ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ
«ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ ΓΙΑ ΣΤΕΛΕΧΗ – EXECUTIVE MBA»

Διπλωματική Εργασία

Η Ασφάλεια Πληροφοριών στις Σύγχρονες Επιχειρήσεις & Μελέτη Περίπτωσης σε μια Εταιρεία

Αντώνιος Π. Γεωργιάδης

Επιβλέπων: Καθηγητής κ. Δημήτριος Γεωργακέλλος

Πειραιάς, Σεπτέμβριος 2018

Παράρτημα Β: Βεβαίωση Εκπόνησης Διπλωματικής Εργασίας

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΧΕΙΡΗΜΑΤΙΚΩΝ ΚΑΙ ΔΙΕΘΝΩΝ ΣΠΟΥΔΩΝ
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΗ ΔΙΟΙΚΗΣΗ ΕΠΙΧΕΙΡΗΣΕΩΝ ΓΙΑ ΣΤΕΛΕΧΗ

ΒΕΒΑΙΩΣΗ ΕΚΠΟΝΗΣΗΣ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

(περιλαμβάνεται ως ξεχωριστή (δεύτερη) σελίδα στο σώμα της διπλωματικής εργασίας)

«Δηλώνω υπεύθυνα ότι η διπλωματική εργασία για τη λήψη του μεταπτυχιακού τίτλου σπουδών, του Πανεπιστημίου Πειραιώς, στη Διοίκηση Επιχειρήσεων για Στελέχη : Ε-ΜΒΑ» με τίτλο: **«Η ασφάλεια πληροφοριών στις σύγχρονες επιχειρήσεις και μελέτη περίπτωσης σε μια εταιρεία»** έχει συγγραφεί από εμένα αποκλειστικά και στο σύνολό της. Δεν έχει υποβληθεί ούτε έχει εγκριθεί στο πλαίσιο κάποιου άλλου μεταπτυχιακού προγράμματος ή προπτυχιακού τίτλου σπουδών, στην Ελλάδα ή στο εξωτερικό, ούτε είναι εργασία ή τμήμα εργασίας ακαδημαϊκού ή επαγγελματικού χαρακτήρα.

Δηλώνω επίσης υπεύθυνα ότι οι πηγές στις οποίες ανέτρεξα για την εκπόνηση της συγκεκριμένης εργασίας, αναφέρονται στο σύνολό τους, κάνοντας πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Υπογραφή Μεταπτυχιακού Φοιτητή:.....

Ονοματεπώνυμο: Αντώνιος Γεωργιάδης

Ημερομηνία: 14/09/2018

Η Ασφάλεια Πληροφοριών στις Σύγχρονες Επιχειρήσεις & Μελέτη Περίπτωσης σε μια Εταιρεία

ΛΕΞΕΙΣ – ΚΛΕΙΔΙΑ: Ασφάλεια πληροφοριών, κυβερνοασφάλεια, προστασία δεδομένων, ψηφιακοί κίνδυνοι και απειλές, διαχείριση κινδύνων, διαχείριση ασφάλειας πληροφοριών, περιστατικό ασφαλείας, GDPR, ISO/IEC 27001

ΠΕΡΙΛΗΨΗ

Στη σημερινή ψηφιακή εποχή οι επιχειρήσεις έχουν αρχίσει να συνειδητοποιούν ότι η μέριμνα για τους κινδύνους στον κυβερνοχώρο και η οικοδόμηση μέτρων ασφαλείας είναι επιτακτική ανάγκη. Δεν είναι μόνο οι κυβερνοεπιθέσεις οι οποίες γίνονται πιο συχνές και πιο περίπλοκες, αλλά και κανονιστικά πλαίσια όπως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) που οδηγούν τις επιχειρήσεις να επενδύσουν στην προστασία των πληροφοριών και των δεδομένων.

Κοινό λάθος των εταιρειών είναι ότι αντιμετωπίζουν την ασφάλεια των πληροφοριών τεχνολογικά και όχι επιχειρησιακά. Σκοπός της διπλωματικής εργασίας είναι να αναδείξει τη σημασία της ασφάλειας των πληροφοριών ως αναπόσπαστο μέρος της επιχειρησιακής στρατηγικής των επιχειρήσεων.

Στα κεφάλαια της εργασίας παρουσιάζουμε τη σωστή προσέγγιση που πρέπει να ακολουθούν οι επιχειρήσεις ώστε να ενισχύουν το ανταγωνιστικό τους πλεονέκτημα μέσα από μία σωστή στρατηγική ασφάλειας πληροφοριών, ορίζοντας αρχικά το σύστημα διαχείρισης ασφάλειας πληροφοριών και τις πολιτικές ασφάλειας που θα ακολουθήσουν και, στη συνέχεια, την ενσωμάτωση των τεχνολογικών λύσεων για την προστασία των πληροφοριακών τους συστημάτων με στόχο την διαφύλαξη της επιχειρηματικής τους δραστηριότητας.

Information Security in Modern-day Businesses & Case Study in a Company

KEYWORDS: Information security, cyber-security, data protection, digital threats, risk management, information security management, security incident, GDPR, ISO/IEC 27001

ABSTRACT

In today's digital age, businesses have begun to realize that taking care of cyber-related risks and building security measures is imperative. Not only the cyber-attacks that are becoming more frequent and more complicated, but also the regulatory frameworks such as the General Data Protection Regulation (GDPR) lead businesses to invest in information and data protection.

The common mistake of the companies is that they face the information security technologically and not operationally. The aim of this master thesis is to highlight the importance of information security as an integral part of the enterprise business strategy.

In the chapters of the thesis we present the right approach that businesses should follow to enhance their competitive advantage through a proper information security strategy by initially defining the information security management system and the security policies to follow and, then, integrating of the technological solutions for the protection of their information systems in order to preserve their businesses activities.

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά όλους όσους με στήριξαν, με ενθάρρυναν, μου έδωσαν δύναμη και ήταν δίπλα μου κατά τη διάρκεια αυτών των δύο χρόνων των μεταπτυχιακών σπουδών μου.

Αρχικά, την οικογένειά μου που πάντα πιστεύει σε μένα και χαίρεται με τις επιτυχίες μου περισσότερο από εμένα.

Όλους τους φίλους που απέκτησα μέσα στο μεταπτυχιακό πρόγραμμα για τις υπέροχες στιγμές που μοιραστήκαμε, κάνοντας αυτό το ταξίδι μία μοναδική εμπειρία ζωής.

Τέλος, θα ήθελα να εκφράσω τις ευχαριστίες μου στον καθηγητή κύριο Δημήτριο Γεωργακέλλο για την υποστήριξη του και την εμπιστοσύνη που μου έδειξε με την ανάθεση της διπλωματικής εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΛΙΣΤΑ ΕΙΚΟΝΩΝ

ΛΙΣΤΑ ΠΙΝΑΚΩΝ

ΛΙΣΤΑ ΑΚΡΩΝΥΜΙΩΝ

ΤΠΕ	*Τεχνολογία Πληροφοριών και Τεχνολογιών*
GDPR | ΓΚΠΔ	*General Data Protection Regulation | Γενικός Κανονισμός Προστασίας Δεδομένων*
ΣΔΑΠ	*Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών*
SQL	*Structured Query Language*
XXS	*Cross-Site Scripting*
USB	*Universal Serial Bus*
FTP	*File Transfer Protocol*
PUP	*Potentially Unwanted Program*
DDos	*Df-service attack, DoS attack*
IP	*Protocol Address*
URL	*Uniform Resource Locator*
SHA-1	*Secure Hash Algorithm 1*
VPN	*Virtual Private Network*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
UTM	*Unified Threat Management*
DLP	*Data Loss Prevention*
BYOD	*Bring Your Own Device*
APT	*Advanced Persistent Threat*
SSH	*Secure Shell*
OWA	*Outlook Web Access*
CAD	*Computer-Aided Design*
IRM	*Information Rights Management*
SIEM	*Security Information and Event Management*
SSL	*Secure Sockets Layer*
S/MIME	*Secure/Multipurpose Internet Mail Extensions*
NAC	*Network Access Control*
IM	*Instant Message*
P2P	*Peer-to-peer*
FTP	*File Transfer Protocol*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
ISO/IEC	*International Organization for Standardization / International Electrotechnical Commission*
ΥΑΠ	*Υπεύθυνος Ασφάλειας Πληροφοριών*
SAN	*Storage Area Network*
NAS	*Network-attached Storage*
RAID	*Redundant Array of Independent Disks*
TLS	*Transport Layer Security*
RSA	*Rivest–Shamir–Adleman*
UPS	*Uninterruptible Power Supply*
CPU	*Central Processing Unit*
NTP	*Network Time Protocol*
DMZ	*Demilitarized Zone*
COTS	*Commercial Off-The-Shelf*

ΕΙΣΑΓΩΓΗ

Τα τελευταία χρόνια με την ανάπτυξη των νέων ψηφιακών τεχνολογιών έννοιες όπως «Μεγάλα Δεδομένα» (Big Data) και «Διαδίκτυο των Πραγμάτων» (Internet of Things), η ανάπτυξη εφαρμογών και συστημάτων στο Cloud («στο σύννεφο»), η εξάπλωση των κοινωνικών δικτύων και η χρήση φορητών συσκευών στο χώρο εργασίας έχουν εξελιχθεί σε παράγοντες επιτυχίας για τις επιχειρήσεις. Ο μεγάλος όγκος δεδομένων που εισρέει στις επιχειρήσεις δεν αποτελεί μόνο σημαντικό εργαλείο λήψης αποφάσεων, αλλά και πηγή ανησυχίας για τη διαχείριση τους.

Ο κυβερνοχώρος εκτός από ευκαιρίες κρύβει και απειλές για τις επιχειρήσεις. Κυβερνοεγκληματίες που σκοπό έχουν να υποκλέψουν εταιρικά δεδομένα, κωδικούς πρόσβασης, αριθμούς πιστωτικών καρτών και τραπεζικών λογαριασμών, νέες αναδυόμενες επιθέσεις τύπου ransomware και επιθέσεις που οδηγούν στην διακοπή παροχής υπηρεσίας, είναι μερικές μόνο από τις απειλές που λαμβάνουν χώρα καθημερινά.

Σύμφωνα με τα στοιχεία της Ευρωπαϊκής Επιτροπής, περισσότερες από 4000 επιθέσεις ransomware έχουν καταγραφεί για το 2016, παρουσιάζοντας αύξηση 300% σε σχέση με το 2015. Οι οικονομικές επιπτώσεις του κυβερνοεγκλήματος έχουν πενταπλασιαστεί το 2017 σε σχέση με το 2013 και αναμένονται να τετραπλασιαστούν το 2019 (σε σχέση με το 2017). Η ίδια έρευνα του Ευρωβαρομέτρου δείχνει ότι το 87% των ερωτηθέντων θεωρεί ότι το έγκλημα στον κυβερνοχώρο αποτελεί σημαντική πρόκληση για την εσωτερική ασφάλεια στην Ευρωπαϊκή Ένωση (ΕΕ), ενώ οι δύο μεγαλύτερες ανησυχίες είναι η κακή χρήση των δεδομένων προσωπικού χαρακτήρα και η ασφάλεια των συναλλαγών [39].

