοστούν ταξινομήσεις για την προστασία της ιδιωτικής ζωής.

13.2.3 Ελαχιστοποίηση πληροφοριών

Για κάθε κατηγορία και ταξινόμηση, ο ΟΠΠ θα πρέπει να επιδεικνύει προσοχή για την ελαχιστοποίηση των πληροφοριών που πρέπει να διανεμηθούν. Η ελαχιστοποίηση είναι απαραίτητη για να αποφευχθεί η υπερφόρτωση πληροφοριών στην πλευρά του αποδέκτη, για να εξασφαλιστεί η αποδοτική χρήση του συστήματος διαμοιρασμού, χωρίς να διακυβεύεται η αποτελεσματικότητα. Ένας άλλος στόχος της ελαχιστοποίησης είναι η παράλειψη των ευαίσθητων πληροφοριών για τη διατήρηση της ιδιωτικής ζωής των ατόμων των ΟΠΠ και των ΟΛΠ. Από αυτή την άποψη, οι ΟΠΠ και ΟΛΠ θα πρέπει να καθορίσουν το επιθυμητό επίπεδο λεπτομερειών, όπου είναι δυνατόν, για κάθε κατηγορία και τη διαβάθμιση των πληροφοριών που μπορούν να εντοπιστούν πριν από την πραγματική κοινοποίηση.

13.2.4 Περιορισμένοι αποδέκτες

Σύμφωνα με την αρχή της ελαχιστοποίησης, μια πολιτική για τον περιορισμό των αποδεκτών, οι οποίοι μπορεί να είναι συγκεκριμένες επαφές, ομάδες ή οργανισμοί, είναι απαραίτητη όταν κοινοποιούνται πληροφορίες που περιέχουν ιδιωτικά ή εμπιστευτικά δεδομένα. Για λιγότερο ευαίσθητες πληροφορίες, μια τέτοια πολιτική θα πρέπει να εξετάζεται για να αποφευχθεί η υπερφόρτωση πληροφοριών, εκτός εάν τα οφέλη της μέγιστης διανομής (όπως η κοινοποίηση κρίσιμων ειδοποιήσεων ασφαλείας) υπερτερούν των επιπτώσεων της υπερφόρτωσης πληροφοριών για τους ΟΛΠ.

13.2.5 Πρωτόκολλο συντονισμού

Θα πρέπει να θεσπιστεί μια υψηλού επιπέδου πολιτική για τον συντονισμό της αίτησης και της διανομής (είτε είναι με πρωτοβουλία του ΟΠΠ είτε με πρωτοβουλία του ΟΛΠ). Μια τέτοια πολιτική επισημοποιεί ένα σχετικό πρωτόκολλο, το οποίο παρέχει ένα μέσο για την αποτελεσματική και αποδοτική ανταπόκριση των ΟΠΠ και των ΟΛΠ. Οι διαδικασίες αμοιβαίας αυθεντικοποίησης και επαλήθευσης θα μπορούσαν στη συνέχεια να βασιστούν σε ένα τέτοιο πρωτόκολλο για να διασφαλιστεί η γνησιότητα της προέλευσης και η απόδειξη της παράδοσης, όπου αυτό είναι επιθυμητό, ιδίως για ευαίσθητες, προσωπικές ή/και εμπιστευτικές πληροφορίες.

13.3 Μέθοδοι και διαδικασίες

13.3.1 Επισκόπηση

Για την εφαρμογή των πολιτικών ανταλλαγής πληροφοριών και τη διασφάλιση της συνέπειας της εφαρμογής, της αποτελεσματικότητας, της αποδοτικότητας και της αξιοπιστίας της εκτέλεσης, θα πρέπει να αναπτυχθούν και να εφαρμοστούν σχετικές μέθοδοι και διαδικασίες. Οι εν λόγω μέθοδοι και διαδικασίες θα πρέπει να βασίζονται σε διαθέσιμα πρότυπα. Διαφορετικά, κατόπιν επικύρωσης από

επιχείρησης, μπορούν να οριστικοποιηθούν για τυποποίηση. Οι ακόλουθες παράγραφοι παρέχουν καθοδήγηση σχετικά με τις μεθόδους και τις διαδικασίες που χρησιμοποιούνται συνήθως από οργανισμούς του κλάδου για την επίτευξη των σχετικών στόχων και πολιτικών ανταλλαγής και συντονισμού πληροφοριών στο πλαίσιο της Κυβερνοασφάλειας.

13.3.2 Διαβάθμιση και κατηγοριοποίηση των πληροφοριών

Οι πληροφορίες που θα κοινοποιούνται θα προέρχονται τόσο από ανοιχτές όσο και από κλειστές πηγές. Οι ανοιχτές πληροφορίες συχνά βρίσκονται στο διαδίκτυο ή σε άλλες δημόσιες πηγές, όπως οι εφημερίδες. Οι πληροφορίες από ανοιχτές πηγές είναι γενικά χαμηλότερης διαβάθμισης, επειδή οι συντάκτες των πληροφοριών μπορεί να είναι πολλαπλοί ή άγνωστοι, η ηλικία των πληροφοριών μπορεί να είναι απροσδιόριστη και η ακρίβειά τους υπόκειται σε αμφισβήτηση. Οι κλειστές πληροφορίες δεν είναι διαθέσιμες στο κοινό, συχνά αποδίδονται σε μια πηγή και έχουν γνωστή ηλικία. Παραδείγματα πληροφοριών κλειστής πηγής είναι η ιδιόκτητη έρευνα και ανάλυση ή οι εμπειρικά συλλεγμένες πληροφορίες.

ΣΗΜΕΙΩΣΗ Η καθοδήγηση για αυτή την παράγραφο μπορεί να βασίζεται στο αποτέλεσμα της Περιόδου Μελέτης για το θέμα αυτό, με αναφορά στο πρότυπο, εάν η ΠΜ προχωρήσει στην ανάπτυξη, ή με την υιοθέτηση μιας περίληψης του κειμένου από την ΠΜ, εάν αυτή τερματιστεί χωρίς περαιτέρω ανάπτυξη.

13.3.3 Συμφωνία εμπιστευτικότητας

Μια ΣΕ μπορεί να χρησιμοποιηθεί για τουλάχιστον δύο σκοπούς στο πλαίσιο της ανταλλαγής πληροφοριών και του συντονισμού για τη βελτίωση της ασφάλειας στον κυβερνοχώρο. Η τυπική χρησιμότητα μιας ΣΕ είναι η διασφάλιση του κατάλληλου χειρισμού και της προστασίας των ευαίσθητων, προσωπικών ή/και εμπιστευτικών πληροφοριών που μοιράζονται μεταξύ ΟΠΠ και ΟΛΠ, καθώς και ο προκαθορισμός των όρων της ανταλλαγής και της περαιτέρω διανομής και χρήσης των εν λόγω πληροφοριών.

Στο πλαίσιο της αντιμετώπισης συμβάντων Κυβερνοασφάλειας, η εκ των προτέρων σύναψη μιας ΣΕ επιτρέπει την ταχεία ανταλλαγή και διανομή μεταξύ εξουσιοδοτημένων οντοτήτων με αποτελεσματικό τρόπο, ακόμη και αν δεν έχει καθοριστεί σαφώς η διαβάθμιση των πληροφοριών.

13.3.4 Κώδικας ορθής πρακτικής

Μια ευρέως χρησιμοποιούμενη μέθοδος για τη διασφάλιση της επαρκούς ανταλλαγής και του χειρισμού των ευαίσθητων πληροφοριών είναι η θέσπιση ενός κώδικα πρακτικής, ο οποίος καλύπτει λεπτομερείς διαδικασίες, αρμοδιότητες και δεσμεύσεις από τους ενδιαφερόμενους οργανισμούς (π.χ. ΟΠΠ και ΟΠΛ) για τις αποκρίσεις και τις ενέργειες που πρέπει να γίνουν από τις αντίστοιχες εμπλεκόμενες οντότητες για κάθε κατηγορία και διαβάθμιση πληροφοριών.

ΠΑΡΑΔΕΙΓΜΑ Βλέπε το μελλοντικό διεθνές πρότυπο ISO/IEC 29147, Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Αποκάλυψη ευπαθειών.

13.3.5 Δοκιμές και ασκήσεις

Για να διασφαλιστεί η αποτελεσματικότητα και η αξιοπιστία και να επιτευχθεί το επιθυμητό επίπεδο αποδοτικότητας, θα πρέπει να αναπτυχθούν μέθοδοι και διαδικασίες για τη διεξαγωγή τακτικών δοκιμών και ασκήσεων σεναρίων.

Μια τυποποιημένη μεθοδολογία θα πρέπει να χρησιμοποιείται ως σημείο αναφοράς για τις δοκιμές ασφαλείας, προκειμένου να προσαρμόζεται και να ταιριάζει με τους στόχους και τις ανάγκες του οργανισμού.

Δοκιμές ασφαλείας μπορούν να εκτελεστούν σε περιουσιακά στοιχεία υψηλού κινδύνου. Αυτό μπορεί να υποβοηθηθεί με τη χρήση της ονοματολογίας διαβάθμισης των δεδομένων του οργανισμού.

Αξιολογήσεις ασφαλείας θα πρέπει να διενεργούνται σε τακτική βάση στις:

- Εφαρμογές

- Λειτουργικά συστήματα

- Συστήματα διαχείρισης βάσεων δεδομένων

13.3.6 Χρονοδιάγραμμα και προγραμματισμός της ανταλλαγής πληροφοριών

Η απαίτηση ανταλλαγής πληροφοριών είτε προληπτικά είτε κατά τη διάρκεια της αντιμετώπισης ενός συμβάντος θα διαφέρει από οντότητα σε οντότητα. Ορισμένοι οργανισμοί θα έχουν ανάγκη για πληροφόρηση σε πραγματικό χρόνο: τη στιγμή που θα εμφανιστεί μια ειδοποίηση ή ένας συναγερμός θα θέλουν τις πληροφορίες για περαιτέρω ανάλυση. Άλλες οντότητες δε διαθέτουν τους πόρους για να διαχειριστούν την ανταλλαγή πληροφοριών σε πραγματικό χρόνο. Στην πραγματικότητα, πολλοί οργανισμοί μπορεί να μην έχουν τη δυνατότητα να διαχειριστούν τον προγραμματισμό της ανταλλαγής πληροφοριών σε οποιοδήποτε χρονικό διάστημα.

Τα χρονοδιαγράμματα και τα προγράμματα ανταλλαγής πληροφοριών θα πρέπει να καθορίζονται με σαφήνεια, με συγκεκριμένους στόχους επιπέδου υπηρεσιών για τις εθελοντικές σχέσεις και με συμφωνίες επιπέδου υπηρεσιών για τις εμπορικές σχέσεις.

13.4 Άνθρωποι και οργανισμοί

13.4.1 Επισκόπηση

Οι άνθρωποι και οι οργανισμοί είναι οι βασικοί παράγοντες που καθορίζουν την επιτυχία της Κυβερνοασφάλειας. Οι άνθρωποι αναφέρονται στα άτομα που εμπλέκονται στην εκτέλεση των μεθόδων και των διαδικασιών για την ανταλλαγή πληροφοριών και τον συντονισμό ώστε να υπάρξει θετική επίδραση στα αποτελέσματα των συμβάντων Κυβερνοασφάλειας. Οι οργανισμοί αναφέρονται είτε σε ομάδες ατόμων εντός μιας εταιρείας έως και σε ολόκληρη την εταιρεία που εμπλέκονται σε τέτοιες δραστηριότητες. Για την αποτελεσματικότητα και την αποδοτικότητα, πρέπει να λαμβάνονται υπόψη οι ανάγκες τόσο των ανθρώπων όσο και των οργανισμών.

13.4.2 Επαφές

Οι ΟΠΠ και οι ΟΠΛ θα πρέπει να καταρτίζουν κατάλογο επαφών και να ανταλλάσσουν αμοιβαία πληροφορίες, έτσι ώστε κάθε οντότητα να μπορεί να εντοπίζει το πρόσωπο που ζήτησε ή έστειλε πληροφορίες στην κοινότητα ανταλλαγής.

Μπορούν επίσης να αναπτυχθούν και να διαμοιραστούν πιο λεπτομερείς κατάλογοι επαφών σύμφωνα με τις πολιτικές περιορισμένων αποδεκτών (παράγραφος 13.2.4) και διαβάθμισης και κατηγοριοποίησης πληροφοριών (παράγραφος 13.2.2).

Ο κατάλογος επαφών δε θα πρέπει να περιέχει ευαίσθητες προσωπικές πληροφορίες, σύμφωνα με την πολιτική ελαχιστοποίησης των πληροφοριών (παράγραφος 13.2.3). Για λόγους προστασίας της ιδιωτικής ζωής, μπορεί επίσης να ληφθεί υπόψη ένα ψευδώνυμο στη θέση του πλήρους ονόματος. Οι ελάχιστες πληροφορίες για τον κατάλογο επαφών θα πρέπει να περιλαμβάνουν όνομα (ή ψευδώνυμο), αριθμούς επικοινωνίας (κινητό τηλέφωνο, αν είναι δυνατόν) και διεύθυνση ηλεκτρονικού ταχυδρομείου. Για κάθε βασικό πρόσωπο στον κατάλογο επαφών μπορεί επίσης να οριστεί μια εναλλακτική επαφή.

Εκτός από έναν κατάλογο επαφών για την ανταλλαγή πληροφοριών και τον συντονισμό, μπορεί επίσης να καταρτιστεί ένας ξεχωριστός κατάλογος επαφών για την κλιμάκωση περιστατικών, ώστε να διευκολύνεται η ταχεία κλιμάκωση. Ένας τέτοιος κατάλογος περιλαμβάνει συνήθως εξωτερικές επαφές που δεν ανήκουν στο δίκτυο ανταλλαγής. Για παράδειγμα, βλέπε παράρτημα Β.

Κατά ελάχιστο, ο κατάλογος επαφών θα πρέπει να προστατεύεται από μη εξουσιοδοτημένη τροποποίηση, ώστε να αποτρέπεται η αλλοίωση και να διατηρείται η ακεραιότητα. Θα πρέπει να εφαρμόζονται τεχνικοί έλεγχοι (παράγραφος 13.5) ανάλογα με την περίπτωση.

13.4.3 Συνασπισμοί

Για τη διευκόλυνση της ανταλλαγής πληροφοριών και την καθιέρωση κοινών και συνεπών πρακτικών που διέπονται από έναν συμφωνημένο κώδικα ορθής πρακτικής και/ή μια ΣΕ, οργανισμοί και ομάδες ατόμων μπορούν να σχηματίζουν συνασπισμούς με βάση τους τομείς ενδιαφέροντός τους, οι οποίοι μπορεί να είναι βιομηχανικοί, τεχνολογικοί ή άλλοι τομείς ειδικού ενδιαφέροντος. Βλέπε παράρτημα Β για έναν δειγματικό κατάλογο υφιστάμενων συνασπισμών και μη κερδοσκοπικών οργανώσεων που εξυπηρετούν έναν τέτοιο σκοπό.

13.4.4 Ενημέρωση και κατάρτιση

Τα άτομα στους οργανισμούς θα πρέπει να ευαισθητοποιούνται σχετικά με τους αναδυόμενους και νέους κινδύνους για την ασφάλεια στον Κυβερνοχώρο και να εκπαιδεύονται έτσι ώστε να αναπτύσσουν τις απαιτούμενες δεξιότητες και την τεχνογνωσία για να ανταποκρίνονται αποτελεσματικά και αποδοτικά όταν αντιμετωπίζουν συγκεκριμένους κινδύνους ή όταν λαμβάνουν πληροφορίες που απαιτούν τις ενέργειές τους για τον μετριασμό ή τη βελτίωση μιας δεδομένης κατάστασης. Για την επίτευξη αυτών των στόχων,

- Θα πρέπει να παρέχονται τακτικές ενημερώσεις σχετικά με την κατάσταση των κινδύνων κυβερνοασφάλειας και τα ευρήματα που αφορούν τον οργανισμό και τον κλάδο.

- Θα πρέπει να σχεδιάζονται, να οργανώνονται και να παραδίδονται εστιασμένες εκπαιδευτικές συνεδρίες με εικονικά σενάρια επίθεσης στον κυβερνοχώρο και συναντήσεις εργασίας σε συγκεκριμένους απαιτούμενους τομείς δράσης, τόσο για τους νεοεισερχόμενους στην ομάδα/οργανισμό, όσο και για ενημερώσεις σε τακτική βάση.

- Τακτικές δοκιμές, με περιήγηση στα σχετικά σενάρια, ώστε να διασφαλίζεται η πλήρης κατανόηση και η ικανότητα εκτέλεσης των διαδικασιών και των συγκεκριμένων εργαλείων.

Η εν λόγω ευαισθητοποίηση, κατάρτιση και δοκιμή μπορεί να πραγματοποιείται από εσωτερικούς εμπειρογνώμονες, εξωτερικούς συμβούλους ή άλλους εμπειρογνώμονες από μέλη των σχετικών συνασπισμών που συμμετέχουν στις προσπάθειες ανταλλαγής πληροφοριών και συντονισμού.

Η χρήση σεναρίων ως μέρος των διαδικασιών κατάρτισης και δοκιμών συνιστάται ανεπιφύλακτα, καθώς μια τέτοια προσέγγιση επιτρέπει στα άτομα να αποκτήσουν σχεδόν πραγματική εμπειρία των σχετικών καταστάσεων και να μάθουν και να εξασκηθούν στις απαιτούμενες αντιδράσεις. Επιπλέον, στο πλαίσιο των σεναρίων μπορούν να χρησιμοποιηθούν περιστατικά του παρελθόντος, ώστε να μεγιστοποιηθεί η ανταλλαγή διδαγμάτων και η κατανόηση που αποκτήθηκε από αυτές τις καταστάσεις.

13.5 Τεχνικά

13.5.1 Επισκόπηση

Οι τεχνικοί έλεγχοι και η τυποποίηση μπορούν να χρησιμοποιηθούν για τη βελτίωση της αποτελεσματικότητας, τη μείωση του ανθρώπινου λάθους και την ενίσχυση της ασφάλειας στις διαδικασίες ανταλλαγής και συντονισμού πληροφοριών. Μπορούν να σχεδιαστούν, να αναπτυχθούν και να εφαρμοστούν διάφορα τεχνικά συστήματα και λύσεις. Το παρόν Διεθνές Πρότυπο παρέχει ορισμένες από τις συνήθως χρησιμοποιούμενες προσεγγίσεις και τεχνικές που έχουν υιοθετηθεί από ορισμένους οργανισμούς και μπορούν να προσαρμοστούν περαιτέρω για τη βελτίωση των αναγκών και των διαδικασιών ανταλλαγής και συντονισμού πληροφοριών για την αντιμετώπιση του μεταβαλλόμενου περιβάλλοντος κινδύνων Κυβερνοασφάλειας.

13.5.2 Τυποποίηση δεδομένων για αυτοματοποιημένο σύστημα

Στο πλαίσιο του δικτύου ανταλλαγής, μπορούν να αναπτυχθούν και να εφαρμοστούν αυτοματοποιημένα συστήματα μεταξύ των οργανισμών συντονισμού για τη συλλογή δεδομένων σχετικά με τα εξελισσόμενα συμβάντα Κυβερνοασφάλειας για ανάλυση και αξιολόγηση σε πραγματικό χρόνο και εκτός σύνδεσης, προκειμένου να προσδιοριστεί η τελευταία κατάσταση της ασφάλειας στον Κυβερνοχώρο εντός των ορίων των εμπλεκόμενων οργανισμών. Τα δεδομένα αυτά μπορεί να περιλαμβάνουν δεδομένα κίνησης δικτύου, ενημερώσεις ασφαλείας για συστήματα λογισμικού και συσκευές υλισμικού, δεδομένα ευπαθειών ασφαλείας και δεδομένα κακόβουλου λογισμικού, ανεπιθύμητης αλληλογραφίας και κατασκοπευτικού λογισμικού, συμπεριλαμβανομένων των ωφέλιμων φορτίων τους και των πληροφοριών που έχουν υποκλαπεί. Τα αυτοματοποιημένα συστήματα που υποστηρίζουν τους πρώτους που ανταποκρίνονται και την κλιμάκωση των περιστατικών, όπως περιγράφεται στην παράγραφο 13.4.2, θα περιέχουν επίσης δεδομένα που αφορούν οργανισμούς και ανθρώπους. Λόγω της ευαισθησίας και του όγκου του περιεχομένου των δεδομένων που εμπλέκονται σε αυτά τα συστήματα, οι οργανισμοί (ιδίως οι συνασπισμοί οργανισμών) θα πρέπει να αξιολογήσουν τα σχήματα και το περιεχόμενο των δεδομένων για να καθορίσουν τους κατάλληλους τεχνικούς ελέγχους για τη βελτίωση της αποδοτικότητας, της αποτελεσματικότητας και της ασφάλειας. Αυτοί μπορεί να περιλαμβάνουν, μεταξύ άλλων, τα εξής:

α) την τυποποίηση του σχήματος των δεδομένων για κάθε κατηγορία και διαβάθμιση των δεδομένων που συλλέγονται με την επιβολή της πολιτικής ελαχιστοποίησης των πληροφοριών και της προστασίας της ιδιωτικής ζωής και με την παροχή τεχνικής διαβεβαίωσης σε όλους τους συμμετέχοντες φορείς, και τους κατόχους δεδομένων για μια τέτοια πρακτική,

β) την τυποποίηση του μορφότυπου των δεδομένων για τη διευκόλυνση της ανταλλαγής και τη βελτίωση της αποθήκευσης, της διαβίβασης, του χειρισμού και της διαλειτουργικότητας μεταξύ των συστημάτων, και

γ) την τυποποίηση των βασικών λειτουργιών επεξεργασίας δεδομένων και των αλγορίθμων που χρησιμοποιούνται, για παράδειγμα, η συνάρτηση κατακερματισμού και διαδικασίες για την ανωνυμοποίηση διευθύνσεων πρωτοκόλλου διαδικτύου και άλλες απαιτήσεις προεπεξεργασίας.