Η παραπάνω πραγματικότητα οδήγησε την ΕΕ στην αυστηριοποίηση του νομικού πλαισίου και στη θέσπιση του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) με σκοπό να θωρακίσει την ιδιωτικότητα και να μεταθέσει την ευθύνη της προστασίας στην ίδια την επιχείρηση, προβλέποντας αυστηρά πρόστιμα σε περιπτώσεις μη συμμόρφωσης με τις απαιτήσεις του.

Σε ένα ψηφιακό περιβάλλον που αλλάζει συνεχώς οι επιχειρήσεις καλούνται να προσαρμοστούν και να θέσουν ως προτεραιότητα τους την ασφάλεια των πληροφοριών και των δεδομένων τους. Ένα από τα μεγαλύτερα προβλήματα στην υιοθέτηση και την εφαρμογή μιας στρατηγικής ασφάλειας πληροφοριών δεν είναι μόνο το κόστος, όπου οι επιχειρήσεις μέσα σε ένα αρνητικό οικονομικό κλίμα δεν επενδύουν στα συστήματα

ασφάλειας τους, αλλά και η έλλειψη κατανόησης της ανάγκης και της χρησιμότητας μιας τέτοιας στρατηγικής.

Σκοπός της παρούσας διπλωματικής εργασίας είναι να αναδείξει το ζήτημα της ασφάλειας των πληροφοριών και να παρουσιάσει με απλό και κατανοητό τρόπο τη σημασία της στη λειτουργία της κάθε επιχείρησης και στην αποτελεσματικότητα της.

Για την επιλογή του θέματος ρόλο έπαιξε και η εργασιακή μου εμπειρία όπου τα τελευταία πέντε χρόνια εργάζομαι σε εταιρεία πληροφορικής με αντικείμενο την ασφάλεια πληροφοριακών συστημάτων. Έχοντας δει τις ανάγκες αλλά και τις ανησυχίες και τους προβληματισμούς των επιχειρήσεων πάνω στον τομέα της ασφάλειας, μπορώ μέσα από μια επαγγελματική προσέγγιση να αποτυπώσω τη διάσταση του θέματος στα πλαίσια των ακαδημαϊκών μου υποχρεώσεων.

Το αντικείμενο της εργασίας θα εστιάσει όχι μόνος στις ψηφιακές απειλές και στις τεχνολογικές λύσεις, αλλά και σε θέματα πολιτικών και διαδικασιών. Θεωρώντας ότι η ασφάλεια πληροφοριών πρέπει να αποτελεί μέρος της επιχειρηματικής στρατηγικής και ευθύνη των ανώτατων στελεχών, είναι απαραίτητο να παρουσιάσουμε την διαχείριση της μέσα από ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών βασισμένο στο πρότυπο ISO/IEC 27001:2013 και να μελετήσουμε πως αυτό μπορεί να εφαρμοστεί σε μία επιχείρηση όπου η ασφάλεια και η διαχείριση πληροφοριών και δεδομένων θεωρείται κρίσιμη.

Ακόμη, λαμβάνοντας υπόψη ότι μελέτη της Lloyd's σε συνεργασία με το Κέντρο Μελετών Κινδύνων του Πανεπιστημίου του Cambridge προβλέπει για την Ελλάδα ότι το κόστος των επιθέσεων στον κυβερνοχώρο που θα δεχθούν οι επιχειρήσεις και οι οργανισμοί την δεκαετία 2015 - 2025 ανέρχεται σε 1,06 δισεκατομμύρια δολάρια του εκτιμώμενου ΑΕΠ της Ελλάδας [40], οι διοικήσεις των επιχειρήσεων θα πρέπει να είναι σε θέση να αναγνωρίζουν τους κινδύνους και τις επιπτώσεις των περιστατικών ασφαλείας και να υλοποιούν έργα σύμφωνα με τις Πολιτικές Ασφάλειας των επιχειρήσεων τους. Θα παρουσιάσουμε, συνεπώς, μία μελέτη ανάλυσης κινδύνων και μία περίπτωση υπολογισμού του κόστους μιας επένδυσης σε συστήματα ασφάλειας πληροφοριών με πραγματικές λύσεις και τιμές μέσα από την σημερινή αγορά του IT security.

Θέτοντας ως αντικειμενικό σκοπό της παρούσας διπλωματικής εργασίας την ανάδειξη της σημασίας της εναρμόνισης της ασφάλειας πληροφοριών με την επιχειρηματική στρατηγική, μέσα στα επόμενα κεφάλαια που θα ακολουθήσουν θα παρουσιάσουμε την πολύπλευρη έννοια της ασφάλειας πληροφοριών και των προκλήσεων της, τη μέθοδο διαχείρισης της, τις ψηφιακές απειλές και τους κινδύνους,

τους τρόπους αντιμετώπισης τους και προστασίας των πληροφοριακών συστημάτων, του κόστους πρόληψης των κινδύνων, αλλά και του έμμεσου κόστους που συνεπάγεται η μη αποτελεσματική διαχείριση του σχετικού ρίσκου.

ΚΕΦΑΛΑΙΟ 1:

ΓΕΝΙΚΑ ΠΕΡΙ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

1.1. Εισαγωγή

Η ασφάλεια πληροφοριών αποτελεί πλέον ένα από τα σημαντικότερα αντικείμενα με τα οποία ασχολείται ένας οργανισμός για την εύρυθμη λειτουργία του. Κάθε οργανισμός ορίζει ένα πλαίσιο μέσα στο οποίο πραγματοποιούνται οι κατάλληλες διεργασίες για να επιτυγχάνονται οι στόχοι της ασφάλειας πληροφοριών. Οι διεργασίες αυτές αποτελούν μέρος της στρατηγικής ασφάλειας η οποία περιλαμβάνει επιμέρους πολιτικές και εναρμονίζει τον οργανισμό με διεθνείς πρακτικές και πρότυπα. Συνεπώς, κάθε οργανισμός στα πλαίσια του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) διεξάγει μία μελέτη ασφάλειας πληροφοριών που ενσωματώνει όλες αυτές τις πολιτικές και διεργασίες οι οποίες επιτρέπουν στις διοικήσεις των οργανισμών να παίρνουν σωστές αποφάσεις και να αποτιμούν την επιτυχία του ΣΔΑΠ που εφαρμόζουν στον οργανισμό τους.

1.2. Βασικές Έννοιες

1.2.1. Πληροφορία

Η *πληροφορία* είναι δεδομένα που έχουν υποστεί επεξεργασία και προορίζονται για έναν τελικό χρήστη. Πρόκειται, συνεπώς, για το αποτέλεσμα των επεξεργασμένων δεδομένων [7].

Σύμφωνα με τον ορισμό του ISO 27000 ως πληροφορία εννοούμε οτιδήποτε έχει αξία για τον οργανισμό. Πρόκειται για τους πόρους της εταιρείας οι οποίοι έχουν αξία και πρέπει να προστατεύονται κατάλληλα.

1.2.2. Ασφάλεια πληροφοριών

Όπως αναφέρεται στην «ΟΔΗΓΙΑ (ΕΕ) 2016/1148 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση», *ασφάλεια συστημάτων δικτύου και πληροφοριών* είναι η ικανότητα συστημάτων δικτύου και πληροφοριών να ανθίστανται, σε 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.

Ως «σύστημα δικτύου και πληροφοριών» εννοείται:

α) ένα δίκτυο ηλεκτρονικών επικοινωνιών κατά την έννοια του άρθρου 2 στοιχείο α) της οδηγίας 2002/21/ΕΚ

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

γ) ψηφιακά δεδομένα που αποθηκεύονται, υποβάλλονται σε επεξεργασία, ανακτώνται ή μεταδίδονται από στοιχεία που καλύπτονται στα σημεία α) και β) για τους σκοπούς της λειτουργίας, χρήσης, προστασίας και συντήρησής τους [1].

Με άλλα λόγια, ο όρος *ασφάλεια πληροφορίας/δεδομένων* χρησιμοποιείται για να περιγράψει τη μεθοδολογία, καθώς και τις μεθόδους και τεχνικές που ακολουθούνται προκειμένου να επιτευχθούν οι εξής στόχοι:

- Εμπιστευτικότητα: Τα δεδομένα δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
- Ακεραιότητα: Τα δεδομένα πρέπει να είναι ακριβή, ακέραια και γνήσια – όχι εσφαλμένα, αλλοιωμένα ή μη ενημερωμένα.
- Διαθεσιμότητα: Τα δεδομένα πρέπει να είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

Τα ανωτέρω αποτελούν τις τρεις θεμελιώδεις ιδιότητες της ασφάλειας πληροφοριών και πλήγμα σε οποιοδήποτε από αυτά –από τυχαία ή εσκεμμένη ενέργεια– συνιστά, γενικά, περιστατικό ασφάλειας [2].

Εκτός από τις παραπάνω βασικές ιδιότητες, η ασφάλεια πληροφοριακών συστημάτων συσχετίζεται με την επιτυχημένη εφαρμογή των ακόλουθων μηχανισμών [10]:

- Αναγνώριση: αφορά τη διαδικασία παρουσίασης της ταυτότητας μιας οντότητας (π.χ. πελάτη) στο σύστημα (π.χ. εξυπηρετητή).
- Αυθεντικοποίηση: αφορά τη διαδικασία επιβεβαίωσης της ταυτότητας που έχει παρουσιάσει μια οντότητα στο σύστημα.
- Εξουσιοδότηση: αφορά τη διαδικασία λήψης απόφασης σχετικά με την αποδοχή ή την απόρριψη ενός αιτήματος πρόσβασης μιας αυθεντικοποιημένης οντότητας στο σύστημα, στη βάση των δικαιωμάτων πρόσβασης που της έχουν ήδη εκχωρηθεί και της πολιτικής ελέγχου πρόσβασης του συστήματος.
- Αδυναμία αποποίησης: αφορά τη διαδικασία αδιαμφισβήτητου καταλογισμού ευθύνης για την επιτέλεση μιας ενέργειας στο σύστημα.

1.3. Το ζήτημα της ασφάλειας παγκοσμίως

Είναι γεγονός ότι η χρήση του Διαδικτύου και των πληροφοριακών συστημάτων εντός των οργανισμών έχει εγείρει σε παγκόσμιο επίπεδο το ζήτημα της ασφάλειας των δικτύων και των πληροφοριών. Τα περιστατικά παραβίασης της ασφάλειας που καλούνται να αντιμετωπίσουν οι επιχειρήσεις καθημερινά έχουν αυξηθεί κατακόρυφα τα τελευταία χρόνια, με τις επιχειρήσεις να διαθέτουν ένα μεγάλο μέρος από τον ετήσιο προϋπολογισμό τους για την ενίσχυση της ασφάλειας τους.

Κάθε χρόνο διενεργούνται πολλές εκθέσεις που καταγράφουν το μέγεθος των περιστατικών ασφάλειας. Στη συνέχεια θα παρουσιαστεί η έρευνα της Kroll με τίτλο «Global Fraud & Risk Report, 10th Annual Edition – 2017/18».

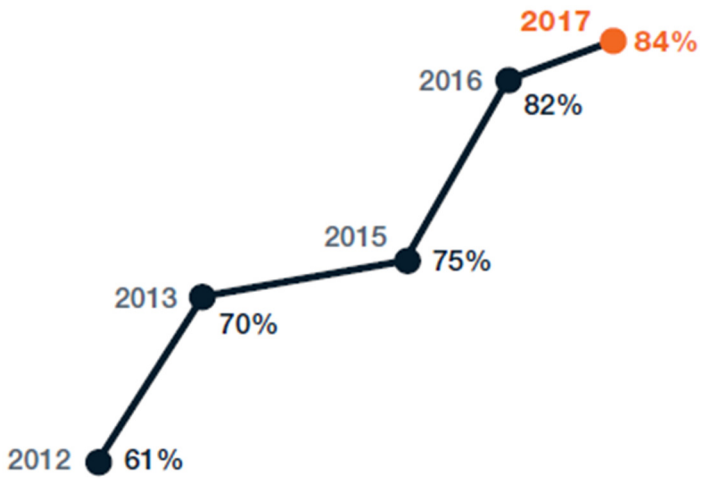
Η έρευνα κατηγοριοποιεί τα περιστατικά ασφάλειας σε τρεις κατηγορίες:

- Περιστατικά απάτης
- Περιστατικά ασφάλειας προερχόμενα από τον κυβερνοχώρο (περιστατικά κυβερνοασφάλειας)
- Συμβάντα ασφάλειας (μη προερχόμενα από τον κυβερνοχώρο)

Λόγω της σύγκλισης μιας παγκόσμιας οικονομίας, των αυξανόμενων ψηφιακών συνδέσεων και των συνεχώς σταθερών παραγόντων ανθρώπινης συμπεριφοράς, οι οργανισμοί πρέπει να υιοθετήσουν μια ολιστική προσέγγιση στη διαχείριση επιχειρηματικών κινδύνων και να αναπτύξουν ολοκληρωμένες στρατηγικές άμβλυνσης του κινδύνου για την αντιμετώπιση αυτού του νέου περιβάλλοντος απειλών.

Σύμφωνα με την παγκόσμια έρευνα της Kroll, το 86% των οργανισμών που ερωτήθηκαν αντιμετώπισαν ένα περιστατικό ασφάλειας προερχόμενο από τον κυβερνοχώρο μέσα στο 2017, ποσοστό αυξημένο κατά 1% σε σχέση με το 2017. Όπως αναφέρεται μάλιστα στην έκθεση, σε ορισμένες χώρες και σε ορισμένους κλάδους το ποσοστό αυτό αγγίζει το 100%.

Επίσης, το ποσοστό των επιχειρήσεων που έπεσαν θύματα απάτης ήταν 84% το 2017 (από 82% το 2016). Το ποσοστό αυτό, μάλιστα, εμφανίζεται συνεχώς αυξανόμενο από το 2012 όπου ήταν 61%.



Εικόνα 1: Ποσοστό ερωτηθέντων που αντιμετώπισαν ένα περιστατικό απάτης

[Πηγή: Kroll Global Fraud & Risk Report, 10th Annual Edition – 2017/18]

Εκτός από την αναφορά εξαιρετικά υψηλών επιπέδων επιπτώσεων, οι ερωτηθέντες της έρευνας ανέφεραν ότι οι επιπτώσεις ήταν τόσο δαπανηρές όσο και εκτεταμένες, με αρνητικό αντίκτυπο στους υπαλλήλους, τους πελάτες, τη φήμη, τις σχέσεις με τις ρυθμιστικές αρχές και τα έσοδα.

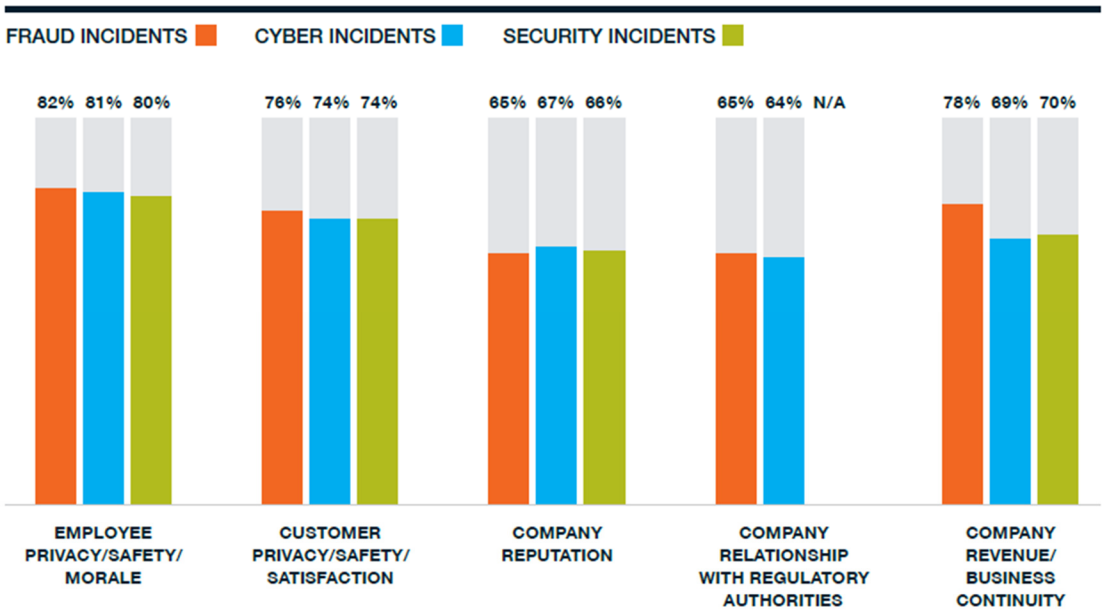
- Δεν αποτελεί έκπληξη το γεγονός ότι η πιο εκτεταμένη επίδραση που παρατηρήθηκε ήταν ο αντίκτυπος στους εργαζομένους: η προστασία της ιδιωτικής ζωής των εργαζομένων/η ασφάλεια/το ηθικό επηρεάστηκε έντονα ή κάπως αρνητικά, σύμφωνα με το 82% των ερωτηθέντων στελεχών των οποίων η εταιρεία υπέστη ένα περιστατικό απάτης, το 81% όσων επλήγησαν από ένα περιστατικό προερχόμενο από τον κυβερνοχώρο και το 80% τα στελέχη των οποίων η εταιρεία υπέστη κάποιο συμβάν ασφάλειας.

- Περίπου τα τρία τέταρτα των ερωτηθέντων δήλωσαν ότι οι πελάτες τους ήταν έντονα ή κάπως αρνητικά επηρεασμένοι από τους τρεις τομείς κινδύνου: απάτη (76%), κυβερνοχώρος (74%) και ασφάλεια (74%).

- Σχεδόν τα δύο τρίτα των στελεχών ανέφεραν ότι πλήγηκε η φήμη της εταιρείας τους: 65%, 67% και 66% για ένα περιστατικό απάτης, κυβερνοχώρου ή ασφάλειας, αντίστοιχα.

- Το 65% των ερωτηθέντων δήλωσε ότι ένα περιστατικό απάτης έχει επηρεάσει έντονα ή κάπως αρνητικά τη σχέση της εταιρείας του με τις ρυθμιστικές αρχές.

- Το 78% των στελεχών των οποίων οι εταιρείες ήταν θύματα απάτης δήλωσε ότι τα έσοδα και η επιχειρηματική συνέχεια επηρεάστηκαν έντονα ή κάπως αρνητικά. Ομοίως, το 70% των ερωτηθέντων που υπέστησαν το περιστατικό ασφάλειας και το 69% εκείνων που αντιμετώπισαν περιστατικό από τον κυβερνοχώρο ανέφεραν δυσμενείς επιπτώσεις στα έσοδα/επιχειρηματική συνέχεια των εταιρειών τους.



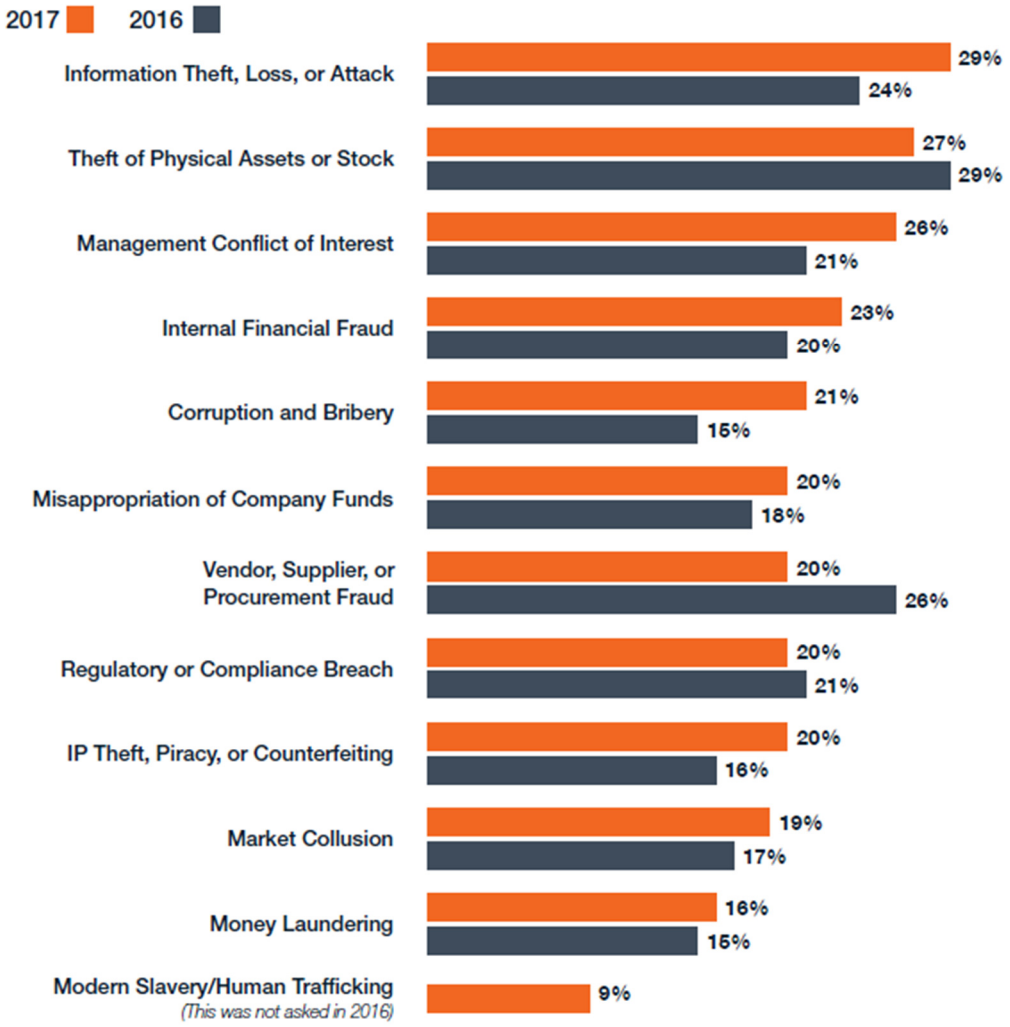
Εικόνα 2: Ποσοστό απαντήσεων στην ερώτηση «Σε ποιο βαθμό έχουν επηρεαστεί αρνητικά από τα γεγονότα [απάτης / κυβερνοχώρου / ασφάλειας] στην εταιρεία σας;»

[Πηγή: Kroll Global Fraud & Risk Report, 10th Annual Edition – 2017/18]

Για πρώτη φορά στα 10 χρόνια της συγκεκριμένης έρευνας που διεξάγει η Kroll, η κλοπή, η απώλεια και η επίθεση πληροφοριών ήταν ο πιο διαδεδομένος τύπος απάτης που παρατηρήθηκε το τελευταίο έτος, το οποίο αναφέρθηκε από το 29% των ερωτηθέντων.