13.5.3 Οπτικοποίηση δεδομένων

Να εξεταστεί το ενδεχόμενο χρήσης τεχνικών οπτικοποίησης δεδομένων για την παρουσίαση πληροφοριών σχετικά με συμβάντα, το οποίο συμβάλλει στη βελτίωση της προβολής των αλλαγών και του εξελισσόμενου συμβάντος ασφάλειας η οποία πραγματοποιείται, χωρίς να χρειάζεται οι χειριστές να διαβάζουν τις λεπτομέρειες κάθε συμβάντος καθώς αυτό εξελίσσεται. Για παράδειγμα, βλ. παράρτημα Α, όπου παρουσιάζεται μια οπτική αναπαράσταση των δραστηριοτήτων του Σκοτεινού Δικτύου, η οποία διευκολύνει την αποτελεσματικότερη ανταπόκριση στις αλλαγές.

13.5.4 Ανταλλαγή κρυπτογραφικών κλειδιών και δημιουργία αντιγράφων ασφαλείας λογισμικού/υλισμικού

Για τη διευκόλυνση της ανταλλαγής εμπιστευτικών πληροφοριών, θα πρέπει να εξεταστεί το ενδεχόμενο εφαρμογής ενός κρυπτογραφικού συστήματος, συμπεριλαμβανομένου ενός συστήματος ανταλλαγής κλειδιών που θα μπορούσε να αναπτυχθεί γρήγορα. Το σύστημα θα πρέπει να περιλαμβάνει επαρκή αντίγραφα ασφαλείας για το λογισμικό και το υλισμικό, καθώς και για τα κλειδιά που χρησιμοποιούνται κατά την προετοιμασία για τον σκοπό της κοινής χρήσης και τις ανάγκες ανάκτησης σε περίπτωση έκτακτης ανάγκης.

13.5.5 Ασφαλής κοινή χρήση αρχείων, ανταλλαγή άμεσων μηνυμάτων, διαδικτυακή πύλη και φόρουμ συζητήσεων

Για τη διευκόλυνση της διαδικτυακής αλληλεπίδρασης και της γρήγορης και ασφαλούς ανταλλαγής πληροφοριών, η οποία μπορεί να περιλαμβάνει την ανταλλαγή ψηφιακού περιεχομένου, όπως αρχεία κειμένου και πολυμέσων, καθώς και διαδικτυακές και μη διαδικτυακές συζητήσεις, οι οργανισμοί ανταλλαγής (ΟΠΠ και ΟΠΛ) θα πρέπει να εξετάσουν το ενδεχόμενο υιοθέτησης κατάλληλων εργαλείων ανταλλαγής αρχείων, άμεσων μηνυμάτων και διαδικτυακών ομάδων συζητήσεων που θα μπορούσαν να καλύψουν τις ανάγκες ασφάλειας, αποτελεσματικότητας, αποδοτικότητας και αξιοπιστίας.

Διαδικτυακή πύλη που θα παρέχει πληροφορίες σχετικά με τα γεγονότα και την κατάσταση της Κυβερνοασφάλειας θα πρέπει να υλοποιηθεί ως μορφή επικοινωνίας τόσο για τη δημόσια όσο και για την ιδιωτική κοινότητα που ενδιαφέρεται και εμπλέκεται, αντίστοιχα. Όταν χρησιμοποιείται μια τέτοια διαδικτυακή πύλη, θα πρέπει να υπάρχει σαφής διαχειριστική κυριότητα και ευθύνη για τη διασφάλιση της ασφάλειας και της διαθεσιμότητάς της, ενώ θα πρέπει να παρέχονται ιδιωτικές περιοχές για περιορισμένη πληροφόρηση του κοινού, όπου αυτό είναι απαραίτητο.

13.5.6 Δοκιμές συστημάτων

Ενώ κάθε τεχνικό σύστημα και οι συναφείς μέθοδοι και διαδικασίες θα πρέπει να δοκιμάζονται αυστηρά για να διασφαλίζεται η αξιοπιστία και η ακεραιότητά τους, θα πρέπει να εξεταστούν ένα ή περισσότερα τεχνικά συστήματα αφιερωμένα στη βελτίωση της αποδοτικότητας και της αποτελεσματικότητας των δοκιμών, ιδίως των δοκιμών σεναρίων. Ένα τέτοιο σύστημα μπορεί να έχει τη μορφή ενός συστήματος προσομοίωσης για την προσομοίωση των λειτουργικών περιβαλλόντων, όπως τα αντιλαμβάνεται κάθε οργανισμός του Κυβερνοχώρου, και της εξελισσόμενης κατάστασης Κυβερνοασφάλειας, παρέχοντας τη

δυνατότητα εισαγωγής μιας σειράς συμβάντων ασφαλείας για τη διευκόλυνση της εκτέλεσης των απαιτούμενων δοκιμών.

13.6 Οδηγίες εφαρμογής

Η εφαρμογή ενός τέτοιου πλαισίου απαιτεί από τους συνεργαζόμενους οργανισμούς και τα άτομα να συγκεντρωθούν (εικονικά ή φυσικά) για να καθορίσουν συγκεκριμένη πολιτική, ελέγχους και μέτρα που πρέπει να ληφθούν προκειμένου να επιτευχθούν οι στόχοι της ασφαλούς, αποτελεσματικής, αξιόπιστης και αποδοτικής ανταλλαγής πληροφοριών και του συντονισμού για την αντιμετώπιση αναδυόμενων περιστατικών Κυβερνοασφάλειας. Τα ακόλουθα βήματα υψηλού επιπέδου συνιστώνται ως οδηγός για την εφαρμογή:

α) Εντοπισμός και συγκέντρωση των σχετικών οργανισμών και ατόμων για τη συγκρότηση της απαιτούμενης κοινότητας δικτύου ανταλλαγής και συντονισμού πληροφοριών, είτε ανεπίσημα είτε επίσημα,

β) Καθορισμός του ρόλου (των ρόλων) κάθε εμπλεκόμενου οργανισμού/ατόμου είτε ως ΟΠΠ είτε ως ΟΛΠ είτε και ως αμφότεροι (παράγραφος 13.2.1).

γ) Καθορισμός του είδους των απαιτούμενων πληροφοριών και του συντονισμού που θα ήταν επωφελής για την κοινότητα,

δ) Πραγματοποίηση κατηγοριοποίησης και ταξινόμησης των πληροφοριών για να προσδιοριστεί εάν εμπλέκονται ευαίσθητες πληροφορίες ή/και πληροφορίες προστασίας της ιδιωτικής ζωής (παράγραφος 13.2.2),

ε) Καθορισμός πολιτικών και αρχών που διέπουν την κοινότητα και τις εμπλεκόμενες πληροφορίες (ενότητα 13.2),

στ) Καθορισμός των μεθόδων και των διαδικασιών που απαιτούνται για κάθε κατηγορία και διαβάθμιση των εμπλεκόμενων πληροφοριών (ενότητα 13.3),

ζ) Καθορισμός των απαιτήσεων και των κριτηρίων απόδοσης, καθώς και θέσπιση κώδικα πρακτικής και υπογραφή ΣΕ, εφόσον απαιτείται (παράγραφοι 13.3.3 και 13.3.4),

η) Προσδιορισμός των απαιτούμενων και κατάλληλων προτύπων και τεχνικών συστημάτων για την υποστήριξη της υλοποίησης και της λειτουργίας της κοινότητας (ενότητα 13.5),

θ) Προετοιμασία για τη λειτουργία- συγκέντρωση καταλόγου επαφών- και τη διεξαγωγή συναντήσεων εργασίας ευαισθητοποίησης και κατάρτισης για την προετοιμασία των ενδιαφερομένων,

ι) Διεξαγωγή τακτικών δοκιμών, συμπεριλαμβανομένης της δοκιμής και προσομοίωσης σεναρίων, ανάλογα με τις ανάγκες (παράγραφοι 13.3.5 και 13.5.6),

ια) Διεξαγωγή περιοδικών αναθεωρήσεων, μετά τη δοκιμή και μετά το συμβάν, για τη βελτίωση των συστημάτων ανταλλαγής και συντονισμού, συμπεριλαμβανομένων των εμπλεκόμενων ανθρώπων, διαδικασιών και τεχνολογίας- επέκταση ή μείωση του μεγέθους της κοινότητας, ανάλογα με τις ανάγκες.

ΣΗΜΕΙΩΣΗ Το ISO/IEC 27001, Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Απαιτήσεις συστημάτων διαχείρισης της ασφάλειας πληροφοριών και το ISO/IEC 27003, Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Οδηγίες εφαρμογής συστημάτων διαχείρισης της ασφάλειας πληροφοριών παρέχουν απαιτήσεις και οδηγίες εφαρμογής αντίστοιχα.

14 Οδηγία NIS2 Υψηλό κοινό επίπεδο ασφάλειας στον κυβερνοχώρο στην ΕΕ

14.1 Επισκόπηση

Η οδηγία για την ασφάλεια δικτύων και πληροφοριών (NIS) είναι η πρώτη νομοθετική πράξη σε επίπεδο ΕΕ για την ασφάλεια στον κυβερνοχώρο με στόχο την επίτευξη υψηλού κοινού επιπέδου ασφάλειας στον κυβερνοχώρο σε όλα τα κράτη μέλη. Αν και αύξησε τις δυνατότητες των κρατών μελών στον τομέα της κυβερνοασφάλειας, η εφαρμογή της αποδείχθηκε δύσκολη, με αποτέλεσμα τον κατακερματισμό σε διαφορετικά επίπεδα σε ολόκληρη την εσωτερική αγορά.

Για να ανταποκριθεί στις αυξανόμενες απειλές που δημιουργεί η ψηφιοποίηση και η έξαρση των επιθέσεων στον κυβερνοχώρο, η Επιτροπή υπέβαλε πρόταση για την αντικατάσταση της οδηγίας NIS και, ως εκ τούτου, την ενίσχυση των απαιτήσεων ασφαλείας, την κάλυψη της ασφάλειας των αλυσίδων εφοδιασμού, τον εξορθολογισμό των υποχρεώσεων υποβολής αναφορών και την εισαγωγή αυστηρότερων εποπτικών μέτρων και αυστηρότερων απαιτήσεων επιβολής, συμπεριλαμβανομένων εναρμονισμένων κυρώσεων σε ολόκληρη την ΕΕ. Η προτεινόμενη επέκταση του πεδίου εφαρμογής που καλύπτεται από την NIS2, με την ουσιαστική υποχρέωση λήψης μέτρων από περισσότερες οντότητες και τομείς, θα συμβάλει στην αύξηση του επιπέδου ασφάλειας στον κυβερνοχώρο στην Ευρώπη μακροπρόθεσμα.

Στο Ευρωπαϊκό Κοινοβούλιο, ο φάκελος έχει ανατεθεί στην Επιτροπή Βιομηχανίας, Έρευνας και Ενέργειας.

14.2 Οι αλλαγές που θα επιφέρει η πρόταση

Η Επιτροπή υπέβαλε στις 16 Δεκεμβρίου 2020 πρόταση οδηγίας για τη θέσπιση μέτρων για τη διασφάλιση υψηλού κοινού επιπέδου ασφάλειας στον κυβερνοχώρο σε ολόκληρη την Ένωση (NIS 2), η οποία θα καταργήσει και θα αντικαταστήσει την ισχύουσα οδηγία για την ασφάλεια στον κυβερνοχώρο (NIS 1). Η προτεινόμενη οδηγία αποσκοπεί στην εξάλειψη των περιορισμών του ισχύοντος καθεστώτος της NIS1. Η νομική βάση τόσο για την NIS1 όσο και για την προτεινόμενη NIS2 είναι το άρθρο 114 της Συνθήκης για τη λειτουργία της Ευρωπαϊκής Ένωσης, στόχος του οποίου είναι η εγκαθίδρυση και η λειτουργία της εσωτερικής αγοράς με την ενίσχυση των μέτρων για τη σύγκλιση των εθνικών κανόνων.

Η προτεινόμενη επέκταση του πεδίου εφαρμογής που καλύπτει η NIS2, με την οποία θα υποχρεωθούν περισσότερες οντότητες και τομείς να λάβουν μέτρα, θα συμβάλει μακροπρόθεσμα στην αύξηση του επιπέδου ασφάλειας στον κυβερνοχώρο στην Ευρώπη.

Συνολικά, η πρόταση NIS2 θέτει τρεις γενικούς στόχους:

- Αύξηση του επιπέδου ανθεκτικότητας στον κυβερνοχώρο για ένα εκτεταμένο φάσμα επιχειρήσεων που δραστηριοποιούνται στην Ευρωπαϊκή Ένωση σε όλους τους σχετικούς τομείς, με τη θέσπιση κανόνων με τους οποίους θα διασφαλίζεται ότι όλες οι δημόσιες και ιδιωτικές οντότητες σε ολόκληρη την εσωτερική αγορά, οι οποίες εκπληρώνουν σημαντικές λειτουργίες για την οικονομία και την κοινωνία στο σύνολό της, υποχρεούνται να λαμβάνουν επαρκή μέτρα κυβερνοασφάλειας. Για παράδειγμα, με την πρόταση επεκτείνεται σημαντικά το πεδίο εφαρμογής της ισχύουσας οδηγίας με την προσθήκη νέων τομέων, όπως οι τηλεπικοινωνίες, οι πλατφόρμες κοινωνικής δικτύωσης και η δημόσια διοίκηση. Προβλέπεται ότι όλες οι μεσαίου και μεγάλου μεγέθους οντότητες που δραστηριοποιούνται στους τομείς που καλύπτονται από το πλαίσιο της NIS2 θα πρέπει να συμμορφώνονται αυτομάτως με

τους κανόνες ασφαλείας που προβλέπονται στην πρόταση και καταργείται η δυνατότητα των κρατών μελών να προσαρμόζουν τις απαιτήσεις σε ορισμένες περιπτώσεις (η οποία είχε οδηγήσει σε μεγάλες αποκλίσεις με την εφαρμογή της NIS1). Καταργείται τη διάκριση που γίνεται μεταξύ των φορέων παροχής θεμελιωδών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών, οι οποίοι επί του παρόντος εμπίπτουν σε τρεις κατηγορίες: διαδικτυακές αγορές, μηχανές αναζήτησης και πάροχοι υπηρεσιών νέφους. Τέλος, εξετάζεται, για πρώτη φορά, η κυβερνοασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ (ιδιαίτερης σημασίας στην περίπτωση του Διαδικτύου των Πραγμάτων (IoT)).

- Μείωση των αποκλίσεων ως προς την ανθεκτικότητα σε ολόκληρη την εσωτερική αγορά στους τομείς που καλύπτονται ήδη από την οδηγία, με περαιτέρω εναρμόνιση i) του πραγματικού πεδίου εφαρμογής, ii) των απαιτήσεων ασφάλειας και αναφοράς συμβάντων, iii) των διατάξεων που διέπουν την εθνική εποπτεία και επιβολή και iv) των δυνατοτήτων των σχετικών αρμόδιων αρχών των κρατών μελών. Η πρόταση περιλαμβάνει κατάλογο επτά βασικών στοιχείων που όλες οι εταιρείες πρέπει να καλύψουν ή να εφαρμόσουν στο πλαίσιο των μέτρων που λαμβάνουν, συμπεριλαμβανομένης της αντιμετώπισης περιστατικών, της ασφάλειας της αλυσίδας εφοδιασμού, της κρυπτογράφησης και της γνωστοποίησης ευπαθειών. Επιπλέον, η πρόταση προβλέπει μια προσέγγιση δύο σταδίων για την αναφορά περιστατικών. Οι εταιρείες που επηρεάζονται έχουν στη διάθεσή τους 24 ώρες από τη στιγμή που αντιλαμβάνονται για πρώτη φορά ένα περιστατικό για να υποβάλουν μια αρχική έκθεση, ακολουθούμενη από μια τελική έκθεση το αργότερο ένα μήνα αργότερα. Όσον αφορά την επιβολή, θεσπίζεται ένας ελάχιστος κατάλογος διοικητικών κυρώσεων κάθε φορά που οι οντότητες παραβιάζουν τους κανόνες σχετικά με τη διαχείριση των κινδύνων στον κυβερνοχώρο ή τις υποχρεώσεις αναφοράς τους που προβλέπονται στην οδηγία NIS. Οι κυρώσεις αυτές περιλαμβάνουν δεσμευτικές οδηγίες, εντολή για την εφαρμογή των συστάσεων που προκύπτουν από επιθεωρήσεις ασφαλείας, εντολή για την εναρμόνιση των μέτρων ασφαλείας με τις απαιτήσεις της NIS και διοικητικά πρόστιμα (έως 10 εκατ. ευρώ ή το 2% του συνολικού κύκλου εργασιών των οντοτήτων παγκοσμίως, ανάλογα με το ποιο είναι υψηλότερο).

- Βελτίωση του επιπέδου της από κοινού επίγνωσης της κατάστασης και της συλλογικής ικανότητας προετοιμασίας και αντίδρασης, i) με τη λήψη μέτρων για την αύξηση του επιπέδου εμπιστοσύνης μεταξύ των αρμόδιων αρχών, ii) με την ανταλλαγή περισσότερων πληροφοριών και iii) με τη θέσπιση κανόνων και διαδικασιών σε περίπτωση συμβάντος ή κρίσης μεγάλης κλίμακας. Οι προτεινόμενοι νέοι κανόνες βελτιώνουν τον τρόπο με τον οποίο η ΕΕ προλαμβάνει, χειρίζεται και αντιδρά σε περιστατικά και κρίσεις κυβερνοασφάλειας μεγάλης κλίμακας, εισάγοντας σαφείς αρμοδιότητες, κατάλληλο σχεδιασμό και μεγαλύτερη συνεργασία σε επίπεδο ΕΕ. Η αναθεωρημένη οδηγία θα δημιουργήσει ένα πλαίσιο διαχείρισης κρίσεων στην ΕΕ, απαιτώντας από τα κράτη μέλη να εγκρίνουν ένα σχέδιο και να ορίσουν τις εθνικές αρμόδιες αρχές που είναι υπεύθυνες για τη συμμετοχή στην αντιμετώπιση περιστατικών και κρίσεων κυβερνοασφάλειας σε επίπεδο ΕΕ. Με την προτεινόμενη οδηγία θα δημιουργηθεί ένα δίκτυο διασύνδεσης οργανισμών για την αντιμετώπιση κρίσεων στον κυβερνοχώρο (EU-CyCLONe) για την υποστήριξη της συντονισμένης διαχείρισης περιστατικών κυβερνοασφάλειας σε επίπεδο ΕΕ, καθώς και για τη διασφάλιση της τακτικής ανταλλαγής πληροφοριών. Η προτεινόμενη οδηγία θα ενισχύσει επίσης τον ρόλο της Ομάδας Συνεργασίας της NIS στη λήψη αποφάσεων και στην αύξηση της συνεργασίας μεταξύ των κρατών μελών. Τα κράτη μέλη θα εξακολουθήσουν να υποχρεούνται να υιοθετήσουν εθνική στρατηγική για την ασφάλεια στον κυβερνοχώρο και να ορίσουν μία ή περισσότερες εθνικές αρμόδιες αρχές για την εποπτεία της συμμόρφωσης με την οδηγία και να ορίσουν Ομάδες Αντιμετώπισης Περιστατικών Ασφάλειας Υπολογιστών (CSIRT) για τη διαχείριση των

κοινοποιήσεων συμβάντων και μοναδικά σημεία επαφής (SPOC) που θα λειτουργούν ως σημείο σύνδεσης με άλλα κράτη μέλη.