Η κλοπή φυσικών περιουσιακών στοιχείων ή αποθεμάτων, μακρά η πιο κοινή μορφή απάτης, ήταν το δεύτερο πιο συχνά αναφερόμενο περιστατικό, το οποίο υπέστη το 27% των ερωτηθέντων.

Η μεγαλύτερη αύξηση σε ετήσια βάση ήταν η διαφθορά και η δωροδοκία, σύμφωνα με το 21% των ερωτηθέντων στελεχών και αυξημένο κατά 6 ποσοστιαίες μονάδες από 15% στην τελευταία έρευνα. Δεδομένου ότι η διαφθορά και η δωροδοκία σχεδόν διπλασιάζονται τα τελευταία δύο χρόνια, ο κίνδυνος για τους οργανισμούς έχει αυξηθεί σημαντικά.



Εικόνα 3: Τύποι περιστατικών απάτης που υπέστησαν οι επιχειρήσεις

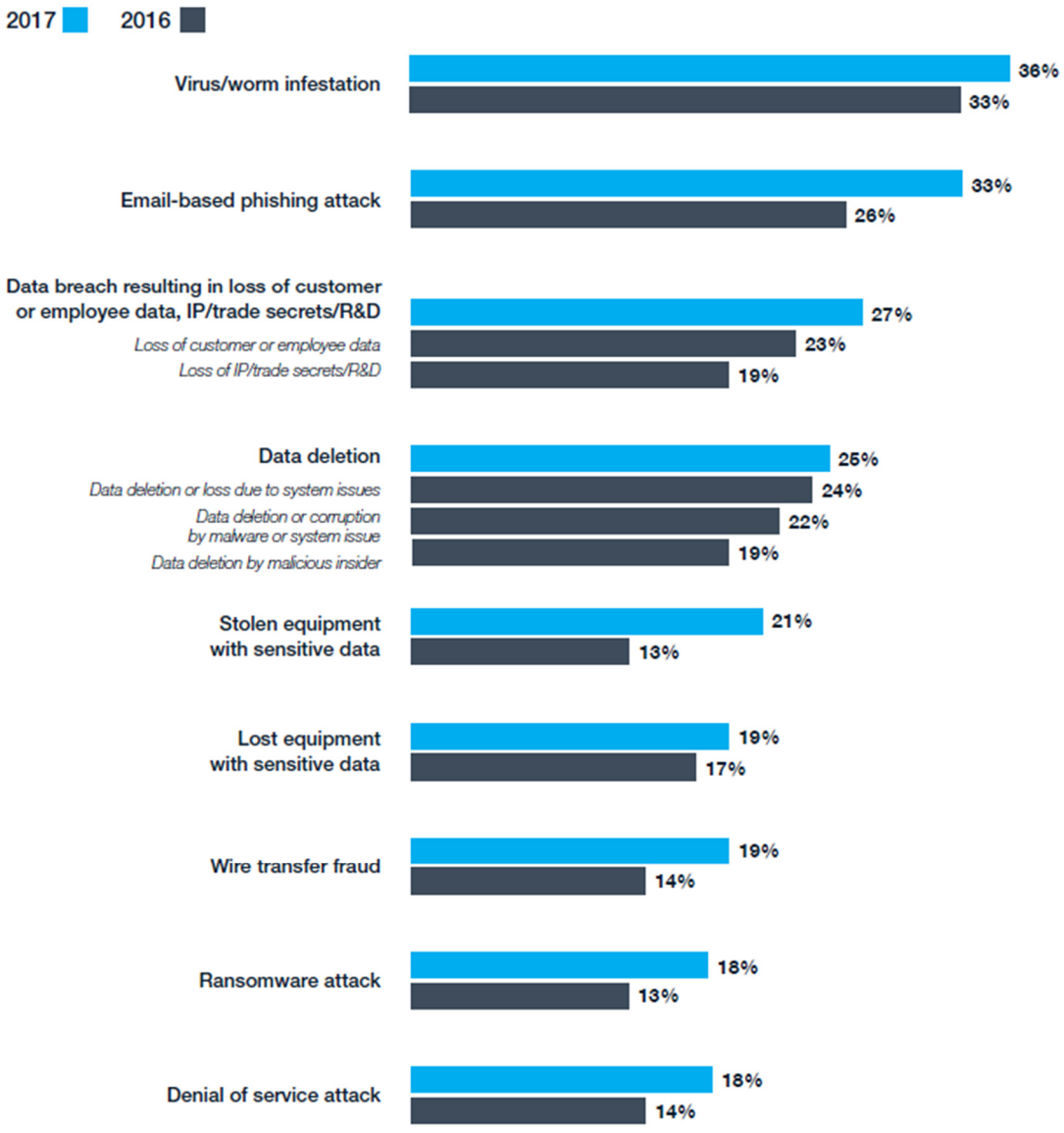
[Πηγή: Kroll Global Fraud & Risk Report, 10th Annual Edition – 2017/18]

Το 2017, έτος κατά το οποίο οι μεγάλοι ιοί, όπως οι WannaCry και Petya, εξαπλώθηκαν σε όλο τον κόσμο, σχεδόν τέσσερα από τα 10 (36%) ερωτηθέντα στελέχη δήλωσαν ότι έχουν πληγεί από επίθεση με ιό ή σκουλήκι (worm), αύξηση 3 ποσοστιαίων μονάδων από το 2016. Οι ιοί και τα σκουλήκια αποτελούν το πιο συχνό είδος επιθέσεων στον κυβερνοχώρο που κατονομάζεται στην έκθεση του 2017.

Ενώ το ένα τέταρτο (26%) των ερωτηθέντων στην έρευνα του 2016 ανέφερε ότι πάσχει από ηλεκτρονική επίθεση μέσω ηλεκτρονικού ταχυδρομείου (phishing), στην έρευνα του 2017, το ένα τρίτο (33%) αντιμετώπισε αυτού του είδους την απειλή.

Επιπλέον, η παραβίαση δεδομένων και η διαγραφή δεδομένων επηρέασε το 27% και το 25% των ερωτηθέντων, αντίστοιχα. Ωστόσο, όλες οι απειλές στον κυβερνοχώρο

δεν περιορίζονταν στην ψηφιακή σφαίρα. Από τα ερωτηθέντα στελέχη, το 21% δήλωσε ότι από την εταιρεία τους έχει κλαπεί εξοπλισμός με ευαίσθητα δεδομένα, ενώ το 19% δήλωσε ότι ο εξοπλισμός έχει «χαθεί», υπογραμμίζοντας τη σύγκλιση φυσικών και ψηφιακών απειλών.

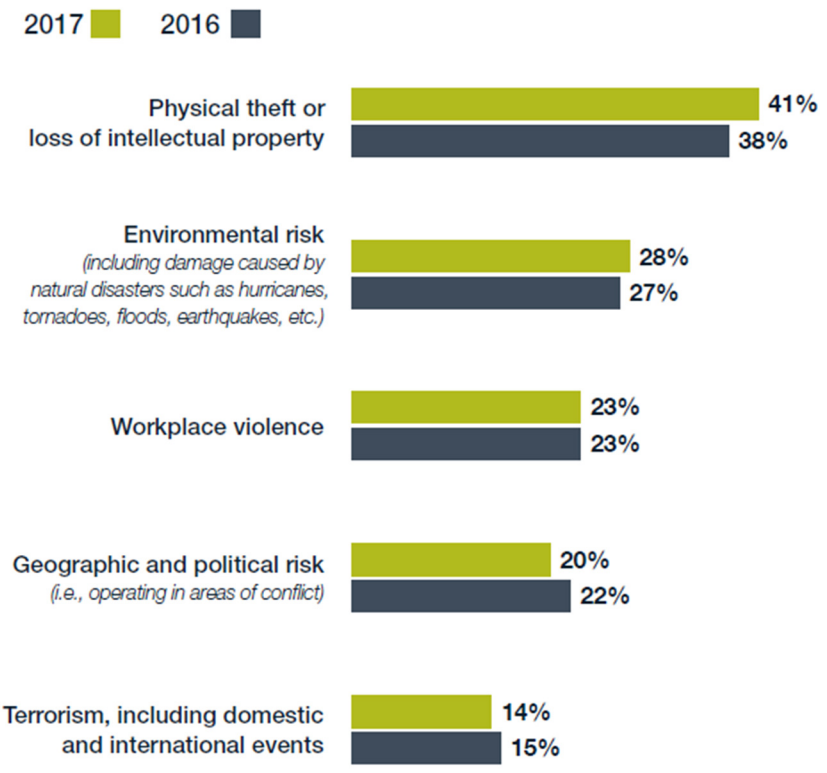


Εικόνα 4: Τύποι περιστατικών κυβερνοασφάλειας που υπέστησαν οι επιχειρήσεις

[Πηγή: Kroll Global Fraud & Risk Report, 10th Annual Edition – 2017/18]

Το 2017 παρουσιάστηκαν μεγάλα περιστατικά παραβίασης της πνευματικής ιδιοκτησίας, που κυμαινόταν από την παραποίηση/απομίμηση προϊόντων μέχρι την παραβίαση εμπορικού σήματος και την κλοπή ιδιοκτησιακών πληροφοριών ή καλλιτεχνικών έργων. Αυτά τα περιστατικά συχνά προκύπτουν από συντονισμένες κυβερνητικές και φυσικές εισβολές.

Η φυσική κλοπή ή η απώλεια πνευματικής ιδιοκτησίας παρέμειναν μακράν ο πιο διαδεδομένος τύπος συμβάντος ασφαλείας. Πράγματι, μεταξύ εκείνων των στελεχών που δήλωσαν ότι αντιμετώπισαν ένα συμβάν ασφάλειας, ένα ιδιαίτερα υψηλό 41% ισχυρίστηκε ότι η εταιρεία τους έπεσε θύμα αυτού του είδους συμβάντος. Οι ερωτηθέντες στον τομέα της μεταποίησης γνώρισαν το υψηλότερο επίπεδο φυσικής κλοπής ή απώλειας πνευματικής ιδιοκτησίας, στο 45%. Οι περιβαλλοντικοί κίνδυνοι έκαναν επίσης την εμφάνιση τους, όπως ανέφερε το 28% των ερωτηθέντων φέτος. Οι κίνδυνοι αυτοί κυριάρχησαν στον τομέα των φυσικών πόρων (42%), ακολουθούμενοι από την υγειονομική περίθαλψη, τα φαρμακευτικά προϊόντα και τη βιοτεχνολογία (35%), την κατασκευές, τη μηχανική και την υποδομές (30%). Σχεδόν το ένα τέταρτο (23%) από όσους αντιμετώπισαν συμβάν ασφαλείας αναφέρθηκε στη βία στο χώρο εργασίας.



Εικόνα 5: Τύποι συμβάντων ασφάλειας που υπέστησαν οι επιχειρήσεις

[Πηγή: Kroll Global Fraud & Risk Report, 10th Annual Edition – 2017/18]

1.4. Οι προκλήσεις της ψηφιακής ασφάλειας

Η ισχυρή ασφάλεια στον ψηφιακό χώρο είναι ολοένα πιο απαραίτητη για όλες τις επιχειρήσεις, με το 78% αυτών να υποστηρίζει πως η ψηφιακή ασφάλεια κατέχει υψηλή θέση στις προτεραιότητες τους σύμφωνα με το Cyber Security Report της Vodafone για το 2017 [31].

Στην συγκεκριμένη αναφορά παρουσιάζονται και οι προκλήσεις της ψηφιακής ασφάλειας που καλούνται να αντιμετωπίσουν οι σύγχρονες επιχειρήσεις.

- **Νέα μοντέλα τηλεργασίας**

Η τηλεργασία κερδίζει συνεχώς έδαφος ως ένα εναλλακτικό μοντέλο εργασίας, καθώς συνδυάζει πτυχές ευελιξίας και ασφάλειας, παρέχοντας μεγαλύτερη αυτονομία στους εργαζόμενους. Αυτό, ωστόσο, σημαίνει ότι χρειάζεται να συνοδεύεται από τις αντίστοιχες λύσεις ψηφιακής ασφάλειας. Για παράδειγμα, η υιοθέτηση μιας βασικής λύσης ασφάλειας φορητών συσκευών είναι απαραίτητη στο νέο ψηφιακό εργασιακό περιβάλλον, όπου υπάρχουν εργαζόμενοι οι οποίοι επεξεργάζονται εταιρικά δεδομένα εκτός γραφείου.

- **Αυξανόμενη χρήση IoT & υπηρεσιών cloud**

Καθώς οι εξελίξεις στη συνδεσιμότητα και τις εφαρμογές IoT (Internet-Of-Things – Διαδίκτυο των Πραγμάτων) είναι συνεχείς, οι επιχειρήσεις αντιμετωπίζουν νέες προκλήσεις. Υπάρχουν, ωστόσο, αξιόπιστες λύσεις που μπορούν να μειώσουν δραστικά κάθε ανησυχία για την ψηφιακή ασφάλεια, εξασφαλίζοντας τη μέγιστη δυνατή προστασία.

- **Διατήρηση της φήμης και αξιοπιστίας κάθε επιχείρησης**

Αξιόπιστες λύσεις ψηφιακής ασφάλειας μπορούν να διασφαλίσουν ότι ένα brand θα είναι συνώνυμο της εμπιστοσύνης για κάθε πελάτη ή συνεργάτη.

- **Νέες μορφές κυβερνοεπιθέσεων**

Καθώς οι οργανισμοί βελτιώνουν την ψηφιακή τους ετοιμότητα, ανοίγουν νέες «λεωφόροι» για διαφορετικές ψηφιακές απειλές. Για παράδειγμα, οι ειδικοί προειδοποιούν για εγκλήματα «υψηλών ταχυτήτων» με επιθέσεις που ως κύριο στόχο θα έχουν αποκλειστικά τα δεδομένα της επιχείρησης. Κατά συνέπεια, είναι πλέον αναγκαία η υιοθέτηση επιχειρησιακής συνέχειας λύσεων που εξασφαλίζουν την ομαλή

και εύρυθμη συνεχή λειτουργία της επιχείρησης, ενώ παράλληλα διασφαλίζουν την προστασία των δεδομένων της, όχι μόνο από επιθέσεις αλλά ακόμα και σε περίπτωση φυσικής καταστροφής.

- **Νέοι νομοθετικοί κανονισμοί**

Καθώς η εξέλιξη της τεχνολογίας προχωρά, αλλάζει και το σχετικό νομοθετικό πλαίσιο στο οποίο οι επιχειρήσεις οφείλουν να εναρμονίζονται διαρκώς. Για παράδειγμα, η έλευση του νέου πλαισίου GDPR (Γενικός Κανονισμός Προστασίας Δεδομένων) τόνισε τη σημασία εφαρμογής νέων διαδικασιών και πολιτικών σε μικρές και μεγάλες επιχειρήσεις.

1.5. Ψηφιακή ασφάλεια και αποτελεσματικότητα επιχειρήσεων

Το Διεθνές Βαρόμετρο Ετοιμότητας για τον Κυβερνοχώρο της Vodafone συνδέει την ψηφιακή ασφάλεια με την αποτελεσματικότητα των επιχειρήσεων, τονίζοντας ότι όσο πιο ασφαλής είναι μια επιχείρηση στον κυβερνοχώρο τόσο καλύτερα επιχειρηματικά αποτελέσματα παρουσιάζει [32].

Στην έρευνα το 48% των επιχειρήσεων που έχουν λάβει μέτρα ψηφιακής ασφάλειας αναφέρουν αύξηση των ετήσιων εσόδων τους κατά 5%, καθώς και υψηλά επίπεδα εμπιστοσύνης των ενδιαφερόμενων μερών (stakeholders).

Το παράδοξο της έρευνας είναι ότι μόνο το 24% των επιχειρήσεων παγκοσμίως πιστεύει ότι είναι πραγματικά έτοιμη σε θέματα ασφάλειας στον κυβερνοχώρο. Κατά την ίδια έκθεση, η ετοιμότητα σε θέματα κυβερνοασφάλειας προϋποθέτει ότι μία επιχείρηση υιοθετεί σειρά διαφορετικών μέτρων, όπως ειδικές λειτουργίες, στρατηγικές και μέτρα ενίσχυσης της ανθεκτικότητας σε κυβερνοεπιθέσεις, καθώς και διαδικασίες για την κατανόηση των κινδύνων και την ευαισθητοποίηση των εργαζομένων.

Τα βασικά ευρήματα της έρευνας όπως τα αποτυπώνει σε άρθρο του το περιοδικό IT Security Pro είναι:

- Οι κλάδοι της υγείας, της τεχνολογίας και των χρηματοπιστωτικών υπηρεσιών διαθέτουν το υψηλότερο επίπεδο ηλεκτρονικής ετοιμότητας, ενώ οι τομείς του λιανεμπορίου και της εκπαίδευσης εμφανίζονται ως οι λιγότερο έτοιμοι.

- Οι μεγαλύτερες επιχειρήσεις είναι πιθανότερο να είναι έτοιμες στον τομέα της ασφάλειας στον κυβερνοχώρο, αλλά ενδέχεται να αντιμετωπίζουν εμπόδια στους τομείς της διαχείρισης και του ελέγχου.
- Οι επιχειρήσεις στην Ινδία, το Ηνωμένο Βασίλειο και τις ΗΠΑ είναι οι πλέον έτοιμες σε θέματα ασφάλειας στον κυβερνοχώρο, ενώ οι εταιρείες από την Ιρλανδία, τη Σιγκαπούρη και τη Γερμανία παρουσιάζουν αδυναμίες.

Μία από τις πιο ενδιαφέρουσες πτυχές, που υπονομεύουν την ετοιμότητα των επιχειρήσεων σε θέματα ψηφιακής ασφάλειας, εντοπίζεται στο γεγονός ότι υπάρχει συχνά αναντιστοιχία μεταξύ αυτού που πιστεύουν οι εργοδότες και του τι συμβαίνει στην πραγματικότητα σε σχέση με τη δραστηριότητα των εργαζομένων.

Το πλέον σημαντικό εύρημα είναι ότι η έκθεση εντοπίζει μία άμεση σχέση ανάμεσα στην ετοιμότητα στον τομέα της κυβερνοασφάλειας και στην επιχειρηματική απόδοση, καθώς και στην καταγραφή ανταγωνιστικού πλεονεκτήματος σε σχέση και με άλλους βασικούς επιχειρηματικούς δείκτες απόδοσης (KPI). Για παράδειγμα, στις πιο προηγμένες επιχειρήσεις:

- Το 68% των επιχειρήσεων που ξεχωρίζουν σε θέματα κυβερνοασφάλειας δηλώνει ότι επικεντρώνεται περισσότερο στην καινοτομία από ό,τι οι άμεσοι ανταγωνιστές τους.
- Το 65% των επιχειρήσεων πιστεύει ότι μπορεί να εστιάσει καλύτερα στους πελάτες τους σε σχέση με τους ανταγωνιστές τους που είναι λιγότερο έτοιμοι σε θέματα κυβερνοασφάλειας.
- Το 59% των επιχειρήσεων, που είναι «cyber ready», πιστεύει ότι διαθέτει ψηφιακό πλεονέκτημα σε σχέση με τον ανταγωνισμό.

1.6. Οι παγκόσμιες δαπάνες για λύσεις ασφάλειας

Υψηλούς ρυθμούς ανάπτυξης θα καταγράψουν οι παγκόσμιες δαπάνες για λύσεις ασφαλείας τα επόμενα χρόνια, καθώς επιχειρήσεις και καταναλωτές αναζητούν προστασία της ψηφιακής τους δραστηριότητας. Υπό αυτό το σκεπτικό, οι σχετικές δαπάνες (σε υλικό, λογισμικό και λύσεις ασφαλείας) αναμένεται να διαμορφωθούν στα επίπεδα των $ 133,7 δισ. το 2022 [33].

Σύμφωνα με την έκθεση «Worldwide Semiannual Security Spending Guide» της International Data Corporation (IDC), ο μέσος ετήσιος ρυθμός ανάπτυξης των δαπανών για την ασφάλεια θα είναι της τάξης του 9,9% έως το 2022. Ως αποτέλεσμα, η συνολική δαπάνη για την ασφάλεια θα αυξηθεί κατά 45% το 2022 σε σχέση με το 2018, οπότε εκτιμάται ότι θα διαμορφωθούν σε $ 92,1 δισ. Πάντως, σύμφωνα με την IDC, η αύξηση των δαπανών για την ασφάλεια θα επιβραδυνθεί σταδιακά κατά την περίοδο της πρόβλεψης έως το 2022. "*Η προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων συγκεντρώνει την προσοχή των επιχειρήσεων, οι οποίες προσπαθούν να εναρμονιστούν με τα νέα πρότυπα συμμόρφωσης, παρόμοια με αυτά του GDPR. Ως αποτέλεσμα, οι δαπάνες για την ασφάλεια θα συνεχίσουν να αυξάνονται στο άμεσο μέλλον"* αναφέρει η εταιρεία.