Προκειμένου να διασφαλιστεί η συνοχή και η συνεκτικότητα με τη σχετική νομοθεσία της ΕΕ, η επανεξέταση της οδηγίας NIS λαμβάνει κυρίως υπόψη τις ακόλουθες τρεις πρωτοβουλίες της Επιτροπής:

- την αναθεώρηση της οδηγίας για την ανθεκτικότητα των κρίσιμων οντοτήτων (CER), η οποία προτάθηκε παράλληλα με την πρόταση NIS2, με στόχο τη βελτίωση της ανθεκτικότητας των κρίσιμων οντοτήτων έναντι φυσικών απειλών σε μεγάλο αριθμό τομέων. Η πρόταση διευρύνει τόσο το πεδίο εφαρμογής όσο και το βάθος της ισχύουσας οδηγίας του 2008, περιλαμβάνοντας την κάλυψη 10 τομέων: ενέργεια, μεταφορές, τράπεζες, υποδομές χρηματοπιστωτικών αγορών, υγεία, πόσιμο νερό, λύματα, ψηφιακές υποδομές, δημόσια διοίκηση και διάστημα,

- την πρωτοβουλία για μια νομοθετική πράξη για την ψηφιακή επιχειρησιακή ανθεκτικότητα του χρηματοπιστωτικού τομέα (DORA),

- την πρωτοβουλία για τη θέσπιση κώδικα για την ασφάλεια στον κυβερνοχώρο στον τομέα των διασυνοριακών ροών ηλεκτρικής ενέργειας, με κανόνες για τον συγκεκριμένο τομέα.

Όσον αφορά τον χρηματοπιστωτικό τομέα, η πρόταση DORA θα παράσχει νομική σαφήνεια σχετικά με το αν και πώς εφαρμόζονται οι ψηφιακές επιχειρησιακές διατάξεις, ιδίως στις διασυνοριακές χρηματοπιστωτικές οντότητες, και θα εξαλείψει την ανάγκη για τα κράτη μέλη να βελτιώσουν μεμονωμένα τους κανόνες, τα πρότυπα και τις προσδοκίες όσον αφορά την επιχειρησιακή ανθεκτικότητα και την ασφάλεια στον κυβερνοχώρο ως απάντηση στην τρέχουσα περιορισμένη κάλυψη των κανόνων της ΕΕ και στον γενικό χαρακτήρα της οδηγίας NIS1. Ταυτόχρονα, είναι σημαντικό να διατηρηθεί μια ισχυρή σχέση για την ανταλλαγή πληροφοριών μεταξύ του χρηματοπιστωτικού τομέα και των άλλων τομέων που καλύπτονται από την NIS2. Για τον σκοπό αυτό, σύμφωνα με την πρόταση DORA, όλες οι χρηματοπιστωτικές εποπτικές αρχές, οι ευρωπαϊκές εποπτικές αρχές για τον χρηματοπιστωτικό τομέα και οι εθνικές αρμόδιες αρχές που σχετίζονται με τον χρηματοπιστωτικό τομέα θα μπορούν να συμμετέχουν στις συζητήσεις της ομάδας συνεργασίας για τις ΝΠΙΔ και να ανταλλάσσουν πληροφορίες και να συνεργάζονται με τα ενιαία σημεία επαφής και με τα εθνικά CSIRT στο πλαίσιο της NIS2. Επιπλέον, τα κράτη μέλη θα πρέπει να συνεχίσουν να συμπεριλαμβάνουν τον χρηματοπιστωτικό τομέα στις στρατηγικές τους για την ασφάλεια στον κυβερνοχώρο και οι εθνικές CSIRT μπορούν να καλύπτουν τον χρηματοπιστωτικό τομέα στις δραστηριότητές τους.

Επιπλέον, η Επιτροπή έχει εναρμονίσει το πεδίο εφαρμογής της πρότασης NIS2 με την πρόταση αναθεώρησης της οδηγίας CER.

Όσον αφορά τον ENISA, θα έχει αυξημένες αρμοδιότητες στο πλαίσιο της υπάρχουσας αρμοδιότητάς του, η οποία περιλαμβάνει την εποπτεία της εφαρμογής της NIS. Ο ENISA θα αναλάβει να συντάσσει ανά διετία έκθεση σχετικά με την κατάσταση της ασφάλειας στον κυβερνοχώρο στην ΕΕ και να διατηρεί ένα ευρωπαϊκό μητρώο ευπαθειών, το οποίο θα παρέχει πρόσβαση σε πληροφορίες σχετικά με τις ευπάθειες των προϊόντων και υπηρεσιών ΤΠΕ που αποκαλύπτονται εθελοντικά από βασικές και σημαντικές οντότητες και τους προμηθευτές τους ΤΠΕ. Ταυτόχρονα, ο ENISA θα πρέπει να δημιουργήσει και να διατηρεί μητρώο, στο οποίο ορισμένοι τύποι οντοτήτων, συμπεριλαμβανομένων των παρόχων υπηρεσιών συστημάτων ονομάτων χώρου, των μητρώων ονομάτων χώρου ανωτάτου επιπέδου, των παρόχων υπηρεσιών υπολογιστικού νέφους, των παρόχων υπηρεσιών κέντρων δεδομένων, των

παρόχων δικτύων διανομής περιεχομένου, καθώς και των διαδικτυακών αγορών, των διαδικτυακών μηχανών αναζήτησης και των πλατφορμών κοινωνικής δικτύωσης, θα γνωστοποιούν την έδρα τους στην ΕΕ. Αυτό γίνεται για να διασφαλιστεί ότι οι εν λόγω οντότητες δεν θα αντιμετωπίζουν πληθώρα διαφορετικών νομικών απαιτήσεων, δεδομένου ότι παρέχουν υπηρεσίες διασυνοριακά σε ιδιαίτερα μεγάλο βαθμό.

Για να αντιμετωπιστούν οι βασικοί κίνδυνοι της αλυσίδας εφοδιασμού και να βοηθηθούν οι φορείς στη διαχείριση των κινδύνων κυβερνοασφάλειας που σχετίζονται με την αλυσίδα εφοδιασμού ΤΠΕ, θα ανατεθεί στην Ομάδα Συνεργασίας της NIS, από κοινού με την Επιτροπή και τον ENISA, η διενέργεια συντονισμένης αξιολόγησης κινδύνων ανά τομέα κρίσιμων υπηρεσιών, συστημάτων ή προϊόντων ΤΠΕ, συμπεριλαμβανομένων των σχετικών απειλών και τρωτών σημείων. Οι εκτιμήσεις κινδύνου της αλυσίδας εφοδιασμού θα εξετάζουν τόσο τεχνικούς παράγοντες (που σχετίζονται με το υλικό ή το λογισμικό) όσο και, κατά περίπτωση, μη τεχνικούς παράγοντες (όπως οι προμηθευτές που υπόκεινται σε παρεμβάσεις από χώρα εκτός ΕΕ ή από παίκτες που υποστηρίζονται από το κράτος). Η προσέγγιση αυτή βασίζεται σε μεγάλο βαθμό στις προηγούμενες εργασίες της Επιτροπής και της ομάδας συνεργασίας NIS σχετικά με την ασφάλεια των δικτύων 5G. Η Επιτροπή δημοσίευσε στις 29 Ιανουαρίου 2020 την εργαλειοθήκη διαχείρισης κινδύνων 5G, στην οποία παρατίθενται μέτρα για τον μετριασμό των απειλών ασφάλειας που συνδέονται με τα δίκτυα 5G. Μεταξύ άλλων, με την αξιολόγηση κινδύνων 5G της ΕΕ εντοπίστηκαν κίνδυνοι ασφαλείας που σχετίζονται με τα δίκτυα 5G και την αλυσίδα εφοδιασμού 5G σε επίπεδο ΕΕ. Για να διασφαλιστεί ότι οι οντότητες συμμορφώνονται με τις υποχρεώσεις τους που αφορούν την ασφάλεια της αλυσίδας εφοδιασμού ΤΠΕ, η νέα οδηγία θα επιτρέψει στα κράτη μέλη να απαιτούν από βασικές και σημαντικές οντότητες να πιστοποιούν συγκεκριμένα προϊόντα, υπηρεσίες και διαδικασίες ΤΠΕ σύμφωνα με την πράξη της ΕΕ για την κυβερνοασφάλεια. Στο πλαίσιο αυτό, το σχέδιο οδηγίας θα εξουσιοδοτήσει την Επιτροπή να καθορίσει ποιες κατηγορίες βασικών οντοτήτων (λόγω της κρισιμότητάς τους) θα πρέπει να λαμβάνουν πιστοποίηση.

Με βάση τον Ευρωπαϊκό Κώδικα Ηλεκτρονικών Επικοινωνιών (EECC) ρυθμίζεται από τον Δεκέμβριο του 2020 η ασφάλεια των παρόχων τηλεπικοινωνιών σχετικά με την παροχή υπηρεσιών ηλεκτρονικών επικοινωνιών στην ΕΕ. Ωστόσο, οι πάροχοι τηλεπικοινωνιών καλύπτονται από το ισχύον πλαίσιο της NIS εάν παρέχουν μη τηλεπικοινωνιακές υπηρεσίες που εμπίπτουν στο πεδίο εφαρμογής της οδηγίας, δηλαδή υπηρεσίες υπολογιστικού νέφους. Συνεπώς, με την προτεινόμενη οδηγία θα καταργηθούν οι αντίστοιχες διατάξεις για την ασφάλεια της EECC και θα ρυθμίζεται πλήρως η ασφάλεια των τηλεπικοινωνιακών παρόχων, και στις περιπτώσεις που παρέχουν υπηρεσίες που σχετίζονται με τον Κώδικα Ηλεκτρονικών Επικοινωνιών. Το ίδιο θα ισχύσει και για τις διατάξεις περί ασφάλειας για τους παρόχους υπηρεσιών εμπιστοσύνης που περιλαμβάνονται επί του παρόντος στον κανονισμό eIDAS.

Παράρτημα Α - Ετοιμότητα Κυβερνοασφάλειας

(Ενημερωτικό)

Α.1 Επισκόπηση

Οι έλεγχοι Κυβερνοασφάλειας που περιγράφονται στην παράγραφο 12 ελαχιστοποιούν την έκθεση και τον κίνδυνο των οργανισμών και των τελικών χρηστών στις περισσότερες από τις γνωστές επιθέσεις Κυβερνοασφάλειας. Κατά την εμφάνιση περιστατικών Κυβερνοασφάλειας, το πλαίσιο ανταλλαγής πληροφοριών και συντονισμού που περιγράφεται στην παράγραφο 11 προβλέπει τη δημιουργία ενός συστήματος ανταλλαγής πληροφοριών και συντονισμού για την προετοιμασία της αντιμετώπισης συμβάντων και περιστατικών Κυβερνοασφάλειας. Οι εν λόγω πληροφορίες προστατεύονται επαρκώς μεταξύ των ΟΠΠ και των ΟΛΠ.

Ενώ οι έλεγχοι αυτοί μειώνουν τον κίνδυνο και βελτιώνουν τον χειρισμό και τη διαχείριση περιστατικών, οι εγκληματίες του κυβερνοχώρου ή άλλοι κακοποιοί θα συνεχίσουν να αναπτύσσουν νέες ή να εξελίσσουν τις τρέχουσες επιθέσεις για να ξεπεράσουν τις υπάρχουσες προστασίες. Ως εκ τούτου, είναι επίσης σημαντικό για τους οργανισμούς να εφαρμόζουν συστήματα και υποδομές που επιτρέπουν μια πιο δυναμική και αυστηρή προσέγγιση στην ανίχνευση, διερεύνηση και αντιμετώπιση επιθέσεων ασφαλείας.

Το ISO/IEC 27031 παρέχει καθοδήγηση σχετικά με τα συστήματα διαχείρισης και τις σχετικές διαδικασίες για την προετοιμασία των συστημάτων ΤΠΕ ενός οργανισμού ώστε να ανιχνεύουν και να ανταποκρίνονται σε προκύπτοντα συμβάντα ασφάλειας, συμπεριλαμβανομένων των συμβάντων Κυβερνοασφάλειας. Η παρούσα κατευθυντήρια γραμμή υπογραμμίζει πρόσθετες τεχνικές προσεγγίσεις που είναι εφαρμόσιμες για τη βελτίωση της ετοιμότητας ενός οργανισμού στον τομέα της Κυβερνοασφάλειας όσον αφορά την ανίχνευση συμβάντων, μέσω της παρακολούθησης του σκοτεινού δικτύου, τη διερεύνηση, μέσω της ανίχνευσης, και την αντιμετώπιση, μέσω της λειτουργιών εξαπάτησης του επιτιθέμενου.

Οι οργανισμοί, ιδίως οι ΠΥΠΖΣ, θα πρέπει να εξετάσουν το ενδεχόμενο να αξιοποιήσουν αυτές τις προσεγγίσεις για να βελτιώσουν την ετοιμότητά τους στον τομέα της Κυβερνοασφάλειας και, ως εκ τούτου, την κατάστασή τους.

Α.2 Παρακολούθηση του σκοτεινού δικτύου

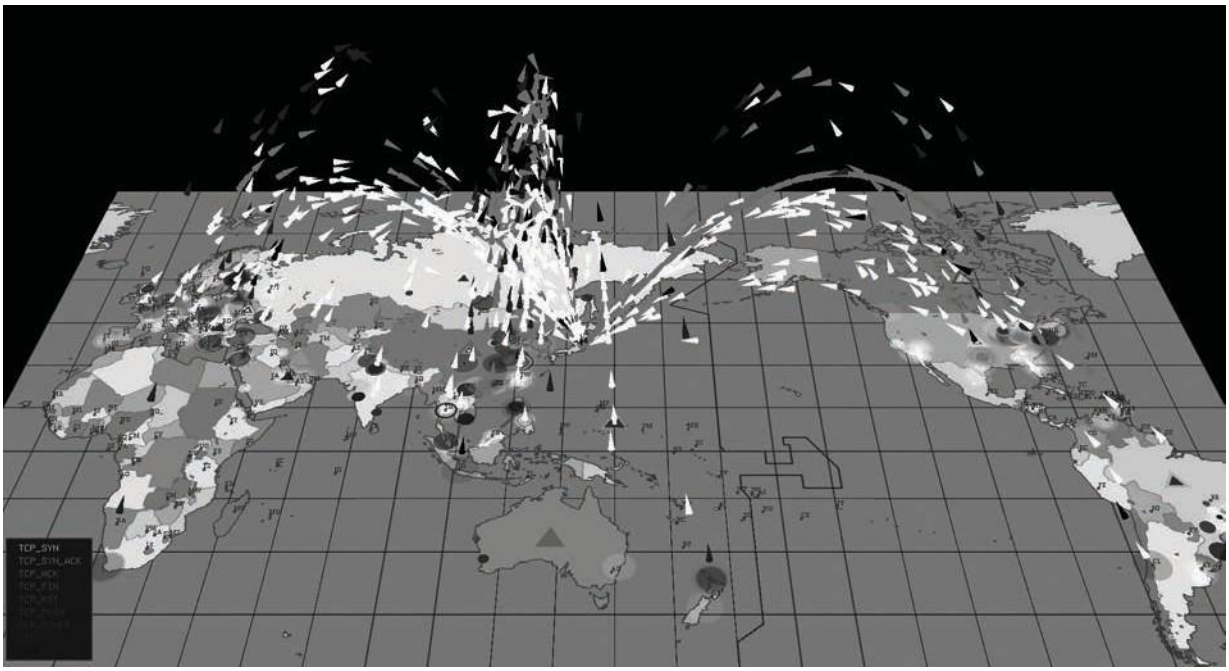
Α.2.1 Εισαγωγή

Το σκοτεινό δίκτυο είναι ένα σύνολο διευθύνσεων ΠΔ που δε χρησιμοποιούνται σε οργανισμούς. Οι διευθύνσεις ΠΔ στο σκοτεινό δίκτυο δεν εκχωρούνται σε λειτουργικούς εξυπηρετητές / συστήματα υπολογιστών. Με τη χρήση των παρακολουθούμενων πακέτων στους τομείς των διευθύνσεων ΠΔ του σκοτεινού δικτύου, οι οργανισμοί θα μπορούσαν να παρατηρήσουν τις αναδυόμενες επιθέσεις δικτύου, συμπεριλαμβανομένης της σάρωσης δικτύου που προκαλείται από κακόβουλο λογισμικό, της συμπεριφοράς μόλυνσης από κακόβουλο λογισμικό και των επιθέσεων ΔΑΕ. Δεδομένου ότι οι διευθύνσεις ΠΔ του σκοτεινού δικτύου είναι δημόσιες, αλλά δεν εκχωρούνται σε νόμιμους κεντρικούς υπολογιστές, όλη η εισερχόμενη κυκλοφορία που ανήκει στους τομείς ΠΔ του σκοτεινού δικτύου μπορεί να θεωρηθεί ως συνέπεια είτε κακόβουλων δραστηριοτήτων είτε εσφαλμένων ρυθμίσεων.

Υπάρχουν, γενικά, τρεις μέθοδοι που χρησιμοποιούνται συνήθως στο σκοτεινό δίκτυο για την παρατήρηση των κακόβουλων δραστηριοτήτων που σχετίζονται με τη διακίνηση στο Διαδίκτυο, δηλαδή η Παρακολούθηση Μαύρων Τρυπών και η Παρακολούθηση Χαμηλών και Υψηλών Αλληλεπιδράσεων.

Α.2.2 Παρακολούθηση μαύρων τρυπών

Η παρακολούθηση Μαύρων Τρυπών αναφέρεται σε συστήματα παρακολούθησης τα οποία δεν ανταποκρίνονται στα εισερχόμενα πακέτα που βρίσκονται εντός των τομέων ΠΔ του Σκοτεινού Δικτύου. Αυτός ο τύπος συστήματος παρακολούθησης χρησιμοποιείται συχνά για την αθόρυβη παρατήρηση της σάρωσης θυρών δικτύου από κακόβουλο λογισμικό και της συμπεριφοράς μόλυνσης από κακόβουλο λογισμικό (ΠΔΧ με ωφέλιμο φορτίο που περιλαμβάνει εκτελέσιμο κώδικα) και των ΔΑΕ. Η σάρωση θυρών δικτύου είναι συχνά το αρχικό βήμα που κάνουν οι επιτιθέμενοι για να αναζητήσουν ευάλωτα συστήματα κεντρικών υπολογιστών που μπορούν να εκμεταλλευτούν. Οι συμπεριφορές μόλυνσης από κακόβουλο λογισμικό είναι συνήθως τα επόμενα βήματα που λαμβάνουν οι επιτιθέμενοι μετά τον εντοπισμό των ευάλωτων συστημάτων υποδοχής. Σε τέτοιες ενέργειες προσβολής παρατηρείται συχνά η χρήση ΠΔΧ με ωφέλιμο φορτίο στην παρακολούθηση μαύρων τρυπών. Επιπλέον, οι ΔΑΕ εντοπίζονται επίσης μέσω της παρακολούθησης Μαύρων Τρύπων στην περίπτωση παραποίησης των διευθύνσεων ΠΔ (επιτιθέμενοι) και ο στόχος της ΔΑΕ μπορεί να αναγνωριστεί από αυτή την κίνηση. Στο Σχήμα Α.1 απεικονίζεται η εικόνα μιας οθόνης της οπτικοποίησης των δραστηριοτήτων κακόβουλου λογισμικού που ανιχνεύονται από ένα σύστημα παρακολούθησης Μαύρων Τρυπών. Ένας σύνδεσμος δείγματος βίντεο μπορεί να βρεθεί εδώ: https://www. youtube.com/watch?v=asemvKgkib4&feature=related.



Εικόνα Α-1 - Παράδειγμα οπτικοποίησης των δραστηριοτήτων κακόβουλου λογισμικού με τη χρήση ενός συστήματος παρακολούθησης Μαύρων Τρυπών

Τα "βέλη" πάνω από τον παγκόσμιο χάρτη (Εικόνα Α.1) απεικονίζουν τη διέλευση των πακέτων ΠΔ από τις πηγές στις στοχευμένες τοποθεσίες. Οι διαφορετικές αποχρώσεις (χρώματα στο βίντεο) απεικονίζουν τον τύπο του πακέτου. Το ύψος κάθε βέλους είναι ανάλογο με τον αριθμό θύρας του.

A.2.3 Παρακολούθηση χαμηλών αλληλεπιδράσεων

Ένα σύστημα παρακολούθησης χαμηλών αλληλεπιδράσεων είναι ένα σύστημα παρακολούθησης του σκοτεινού δικτύου που ανταποκρίνεται στα ανιχνευμένα πακέτα ΠΔ του σκοτεινού δικτύου επιχειρώντας να συνδεθεί ξανά με τα ύποπτα συστήματα φιλοξενίας. Ο σκοπός της απόπειρας σύνδεσης είναι να αποκτηθούν περισσότερες πληροφορίες σχετικά με τα επιτιθέμενα συστήματα κεντρικών υπολογιστών, τις διαδρομές δικτύου επίθεσης που χρησιμοποιούνται και άλλες σχετικές πληροφορίες επίθεσης, εάν είναι δυνατόν. Το σύστημα παρακολούθησης συχνά διαμορφώνεται έτσι ώστε να μεταμφιέζεται ως σύστημα με τρωτά σημεία που δεν έχουν επιδιορθωθεί για να προσελκύσει επιθέσεις. Το σύστημα παρακολούθησης χαμηλής αλληλεπίδρασης χρησιμοποιείται επίσης για την παρατήρηση περαιτέρω αντιδράσεων κακόβουλης συμπεριφοράς και δραστηριοτήτων, όπως η εκτέλεση κακόβουλου κώδικα μετά τις αρχικές σαρώσεις των θυρών του δικτύου.

A.2.4 Παρακολούθηση υψηλών αλληλεπιδράσεων

Ένα σύστημα παρακολούθησης υψηλών αλληλεπιδράσεων (που αναφέρεται επίσης ως honeypot υψηλών αλληλεπιδράσεων) είναι επίσης ένα σύστημα παρακολούθησης του σκοτεινού δικτύου που ανταποκρίνεται στα ανιχνευμένα πακέτα ΠΔ του σκοτεινού δικτύου με το να προσπαθεί να επανασυνδεθεί με τα ύποπτα συστήματα υποδοχής και να αλληλεπιδράσει με τα συστήματα όσο το δυνατόν περισσότερο. Ο σκοπός της αλληλεπίδρασης είναι η απόκτηση πολύ βαθύτερων πληροφοριών, συμπεριλαμβανομένης της στρατηγικής εκμετάλλευσης των ευπαθειών, των εκτελέσιμων αρχείων κακόβουλου λογισμικού που εισάγονται μετά την εισβολή και της συμπεριφοράς του κακόβουλου λογισμικού. Το σύστημα παρακολούθησης υψηλών αλληλεπιδράσεων μπορεί να εφαρμοστεί σε πραγματικά ή εικονικά συστήματα λειτουργίας με ανοιχτές ευπάθειες, έτσι ώστε να προσελκυθεί η προσοχή των επιτιθέμενων, να γίνει εκμετάλλευση και, τέλος, να συλληφθούν δείγματα του κακόβουλου λογισμικού.

A.3 Λειτουργία εξαπάτησης του επιτιθέμενου

Η λειτουργία εξαπάτησης του επιτιθέμενου ορίζεται ως μια μέθοδος ανακατεύθυνσης συγκεκριμένης κυκλοφορίας ΠΔ σε μια συσκευή εξαπάτησης (π.χ. δρομολογητή εξαπάτησης) με σκοπό την ανάλυση της κυκλοφορίας, την εκτροπή επιθέσεων και την ανίχνευση ανώμαλων συμπεριφορών σε ένα δίκτυο. Για παράδειγμα, εάν η επιχειρηματική λειτουργία ενός συστήματος-στόχου διαταράσσεται μέσω μιας επίθεσης ΔΑΕ, μια από τις αποτελεσματικές λύσεις είναι η έναρξη μιας λειτουργίας εξαπάτησης με την εισαγωγή μιας εναλλακτικής διαδρομής για τον στόχο και την ανακατεύθυνση της κυκλοφορίας ΔΑΕ κατά μήκος της διαδρομής αντί να της επιτραπεί να ρέει προς τον αρχικό στόχο. Η συσκευή εξαπάτησης είναι ικανή να απορροφά, να αναλύει ή/και να απορρίπτει την κίνηση ΔΑΕ. Η διαδρομή ανακατεύθυνσης του στόχου, η οποία κατευθύνεται προς έναν δρομολογητή εξαπάτησης, απελευθερώνεται συνήθως από έναν δρομολογητή ορίων. Η λειτουργία εξαπάτησης με χρήση της διαμόρφωσης περιγράφεται στο RFC 3882. Ένα μειονέκτημα αυτής της μεθόδου είναι ότι η διεύθυνση ΠΔ που δέχεται την επίθεση δεν μπορεί να χρησιμοποιηθεί για επικοινωνία με άλλους χρήστες του δικτύου έως ότου καταργηθεί η διαδρομή.

Οι λειτουργίες εξαπάτησης χρησιμοποιούνται συχνά για την προστασία από επιθέσεις ΔΑΕ, όπως περιγράφεται παραπάνω. Έχει επίσης αναπτυχθεί για την προστασία από επιθέσεις δικτύων ρομπότ με την ανακατεύθυνση των εντολών και του ελέγχου (E&E - Command and Control, C&C) του δικτύου ρομπότ σε μια συσκευή εξαπάτησης. Δεδομένου ότι κάθε ρομπότ πρέπει να δημιουργήσει συνδέσεις με έναν διακομιστή E&E προκειμένου να λάβει οδηγίες επίθεσης από έναν ελεγκτή δικτύου ρομπότ, στέλνει ερωτήματα Συστήματος Ονοματοδοσίας Διαδικτύου για την επίλυση της διεύθυνσης ΕΕΠ του διακομιστή

Ε&Ε. Στη συνέχεια, οι διακομιστές Συστήματος Ονοματοδοσίας Διαδικτύου στέλνουν μια διεύθυνση ΠΔ της συσκευής εξαπάτησης στα ρομπότ αντί της γνήσιας διεύθυνσης ΠΔ του διακομιστή Ε&Ε. Κατά συνέπεια, ο ελεγκτής του δικτύου ρομπότ στερείται της σύνδεσης με τα ρομπότ, ώστε να μην μπορεί να τους στείλει οδηγίες επίθεσης.

Α.4 Εντοπισμός ιχνών

Προκειμένου να αυτοματοποιηθεί ή να επιταχυνθεί ο χειροκίνητος εντοπισμός των κακόβουλων επιθέσεων, όπως οι επιθέσεις ΑΕ όπου ο υπολογιστής φιλοξενίας παραποιείται, έχουν μελετηθεί πολλές τεχνικές αυτόματης ανίχνευσης. Οι τεχνικές εντοπισμού ιχνών αναγνωρίζονται ως τεχνικές που ανακατασκευάζουν τη διαδρομή της επίθεσης και εντοπίζουν τους κόμβους του επιτιθέμενου με τη διόρθωση της κίνησης της επίθεσης, των πληροφοριών δρομολόγησης, των σημασμένων πακέτων ή του αρχείου καταγραφής ελέγχου της κίνησης της επίθεσης.

Δεν υπάρχουν ακόμη τεχνικές εντοπισμού ιχνών, οι οποίες να μπορούν να ανακατασκευάσουν τη διαδρομή της επίθεσης σε διάφορους τομείς δικτύου, που να χρησιμοποιούνται ή να εφαρμόζονται στο πραγματικό περιβάλλον λειτουργίας του δικτύου. Οι δυσκολίες της ανάπτυξης τεχνικών εντοπισμού ιχνών μεταξύ των τομέων (σε διάφορους τομείς δικτύου) προκύπτουν από τα ακόλουθα λειτουργικά ζητήματα:

α) Για τους σκοπούς του εντοπισμού ιχνών μεταξύ τομέων, η ανταλλαγή ευαίσθητων πληροφοριών, όπως η λεπτομερής τοπολογία του δικτύου κορμού, μπορεί να προκαλέσει σοβαρά προβλήματα στους φορείς εκμετάλλευσης δικτύων.

β) Δεδομένου ότι η λειτουργία εντοπισμού ιχνών μπορεί να είναι στενά συνδεδεμένη με την ασφάλεια του δικτύου του κορμού των ΠΥΔ, οι αυθαίρετες δοκιμές προσπαθειών εντοπισμού ιχνών από μη εξουσιοδοτημένα άτομα δε θα ήταν αποδεκτές από τους περισσότερους ΠΥΔ. Ως εκ τούτου, υπάρχει φόβος κακής χρήσης της τεχνικής εντοπισμού ιχνών σε όλους τους τομείς του δικτύου από τρίτους.

γ) Εάν μια ενιαία και συγκεκριμένη τεχνική εντοπισμού ιχνών μεταξύ τομέων εφαρμοστεί σε πολλούς τομείς δικτύου, η μοναδική ενιαία τεχνική θα πρέπει να αναπτυχθεί ταυτόχρονα από τα συμμετέχοντα Αυτόνομα Συστήματα (ΑΣ - Autonomous Systems, AS). Επιπλέον, οι επιτιθέμενοι αργά ή γρήγορα θα αναπτύξουν επιθέσεις αποφυγής. Πρακτικά, πολλοί ΠΥΔ χρησιμοποιούν πολλαπλά εργαλεία ανίχνευσης και εντοπισμού στα δίκτυά τους.

Τα παραπάνω λειτουργικά ζητήματα ανακύπτουν όταν μια δοκιμή εντοπισμού προσπαθεί να επεκταθεί πέρα από τα όρια του δικτύου. Οι τεχνικές εντοπισμού ιχνών θα πρέπει να λαμβάνουν υπόψη τα όρια λειτουργίας του δικτύου και τη διαφορά των επιχειρησιακών πολιτικών μεταξύ διαφορετικών τομέων δικτύου. Πιστεύεται ακράδαντα ότι οι μηχανισμοί εντοπισμού ιχνών και μετριασμού των επιθέσεων μεταξύ τομέων πρέπει να αναπτυχθούν παντού στο Διαδίκτυο.

Κατά την ανάπτυξη τεχνικών και συστημάτων εντοπισμού ιχνών μεταξύ τομέων στην πράξη, θα πρέπει να λαμβάνεται υπόψη η ακόλουθη αρχιτεκτονική ανίχνευσης:

α) Για τη διατήρηση των ορίων λειτουργίας του δικτύου, η αρχιτεκτονική εντοπισμού ιχνών πρέπει να αφήνει σε κάθε ΑΣ να αποφασίζει αν θα δεχτεί ένα αίτημα εντοπισμού από την επιχειρησιακή πολιτική κάθε ΑΣ,

β) Η αρχιτεκτονική εντοπισμού ιχνών θα πρέπει επίσης να αφήνει σε κάθε ΠΣ να αποφασίζει αν θα διερευνήσει ή όχι βαθύτερα το εσωτερικό του δικού του δικτυακού τομέα,

γ) Η αρχιτεκτονική θα πρέπει επίσης να αφήνει κάθε υποπεριοχή ενός ΑΣ να αποφασίζει αν θα επιθεωρεί ή όχι το δίκτυο κάθε υποπεριοχής από την πολιτική λειτουργίας του. Η λειτουργία του εντοπισμού ιχνών θα καταναλώσει πολλούς πόρους στα σχετικά ΑΣ - επομένως, η αρχιτεκτονική εντοπισμού ιχνών δε θα πρέπει να παράγει ή να πλημμυρίζει άσκοπα αιτήματα, αν είναι δυνατόν - επομένως, η αρχιτεκτονική εντοπισμού ιχνών δε θα πρέπει να προωθεί μηνύματα αιτημάτων σε ΑΣ που δεν έχουν καμία σχέση με την επιτιθέμενη επίθεση,

δ) Προκειμένου να μειωθεί η ζημία από καταχρήσεις, το μήνυμα δε θα πρέπει να μεταφέρει ευαίσθητες πληροφορίες που θα μπορούσαν να προκαλέσουν διαρροή μυστικών ή καταπάτηση εμπιστοσύνης ενός ΠΣ - συνεπώς, η αρχιτεκτονική εντοπισμού ιχνών δε θα πρέπει να αποκαλύπτει ευαίσθητες πληροφορίες ενός ΠΣ σε άλλους,

ε) Ακόμα και όταν γίνεται κατάχρηση ή συμβιβαστική ενέργεια, η ιχνηλασιμότητα του μηνύματος θα προσδιορίζει τον δράστη, επομένως, ένα μήνυμα που ανταλλάσσεται στην αρχιτεκτονική θα πρέπει να έχει τη δική του ιχνηλασιμότητα για να αποδεικνύει ή να επιβεβαιώνει τους δημιουργούς του,

στ) Εάν η αρχιτεκτονική εξαρτάται από μια συγκεκριμένη τεχνική εντοπισμού ιχνών, οι επιτιθέμενοι θα αναπτύξουν επιθέσεις αποφυγής και θα αποκρύψουν τη θέση των κόμβων του επιτιθέμενου. Για να ξεπεραστούν οι επιθέσεις διαφυγής, η αρχιτεκτονική εντοπισμού ιχνών θα πρέπει να είναι ανεξάρτητη από συγκεκριμένες τεχνικές ιχνηλάτησης,

ζ) Πολλά συστήματα λειτουργίας έρχονται να υποστηρίξουν την IPv4/IPv6 και αρκετές επιθέσεις έρχονται μέσω μιας σήραγγας 6to4 IPv6. Εάν η αρχιτεκτονική εντοπισμού δεν μπορεί να εντοπίσει επιθέσεις στο δίκτυο IPv6 ή επιθέσεις μέσω κάποιων μεταφραστών, η πλειονότητα των επιθέσεων θα μετατοπιστεί σε μια τέτοια σύνθετη επίθεση. Επομένως, η αρχιτεκτονική εντοπισμού θα πρέπει να εντοπίζει μια επίθεση σε περιβάλλον διπλής στοίβας, ακόμη και όταν η επίθεση χρησιμοποιεί κάποιες τεχνικές μετάφρασης διευθύνσεων,

η) Για την αυτοματοποίηση της διαδικασίας μετριασμού των επιθέσεων, η αρχιτεκτονική θα πρέπει να είναι σε θέση να εξάγει το αποτέλεσμα μιας δοκιμής εντοπισμού ιχνών ως έναυσμα για τον μετριασμό της επίθεσης. Ως εκ τούτου, η αρχιτεκτονική εντοπισμού ιχνών θα πρέπει να επιτρέπει σε κάθε ΠΣ να αναλαμβάνει μια άλλη ενέργεια μαζί με το αποτέλεσμα της ιχνηλάτησης, όπως ένα φιλτράρισμα ή μια άλλη ιχνηλάτηση,

θ) Η αρχιτεκτονική θα πρέπει να έχει τη δυνατότητα συνεργασίας με συστήματα ανίχνευσης ή προστασίας,

ι) Ένας επιτιθέμενος μπορεί να αλλάξει το μοτίβο της κίνησης επίθεσης για να αποφύγει την επίδραση αυτών των ενεργειών μετριασμού. Καταπολεμώντας τις αλλαγές μιας σύνθετης επίθεσης, ο χρόνος που δαπανάται για την ανίχνευση μιας διαδρομής επίθεσης θα πρέπει να είναι όσο το δυνατόν μικρότερος. Ως εκ τούτου, η αρχιτεκτονική θα πρέπει να αποκλείει όσο το δυνατόν περισσότερο τον άνθρωπο.

Παράρτημα Β – Επιπρόσθετες πηγές

(Ενημερωτικό)

Β.1 Αναφορές σε θέματα ασφάλειας στο διαδίκτυο και προστασίας από προγράμματα κατασκοπείας

Υπάρχουν διάφοροι ιστότοποι που μπορούν να αναφερθούν και να αξιοποιηθούν για περισσότερες πληροφορίες σχετικά με την ασφάλεια στο Διαδίκτυο και την Κυβερνοασφάλεια. Ακολουθεί μη εξαντλητικός κατάλογος παραδειγμάτων:

- **Συμμαχία κατά του λογισμικού κατασκοπείας** (http://www.antispywarecoalition.org/) - Μια ομάδα αφιερωμένη στη δημιουργία συναίνεσης σχετικά με τους ορισμούς και τις βέλτιστες πρακτικές στη συζήτηση γύρω από το λογισμικό κατασκοπείας και άλλες δυνητικά ανεπιθύμητες τεχνολογίες. Αποτελούμενη από εταιρείες λογισμικού κατά του κατασκοπευτικού λογισμικού, ακαδημαϊκούς και ομάδες καταναλωτών, η ASC επιδιώκει να συγκεντρώσει ένα ευρύ φάσμα απόψεων σχετικά με το πρόβλημα του ελέγχου του λογισμικού κατασκοπείας και άλλων δυνητικά ανεπιθύμητων τεχνολογιών.

- **APWG** (http://www.antiphishing.org) - Ένας ιστότοπος εκπαίδευσης και ευαισθητοποίησης σχετικά με το ηλεκτρονικό ψάρεμα που παρέχει τριμηνιαία επικαιροποιημένα ενημερωτικά έγγραφα σχετικά με τις τάσεις των επιθέσεων, τη διανομή, τις επιπτώσεις και τα νέα.

- **Be Web Aware** (http://www.bewebaware.ca) - Εθνικό, δίγλωσσο πρόγραμμα δημόσιας εκπαίδευσης για την ασφάλεια στο Διαδίκτυο, σχεδιασμένο για να διασφαλίσει ότι οι νέοι Καναδοί επωφελούνται από το Διαδίκτυο, ενώ παράλληλα είναι ασφαλείς και υπεύθυνοι στις διαδικτυακές τους δραστηριότητες.

- **Κέντρο Ασφαλούς και Υπεύθυνης Χρήσης του Διαδικτύου** (http://csriu.org) - Οργάνωση που παρέχει υπηρεσίες προβολής για θέματα ασφαλούς και υπεύθυνης χρήσης του Διαδικτύου.

- **Childnet International** (http://www.childnet-int.org) - Μη κερδοσκοπικός οργανισμός που συνεργάζεται με άλλους φορείς σε όλο τον κόσμο για να βοηθήσει να γίνει το Διαδίκτυο ένα σπουδαίο και ασφαλές μέρος για τα παιδιά.

- **ECPAT** (http://www.ecpat.net) - Δίκτυο οργανώσεων και ατόμων που εργάζονται από κοινού για την εξάλειψη της εμπορικής σεξουαλικής εκμετάλλευσης των παιδιών.

- **GetNetWise** (http://www.getnetwise.org) - Δημόσια υπηρεσία που προσφέρεται από έναν συνασπισμό εταιρειών της βιομηχανίας του Διαδικτύου και οργανώσεων δημοσίου συμφέροντος που θέλουν οι χρήστες να βρίσκονται μόνο "ένα κλικ μακριά" από τους πόρους που χρειάζονται για να λαμβάνουν τεκμηριωμένες αποφάσεις σχετικά με τη χρήση του Διαδικτύου από τους ίδιους και την οικογένειά τους.

- **Παγκόσμια Συμμαχία Υποδομών για την Ασφάλεια στο Διαδίκτυο** (Global Infrastructure Alliance for Internet Safety, GIAIS) (http://www.microsoft.com/security/ msra/default.mspx) - Μια συμμαχία ορισμένων παρόχων υπηρεσιών, οι οποίοι έχουν οργανωθεί για να βελτιώσουν την ασφάλεια και την προστασία στον Παγκόσμιο Ιστό, να διαχειριστούν με συνέπεια τις απειλές σε ένα ευρύ φάσμα και να εντοπίσουν και να μετριάσουν τα υπάρχοντα τρωτά σημεία.

- **INHOPE** (http://inhope.org) - Διεθνής ένωση που υποστηρίζει τις τηλεφωνικές γραμμές του Διαδικτύου με στόχο να ανταποκρίνονται στις αναφορές παράνομου περιεχομένου και να καθιστούν το Διαδίκτυο ασφαλέστερο.

- **Ομάδα Ασφάλειας Διαδικτύου** (www.netsafe.org.nz) - Ο δικτυακός τόπος NetSafe είναι το διαδικτυακό σπίτι της Ομάδας Ασφάλειας Διαδικτύου της Νέας Ζηλανδίας (ISG) και του Έκτορα του Προστάτη.

- **Ιντερπόλ** (http://www.interpol.int) - Διεθνής αστυνομικός οργανισμός που διευκολύνει τη διασυνοριακή αστυνομική συνεργασία και υποστηρίζει και βοηθά όλους τους οργανισμούς, τις αρχές και τις υπηρεσίες που έχουν ως αποστολή την πρόληψη ή την καταπολέμηση του διεθνούς εγκλήματος.

- **iSafe** (http://www.isafe.org) - Παγκόσμιος ηγέτης στην εκπαίδευση για την ασφάλεια στο Διαδίκτυο- ενσωματώνει διδακτέα ύλη στην τάξη με δυναμική δράση στην κοινότητα για την ενδυνάμωση των μαθητών, των εκπαιδευτικών, των γονέων, των αρχών επιβολής του νόμου και των ενηλίκων που ενδιαφέρονται να κάνουν το Διαδίκτυο ένα ασφαλέστερο μέρος.

- **ISECOM** (http://www.isecom.org) - Ελεύθερες μεθοδολογίες ανοικτού κώδικα (FDL) για επαγγελματικές δοκιμές ασφαλείας (αξιολόγηση ευπάθειας, δοκιμή διείσδυσης, ηθικό hacking), αξιολόγηση τεχνικών κινδύνων. Η ISECOM διαχειρίζεται το Εγχειρίδιο Μεθοδολογίας Δοκιμών Ασφαλείας Ανοικτού Κώδικα (Open Source Security Testing Methodology Manual, OSSTMM), ένα παγκόσμιο de facto πρότυπο για την εκτέλεση δοκιμών ασφαλείας ΤΠ/ΤΠΕ (http://www.osstmm.org).

- **COP** (http://www.itu.int/cop/) - Η Προστασία των Παιδιών στο Διαδίκτυο (Children Online Protection, COP) είναι ένα ειδικό έργο που υλοποιείται από τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunication Union, ITU) και άλλους εξειδικευμένους οργανισμούς/επιχειρήσεις, παρέχοντας κατευθυντήριες γραμμές ασφαλείας για: Παιδιά, γονείς, κηδεμόνες και εκπαιδευτικούς, τη βιομηχανία και τους υπεύθυνους χάραξης πολιτικής.