Οι υπηρεσίες που σχετίζονται με την ασφάλεια θα είναι η μεγαλύτερη κατηγορία των δαπανών ($ 40,2 δισ. το 2018) και η ταχύτερα αναπτυσσόμενη (μέσος ετήσιος ρυθμός ανάπτυξης 11,9%). Το λογισμικό για την ψηφιακή ασφάλεια θα είναι η δεύτερη μεγαλύτερη κατηγορία, με τις σχετικές δαπάνες να ανέρχονται συνολικά σε $ 34,4 δισ. το 2018.

Οι τράπεζες θα είναι ο κλάδος που θα πραγματοποιήσει τη μεγαλύτερη επένδυση σε λύσεις ασφάλειας, δαπανώντας $ 10,5 δισ. το 2018 και $ 16 δισ. το 2022. Οι υπηρεσίες που σχετίζονται με την ασφάλεια θα αντιπροσωπεύουν περισσότερο από το ήμισυ των δαπανών των τραπεζών για την ασφάλεια σε όλη την περίοδο της πρόβλεψης. Ο δεύτερος μεγαλύτερος κλάδος για την ψηφιακή ασφάλεια θα είναι η βιομηχανική παραγωγή και ο τρίτος ο δημόσιος τομέας με δαπάνες $ 8,9 δισ. και $ 7,8 δισ. το 2018 αντίστοιχα. Οι υπηρεσίες θα αντιπροσωπεύουν και στις δύο περιπτώσεις το ήμισυ περίπου των συνολικών δαπανών. Οι κλάδοι, που θα δουν την ταχύτερη αύξηση των δαπανών για την ασφάλεια, θα είναι οι τηλεπικοινωνίες (μέσος ετήσιος ρυθμός ανάπτυξης 13,1%) και ο ευρύτερος δημόσιος τομέας (με μέση ετήσια ανάπτυξη 12,3%).

Οι ΗΠΑ θα είναι η μεγαλύτερη αγορά για τις λύσεις ασφάλειας με συνολική δαπάνη $ 39,3 δισ. το 2018, με το Ηνωμένο Βασίλειο να ακολουθεί με $ 6,1 δισ., την Κίνα να έπεται με $ 5,6 δισ., την Ιαπωνία να βρίσκεται στην επόμενη θέση με $ 5,1 δισ. και τη Γερμανία να βρίσκεται στην επόμενη θέση με $ 4,6 δισ.

ΚΕΦΑΛΑΙΟ 2:

ΑΝΤΙΜΕΤΩΠΙΣΗ ΤΟΥ ΖΗΤΗΜΑΤΟΣ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

2.1 Εισαγωγή

Είναι προφανές ότι η ανάπτυξη της τεχνολογίας και η ενσωμάτωση της στις λειτουργίες ενός οργανισμού έχει φέρει το ζήτημα της ασφάλειας στο προσκήνιο των διοικητικών αποφάσεων. Το ψηφιακό μάρκετινγκ, τα κοινωνικά δίκτυα και οι ηλεκτρονικές επικοινωνίες των επιχειρήσεων με τους πελάτες τους καθιστούν την προστασία των προσωπικών δεδομένων πιο επιτακτική από ποτέ.

2.2. Νομοθεσία στην Ελλάδα

Στην Ελλάδα αρμόδιος φορέας είναι η *Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)* η οποία είναι μια ανεξάρτητη Αρχή που ιδρύθηκε με το νόμο 2472/1997, ο οποίος ενσωματώνει στο ελληνικό δίκαιο την Ευρωπαϊκή Οδηγία 95/46/ΕΚ.

Αποστολή της Αρχής αποτελεί η προστασία των δικαιωμάτων της προσωπικότητας και της ιδιωτικής ζωής του ατόμου στην Ελλάδα. Πρωταρχικός σκοπός της Αρχής είναι η προστασία του πολίτη από την παράνομη επεξεργασία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση που διαπιστώνεται παραβίαση των σχετικών δικαιωμάτων του σε κάθε επιχειρησιακό τομέα (χρηματοπιστωτικά, υγεία, ασφάλιση, εκπαίδευση, δημόσια διοίκηση, μεταφορές, ΜΜΕ, κλπ.). Επίσης, σκοπός της Αρχής είναι η υποστήριξη και καθοδήγηση των υπεύθυνων επεξεργασίας στην εκπλήρωση των υποχρεώσεων τους απέναντι στο νόμο, λαμβάνοντας υπόψη τις νέες ανάγκες υπηρεσιών της ελληνικής κοινωνίας, καθώς και την διείσδυση των σύγχρονων ψηφιακών επικοινωνιών και δικτύων. Ως εκ τούτου, η Αρχή στρέφει ιδιαίτερα την προσοχή της μεταξύ άλλων στην παρατήρηση και

αντιμετώπιση ζητημάτων που προκύπτουν με την εξέλιξη των νέων τεχνολογιών και εφαρμογών.

Όσον αφορά την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, η ΑΠΔΠΧ εφαρμόζει το νόμο 3471/2006 που αντίστοιχα ενσωματώνει στο εθνικό δίκαιο την Ευρωπαϊκή Οδηγία 58/2002.

Ο νόμος περιλαμβάνει κυρίως υποχρεώσεις που αφορούν τους φορείς παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, από τις οποίες προκύπτουν και τα δικαιώματα των συνδρομητών των υπηρεσιών αυτών. Επιπλέον, προβλέπονται ρυθμίσεις οι οποίες έχουν εφαρμογή σε όλους τους υπευθύνους επεξεργασίας, όπως αυτές για την καταγραφή κλήσεων, τις προϋποθέσεις πρόσβασης σε πληροφορία αποθηκευμένη σε τερματικό εξοπλισμό χρήστη (π.χ. cookies), σχετικά με τη νομιμότητα προώθησης προϊόντων και υπηρεσιών μέσω τηλεφώνου και την αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου και SMS προωθητικού χαρακτήρα.

2.3. Εθνική Στρατηγική Κυβερνοασφάλειας

Οι κυβερνοεπιθέσεις αποτελούν πλέον καθημερινότητα για τις επιχειρήσεις και τους δημόσιους οργανισμούς. Είτε πρόκειται για ένα phishing email («email ψαρέματος»), είτε για μια μαζική επίθεση που επηρεάζει συνολικά τη λειτουργία ενός οργανισμού τοπικά ή και σε διεθνές επίπεδο, οι κυβερνοεπιθέσεις αποτελούν σήμερα μια από τις βασικές ανησυχίες όχι μόνο των υπεύθυνων IT, αλλά και των διοικήσεων των εταιρειών καθώς μπορούν να οδηγήσουν σε απώλειες τόσο σε οικονομικό, όσο και σε επίπεδο αξιοπιστίας προς τους πελάτες και συνεργάτες.

Με απόφαση του Υπουργού Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, Νίκου Παππά, εγκρίθηκε στις 7/3/2018 η Εθνική Στρατηγική Κυβερνοασφάλειας [6].

Με την Εθνική Στρατηγική Κυβερνοασφάλειας αναπτύσσεται ο κεντρικός σχεδιασμός της Ελληνικής Πολιτείας για την ασφάλεια στον κυβερνοχώρο. Η σημασία της είναι κρίσιμη με δεδομένη την ολοένα αυξανόμενη χρήση του Διαδικτύου και των Τεχνολογιών Πληροφορικής και Επικοινωνιών σε κάθε πτυχή των δραστηριοτήτων του δημόσιου και του ιδιωτικού τομέα. Στόχος είναι η δημιουργία ενός ασφαλούς περιβάλλοντος Διαδικτύου, υποδομών και υπηρεσιών, που θα τονώσει την εμπιστοσύνη

των πολιτών και θα τους οδηγήσει στην περαιτέρω χρήση νέων ψηφιακών προϊόντων και υπηρεσιών και στην τόνωσης της οικονομικής ανάπτυξης της χώρας μας.

Την συνολική ευθύνη για την εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας φέρει η Εθνική Αρχή Κυβερνοασφάλειας, που συστάθηκε και λειτουργεί στη Γενική Γραμματεία Ψηφιακής Πολιτικής του Υπουργείου Ψηφιακής Πολιτικής Τηλεπικοινωνιών και Ενημέρωσης. Η Αρχή αυτή, ως φορέας υψηλού πολιτικού-κυβερνητικού επιπέδου με εξειδικευμένα στελέχη, παρακολουθεί και υλοποιεί τις δράσεις της Εθνικής Στρατηγικής Κυβερνοασφάλειας. Είναι επίσης αρμόδια για τον συντονισμό μεταξύ των φορέων που δραστηριοποιούνται στην Ελλάδα στον τομέα της ασφάλειας στον κυβερνοχώρο, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα. Στις προτεραιότητες της Εθνικής Αρχής Κυβερνοασφάλειας εντάσσεται η συνεργασία με τους αρμόδιους φορείς για την ενσωμάτωση της Οδηγίας (ΕΕ) 2016/1148 «Σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση» (NIS Directive) στο ελληνικό δίκαιο.

2.4. Κοινοτική νομοθεσία

Η Ευρωπαϊκή Ένωση δίνει ιδιαίτερη βαρύτητα στην κυβερνοασφάλεια και την ασφάλεια των ηλεκτρονικών συναλλαγών των πολιτών της, ψηφίζοντας μια σειρά από Οδηγίες που αφορούν τις ηλεκτρονικές συναλλαγές και την προστασία των προσωπικών δεδομένων.

Η πιο πρόσφατη και σημαντική Οδηγία είναι ο νέος *Ευρωπαϊκός Κανονισμός Προστασίας Προσωπικών Δεδομένων (ΓΚΠΔ 2016/679 | General Data Protection Regulation, GDPR)* που έχει τεθεί σε εφαρμογή από την 25η Μαΐου 2018, και καθορίζει ένα νέο νομικό πλαίσιο για την διακυβέρνηση της επεξεργασίας αλλά και της ασφάλειας των προσωπικών δεδομένων για τους οργανισμούς της Ευρωπαϊκής Ένωσης (European Commission, 2018). Ο κανονισμός τυποποιεί τους κανόνες στην ΕΕ, ώστε να εξασφαλιστεί αυστηρότερος έλεγχος των οργανισμών που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα, με αυστηρά πρόστιμα για μη συμμόρφωση.

Παράλληλα με τον κανονισμό GDPR, η ΕΕ έχει νομοθετήσει την *Οδηγία 2016/1148/ΕΕ* σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση – καλούμενη και ως οδηγία NIS από

τα αρχικά του αγγλικού όρου Network and Information Systems – η οποία στοχεύει στην υιοθέτηση μέτρων από όλα τα κράτη μέλη για ένα υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε όλη την ΕΕ [13].

Άλλες οδηγίες της ΕΕ που αναφέρονται σε θέματα προστασίας προσωπικών δεδομένων και ασφάλειας ηλεκτρονικών συναλλαγών και οι οποίες έχουν ενσωματωθεί στο εσωτερικό Δίκαιο της Ελλάδας είναι οι εξής:

- Η Οδηγία 95/46, που ενσωματώθηκε στο εθνικό δίκαιο με τον Νόμο 2476 και αφορά στη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Η Οδηγία 97/66, που ενσωματώθηκε στο εθνικό δίκαιο με τον Νόμο 2774 και αφορά στην προστασία των θεμελιωδών δικαιωμάτων της ιδιωτικής ζωής των ατόμων και στη θέσπιση των προϋποθέσεων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα.
- Η Οδηγία 99/93, που ενσωματώθηκε στο εθνικό δίκαιο με το Προεδρικό Διάταγμα 150/2001 και αφορά στο νομικό πλαίσιο που διέπει την χρήση των ηλεκτρονικών υπογραφών.