- **Microsoft Security At Home** (http://www.microsoft.com/protect) - Πληροφορίες και πόροι που βοηθούν το κοινό να προστατεύσει τους υπολογιστές του, τον εαυτό του και τις οικογένειές του.

- **Εθνικό Ινστιτούτο Τεχνολογιών Τηλεπικοινωνιών (National Institute of Telecommunications Technologies, INTECO)** (http://www.inteco.es, http://cert. inteco.es, http://www.osi.es, http://observatorio.inteco.es) - Δωρεάν δημόσια υπηρεσία που προσφέρεται από την ισπανική δημόσια διοίκηση για την προώθηση της εμπιστοσύνης και της ασφάλειας στο Διαδίκτυο για τους πολίτες, τις ΜΜΕ, τους τεχνικούς, τα παιδιά κ.λπ., μέσω μιας ομάδας αντιμετώπισης εκτάκτων αναγκών υπολογιστών (INTECO- OAEAY), ενός γραφείου βοήθειας για την ασφάλεια των πολιτών και ενός παρατηρητηρίου ασφάλειας πληροφοριών.

- **Net Family News** (http://netfamilynews.org) - Μη κερδοσκοπική δημόσια υπηρεσία που παρέχει ένα φόρουμ και "ειδήσεις τεχνολογίας για παιδιά" για γονείς και εκπαιδευτικούς σε περισσότερες από 50 χώρες.

- **NetAlert Limited** (http://www.netalert.net.au) - Μη κερδοσκοπικός κοινοτικός οργανισμός που ιδρύθηκε από την αυστραλιανή κυβέρνηση για την παροχή ανεξάρτητων συμβουλών και εκπαίδευσης σχετικά με τη διαχείριση της πρόσβασης σε διαδικτυακό περιεχόμενο.

- **NetSmartzKids** (http://www.netsmartzkids.org) - Το NetSmartz είναι μια διαδραστική, εκπαιδευτική πηγή ασφάλειας από το Εθνικό Κέντρο για τα Εξαφανισμένα και Εκμεταλλευόμενα Παιδιά (National

Centre for Missing and Exploited Children, NCMEC) και τις Λέσχες Αγοριών και Κοριτσιών της Αμερικής (Boys and Girls Clubs of America, BGCA) για παιδιά ηλικίας 5 έως 17 ετών, γονείς, κηδεμόνες, εκπαιδευτικούς και φορείς επιβολής του νόμου, η οποία χρησιμοποιεί τρισδιάστατες δραστηριότητες κατάλληλες για την ηλικία των παιδιών για να τους διδάξει πώς να παραμένουν ασφαλέστερα στο Διαδίκτυο.

- **Saferinternet.be** (www.saferinternet.be) - Ο δικτυακός αυτός τόπος προσφέρει χρήσιμες πληροφορίες σχετικά με τους σημαντικότερους κινδύνους και το επιβλαβές περιεχόμενο με το οποίο οι ανήλικοι μπορούν να έρθουν αντιμέτωποι στο διαδίκτυο και γενικότερα στον τομέα των ΤΠΕ (άρα και μέσω δικτύων κινητής τηλεφωνίας κ.λπ.), δηλαδή παιδική πορνογραφία, ρατσισμός και διακρίσεις, αιρέσεις, παράνομες εμπορικές πρακτικές και απάτες και, τέλος, τεχνικοί κίνδυνοι. Ο δικτυακός τόπος, που παρουσιάζει επίσης στρατηγικές για τη σωστή αντιμετώπιση αυτών των κινδύνων, αποτελείται από διάφορες ενότητες που επικεντρώνονται σε διάφορες ομάδες-στόχους. Παρέχει μεταξύ άλλων παιδαγωγικά και τεχνικά αρχεία για τους εκπαιδευτικούς (γονείς και καθηγητές), παιχνίδια για παιδιά (ηλικίας 6 έως 12 ετών) και έναν εντελώς ξεχωριστό ιστότοπο (web4me.be) για εφήβους.

- **SafeKids.com** (http://www.safekids.com) - Πόροι που βοηθούν τις οικογένειες να κάνουν το Διαδίκτυο και την τεχνολογία διασκεδαστικά, ασφαλή και παραγωγικά.

- **StaySafe.org** (http://www.staysafe.org) - Εκπαιδευτικός ιστότοπος με σκοπό να βοηθήσει τους καταναλωτές να κατανοήσουν τόσο τις θετικές πτυχές του Διαδικτύου όσο και τον τρόπο διαχείρισης διαφόρων θεμάτων ασφάλειας και προστασίας που υπάρχουν στο Διαδίκτυο.

- **UNICEF** (http://www.unicef.org) - Παγκόσμιος συνήγορος για την προστασία των δικαιωμάτων των παιδιών, αφιερωμένος στην παροχή μακροπρόθεσμης ανθρωπιστικής και αναπτυξιακής βοήθειας σε παιδιά και γονείς στις αναπτυσσόμενες χώρες.

- **WebSafe Crackerz** (http://www.websafecrackerz.com) - Διαδραστικά παιχνίδια και παζλ σχεδιασμένα να βοηθούν τους εφήβους και να προσφέρουν στρατηγικές για την αντιμετώπιση διαφόρων καταστάσεων στο διαδίκτυο, όπως ανεπιθύμητη αλληλογραφία, ηλεκτρονικό ψάρεμα και απάτες.

Β.2 Δείγμα καταλόγου επαφών κλιμάκωσης συμβάντων

Ο πίνακας Β.1 παρακάτω παρέχει έναν μη εξαντλητικό κατάλογο παραδειγμάτων επαφών κλιμάκωσης περιστατικών ασφάλειας στο Διαδίκτυο:

Πίνακας Β.1 - Δείγμα λίστας με τα στοιχεία επικοινωνίας για την κλιμάκωση της ασφάλειας

Οργανισμός	Επαφή
Cisco Systems Inc.	mailto:safetyandsecurity@cisco.com http://www.cisco.com/security
Microsoft Corporation	mailto:avsubmit@submit.microsoft.com mailto:secure@microsoft.com
Ομάδα αντιμετώπισης περιστατικών και ομάδες ασφάλειας (Forum of Incident Response and Security Teams, FIRST)	http://www.first.org/about/organization/teams/
Συναφείς εθνικές ομάδες (π.χ. ΟΑΕΑΥ)	
Εθνικό Ινστιτούτο Τεχνολογιών Τηλεπικοινωνιών (National Institute of Telecommunications Technologies, INTECO), Spain	http://cert.inteco.es (English: http://cert.inteco.es/cert/INTECOCERT_1/?postAction=getCertHome)
Telecom-ISAC Japan	https://www.telecom-isac.jp/contact/index.html

KrCERT/CC (Κέντρο Ασφαλείας Διαδικτύου Κορέας)	http://www.krcert.or.kr/index.jsp

Παράρτημα Γ – Παραδείγματα σχετικών εγγράφων

(Ενημερωτικό)

Γ.1 Εισαγωγή

Το παρόν παράρτημα παρέχει έναν μη εξαντλητικό κατάλογο παραδειγμάτων εγγράφων που μπορεί να είναι χρήσιμα κατά την εξέταση της Κυβερνοασφάλειας. Δεν προορίζεται να αποτελέσει πλήρη κατάλογο των διεθνών προτύπων και τεχνικών εκθέσεων για την Κυβερνοασφάλεια.

Γ.2 ISO και IEC

Πίνακας Γ.1 – Συστήματα διαχείρισης ασφάλειας πληροφοριών

Αναφορά	Τίτλος
ISO/IEC 27000	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Συστήματα διαχείρισης της ασφάλειας πληροφοριών - Επισκόπηση και λεξιλόγιο
ISO/IEC 27001	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Συστήματα διαχείρισης της ασφάλειας πληροφοριών – Απαιτήσεις
ISO/IEC 27002	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κώδικας πρακτικής για τη διαχείριση της ασφάλειας των πληροφοριών
ISO/IEC 27003	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Οδηγίες εφαρμογής συστήματος διαχείρισης της ασφάλειας πληροφοριών
ISO/IEC 27010	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Διαχείριση της ασφάλειας πληροφοριών για διατομεακές επικοινωνίες

Πίνακας Γ.2 – Διαχείριση κινδύνων

Αναφορά	Τίτλος
ISO/IEC 27005	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Διαχείριση κινδύνων ασφάλειας πληροφοριών
ISO/IEC 16085	Μηχανική συστημάτων και λογισμικού - Διαδικασίες κύκλου ζωής - Διαχείριση κινδύνων

Πίνακας Γ.3 – Αξιολόγηση της ασφάλειας ΤΠ

Αναφορά	Τίτλος
ISO/IEC 15408	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κριτήρια αξιολόγησης της ασφάλειας ΤΠ
ISO/IEC 28045	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Μεθοδολογία για την αξιολόγηση της ασφάλειας ΤΠ
ISO/IEC TR 19791	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Αξιολόγηση της ασφάλειας των συστημάτων λειτουργίας

Πίνακας Γ.4 – Διασφάλιση της ασφάλειας

Αναφορά	Τίτλος
ISO/IEC TR 15443	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Πλαίσιο για τη διασφάλιση της ασφάλειας ΤΠ
ISO/IEC 15026	Μηχανική συστημάτων και λογισμικού - Διασφάλιση συστημάτων και λογισμικού

Πίνακας Γ.5 – Σχεδιασμός και υλοποίηση

Αναφορά	Τίτλος
ISO/IEC 12207	Μηχανική συστημάτων και λογισμικού - Διαδικασίες κύκλου ζωής λογισμικού
ISO/IEC 14764	Μηχανική λογισμικού - Διαδικασίες κύκλου ζωής λογισμικού - Συντήρηση
ISO/IEC 15288	Μηχανική συστημάτων και λογισμικού - Διαδικασίες κύκλου ζωής συστήματος
ISO/IEC 23026	Μηχανική λογισμικού - Συνιστώμενη πρακτική για το Διαδίκτυο - Μηχανική ιστοτόπων, διαχείριση ιστοτόπων και κύκλος ζωής ιστοτόπων
ISO/IEC 42010	Μηχανική συστημάτων και λογισμικού - Περιγραφή αρχιτεκτονικής

Πίνακας Γ.6 – Εξωτερικές αναθέσεις και υπηρεσίες από τρίτους

Αναφορά	Τίτλος
ISO/IEC TR 14516	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κατευθυντήριες γραμμές για τη χρήση και τη διαχείριση των υπηρεσιών έμπιστων τρίτων μερών
ISO/IEC 15945	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Προδιαγραφές αξιόπιστων υπηρεσιών τρίτων για την υποστήριξη της εφαρμογής ψηφιακών υπογραφών

Πίνακας Γ.7 – Ασφάλεια δικτύου και εφαρμογών

Αναφορά	Τίτλος
ISO/IEC 18028	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Ασφάλεια δικτύων πληροφορικής
ISO/IEC 18043	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Επιλογή, ανάπτυξη και λειτουργία συστημάτων ανίχνευσης εισβολών
ISO/IEC 27033	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Ασφάλεια δικτύων
ISO/IEC 27034	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κατευθυντήριες γραμμές για την ασφάλεια εφαρμογών

Πίνακας Γ.8 – Διαχείριση συνέχειας και συμβάντων

Αναφορά	Τίτλος
ISO/IEC TR 18044	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Διαχείριση περιστατικών ασφάλειας πληροφοριών
ISO/IEC 24762	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κατευθυντήριες γραμμές για υπηρεσίες αποκατάστασης μετά από καταστροφές στην τεχνολογία πληροφοριών και επικοινωνιών
ISO/IEC 27031	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Κατευθυντήριες γραμμές για την ετοιμότητα των ΤΠΕ για την επιχειρησιακή συνέχεια
ISO/IEC 27035	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Διαχείριση περιστατικών ασφάλειας πληροφοριών

Πίνακας Γ.9 – Διαχείριση ταυτότητας

Αναφορά	Τίτλος
ISO/IEC 24760	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Πρότυπο διαχείρισης ταυτότητας

Πίνακας Γ.10 – Ιδιωτικότητα

Αναφορά	Τίτλος
ISO/IEC 29100	Τεχνολογία πληροφοριών - Τεχνικές ασφάλειας - Πρότυπο προστασίας της ιδιωτικής ζωής

Πίνακας Γ.11 – Διαχείριση περιουσιακών στοιχείων

Αναφορά	Τίτλος
ISO/IEC 19770	Τεχνολογία πληροφοριών - Διαχείριση περιουσιακών στοιχείων λογισμικού

Πίνακας Γ.12 – Διαχείριση υπηρεσιών

Αναφορά	Τίτλος
ISO/IEC 20000	Τεχνολογία πληροφοριών - Διαχείριση υπηρεσιών

Γ.3 ISO και IEC

Πίνακας Γ.13 – Κυβερνοασφάλεια

Αναφορά	Τίτλος
ITU-T X.1200 –	Σειρά X: Δίκτυα Δεδομένων, Επικοινωνίες και Ασφάλεια Ανοικτών Συστημάτων, Ασφάλεια Τηλεπικοινωνιών - Ασφάλεια στον κυβερνοχώρο

X.1299 Series	
ITU-T X.1205	Σειρά Χ: Δίκτυα Δεδομένων, Επικοινωνίες και Ασφάλεια Ανοικτών Συστημάτων, Ασφάλεια Τηλεπικοινωνιών - Επισκόπηση της Κυβερνοασφάλειας

Πίνακας Γ.14 – Διαχείριση συνέχειας και συμβάντων

Αναφορά	Τίτλος
ITU-T X.1206	Σειρά Χ: Δίκτυα Δεδομένων, Επικοινωνίες και Ασφάλεια Ανοικτών Συστημάτων, Ασφάλεια Τηλεπικοινωνιών - Ένα ουδέτερο πρότυπο προμηθευτών για την αυτόματη κοινοποίηση πληροφοριών σχετικών με την ασφάλεια και τη διάδοση ενημερώσεων

Πίνακας Γ.15 – Ανεπιθύμητο λογισμικό

Αναφορά	Τίτλος
ITU-T X.1207	Σειρά Χ: Δίκτυα Δεδομένων, Επικοινωνίες και Ασφάλεια Ανοικτών Συστημάτων, Ασφάλεια τηλεπικοινωνιών - Κατευθυντήριες γραμμές για τους παρόχους τηλεπικοινωνιακών υπηρεσιών για την αντιμετώπιση του κινδύνου από κατασκοπευτικό λογισμικό και δυνητικά ανεπιθύμητο λογισμικό

Πίνακας Γ.16 – Ανεπιθύμητη αλληλογραφία

Αναφορά	Τίτλος
ITU-T X.1231	Σειρά Χ: Δίκτυα Δεδομένων, Επικοινωνίες και Ασφάλεια Ανοικτών Συστημάτων, Ασφάλεια τηλεπικοινωνιών - Τεχνικές στρατηγικές για την αντιμετώπιση της ανεπιθύμητης αλληλογραφίας
ITU-T X.1240	Σειρά Χ: Δίκτυα Δεδομένων, Επικοινωνίες και Ασφάλεια Ανοικτών Συστημάτων, Ασφάλεια τηλεπικοινωνιών - Τεχνικές στρατηγικές για την αντιμετώπιση της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας
ITU-T X.1241	Σειρά Χ: Δίκτυα Δεδομένων, Επικοινωνίες και Ασφάλεια Ανοικτών Συστημάτων, Ασφάλεια τηλεπικοινωνιών – Τεχνικό πρότυπο για την αντιμετώπιση της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας
ITU-T X.1244	Σειρά Χ: Δίκτυα Δεδομένων, Επικοινωνίες και Ασφάλεια Ανοικτών Συστημάτων, Ασφάλεια τηλεπικοινωνιών - Γενικές πτυχές της αντιμετώπισης της ανεπιθύμητης αλληλογραφίας σε εφαρμογές πολυμέσων βασισμένες σε ΠΔ

Πίνακας Γ.17 – Ανταλλαγή πληροφοριών για την Κυβερνοασφάλεια

Αναφορά	Τίτλος
ITU-T X.1500 –X.1598 Series (CYBEX)	Σειρά Χ: Δίκτυα Δεδομένων, Επικοινωνίες και Ασφάλεια Ανοικτών Συστημάτων, Ασφάλεια τηλεπικοινωνιών - Ανταλλαγή πληροφοριών για την Κυβερνοασφάλεια

ΣΗΜΕΙΩΣΗ: Από τον Σεπτέμβριο του 2011, καθώς οι εργασίες του CYBEX βρίσκονται σε εξέλιξη στην ITU-T, μόνο τα X.1500, X.1520, X.1521 και X.1570 είναι διαθέσιμα ως συστάσεις ή σχέδια. Αρκετές άλλες θα ακολουθήσουν στο μέλλον, οπότε συνιστάται στους χρήστες να ελέγχουν τον δικτυακό τόπο της ITU-T για τις τελευταίες διαθέσιμες πληροφορίες.

Παράρτημα Δ – ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜΩΝ 4577 – 3 ΔΕΚΕΜΒΡΙΟΥ 2018

Γ.1 Εισαγωγή

Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις.

ΚΕΦΑΛΑΙΟ Α΄ ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 1 Αντικείμενο και πεδίο εφαρμογής (άρθρο 1 παράγραφοι 1, 3, 4, 5, 6, 7 της Οδηγίας 2016/1148/ΕΕ)

1. Σκοπός του παρόντος είναι η ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 6ης Ιουλίου 2016 (ΕΕ L 194), με την οποία θεσπίζονται μέτρα για την επίτευξη υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών.

2. Οι απαιτήσεις ασφάλειας και κοινοποίησης που προβλέπονται στον παρόντα νόμο δεν εφαρμόζονται σε επιχειρήσεις που πληρούν τις προϋποθέσεις της παρ. 1 του άρθρου 33 του ν. 4070/2012 (Α΄ 82) ή σε παρόχους υπηρεσιών εμπιστοσύνης που εμπίπτουν στο άρθρο 19 του Κανονισμού (ΕΕ) 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 (ΕΕL 257).

3. Ο παρών νόμος εφαρμόζεται με την επιφύλαξη των διατάξεων του π.δ. 39/2011 (Α΄ 104) και των νόμων 4267/2014 (Α΄ 137) και 4360/2016 (Α΄ 9).

4. Με την επιφύλαξη του άρθρου 346 της Συνθήκης Λειτουργίας της Ευρωπαϊκής Ένωσης (ΣΛΕΕ), πληροφορίες που είναι απόρρητες σύμφωνα με ενωσιακούς και εθνικούς κανόνες, όπως κανόνες περί επιχειρηματικού απορρήτου, ανταλλάσσονται με την Επιτροπή και άλλες αρμόδιες αρχές, μόνον εφόσον η ανταλλαγή αυτή είναι αναγκαία για την εφαρμογή του παρόντος. Οι πληροφορίες, που ανταλλάσσονται, περιορίζονται σε ό,τι είναι συναφές και αναλογικό προς το σκοπό της ανταλλαγής αυτής. Η εν λόγω ανταλλαγή πληροφοριών διαφυλάσσει το απόρρητο αυτών των πληροφοριών και προστατεύει τα συμφέροντα ασφάλειας και τα εμπορικά συμφέροντα των φορέων εκμετάλλευσης βασικών υπηρεσιών και των παρόχων ψηφιακών υπηρεσιών.

5. Με τον παρόντα δεν θίγονται τα μέτρα που λαμβάνει η χώρα μας για τη διαφύλαξη των ουσιωδών κρατικών λειτουργιών και ιδίως για τη διαφύλαξη της εθνικής ασφάλειας, συμπεριλαμβανομένων των μέτρων για την προστασία πληροφοριών, των οποίων η διάδοση θεωρείται αντίθετη προς τα ουσιώδη συμφέροντα ασφάλειας, καθώς και για τη διατήρηση του νόμου και της τάξης και ιδίως για τη διευκόλυνση της διερεύνησης, της ανίχνευσης και της δίωξης ποινικών αδικημάτων.

6. Αν μία τομεακή νομική πράξη της Ευρωπαϊκής Ένωσης απαιτεί από τους φορείς εκμετάλλευσης βασικών υπηρεσιών ή τους παρόχους ψηφιακών υπηρεσιών είτε να εξασφαλίζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών τους είτε να κοινοποιούν συμβάντα, εφαρμόζονται οι διατάξεις της εν λόγω τομεακής νομικής πράξης, υπό την προϋπόθεση ότι οι εν λόγω απαιτήσεις είναι τουλάχιστον ισοδύναμες ως προς το αποτέλεσμα με τις υποχρεώσεις που θεσπίζονται στον παρόντα νόμο.

Άρθρο 2 (Άρθρο 2 της Οδηγίας 2016/1148/ΕΕ)

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, που γίνεται κατά τον παρόντα νόμο, διενεργείται σύμφωνα με τον Κανονισμό (ΕΚ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (ΕΕ L 119) και το ν. 2472/1997 (Α΄ 50).