2.5. Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

2.5.1. Περιγραφή

Τα δεδομένα είναι το “πετρέλαιο” της 4ης βιομηχανικής επανάστασης. Σύμφωνα με εκτιμήσεις, η αξία της αγοράς των προσωπικών δεδομένων υπολογίζεται ότι θα ανέλθει σε σχεδόν €1 τρισ. το 2020, ενώ έως το 2025 εκτιμάται ότι ο όγκος των δεδομένων θα αυξηθεί από 16,1 ZB σε 163 ZB (όπου *1 ZB = 1021 bytes)*. Αναμενόμενα, καθώς τα ίδια τα δεδομένα και η αγορά που διαμορφώνεται γύρω από αυτά διογκώνονται, αυξάνονται εκθετικά και οι κίνδυνοι παραβίασής τους ακόμη και σε μεγάλες επιχειρήσεις, με εξαιρετικά δυσμενείς επιπτώσεις. Ταυτόχρονα, η διαχείρισή τους με σεβασμό στην προσωπικότητα και την ιδιωτική ζωή του καθενός μας, θα γίνει σταδιακά βασικό κριτήριο αξιολόγησης κάθε επιχείρησης που χειρίζεται προσωπικά δεδομένα, δηλαδή πρακτικά όλων [3].

Η αλυσίδα τέτοιων φαινομένων, αλλά και η ανάγκη ρύθμισης της αγοράς των προσωπικών δεδομένων, οδήγησαν στην αυστηριοποίηση του νομικού πλαισίου πανευρωπαϊκά και στη θέσπιση του νέου Γενικού Κανονισμού GDPR. Με έναρξη εφαρμογής την 25η Μαΐου 2018, ο νέος Κανονισμός, προβλέποντας ένα αρκετά αυστηρό και γραφειοκρατικό πλαίσιο, ήρθε να θωρακίσει την ιδιωτικότητα και να μεταθέσει την ευθύνη της προστασίας στην ίδια την επιχείρηση, προβλέποντας κυρώσεις ύψους έως και 4% του παγκόσμιου τζίρου για όσους αποτύχουν να συμμορφωθούν με τις απαιτήσεις του.

Με τίτλο «ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)» το GDPR δεν ισχύει μόνο για οργανισμούς εγκατεστημένους εντός της ΕΕ, αλλά ισχύει και για οργανισμούς που βρίσκονται εκτός της ΕΕ, εφόσον προσφέρουν αγαθά ή υπηρεσίες ή παρακολουθούν τη συμπεριφορά των δεδομένων των πολιτών της ΕΕ. Εφαρμόζεται σε όλες τις εταιρείες που επεξεργάζονται και κατέχουν τα προσωπικά δεδομένα των πολιτών που διαμένουν στην Ευρωπαϊκή Ένωση, ανεξαρτήτως της τοποθεσίας της εταιρείας [9].

Στους οργανισμούς μπορούν να επιβληθούν πρόστιμα έως 4% του ετήσιου παγκόσμιου κύκλου εργασιών για παραβίαση του GDPR ή 20 εκατομμυρίων ευρώ. Πρόκειται για το μέγιστο πρόστιμο που μπορεί να επιβληθεί για τις πιο σοβαρές παραβάσεις, π.χ. δεν υπάρχει επαρκής συναίνεση του πελάτη για επεξεργασία δεδομένων ή παραβίαση του πυρήνα των εννοιών «Απόρρητο από το σχεδιασμό». Υπάρχει μια κλιμακωτή προσέγγιση στα πρόστιμα, π.χ. σε μια εταιρεία μπορεί να επιβληθεί πρόστιμο κατά 2% για μη τήρηση των αρχείων της (άρθρο 28), μη κοινοποίηση στην εποπτεύουσα αρχή και στον πολίτη σχετικά με την παραβίαση προσωπικών δεδομένων ή μη διενέργεια εκτίμησης επιπτώσεων.

Το GDPR ισχύει για τα «προσωπικά δεδομένα», δηλαδή για κάθε πληροφορία που σχετίζεται με αναγνωρίσιμο πρόσωπο το οποίο μπορεί να προσδιοριστεί άμεσα ή έμμεσα, ιδίως με αναφορά σε ένα αναγνωριστικό στοιχείο. Αυτός ο ορισμός παρέχει ένα ευρύ φάσμα προσωπικών αναγνωριστικών τα οποία συνιστούν δεδομένα προσωπικού χαρακτήρα, συμπεριλαμβανομένου του ονόματος, του αριθμού ταυτότητας, των δεδομένων τοποθεσίας ή του ηλεκτρονικού αναγνωριστικού, που αντικατοπτρίζει τις

αλλαγές στην τεχνολογία και τον τρόπο με τον οποίο οι οργανισμοί συλλέγουν πληροφορίες για τους ανθρώπους.

Ο νόμος έχει σχεδιαστεί για να προστατεύσει όλους τους Ευρωπαίους πολίτες από τις παραβιάσεις της ιδιωτικότητας και των προσωπικών δεδομένων τους, σε ένα κόσμο που είναι ολοένα και περισσότερο καθοδηγούμενος από τα δεδομένα. Αυτός ο κόσμος, είναι σήμερα πολύ διαφορετικός από αυτόν που υπήρχε το 1995, όταν και σε ισχύ τέθηκε η Ευρωπαϊκή οδηγία 95/46/ΕΚ. Μια άλλη πτυχή του ευρωπαϊκού κανονισμού είναι να δοθεί στους πολίτες μεγαλύτερος έλεγχος των δεδομένων τους καθώς και να γίνει πιο εύκολη η πρόσβαση σε αυτά. Επιπλέον, μία από τις απαιτήσεις του νέου κανονισμού είναι να διευκολύνεται η διαγραφή και η φορητότητα των δεδομένων. Επομένως, αν κάποιος χρήστης επιθυμεί να διαγραφούν τελείως ή να μεταφερθούν τα δεδομένα του από έναν πάροχο ή φορέα σε έναν άλλο, αυτό θα πρέπει να γίνεται απρόσκοπτα και με ασφάλεια.

Τα οφέλη που προκύπτουν από τη νέα ρύθμιση για τους πολίτες είναι ότι τους δίνει δικαίωμα στη λήθη, ρητή τους συγκατάθεση για την επεξεργασία των προσωπικών τους δεδομένων, ευκολότερη πρόσβαση στα δεδομένα τους, δυνατότητα ασφαλούς φορητότητας δεδομένων και μεγαλύτερη γνώση για το πώς αντιμετωπίζονται αυτά.

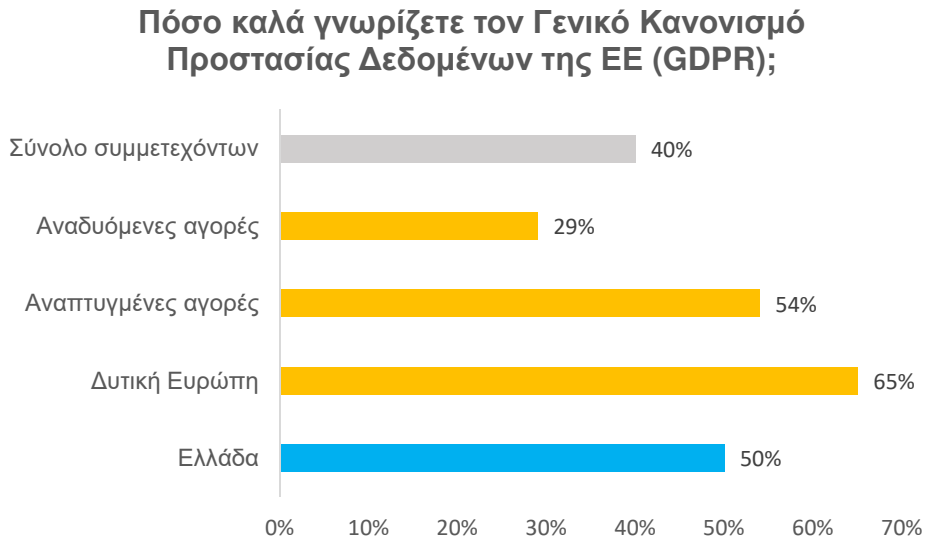
Αυτό σημαίνει ότι οι επιχειρήσεις θα πρέπει να έχουν αναλύσει και να γνωρίζουν τι είδους δεδομένα συλλέγουν και διαχειρίζονται, πού αποθηκεύονται αυτά τα δεδομένα, καθώς και να έχουν τη συγκατάβαση των χρηστών σχετικά με το αν επιθυμούν τα δεδομένα τους να διαμοιράζονται με τρίτους.

Επίσης, κάθε οργανισμός με περισσότερους από 250 εργαζομένους θα πρέπει να διαθέτει έναν Επόπτη Προστασίας Δεδομένων (Data Protection Officer) ο οποίος θα πρέπει να φροντίζει να διασφαλίζεται η συμμόρφωση του οργανισμού με το νέο γενικό κανονισμό. Μια ακόμη υποχρέωση είναι ότι σε περίπτωση απώλειας ή διαρροής δεδομένων, ο οργανισμός θα πρέπει να ειδοποιεί άμεσα τους εμπλεκόμενους πολίτες και εντός 72 ωρών τις αρχές. Επομένως, θα πρέπει να έχει γίνει σχετική προετοιμασία, ώστε να είναι σε θέση να παρέχει την απαραίτητη τεκμηρίωση και τα εν λόγω λεπτομερή στοιχεία. Οι πολίτες, επίσης, θα μπορούν να ζητήσουν τα δεδομένα τους, και οι εταιρείες και οι οργανισμοί θα πρέπει να είναι σε θέση να μπορούν να παρέχουν σχετικό ψηφιακό αντίγραφο τους ή να τα διαγράψουν άμεσα και το κυριότερο, θα πρέπει να είναι σε θέση να εγγυηθούν την ασφάλεια τους.