Άρθρο 3 Ορισμοί (Άρθρο 4 της Οδηγίας 2016/1148/ΕΕ)

Για τους σκοπούς του παρόντος νόμου, ισχύουν οι εξής ορισμοί:

1) «σύστημα δικτύου και πληροφοριών»:

α) ένα δίκτυο ηλεκτρονικών επικοινωνιών, σύμφωνα με την περίπτωση ιζ΄ της Ενότητας Α΄ παράγραφος του άρθρου 2 του ν. 4070/2012,

β) κάθε συσκευή ή ομάδα διασυνδεδεμένων ή σχετιζόμενων συσκευών από τις οποίες μία ή περισσότερες εκτελούν, βάσει προγράμματος, αυτόματη επεξεργασία ψηφιακών δεδομένων,

γ) ψηφιακά δεδομένα που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται από στοιχεία που καλύπτονται στις περιπτώσεις α΄ και β΄ για τους σκοπούς της λειτουργίας, της χρήσης, της προστασίας και της συντήρησής τους,

2) «ασφάλεια συστημάτων δικτύου και πληροφοριών»: η ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται, με δεδομένο βαθμό αξιοπιστίας, σε ενέργειες που πλήττουν τη διαθεσιμότητα, την αυθεντικότητα, την ακεραιότητα ή το απόρρητο των δεδομένων που αποθηκεύονται, μεταδίδονται ή υποβάλλονται σε επεξεργασία ή των συναφών υπηρεσιών που προσφέρονται ή είναι προσβάσιμες μέσω των εν λόγω συστημάτων δικτύου και πληροφοριών,

3) «εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών»: πλαίσιο το οποίο παρέχει στρατηγικούς στόχους και προτεραιότητες για την ασφάλεια συστημάτων δικτύου και πληροφοριών σε εθνικό επίπεδο,

4) «φορέας εκμετάλλευσης βασικών υπηρεσιών»: δημόσια ή ιδιωτική οντότητα είδους αναφερόμενου στο Παράρτημα Ι, η οποία πληροί τα κριτήρια που ορίζονται στην παράγραφο 2 του άρθρου 4,

5) «ψηφιακή υπηρεσία»: υπηρεσία σύμφωνα με την περίπτωση β΄ της παρ. 1 του άρθρου 2 του π.δ. 81/2018 (Α΄ 151), η οποία είναι είδος αναφερόμενο στο Παράρτημα ΙΙ,

6) «πάροχος ψηφιακών υπηρεσιών»: νομικό πρόσωπο που παρέχει ψηφιακή υπηρεσία,

7) «συμβάν»: κάθε γεγονός που έχει στην πραγματικότητα μια δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών,

8) «χειρισμός συμβάντων»: το σύνολο των διαδικασιών που υποστηρίζουν τον εντοπισμό, την ανάλυση και την ανάσχεση ενός συμβάντος, καθώς και την παρέμβαση για την αντιμετώπισή του,

9) «κίνδυνος»: κάθε εύλογα διαπιστώσιμη περίσταση ή γεγονός με ενδεχομένως δυσμενή επίπτωση στην ασφάλεια συστημάτων δικτύου και πληροφοριών,

10) «αντιπρόσωπος»: κάθε φυσικό ή νομικό πρόσωπο εγκατεστημένο στην Ευρωπαϊκή Ένωση, που ρητώς έχει οριστεί να ενεργεί εξ ονόματος παρόχου ψηφιακών υπηρεσιών μη εγκατεστημένου στην Ευρωπαϊκή Ένωση, στο οποίο μπορεί να απευθύνεται η εθνική αρμόδια αρχή ή η Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team - CSIRT) του άρθρου 8 παράγραφος 1 αντί του παρόχου ψηφιακών υπηρεσιών, όσον αφορά τις υποχρεώσεις αυτού σύμφωνα με τον παρόντα νόμο,

11) «πρότυπο»: πρότυπο σύμφωνα με το σημείο 1 του άρθρου 2 του Κανονισμού (ΕΕ) 1025/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 25ης Οκτωβρίου 2012 (ΕΕ L 316),

12) «προδιαγραφή»: τεχνική προδιαγραφή σύμφωνα με το σημείο 4 του άρθρου 2 του Κανονισμού (ΕΕ) 1025/2012,

13) «σημείο ανταλλαγής κίνησης διαδικτύου (Internet Exchange Point - IXP)»: δικτυακή υποδομή που επιτρέπει τη διασύνδεση περισσότερων από δύο ανεξάρτητων αυτόνομων συστημάτων, κυρίως με σκοπό τη διευκόλυνση της ανταλλαγής κίνησης διαδικτύου, και η οποία διασυνδέει μόνον αυτόνομα συστήματα. Το IXP δεν αναγκάζει την κίνηση διαδικτύου που διέρχεται μεταξύ ζεύγους συμμετεχόντων αυτόνομων συστημάτων να διέλθει από τρίτο αυτόνομο σύστημα ούτε την τροποποιεί ούτε παρεμβαίνει με άλλον τρόπο σε αυτήν,

14) «σύστημα ονομάτων χώρου (Domain Name System - DNS)»: ιεραρχικά κατανεμημένο σύστημα ονοματοδοσίας εντός ενός δικτύου, το οποίο εκτελεί παραπομπές αιτημάτων για ονόματα τομέων,

15) «πάροχος υπηρεσιών συστήματος ονομάτων χώρου»: οντότητα που παρέχει υπηρεσίες συστήματος ονομάτων χώρου στο διαδίκτυο,

16) «μητρώο ονομάτων χώρου ανώτατου επιπέδου» (top-level domain name registry): οντότητα που διαχειρίζεται και εκμεταλλεύεται την καταχώριση ονομάτων διαδικτυακών χώρων εντός συγκεκριμένου χώρου ανώτατου επιπέδου (TLD),

17) «επιγραμμική αγορά» (online marketplace): ψηφιακή υπηρεσία που επιτρέπει σε καταναλωτές ή και εμπόρους, όπως ορίζονται στις περιπτώσεις α΄ και β΄ της παρ. 1 του άρθρου 4 της 70330οικ./30.6.2015 κοινής απόφασης των Υπουργών Οικονομίας, Υποδομών, Ναυτιλίας και Τουρισμού και Δικαιοσύνης, Διαφάνειας και Ανθρώπινων Δικαιωμάτων (Β΄ 1421), να συνάπτουν επιγραμμικές συμβάσεις πώλησης ή παροχής υπηρεσιών με εμπόρους είτε στον ιστοχώρο της επιγραμμικής αγοράς είτε σε ιστοχώρο εμπόρου που χρησιμοποιεί υπηρεσίες υπολογιστικής παρεχόμενες από την επιγραμμική αγορά,

18) «επιγραμμική μηχανή αναζήτησης» (online search engine): ψηφιακή υπηρεσία που επιτρέπει στους χρήστες να εκτελούν αναζητήσεις καταρχήν σε όλους τους ιστοχώρους ή σε ιστοχώρους συγκεκριμένης γλώσσας βάσει ερωτήματος για οποιοδήποτε θέμα, με τη μορφή λέξης-κλειδιού, φράσης ή άλλων δεδομένων, και επιστρέφει ως αποτέλεσμα συνδέσμους όπου μπορεί κανείς να βρει πληροφορίες σχετικές με το περιεχόμενο που έχει ζητηθεί,

19) «υπηρεσία νεφοϋπολογιστικής»: ψηφιακή υπηρεσία που επιτρέπει την πρόσβαση σε κλιμακοθετήσιμο και ελαστικό σύνολο κοινόχρηστων υπολογιστικών πόρων.

Άρθρο 4 Φορείς εκμετάλλευσης βασικών υπηρεσιών (Άρθρο 5 της Οδηγίας 2016/1148/ΕΕ)

1. Η Εθνική Αρχή Κυβερνοασφάλειας της παραγράφου 1 του άρθρου 7, σε συνεργασία με τις ανά τομέα βασικής υπηρεσίας αρμόδιες ρυθμιστικές/εποπτικές αρχές και λοιπούς εμπλεκόμενους εθνικούς φορείς, προσδιορίζει, για κάθε τομέα και υποτομέα του Παραρτήματος Ι, τους φορείς εκμετάλλευσης βασικών υπηρεσιών που είναι εγκατεστημένοι στην Ελληνική Επικράτεια.

Με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, ύστερα από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας, ορίζονται οι φορείς εκμετάλλευσης βασικών υπηρεσιών.

2. Τα κριτήρια για τον προσδιορισμό των φορέων εκμετάλλευσης βασικών υπηρεσιών της περίπτωσης 4 του άρθρου 3 είναι τα εξής:

α) ο φορέας να παρέχει υπηρεσία ουσιώδη για τη διατήρηση κρίσιμων κοινωνικών ή και οικονομικών δραστηριοτήτων,

β) η παροχή της υπηρεσίας αυτής να στηρίζεται σε συστήματα δικτύου και πληροφοριών και

γ) η πρόκληση σοβαρής διατάραξης της παροχής της εν λόγω υπηρεσίας, κατά τα οριζόμενα στο άρθρο 5, από τυχόν συμβάν.

3. Για τους σκοπούς της παραγράφου 1, η Εθνική Αρχή Κυβερνοασφάλειας καταρτίζει κατάλογο τόσο των βασικών υπηρεσιών όσο και των φορέων εκμετάλλευσής τους. Οι κατάλογοι αυτοί επανεξετάζονται σε τακτική βάση, τουλάχιστον ανά διετία και, εφόσον κριθεί αναγκαίο, επικαιροποιούνται.

4. Για τους σκοπούς της παραγράφου 1, όταν φορέας εκμετάλλευσης βασικών υπηρεσιών παρέχει και σε άλλο ή άλλα κράτη-μέλη της ΕΕ υπηρεσία που αναφέρεται στην παράγραφο 2, η Εθνική Αρχή Κυβερνοασφάλειας διαβουλεύεται με τις αντίστοιχες αρχές του ή των άλλων κρατών-μελών πριν από τη λήψη απόφασης για τον προσδιορισμό του.

5. Η Εθνική Αρχή Κυβερνοασφάλειας της παραγράφου 1 του άρθρου 7 υποβάλλει στην Επιτροπή ανά διετία τις πληροφορίες που είναι αναγκαίες για την αξιολόγηση της εφαρμογής της Οδηγίας που ενσωματώνεται με τον παρόντα νόμο. Στις πληροφορίες αυτές περιλαμβάνονται τουλάχιστον τα εξής:

α) τα εθνικά κριτήρια βάσει των οποίων προσδιορίζονται οι φορείς εκμετάλλευσης βασικών υπηρεσιών,

β) ο κατάλογος των υπηρεσιών που αναφέρεται στην παράγραφο 3,

γ) ο αριθμός των φορέων εκμετάλλευσης βασικών υπηρεσιών που έχουν προσδιοριστεί για κάθε τομέα του Παραρτήματος Ι και αναφορά της σημασίας τους σε σχέση με τον εν λόγω τομέα,

δ) τα κατώτατα όρια, εφόσον υπάρχουν, για τον προσδιορισμό του σχετικού επιπέδου παροχής υπηρεσιών με αναφορά στον αριθμό των χρηστών που εξαρτώνται από την υπηρεσία αυτή, όπως αναφέρεται στην περίπτωση α΄ της παραγράφου 2 του άρθρου 5, ή της σημασίας του συγκεκριμένου φορέα εκμετάλλευσης βασικών υπηρεσιών, όπως αναφέρεται στην περίπτωση στ΄ της παραγράφου 2 του άρθρου 5.

Άρθρο 5 Σοβαρή διατάραξη (Άρθρο 6 της Οδηγίας 2016/1148/ΕΕ)

1. Η Εθνική Αρχή Κυβερνοασφάλειας της παραγράφου 1 του άρθρου 7 σε συνεργασία με τις, ανά τομέα βασικής υπηρεσίας, αρμόδιες ρυθμιστικές ή εποπτικές αρχές και λοιπούς εμπλεκόμενους εθνικούς φορείς, καθορίζει τα κριτήρια προσδιορισμού ενός συμβάντος ως σοβαρής διατάραξης.

2. Κατά τον προσδιορισμό της σοβαρότητας της διατάραξης που αναφέρεται στην περίπτωση γ΄ της παραγράφου 2 του άρθρου 4 λαμβάνονται υπόψη τουλάχιστον οι εξής παράγοντες:

α) ο αριθμός των χρηστών που εξαρτώνται από την υπηρεσία, η οποία παρέχεται από τον οικείο φορέα εκμετάλλευσης,

β) η εξάρτηση άλλων τομέων που αναφέρονται στο Παράρτημα Ι από την υπηρεσία που παρέχεται από τον εν λόγω φορέα εκμετάλλευσης,

γ) ο αντίκτυπος που θα μπορούσαν να έχουν τα συγκεκριμένα περιστατικά διατάραξης, από άποψη βαθμού και διάρκειας, σε οικονομικές και κοινωνικές δραστηριότητες ή στη δημόσια ασφάλεια,

δ) το μερίδιο αγοράς του οικείου φορέα εκμετάλλευσης,

ε) το γεωγραφικό εύρος της περιοχής που θα μπορούσε να επηρεαστεί από ένα περιστατικό,

στ) η σημασία του εν λόγω φορέα για τη διατήρηση επαρκούς επιπέδου της υπηρεσίας, λαμβανομένων υπόψη των διαθέσιμων εναλλακτικών μέσων για την παροχή της εν λόγω υπηρεσίας,

ζ) οι ειδικότεροι παράγοντες που αφορούν το συγκεκριμένο τομέα.

ΚΕΦΑΛΑΙΟ Β΄ ΕΘΝΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΔΙΚΤΥΩΝ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ

Άρθρο 6 Εθνική Στρατηγική Κυβερνοασφάλειας (Άρθρο 7 της Οδηγίας 2016/1148/ΕΕ)

1. Η Εθνική Αρχή Κυβερνοασφάλειας επικαιροποιεί την «Εθνική Στρατηγική Κυβερνοασφάλειας» που έχει εγκριθεί με την υπουργική απόφαση 3218/2018 του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης (ΑΔΑ: Ψ4Ρ7465ΧΘ0-Ζ6Ω) και την κοινοποιεί στην Επιτροπή μέσα σε τρεις (3) μήνες από την έγκρισή της από τον Υπουργό Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης.

Από την κοινοποίηση αυτή εξαιρούνται στοιχεία της στρατηγικής που συνδέονται με την εθνική ασφάλεια. Η Εθνική Αρχή Κυβερνοασφάλειας, στο πλαίσιο των αρμοδιοτήτων της και για τις ανάγκες της παραγράφου αυτής, μπορεί να συνεργάζεται με τις αρμόδιες ρυθμιστικές/εποπτικές αρχές και τους λοιπούς εμπλεκόμενους εθνικούς φορείς.

2. Η Εθνική Στρατηγική Κυβερνοασφάλειας, η οποία αποτελεί την εθνική στρατηγική για την ασφάλεια συστημάτων δικτύου και πληροφοριών, περιλαμβάνει τα εξής:

α) τους στόχους και τις προτεραιότητες της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύου και πληροφοριών,

β) το πλαίσιο διακυβέρνησης για την επίτευξη των στόχων και των προτεραιοτήτων της εθνικής στρατηγικής για την ασφάλεια συστημάτων δικτύων και πληροφοριών, συμπεριλαμβανομένων του ρόλου και των αρμοδιοτήτων των κυβερνητικών οργάνων και των λοιπών αρμόδιων φορέων,

γ) τον προσδιορισμό των μέτρων ετοιμότητας, απόκρισης και αποκατάστασης, συμπεριλαμβανομένης της συνεργασίας ανάμεσα στο δημόσιο και ιδιωτικό τομέα,

δ) αναφορά των προγραμμάτων εκπαίδευσης, ευαισθητοποίησης και κατάρτισης σε σχέση με την εθνική στρατηγική ασφάλειας δικτύων και συστημάτων πληροφοριών,

ε) αναφορά των σχεδίων έρευνας και ανάπτυξης σχετικά με την εθνική στρατηγική ασφάλειας συστημάτων δικτύου και πληροφοριών,

στ) σχέδιο εκτίμησης κινδύνου για τον προσδιορισμό κινδύνων,

ζ) κατάλογο των διαφόρων φορέων που εμπλέκονται στην υλοποίηση της εθνικής στρατηγικής ασφάλειας συστημάτων δικτύου και πληροφοριών.

Άρθρο 7 Εθνική Αρχή Κυβερνοασφάλειας (Άρθρο 8 της Οδηγίας 2016/1148/ΕΕ)

1. Ως Εθνική Αρμόδια Αρχή για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, εφεξής «Αρμόδια Αρχή» ή «Εθνική Αρχή Κυβερνοασφάλειας», ορίζεται η Διεύθυνση Κυβερνοασφάλειας της Γενικής Γραμματείας Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης (άρθρο 15 του π.δ. 82/2017, Α΄ 117). Η Εθνική Αρχή καλύπτει τους τομείς που αναφέρονται στο Παράρτημα Ι και τις υπηρεσίες που αναφέρονται στο Παράρτημα ΙΙ.

2. Η Εθνική Αρχή Κυβερνοασφάλειας:

α) παρακολουθεί την εφαρμογή του παρόντος,

β) ορίζεται ως το εθνικό ενιαίο κέντρο επαφής, εφεξής «Ενιαίο Κέντρο Επαφής», για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, ασκώντας καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών των κρατών-μελών, καθώς και με τις Αρμόδιες Αρχές άλλων κρατών-μελών στο πλαίσιο των μηχανισμών συνεργασίας, όπως αυτοί προσδιορίζονται στα άρθρα 11 και 12 της Οδηγίας που ενσωματώνεται με τον παρόντα,

γ) ως ενιαίο κέντρο επαφής υποβάλλει ετησίως στην ομάδα συνεργασίας του άρθρου 11 της ανωτέρω Οδηγίας, συνοπτική έκθεση σχετικά με τις κοινοποιήσεις που έχει παραλάβει, συμπεριλαμβανομένου του αριθμού των κοινοποιήσεων και της φύσης των κοινοποιημένων συμβάντων, καθώς και τα μέτρα που έχουν ληφθεί σύμφωνα με τα άρθρα 9 και 11,

δ) συνεργάζεται με την αρμόδια CSIRT της παραγράφου 1 του άρθρου 8, με σκοπό την αμοιβαία και από κοινού τήρηση των υποχρεώσεων της χώρας στο πλαίσιο του παρόντος νόμου,

ε) διαβουλεύεται και συνεργάζεται με τις Αρμόδιες Εθνικές Αρχές επιβολής του νόμου, την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), καθώς και τις λοιπές αρμόδιες ρυθμιστικές ή εποπτικές αρχές και τους λοιπούς εμπλεκόμενους εθνικούς φορείς αναφορικά με τα θέματα που άπτονται της εφαρμογής του παρόντος,

στ) συνεργάζεται με τις Αρμόδιες Αρχές των λοιπών κρατών-μελών, στο πλαίσιο των μηχανισμών συνεργασίας, όπως αυτοί προσδιορίζονται στα άρθρα 11 και 12 της Οδηγίας που ενσωματώνεται με τον παρόντα νόμο,

ζ) συμμετέχει στην ομάδα συνεργασίας του άρθρου 11 της ως άνω Οδηγίας, ορίζει τους εθνικούς αντιπροσώπους της χώρας σ΄ αυτήν και ενημερώνει τους λοιπούς εμπλεκόμενους εθνικούς φορείς αναφορικά με τις εργασίες και τις αποφάσεις που λαμβάνονται στο πλαίσιο αυτής,

η) συνεργάζεται με σχετικούς με θέματα κυβερνοασφάλειας και προστασίας κρίσιμων υποδομών διεθνείς οργανισμούς και όργανα ή υπηρεσίες της Ευρωπαϊκής Ένωσης ή άλλων κρατών και συμμετέχει στις αντίστοιχες συναντήσεις συναφών με τα ανωτέρω, επιτροπών και ομάδων εργασίας.

3. Ο ορισμός της Αρμόδιας Αρχής και του ενιαίου κέντρου επαφής, τα καθήκοντά τους, καθώς και κάθε μεταγενέστερη σχετική τροποποίηση δημοσιοποιούνται και κοινοποιούνται, χωρίς καθυστέρηση, στην Επιτροπή.

Άρθρο 8 Ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT) (Άρθρο 9 της Οδηγίας 2016/1148/ΕΕ)

1. Αρμόδια Ομάδα Απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Team - CSIRT εφεξής «αρμόδια CSIRT»), η οποία καλύπτει τους τομείς του Παραρτήματος Ι και τις υπηρεσίες του Παραρτήματος ΙΙ του παρόντος, και είναι υπεύθυνη για το χειρισμό κινδύνων και συμβάντων βάσει επακριβώς καθορισμένης διαδικασίας, είναι η Διεύθυνση Κυβερνοάμυνας του ΓΕΕΘΑ.

2. Η αρμόδια CSIRT:

α) εξασφαλίζει υψηλό επίπεδο διαθεσιμότητας των υπηρεσιών επικοινωνιών της, αποφεύγοντας μοναδικά σημεία αστοχίας και διαθέτει διάφορους τρόπους για εισερχόμενη και εξερχόμενη επικοινωνία με τρίτους ανά πάσα στιγμή. Επιπλέον, οι δίαυλοι επικοινωνίας είναι σαφώς προσδιορισμένοι και ευρύτερα γνωστοί στα μέλη της περιοχής ευθύνης και τους συνεργαζόμενους εταίρους,

β) τα γραφεία της και τα υποστηρικτικά συστήματα πληροφοριών εγκαθίστανται σε ασφαλείς χώρους,

γ) αναφορικά με τη συνέχεια της επιχειρησιακής δραστηριότητάς της, η αρμόδια CSIRT:

αα) είναι εφοδιασμένη με κατάλληλο σύστημα διαχείρισης και δρομολόγησης αιτημάτων, προκειμένου να διευκολύνεται η παράδοση καθηκόντων,

ββ) είναι επαρκώς στελεχωμένη ώστε να εξασφαλίζεται η διαθεσιμότητα ανά πάσα στιγμή,

γγ) βασίζεται σε υποδομή, η συνέχεια της οποίας είναι διασφαλισμένη. Για τον σκοπό αυτό, διατίθενται πλεονάζοντα συστήματα και εφεδρικοί χώροι εργασίας,

δ) συμμετέχει σε διεθνή δίκτυα συνεργασίας.

3. Οι αρμοδιότητες της αρμόδιας CSIRT είναι οι εξής:

α) η παρακολούθηση συμβάντων σε εθνικό επίπεδο,

β) η παροχή έγκαιρων προειδοποιήσεων, ειδοποιήσεων επαγρύπνησης και ανακοινώσεων, καθώς και η διάδοση πληροφοριών σε ενδιαφερόμενους φορείς σχετικά με κινδύνους και συμβάντα,

γ) η παρέμβαση σε περίπτωση συμβάντος,

δ) η παροχή δυναμικής ανάλυσης κινδύνων και συμβάντων, καθώς και η επίγνωση της κατάστασης,

ε) η συμμετοχή στο δίκτυο CSIRT και η συνεργασία με τις αντίστοιχες υπηρεσίες των υπόλοιπων κρατών - μελών στο πλαίσιο του δικτύου CSIRT του άρθρου 12 της Οδηγίας που ενσωματώνεται με τον παρόντα νόμο,

στ) η λήψη των κοινοποιήσεων συμβάντων που υποβάλλονται σύμφωνα με τον παρόντα νόμο,

ζ) η ενημέρωση του Εθνικού Ενιαίου Κέντρου Επαφής της περίπτωσης β΄ της παραγράφου 2 του άρθρου 7, σχετικά με τις κοινοποιήσεις των συμβάντων που υποβάλλονται σύμφωνα με τον παρόντα νόμο,

η) η εγκαθίδρυση σχέσεων συνεργασίας με τον ιδιωτικό τομέα,

θ) η προώθηση, η υιοθέτηση και η χρήση κοινών ή τυποποιημένων πρακτικών για:

αα) τις διαδικασίες χειρισμού συμβάντων και κινδύνων,

ββ) τα συστήματα ταξινόμησης συμβάντων, κινδύνων και πληροφοριών.

4. Συνεργάζεται με την Εθνική Αρχή Κυβερνοασφάλειας της παραγράφου 1 του άρθρου 7, με σκοπό την αμοιβαία και από κοινού τήρηση των υποχρεώσεων της χώρας στο πλαίσιο του παρόντος.

ΚΕΦΑΛΑΙΟ Γ΄ ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΔΙΚΤΥΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΤΩΝ ΦΟΡΕΩΝ ΕΚΜΕΤΑΛΛΕΥΣΗΣ ΒΑΣΙΚΩΝ ΥΠΗΡΕΣΙΩΝ

Άρθρο 9 Απαιτήσεις ασφάλειας και κοινοποίηση συμβάντων (Άρθρο 14 της Οδηγίας 2016/1148/ΕΕ)

1. Η Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με την αρμόδια CSIRT και τους λοιπούς, ανά τομέα βασικής υπηρεσίας, εμπλεκόμενους φορείς:

α) αξιολογεί τα τεχνικά και οργανωτικά μέτρα που λαμβάνουν οι φορείς εκμετάλλευσης βασικών υπηρεσιών για τη διαχείριση των κινδύνων που αφορούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στις δραστηριότητές τους, ως προς την καταλληλότητα και την αναλογικότητά τους,

β) αξιολογεί την καταλληλότητα των μέτρων που λαμβάνουν οι φορείς εκμετάλλευσης βασικών υπηρεσιών για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή των βασικών υπηρεσιών, με σκοπό τη διασφάλιση της επιχειρησιακής συνέχειάς τους,

γ) καθορίζει τη διαδικασία κοινοποίησης που πρέπει να τηρούν οι φορείς εκμετάλλευσης βασικών υπηρεσιών, προκειμένου να κοινοποιήσουν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT συμβάντα με σοβαρές επιπτώσεις στην επιχειρησιακή συνέχεια των βασικών υπηρεσιών που αυτοί παρέχουν. Οι ανωτέρω κοινοποιήσεις εκ μέρους των φορέων εκμετάλλευσης βασικών υπηρεσιών πρέπει να πραγματοποιούνται χωρίς αδικαιολόγητη καθυστέρηση και να περιλαμβάνουν πληροφορίες που να επιτρέπουν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT να προσδιορίσουν τόσο τη σοβαρότητα όσο και τις διασυνοριακές επιπτώσεις, λόγω του κοινοποιούμενου περιστατικού. Η κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη για τον κοινοποιούντα.

2. Για να προσδιοριστεί η σοβαρότητα του αντίκτυπου ενός συμβάντος, λαμβάνονται υπόψη ειδικότερα οι εξής παράμετροι:

α) ο αριθμός των χρηστών που επηρεάζονται από τη διατάραξη της βασικής υπηρεσίας,

β) η διάρκεια του συμβάντος,

γ) το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν.

3. Βάσει των πληροφοριών που παρέχονται στην κοινοποίηση από το φορέα εκμετάλλευσης βασικών υπηρεσιών, η Εθνική Αρχή Κυβερνοασφάλειας ενημερώνει το ή τα άλλα επηρεαζόμενα κράτη-μέλη, εφόσον το κοινοποιούμενο συμβάν έχει σοβαρό αντίκτυπο στην επιχειρησιακή συνέχεια των βασικών υπηρεσιών στο εν λόγω κράτος-μέλος. Στο πλαίσιο της ανωτέρω ενημέρωσης, διαφυλάσσεται, σύμφωνα με το ενωσιακό δίκαιο ή με την εθνική νομοθεσία, η ασφάλεια και τα εμπορικά συμφέροντα του κοινοποιούντος φορέα εκμετάλλευσης βασικών υπηρεσιών, καθώς και το απόρρητο των πληροφοριών που έχουν παρασχεθεί στην κοινοποίησή του.

Όταν οι περιστάσεις το επιτρέπουν, η Εθνική Αρχή Κυβερνοασφάλειας ή η αρμόδια CSIRT παρέχει στον κοινοποιούντα φορέα εκμετάλλευσης βασικών υπηρεσιών πληροφορίες όσον αφορά τις ενέργειες που έλαβαν χώρα σε συνέχεια της κοινοποίησής του, όπως πληροφορίες που θα μπορούσαν να υποστηρίξουν την αποτελεσματική διαχείριση του περιστατικού.

Μετά από αίτηση της αρμόδιας αρχής ή του CSIRT, το ενιαίο κέντρο επαφής διαβιβάζει τις κοινοποιήσεις συμβάντων που αναφέρονται στο πρώτο εδάφιο της παρούσας στα ενιαία κέντρα επαφής των άλλων επηρεαζόμενων κρατών-μελών.

4. Ύστερα από διαβούλευση με τον κοινοποιούντα φορέα εκμετάλλευσης βασικών υπηρεσιών, η Εθνική Αρχή Κυβερνοασφάλειας μπορεί να ενημερώνει το κοινό σχετικά με μεμονωμένα συμβάντα, αν η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη μελλοντικού συμβάντος ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη.

5. Η Εθνική Αρχή Κυβερνοασφάλειας μπορεί να καταρτίζει και να εκδίδει κατευθυντήριες γραμμές σχετικά με τις περιστάσεις υπό τις οποίες οι φορείς εκμετάλλευσης βασικών υπηρεσιών είναι υποχρεωμένοι να κοινοποιούν συμβάντα, συμπεριλαμβανομένων μεταξύ άλλων των παραμέτρων που προσδιορίζουν τη σοβαρότητα των επιπτώσεων ενός συμβάντος, όπως αυτές αναφέρονται στην παράγραφο 2.

Άρθρο 10 Εφαρμογή και επιβολή (Άρθρο 15 της Οδηγίας 2016/1148/ΕΕ)

1. Η Εθνική Αρχή Κυβερνοασφάλειας:

α) αξιολογεί τη συμμόρφωση των φορέων εκμετάλλευσης βασικών υπηρεσιών προς τις υποχρεώσεις τους, σύμφωνα με το άρθρο 9 και των επιπτώσεών τους στην ασφάλεια των συστημάτων δικτύου και πληροφοριών,

β) απαιτεί από τους φορείς εκμετάλλευσης βασικών υπηρεσιών να παρέχουν:

αα) τις απαραίτητες πληροφορίες για την εκτίμηση της ασφάλειας των συστημάτων δικτύου και των πληροφοριών τους, συμπεριλαμβανομένων, μεταξύ άλλων, τεκμηριωμένων και εγκεκριμένων πολιτικών ασφάλειας,

ββ) στοιχεία που να αποδεικνύουν την ουσιαστική εφαρμογή πολιτικών ασφάλειας, όπως τα αποτελέσματα επιθεώρησης ασφάλειας που έχει διενεργηθεί είτε από την Εθνική Αρχή Κυβερνοασφάλειας είτε από εξουσιοδοτημένο από αυτήν όργανο και, στη δεύτερη αυτή περίπτωση, να θέτουν τα αποτελέσματά τους, καθώς και όλα τα σχετικά στοιχεία στη διάθεση της Εθνικής Αρχής Κυβερνοασφάλειας.

Όταν ζητούνται αυτές οι πληροφορίες ή τα στοιχεία, η Εθνική Αρχή Κυβερνοασφάλειας δηλώνει τον σκοπό του αιτήματος και προσδιορίζει τις ειδικότερες πληροφορίες που ζητούνται.

2. Μετά την αξιολόγηση των πληροφοριών ή των αποτελεσμάτων των επιθεωρήσεων ασφάλειας που αναφέρονται στην περίπτωση β΄ της παραγράφου 1, η Εθνική Αρχή Κυβερνοασφάλειας μπορεί να εκδίδει δεσμευτικές οδηγίες προς τους φορείς εκμετάλλευσης βασικών υπηρεσιών για την αποκατάσταση των εντοπισμένων ελλείψεων.

3. Κατά την αντιμετώπιση συμβάντων που οδηγούν σε παραβιάσεις προσωπικών δεδομένων, συνεργάζεται με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

4. Με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, ύστερα από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας καθορίζονται η μεθοδολογία αξιολόγησης της περίπτωσης α΄ και η διαδικασία παροχής πληροφοριών της περίπτωσης β΄ της παραγράφου 1.

ΚΕΦΑΛΑΙΟ Δ΄ ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ΔΙΚΤΥΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ ΤΩΝ ΠΑΡΟΧΩΝ ΨΗΦΙΑΚΩΝ ΥΠΗΡΕΣΙΩΝ

Άρθρο 11 Απαιτήσεις ασφάλειας και κοινοποίηση συμβάντων (Άρθρο 16 της Οδηγίας 2016/1148/ΕΕ)

1. Η Εθνική Αρχή Κυβερνοασφάλειας σε συνεργασία με την αρμόδια CSIRT και τους λοιπούς εμπλεκόμενους φορείς:

α) αξιολογεί τα τεχνικά και οργανωτικά μέτρα για τη διαχείριση των κινδύνων που πρέπει να λάβουν οι πάροχοι ψηφιακών υπηρεσιών, όσον αφορά την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στο πλαίσιο της παροχής, εντός της Ευρωπαϊκής Ένωσης, των υπηρεσιών του Παραρτήματος ΙΙ. Τα μέτρα αυτά πρέπει να εξασφαλίζουν επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών ανάλογο προς τον εκάστοτε κίνδυνο και να συνεκτιμούν ιδίως τα εξής στοιχεία:

αα) την ασφάλεια των συστημάτων και των εγκαταστάσεων,

ββ) τη διαχείριση συμβάντων,

γγ) τη διαχείριση της επιχειρησιακής συνέχειας,

δδ) την παρακολούθηση, τους ελέγχους και τις δοκιμές δικτύων και πληροφοριακών συστημάτων,

εε) τη συμμόρφωση με διεθνή πρότυπα,

β) αξιολογεί τα μέτρα για την αποτροπή και την ελαχιστοποίηση των επιπτώσεων συμβάντων, τα οποία πρέπει να λάβουν οι πάροχοι ψηφιακών υπηρεσιών και επηρεάζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν σε σχέση με τις υπηρεσίες του Παραρτήματος ΙΙ, οι οποίες προσφέρονται εντός της Ευρωπαϊκής Ένωσης, με σκοπό τη διασφάλιση της επιχειρησιακής συνέχειάς τους,

γ) καθορίζει τη διαδικασία κοινοποίησης που πρέπει να τηρούν οι πάροχοι ψηφιακών υπηρεσιών, προκειμένου να κοινοποιούν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT, χωρίς αδικαιολόγητη καθυστέρηση, κάθε συμβάν που έχει σημαντικές επιπτώσεις στην παροχή της υπηρεσίας, η οποία υπάγεται σε κατηγορία υπηρεσιών που αναφέρεται στο Παράρτημα ΙΙ και παρέχεται από αυτούς εντός της Ευρωπαϊκής Ένωσης. Οι ανωτέρω κοινοποιήσεις περιλαμβάνουν πληροφορίες που επιτρέπουν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT να προσδιορίσουν τόσο τη

σοβαρότητα του συμβάντος όσο και τις διασυνοριακές επιπτώσεις. Η κοινοποίηση δεν συνεπάγεται αυξημένη ευθύνη για τον κοινοποιούντα πάροχο.

2. Για να προσδιοριστεί αν οι επιπτώσεις ενός συμβάντος είναι σημαντικές, λαμβάνονται υπόψη ειδικότερα οι εξής παράμετροι:

α) ο αριθμός των χρηστών που επηρεάζονται από το συμβάν, ιδίως αυτών που εξαρτώνται από την υπηρεσία για την παροχή των δικών τους υπηρεσιών,

β) η διάρκεια του συμβάντος,

γ) το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν,

δ) το μέγεθος της διατάραξης της λειτουργίας της υπηρεσίας,

ε) η έκταση των επιπτώσεων στις οικονομικές και κοινωνικές δραστηριότητες.

Η υποχρέωση κοινοποίησης συμβάντος εφαρμόζεται μόνο αν ο πάροχος ψηφιακών υπηρεσιών έχει πρόσβαση στις πληροφορίες που απαιτούνται για να εκτιμηθεί ο αντίκτυπος του συμβάντος έναντι των παραμέτρων που αναφέρονται στις περιπτώσεις α΄ έως ε΄.

3. Όταν ένας φορέας εκμετάλλευσης βασικών υπηρεσιών εξαρτάται από τρίτο φορέα παροχής ψηφιακών υπηρεσιών για την παροχή υπηρεσίας που είναι ουσιώδης για τη διατήρηση κρίσιμων οικονομικών και κοινωνικών δραστηριοτήτων, κοινοποιείται από τον εν λόγω φορέα κάθε σοβαρή επίπτωση επί της συνέχειας των βασικών υπηρεσιών που οφείλεται σε συμβάν το οποίο επηρεάζει τον πάροχο ψηφιακών υπηρεσιών.

4. Κατά περίπτωση, και συγκεκριμένα αν το συμβάν με σημαντικές επιπτώσεις που αναφέρεται στην περίπτωση γ΄ της παραγράφου 1 αφορά δύο (2) ή περισσότερα κράτη-μέλη, η Εθνική Αρχή Κυβερνοασφάλειας ενημερώνει τα άλλα κράτη-μέλη που επηρεάζονται από το συμβάν. Στο πλαίσιο της ενημέρωσης αυτής, το ενιαίο κέντρο επαφής σε συνεργασία με την αρμόδια CSIRT πρέπει, σύμφωνα με το ενωσιακό δίκαιο και την εθνική νομοθεσία που είναι σύμφωνη προς το ενωσιακό δίκαιο, να διαφυλάσσουν την ασφάλεια και τα εμπορικά συμφέροντα του παρόχου ψηφιακών υπηρεσιών, καθώς και το απόρρητο των πληροφοριών που ο τελευταίος έχει παράσχει. Το εθνικό ενιαίο κέντρο επαφής διαβιβάζει τις κοινοποιήσεις συμβάντων που αναφέρονται στο πρώτο εδάφιο της παρούσας στα ενιαία κέντρα επαφής των άλλων επηρεαζόμενων κρατών-μελών.

5. Ύστερα από διαβούλευση με τον ενδιαφερόμενο πάροχο ψηφιακών υπηρεσιών, η Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με την αρμόδια CSIRT, και, κατά περίπτωση, οι αρμόδιες αρχές ή τα αρμόδια CSIRT άλλων ενδιαφερόμενων κρατών-μελών μπορούν να ενημερώνουν το κοινό σχετικά με μεμονωμένα συμβάντα ή να απαιτούν από τον πάροχο ψηφιακών υπηρεσιών να το πράξει, όταν η ενημέρωση του κοινού είναι απαραίτητη για την πρόληψη συμβάντος ή την αντιμετώπιση συμβάντος που βρίσκεται σε εξέλιξη ή αν η αποκάλυψη του συμβάντος εξυπηρετεί το δημόσιο συμφέρον.

6. Με την επιφύλαξη της παραγράφου 5 του άρθρου 1, δεν επιβάλλονται οποιεσδήποτε περαιτέρω υποχρεώσεις ασφάλειας ή κοινοποίησης στους παρόχους ψηφιακών υπηρεσιών.

7. Τα άρθρα 11 έως 13 δεν εφαρμόζονται σε πολύ μικρές και μικρές επιχειρήσεις, όπως αυτές ορίζονται στη σύσταση 2003/361/ΕΚ της Επιτροπής της 6ης Μαΐου 2003 (ΕΕ L 124).

Άρθρο 12 Εφαρμογή και επιβολή (Άρθρο 17 της Οδηγίας 2016/1148/ΕΕ)

1. Η Εθνική Αρχή Κυβερνοασφάλειας:

α) αξιολογεί και αναλαμβάνει δράση επιβάλλοντας τα απαραίτητα εποπτικά μέτρα, όταν της παρέχονται στοιχεία που αποδεικνύουν ότι πάροχος ψηφιακών υπηρεσιών δεν πληροί τις απαιτήσεις που ορίζονται στο άρθρο 11. Τα εν λόγω αποδεικτικά στοιχεία μπορεί να υποβάλλονται από μια αρμόδια αρχή άλλου κράτους-μέλους, στο οποίο παρέχεται η υπηρεσία,

β) απαιτεί από τους παρόχους ψηφιακών υπηρεσιών:

αα) να παρέχουν τις απαραίτητες πληροφορίες για την εκτίμηση της ασφάλειας των συστημάτων δικτύου και των πληροφοριών τους, συμπεριλαμβανομένων τεκμηριωμένων και εγκεκριμένων πολιτικών ασφάλειας,

ββ) να διορθώνουν οποιαδήποτε παράλειψη συμμόρφωσης προς τις απαιτήσεις που ορίζονται στο άρθρο 11.

2. Αν ένας πάροχος ψηφιακών υπηρεσιών έχει την κύρια εγκατάστασή του ή αντιπρόσωπο σε ένα κράτος-μέλος, αλλά τα συστήματα δικτύου και πληροφοριών του βρίσκονται σε ένα ή περισσότερα άλλα κράτη-μέλη, η αρμόδια αρχή του κράτους-μέλους της κύριας εγκατάστασης ή του αντιπροσώπου και οι αρμόδιες αρχές των άλλων κρατών-μελών συνεργάζονται και παρέχουν αμοιβαία συνδρομή, εφόσον απαιτείται. Η συνδρομή και η συνεργασία μπορεί να καλύπτουν ανταλλαγές πληροφοριών μεταξύ των σχετικών αρμόδιων αρχών και αιτήματα για τη λήψη των ανωτέρω αναφερόμενων εποπτικών μέτρων.

3. Με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, ύστερα από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας, καθορίζονται τα μέτρα της περίπτωσης α΄ και η διαδικασία παροχής πληροφοριών της περίπτωσης β΄ της παραγράφου 1.

Άρθρο 13 Δικαιοδοσία και εδαφικότητα (Άρθρο 18 της Οδηγίας 2016/1148/ΕΕ)

1. Ο πάροχος ψηφιακών υπηρεσιών υπόκειται στη δικαιοδοσία των Ελληνικών αρχών όταν έχει την κύρια εγκατάστασή του στην Ελληνική Επικράτεια. Ο πάροχος ψηφιακών υπηρεσιών θεωρείται ότι έχει την κύρια εγκατάστασή του στην Ελληνική Επικράτεια όταν έχει την έδρα του σε αυτήν.

2. Ο πάροχος ψηφιακών υπηρεσιών που δεν είναι εγκατεστημένος στην Ευρωπαϊκή Ένωση αλλά προσφέρει, εντός της Ευρωπαϊκής Ένωσης, υπηρεσίες που αναφέρονται στο Παράρτημα ΙΙ ορίζει αντιπρόσωπο στην Ένωση. Ο αντιπρόσωπος είναι εγκατεστημένος σε ένα από τα κράτη - μέλη στα οποία προσφέρονται οι υπηρεσίες. Ο πάροχος ψηφιακών υπηρεσιών θεωρείται ότι υπόκειται στη δικαιοδοσία του κράτους - μέλους στο οποίο είναι εγκατεστημένος ο αντιπρόσωπος.

3. Ο ορισμός αντιπροσώπου από τον πάροχο ψηφιακών υπηρεσιών δεν θίγει τις νομικές ενέργειες που μπορεί να αναληφθούν κατά του ίδιου του παρόχου ψηφιακών υπηρεσιών.

ΚΕΦΑΛΑΙΟ Ε΄ ΤΕΛΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

Άρθρο 14 Εθελούσια κοινοποίηση (Άρθρο 20 της Οδηγίας 2016/1148/ΕΕ)

1. Οντότητες που δεν έχουν προσδιοριστεί ως φορείς εκμετάλλευσης βασικών υπηρεσιών και δεν είναι πάροχοι ψηφιακών υπηρεσιών μπορεί να κοινοποιούν σε εθελούσια βάση συμβάντα με σοβαρές επιπτώσεις στη επιχειρησιακή συνέχεια των υπηρεσιών που παρέχουν.

2. Κατά την επεξεργασία των κοινοποιήσεων, οι αρμόδιες αρχές ενεργούν σύμφωνα με τη διαδικασία που προβλέπεται στο άρθρο 9. Οι αρμόδιες αρχές μπορεί να δίνουν προτεραιότητα στην επεξεργασία των υποχρεωτικών έναντι των εθελούσιων κοινοποιήσεων. Οι εθελούσιες κοινοποιήσεις υποβάλλονται σε επεξεργασία μόνον εφόσον η επεξεργασία αυτή δεν συνιστά δυσανάλογη ή περιττή επιβάρυνση για τα οικεία κράτη - μέλη.

Η εθελούσια κοινοποίηση δεν συνεπάγεται την επιβολή στην κοινοποιούσα οντότητα υποχρεώσεων τις οποίες δεν θα είχε αν δεν προέβαινε στην εν λόγω κοινοποίηση.

Άρθρο 15 Κυρώσεις (Άρθρο 21 της Οδηγίας 2016/1148/ΕΕ)

1. Ο Υπουργός Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, ύστερα από εισήγηση της Εθνικής Αρχής Κυβερνοασφάλειας, επιβάλλει κυρώσεις σε φυσικό ή νομικό πρόσωπο, σε περίπτωση παραβίασης των διατάξεων του παρόντος νόμου, ως εξής:

α) Αν διαπιστωθεί ότι φορέας εκμετάλλευσης βασικών υπηρεσιών ή φορέας παροχής ψηφιακών υπηρεσιών δεν κοινοποιεί ή κοινοποιεί με αδικαιολόγητη καθυστέρηση συμβάν με σοβαρό αντίκτυπο στη συνέχεια των βασικών υπηρεσιών του, επιβάλλεται:

αα) πρόστιμο μέχρι του ποσού των δεκαπέντε χιλιάδων (15.000) ευρώ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων,

ββ) πρόστιμο μέχρι του ποσού των διακοσίων χιλιάδων (200.000) ευρώ σε περίπτωση υποτροπής.

β) Αν διαπιστωθεί ότι φορέας εκμετάλλευσης βασικών υπηρεσιών ή φορέας παροχής ψηφιακών υπηρεσιών δεν λαμβάνει κατάλληλα και αναλογικά, τεχνικά και οργανωτικά, προληπτικά μέτρα για τη διαχείριση των κινδύνων όσον αφορά την ασφάλεια των δικτύων και των συστημάτων πληροφοριών που χρησιμοποιεί για τις υπηρεσίες αυτές, επιβάλλεται:

αα) πρόστιμο μέχρι του ποσού των πενήντα χιλιάδων (50.000) ευρώ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων,

ββ) πρόστιμο μέχρι του ποσού των διακοσίων χιλιάδων (200.000) ευρώ σε περίπτωση υποτροπής.

γ) Αν διαπιστωθεί ότι φυσικό ή νομικό πρόσωπο δεν παρέχει ή παρέχει με αδικαιολόγητη καθυστέρηση οποιαδήποτε σχετική πληροφορία που ζητείται κατά τη διενέργεια ελέγχου ή τη διερεύνηση περιστατικού, επιβάλλεται:

αα) πρόστιμο μέχρι του ποσού των πενήντα χιλιάδων (50.000) ευρώ με σύσταση για συμμόρφωση και προειδοποίηση επιβολής περαιτέρω κυρώσεων,

ββ) πρόστιμο μέχρι του ποσού των διακοσίων χιλιάδων (200.000) ευρώ σε περίπτωση υποτροπής.

2. Πριν από την επιβολή κυρώσεων, η Εθνική Αρχή Κυβερνοασφάλειας ειδοποιεί εγγράφως το ενδιαφερόμενο φυσικό ή νομικό πρόσωπο, παρέχοντας σε αυτό το δικαίωμα ακρόασης και παροχής εξηγήσεων σε ημερομηνία, που απέχει πέντε (5) τουλάχιστον εργάσιμες ημέρες από την κοινοποίηση της ειδοποίησης.

Οι κυρώσεις επιβάλλονται με γραπτή και αιτιολογημένη απόφαση, η οποία κοινοποιείται στο ενδιαφερόμενο φυσικό ή νομικό πρόσωπο και στην οποία προσδιορίζεται η παράβαση. Οι κυρώσεις που επιβάλλονται στις ανωτέρω περιπτώσεις αναρτώνται στην επίσημη ιστοσελίδα της Εθνικής Αρχής Κυβερνοασφάλειας.

Άρθρο 16

Προσαρτώνται στον παρόντα νόμο και αποτελούν αναπόσπαστο τμήμα αυτού τα Παραρτήματα Ι και ΙΙ.

Άρθρο 17 Τροποποίηση του άρθρου 31 του ν. 3986/2011

Το άρθρο 31 του ν. 3986/2011 (Α΄ 152) τροποποιείται ως εξής:

1. Στην περίπτωση ε΄ της παραγράφου 1 του άρθρου 31, προστίθεται δεύτερο εδάφιο ως εξής: «Από 1.1.2019 καταργείται η υποχρέωση του προηγούμενου εδαφίου.».

2. Το τέταρτο εδάφιο της παραγράφου 3 του άρθρου 31 αντικαθίσταται ως εξής:

«Από το φορολογικό έτος 2018 και εφεξής εξαιρούνται από την υποχρέωση καταβολής τέλους οι αγρότες – μέλη αγροτικών συνεταιρισμών που πληρούν τις προϋποθέσεις του άρθρου 8 του ν. 4384/2016 (Α΄ 78), οι αγροτικοί συνεταιρισμοί, οι σχολικοί συνεταιρισμοί του άρθρου 46 του ν. 1566/1985 (Α΄ 167), οι Φορείς Κοινωνικής και Αλληλέγγυας Οικονομίας με τη μορφή Κοινωνικής Συνεταιριστικής Επιχείρησης ή Συνεταιρισμού Εργαζομένων, καθώς και οι επιχειρήσεις ανεξαρτήτως νομικής μορφής που βρίσκονται σε εκκαθάριση, πτώχευση ή αδράνεια. Σε περίπτωση που η αδράνεια δεν καταλαμβάνει ολόκληρο το φορολογικό έτος εφαρμόζεται αναλογικά η παράγραφος 2.».

Άρθρο 18

1. Στο τρίτο εδάφιο του άρθρου 37 του ν. 4262/2014 (Α΄ 114) οι λέξεις «περιεχόμενα περιφερειακών τηλεοπτικών σταθμών» αντικαθίστανται από τις λέξεις «προγράμματα παρόχων περιεχομένου περιφερειακής εμβέλειας».

2. Το τέταρτο και πέμπτο εδάφιο του άρθρου 37 του ν. 4262/2014 αντικαθίστανται ως εξής:

«Η κατά τα ανωτέρω εγκατάσταση επιτρέπεται με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης μετά από υποβολή κοινής αίτησης από τους παρόχους περιεχομένου ενός διαύλου (πολυπλέκτη) περιφερειακής εμβέλειας που επιθυμούν να μεταδοθεί το πρόγραμμά τους από ΣΕΕ εντός αποκλειστικής προθεσμίας είκοσι (20) εργάσιμων ημερών από τη δημοσίευση της απόφασης του επόμενου εδαφίου. Με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, ύστερα από γνώμη της ΕΕΤΤ, ορίζονται οι όροι και οι προϋποθέσεις εγκατάστασης και λειτουργίας των ΣΕΕ, τα δικαιολογητικά έγγραφα που συνοδεύουν την ανωτέρω αίτηση περί λειτουργίας ΣΕΕ και κάθε άλλο σχετικό ζήτημα. Το κόστος αγοράς, εγκατάστασης, λειτουργίας, μεταφοράς του σήματος στις ΣΕΕ και συντήρησης των ανωτέρω ΣΕΕ βαρύνει τους αιτούντες παρόχους περιεχομένου και σε καμία περίπτωση δεν εντάσσεται στα κόστη λειτουργίας του δικτύου και δεν επηρεάζει το Ανώτατο Όριο Τιμών (ΑΟΤ).».

Άρθρο 19 Έναρξη ισχύος

Η ισχύς του παρόντος νόμου αρχίζει από τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως, εκτός αν άλλως ορίζεται στις επιμέρους διατάξεις.

Παράρτημα Ε: ΕΙΔΟΣ ΟΝΤΟΤΗΤΩΝ ΓΙΑ ΤΟΥΣ ΣΚΟΠΟΥΣ ΤΟΥ ΑΡΘΡΟΥ 3 ΠΑΡΑΓΡΑΦΟΣ 4

Τομέας	Υποτομέας	Είδος οντότητας
1. Ενέργεια	Α) Ηλεκτρική ενέργεια	- Επιχειρήσεις ηλεκτρικής ενέργειας, όπως ορίζονται στην περίπτ. ιη' της παρ. 3 του άρθρου 2 του ν. 4001/2011 (Α' 179), οι οποίες ασκούν τη δραστηριότητα «προμήθεια», όπως ορίζεται στην περίπτ. κα' της παρ.1 του άρθρου 2 του ανωτέρω νόμου
		- Διαχειριστές δικτύου διανομής, όπως ορίζονται στην περίπτ. στ' της παρ. 1 του άρθρου 2 του ν. 4001/20011
		- Διαχειριστές συστήματος μεταφοράς, όπως ορίζονται στην περίπτ. ια' της παρ. 3 του άρθρου 2 του ν. 4001/2011
	Β) Πετρέλαιο	- Διαχειριστές αγωγών μεταφοράς πετρελαίου
		- Διαχειριστές παραγωγής πετρελαίου. Εγκαταστάσεων διύλισης και επεξεργασίας αποθήκευσης και μεταφοράς πετρελαίου
	Γ) Αέριο	- Επιχειρήσεις προμήθειας, όπως ορίζονται στην περίπτ. κβ' της παρ. 1 και στην περίπτ. κβ' της παρ. 2 του άρθρου 2 του ν. 4001/2021
		- Διαχειριστές δικτύου διανομής, όπως ορίζονται στην περίπτ. στ' της παρ. 1 του άρθρου 2 του ν. 4001/2011
		- Διαχειριστές συστήματος μεταφοράς, όπως ορίζονται στα άρθρα 61, 62, στην περίπτ. α' της παρ. 1, στις περιπτ. στ', ζ' και η΄της παρ. 2 του άρθρου 2 του ν. 4001/2011
		- Διαχειριστές συστήματος αποθήκευσης, όπως ορίζονται στο άρθρο 2 σημείο 10 της Οδηγίας 2009/73/ΕΚ
		- Διαχειριστές συστήματος ΥΦΑ, όπως ορίζονται στο άρθρο 2 σημείο 12 της Οδηγίας 2009/73/ΕΚ
		- Επιχειρήσεις φυσικού αερίου, όπως ορίζονται στην περίπτ. ιδ' της παρ. 2 του άρθρου 2 του ν. 4001/2011
		- Διαχειριστές εγκαταστάσεων διύλισης και επεξεργασίας φυσικού αερίου

2. Μεταφορές	Α) Αεροπορικές μεταφορές	- Αερομεταφορείς, όπως ορίζονται στο σημείο 4 του άρθρου 3 του Κανονισμού (ΕΚ) 300/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Μαρτίου 2008 (ΕΕ L 97)
		- Φορείς διαχείρισης αερολιμένα, όπως ορίζονται στην περίπτ. β' της παρ. 1 του άρθρου 2 του π.δ. 52/2012 (Α' 102), αερολιμένες, όπως ορίζονται στην περίπτ. α' της παρ. 1 του άρθρου 2 του ίδιου π.δ., συμπεριλαμβανομένων των κεντρικών αερολιμένων που απαριθμούνται στο τμήμα 2 του Παραρτήματος ΙΙ του Κανονισμού (ΕΕ) 1315/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 11ης Δεκεμβρίου 2013 (ΕΕ L 348), και φορείς εκμετάλλευσης βοηθητικών εγκαταστάσεων που βρίσκονται εντός των αερολιμένων
		- Φορείς εκμετάλλευσης ελέγχου διαχείρισης κυκλοφορίας που παρέχουν υπηρεσίες ελέγχου εναέριας κυκλοφορίας όπως ορίζονται στο σημείο 1 του άρθρου 2 του Κανονισμού (ΕΚ) 549/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 10ης Μαρτίου 2004 (ΕΕ L 96)
	Β) Σιδηροδρομικές μεταφορές	- Διαχειριστές της υποδομής, όπως ορίζονται στην παρ. 2 του άρθρου 3 του ν. 4408/2016 (Α' 135)
		- Σιδηροδρομικές επιχειρήσεις, όπως ορίζονται στην παρ. 1 του άρθρου 3 του ν. 4408/2016, συμπεριλαμβανομένων των φορέων εκμετάλλευσης εγκαταστάσεων για την παροχή υπηρεσιών, όπως ορίζονται στην παρ. 12 του άρθρου 3 του ιδίου νόμου
	Γ) Πλωτές μεταφορές	- Εσωτερικές πλωτές, θαλάσσιες και ακτοπλοϊκές εταιρείες μεταφοράς επιβατών και εμπορευμάτων, όπως ορίζονται για τις θαλάσσιες μεταφορές στο Παράστημα Ι του Κανονισμού (ΕΚ) 725/2004 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 31ης Μαρτίου 2004 (ΕΕ L 129), μη συμπεριλαμβανομένων των

		μεμονωμένων πλοίων που χρησιμοποιούνται από τις εταιρείες αυτές
		- Διαχειριστικοί φορείς των λιμένων, όπως ορίζονται στην παρ. 11 του άρθρου 2 του ν. 3622/2007 (Α' 281), συμπεριλαμβανομένων των λιμενικών τους εγκαταστάσεων όπως ορίζονται στο σημείο 11 του άρθρου 2 του Κανονισμού (ΕΚ) 725/2004, και φορείς εκμετάλλευσης έργων και εξοπλισμού που βρίσκονται εντός των λιμένων
		- Φορείς εκμετάλλευσης υπηρεσιών εξυπηρέτησης κυκλοφορίας πλοίων (VTS), όπως ορίζονται στην περίπτ. κ' του άρθρου 3 του π.δ. 49/2005 (Α' 66)
	Δ) Οδικές μεταφορές	- Οδικές αρχές, όπως ορίζονται στο σημείο 12 του άρθρου 2 και κατ' εξουσιοδότηση Κανονισμού (ΕΕ) 2015/962 της Επιτροπής της 18ης Δεκεμβρίου 2015 (ΕΕ L 157) που είναι υπεύθυνες για τον έλεγχο διαχείρισης της κυκλοφορίας
		- Φορείς εκμετάλλευσης συστημάτων ευφυών μεταφορών (ITS), όπως ορίζονται στην παρ. 1 του άρθρου 4 του π.δ. 50/2012 (Α' 100)
3. Τράπεζες		Πιστωτικά ιδρύματα, όπως ορίζονται στο σημείο 1 του άρθρου 4 του Κανονισμού (ΕΕ) 575/2013 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 26ης Ιουνίου 2013 (ΕΕ L 176)
4. Υποδομές χρηματοπιστωτικών αγορών		- Φορείς εκμετάλλευσης τόπων διαπραγμάτευσης, όπως ορίζονται στην παρ. 24 του άρθρου 4 του ν. 4514/2018 (Α' 14)
		- Κεντρικοί αντισυμβαλλόμενοι (CCP), όπως ορίζονται στο σημείο 1 του άρθρου 2 του Κανονισμού (ΕΕ) 648/2012 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 4ης Ιουλίου 2012 (ΕΕ L 201)
5. Τομέας της υγείας	Περιβάλλοντα υγειονομικής περίθαλψης (μεταξύ άλλων νοσοκομεία και ιδιωτικές κλινικές)	Πάροχοι υγειονομικής περίθαλψης, όπως ορίζονται στην περίπτ. ζ' του άρθρου 3 του ν. 4213/2013 (Α' 261)

6. Προμήθεια και διανομή πόσιμου νερού		Προμηθευτές και διανομείς νερού ανθρώπινης κατανάλωσης, όπως ορίζονται στην περίπτ. α’ της παρ. 1 του άρθρου 2 της Γ1(δ)/ΓΠ οικ.67322 κοινής απόφασης των Υπουργών Εσωτερικών, Οικονομίας και Ανάπτυξης, Υγείας, Περιβάλλοντος και Ενέργειας (Β’ 3282), αλλά εξαιρουμένων των διανομέων για τους οποίους η διανομή νερού ανθρώπινης κατανάλωσης αποτελεί μόνο μέρος της γενικής τους δραστηριότητας διανομής λοιπών προϊόντων και αγαθών που δε θεωρούνται βασικές υπηρεσίες
7. Ψηφιακή υποδομή		- Σημεία ανταλλαγής κίνησης διαδικτύου (IXP)
		- Πάροχοι υπηρεσιών συστήματος ονομάτων χώρου
		- Μητρώα ονομάτων χώρου ανώτατου επιπέδου (TLD)

Παράρτημα Στ: ΕΙΔΗ ΨΗΦΙΑΚΩΝ ΥΠΗΡΕΣΙΩΝ ΓΙΑ ΤΟΥΣ ΣΚΟΠΟΥΣ ΤΟΥ ΑΡΘΡΟΥ 3 ΠΑΡΑΓΡΑΦΟΣ 5

1. Επιγραμμική αγορά
2. Επιγραμμική μηχανή αναζήτησης
3. Υπηρεσία νεφοϋπολογιστικής

Βιβλιογραφία

[1] An Autonomous Architecture for Inter-Domain Trace back across the Borders of Network Operation (iscc06)

[2] IETF RFC 3882, Configuring BGP to Block Denial-of-Service Attacks

[3] ISO Guide 73:2009, *Risk management — Vocabulary*

[4] ISO/IEC 12207:2008, *Systems and software engineering — Software life cycle processes*

[5] ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security —*
Part 1: Introduction and general model

[6] ISO/IEC 19770-1, *Information technology — Software asset management — Part 1: Processes and tiered assessment of conformance*

[7] ISO/IEC TR 19791, *Information technology — Security techniques — Security assessment of operational systems*

[8] ISO/IEC 20000-1, *Information technology — Service management — Part 1: Service management system requirements*

[9] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*

[10] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*

[11] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[12] ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

[13] ISO/IEC 27031, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[14] ISO/IEC 27032, *Information technology — Security techniques — Guidelines for cybersecurity*

[15] ISO/IEC 27033 (all parts), *Information technology — Security techniques — Network security*

[16] ISO/IEC 27034 (all parts), *Information technology — Security techniques — Application security*

[17] ISO/IEC 27035, *Information technology — Security techniques — Information security incident management*

[18] ISO/IEC 29147, *Information technology — Security techniques — Vulnerability disclosure*[2)]

[19] ISO 31000, *Risk management — Principles and guidelines*

[20] ITU-T X.1200 – X.1299, Series X: Data Networks, Open System Communications and Security, Telecommunication Security – Cyberspace security

[21] ITU-T X.1500 – X.1598, Series X: Data Networks, Open System Communications and Security – Cybersecurity Information Exchange