2.5.2. Παγκόσμια έρευνα για τη γνώση του GDPR από τα στελέχη

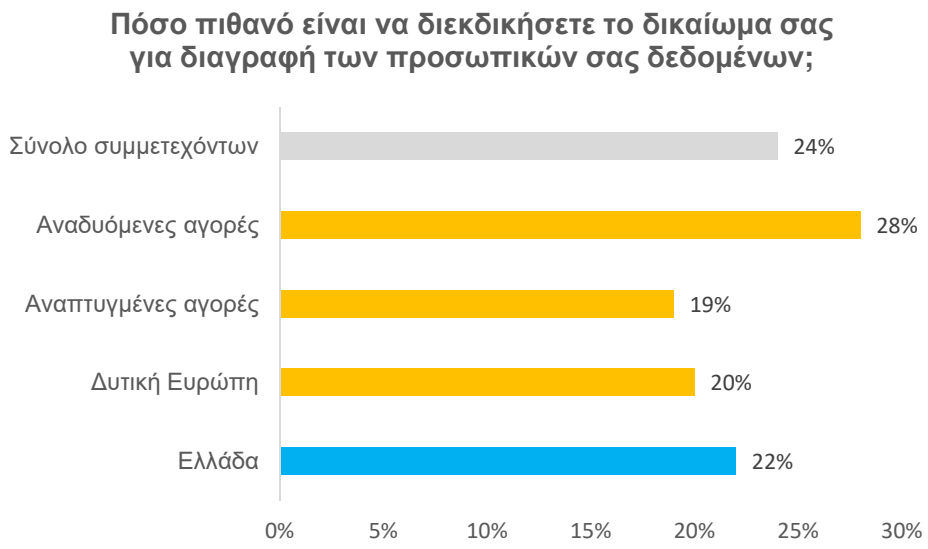
Σύμφωνα με την έρευνα της Ernst & Young (EY) το ποσοστό των στελεχών στην Ελλάδα το οποίο δηλώνει ότι γνωρίζει τι προβλέπει ο κανονισμός GDPR είναι 50%, υψηλότερο σε σχέση με τον παγκόσμιο μέσο όρο που είναι 40% [28].

Σύμφωνα με την ίδια έρευνα μόνο το 22% των Ελλήνων απαντούν καταφατικά στην ερώτηση *"πόσο πιθανό είναι να εξασκήσετε το δικαίωμά σας να ζητήσετε να διαγραφούν τα προσωπικά σας στοιχεία;",* καταλήγοντας η έρευνα στο συμπέρασμα ότι *"Είναι προφανές ότι, στην Ελλάδα, απαιτείται εντατικοποίηση των προσπαθειών για την ενημέρωση, τόσο των καταναλωτών, όσο και των επιχειρήσεων και του Δημόσιου Τομέα για τα ζητήματα που άπτονται του ΓΚΠΔ, καθώς η μη συμμόρφωση επιφέρει σημαντικές ποινές και κυρώσεις".* Το αντίστοιχο ποσοστό παγκοσμίως είναι 24%.



Εικόνα 6: Ποσοστό όσων απάντησαν «Αρκετά» και «Πολύ καλά» στην ερώτηση «Πόσο καλά γνωρίζετε τον Γενικό Κανονισμό Προστασίας Δεδομένων της ΕΕ (GDPR);»,

[Πηγή: EY 15η Global Fraud Survey 2018]



Εικόνα 7: Ποσοστό όσων απάντησαν «Αρκετά» και «Πολύ πιθανό» στην ερώτηση «Πόσο πιθανό είναι να διεκδικήσετε το δικαίωμα σας για διαγραφή των προσωπικών σας δεδομένων;», [Πηγή: ΕΥ 15η Global Fraud Survey 2018]

2.6. Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA)

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), είναι ένα ευρωπαϊκό κέντρο εμπειρογνωσίας για την ασφάλεια στον κυβερνοχώρο. Ο ENISA βοηθά την ΕΕ και τα κράτη μέλη της να εξοπλίζονται και να προετοιμάζονται καλύτερα ώστε να προλαμβάνουν, να εντοπίζουν και να αντιμετωπίζουν προβλήματα που αφορούν την ασφάλεια των πληροφοριών [11].

Ο ENISA παρέχει πρακτικές συμβουλές και λύσεις σε φορείς του δημόσιου και του ιδιωτικού τομέα των χωρών της ΕΕ, καθώς και στα θεσμικά όργανα της ΕΕ. Συμβάλλει ειδικότερα στα εξής:

- ανάπτυξη πανευρωπαϊκών ασκήσεων αντιμετώπισης κρίσεων στον κυβερνοχώρο
- ανάπτυξη εθνικών στρατηγικών ασφάλειας στον κυβερνοχώρο
- προώθηση της συνεργασίας μεταξύ ομάδων αντιμετώπισης έκτακτων αναγκών στην πληροφορική, καθώς και της ανάπτυξης ικανοτήτων.

Ο ENISA δημοσιεύει, επίσης, εκθέσεις και μελέτες για την ασφάλεια στον κυβερνοχώρο. Έχει εκπονήσει μελέτες σχετικά με:

- την ασφάλεια στο υπολογιστικό νέφος
- την προστασία των δεδομένων
- τις τεχνολογίες για τη βελτίωση της προστασίας του ιδιωτικού βίου & την εξασφάλιση αυτής της προστασίας στις νέες τεχνολογίες
- την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπίστευσης για τις ηλεκτρονικές συναλλαγές
- τον εντοπισμό απειλών στον κυβερνοχώρο

Τέλος, ο ENISA συμβάλλει στον σχεδιασμό της πολιτικής και της νομοθεσίας της ΕΕ σχετικά με την ασφάλεια δικτύων και πληροφοριών, καθώς και στην οικονομική ανάπτυξη στην εσωτερική αγορά της Ευρώπης.

Το Ιούνιο του 2018 η ΕΕ ανακοίνωσε ότι πρόκειται να ενισχύσει την ανθεκτικότητα στον κυβερνοχώρο μέσω της δημιουργίας ενός πανευρωπαϊκού πλαισίου πιστοποίησης για τα προϊόντα, τις υπηρεσίες και τις διαδικασίες τεχνολογίας των πληροφοριών και των επικοινωνιών (ΤΠΕ). Η βιομηχανία θα μπορούσε να αξιοποιήσει το νέο μηχανισμό για την πιστοποίηση προϊόντων όπως τα συνδεδεμένα αυτοκίνητα και τα έξυπνα ιατροτεχνολογικά βοηθήματα. Το Συμβούλιο κατέληξε σε γενική προσέγγιση όσον αφορά την πρόταση, γνωστή ως πράξη για την ασφάλεια στον κυβερνοχώρο. Στόχος της πρότασης θα είναι επίσης η αναβάθμιση του υφιστάμενου Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) σε μόνιμη Υπηρεσία της ΕΕ για την κυβερνοασφάλεια [12].

Το σχέδιο κανονισμού προβλέπει τη θέσπιση μηχανισμού για τη δημιουργία ευρωπαϊκών συστημάτων πιστοποίησης της κυβερνοασφάλειας για ειδικές διαδικασίες, προϊόντα και υπηρεσίες ΤΠΕ. Τα πιστοποιητικά που εκδίδονται στο πλαίσιο των συστημάτων θα ισχύουν σε όλες τις χώρες της ΕΕ, έτσι ώστε να είναι ευκολότερο για τους χρήστες να αποκτήσουν εμπιστοσύνη στην ασφάλεια των τεχνολογιών αυτών, οι δε εταιρείες να διεξάγουν τις επιχειρηματικές τους δραστηριότητες πέραν των συνόρων. Η πιστοποίηση θα είναι εθελοντική, εκτός αν άλλως ορίζεται στη νομοθεσία της ΕΕ ή των κρατών μελών. Μεταξύ των χαρακτηριστικών που καλύπτονται θα συγκαταλέγονται η ανθεκτικότητα σε τυχαία ή κακόβουλη απώλεια ή αλλοίωση δεδομένων. Θα διακρίνονται τρία διαφορετικά επίπεδα διασφάλισης: βασικό, σημαντικό ή υψηλό. Για το βασικό

επίπεδο, οι κατασκευαστές ή οι πάροχοι υπηρεσιών θα μπορούν να διενεργήσουν οι ίδιοι αξιολόγηση της συμμόρφωσης.

Οι νέοι κανόνες θα χορηγήσουν στον ENISA μόνιμη εντολή και θα αποσαφηνίσουν το ρόλο του ως οργανισμού της ΕΕ για την κυβερνοασφάλεια. Νέα καθήκοντα θα ανατεθούν στον ENISA για την παροχή στήριξης στα κράτη μέλη, τα θεσμικά όργανα της ΕΕ και άλλους φορείς σε θέματα κυβερνοχώρου. Σε επίπεδο ΕΕ, θα διοργανώνει τακτικές ασκήσεις κυβερνοασφάλειας και θα υποστηρίζει και προωθεί την πολιτική της ΕΕ για την πιστοποίηση της κυβερνοασφάλειας. Η πρώτη νομοθετική πράξη της ΕΕ στον τομέα της κυβερνοασφάλειας - η οδηγία του 2016 σχετικά με την ασφάλεια δικτύων και πληροφοριών (NIS) - είχε ήδη προσδώσει στον ENISA βασικό ρόλο στην στήριξη της εφαρμογής της οδηγίας.

Η εντολή προβλέπει, επίσης, ένα δίκτυο εθνικών υπαλλήλων-συνδέσμων με σκοπό τη διευκόλυνση της ανταλλαγής πληροφοριών μεταξύ του ENISA και των κρατών μελών.

ΚΕΦΑΛΑΙΟ 3:

ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

3.1. Εισαγωγή

Η διαχείριση της ασφάλειας πληροφοριών στοχεύει στην προστασία των πληροφοριακών συστημάτων, περιορίζοντας την επικινδυνότητα σε αποδεκτό επίπεδο. Περιλαμβάνει:

- Την αξιολόγηση της επικινδυνότητας και τον προσδιορισμό του αποδεκτού επιπέδου ασφάλειας
- Την ανάπτυξη και εφαρμογή της Πολιτικής Ασφάλειας
- Την δημιουργία του κατάλληλου οργανωτικού πλαισίου και εξασφάλιση των απαιτούμενων πόρων για την εφαρμογή της Πολιτικής Ασφάλειας
- Την εκπαίδευση, ενημέρωση και ευαισθητοποίηση των χρηστών των πληροφοριακών συστημάτων για ζητήματα ασφάλειας

Το σημαντικό είναι να κατανοήσουμε ότι η διαχείριση της ασφάλειας πληροφοριών είναι μία επιχειρησιακή διαδικασία η οποία δεν περιλαμβάνει μόνο τεχνικά ζητήματα τα οποία πρέπει να προσδιορίσει ο οργανισμός, αλλά συμπεριλαμβάνει και ζητήματα από άλλους χώρους όπως οικονομία, διοίκηση, κοινωνία κτλ. Είναι συνολική δουλειά όλου του οργανισμού και όλου του προσωπικού και δεν αφορά μόνο την διευθέτηση τεχνικών θεμάτων που άπτονται στις αρμοδιότητες ενός IT manager.

Ο σκοπός της διαχείρισης ασφάλειας πληροφοριών είναι να δώσει όλα τα κατάλληλα εργαλεία λήψης αποφάσεων στη διοίκηση. Όπως αναφέρει και η PwC στην έρευνα της για την ασφάλεια πληροφοριών στην Ελλάδα (*PwC Παγκόσμια Έρευνα για την Ασφάλεια των Πληροφοριών 2013) «οι επικεφαλής της ασφάλειας πληροφοριών θα έπρεπε να έχουν στρατηγικό ρόλο στη λήψη σημαντικών αποφάσεων καθώς αυτές επηρεάζουν σημαντικά τη λειτουργία και την πορεία μια επιχείρησης. Γι' αυτό και ο ρόλος τους θα πρέπει να είναι αναβαθμισμένος και να έχουν πρόσβαση στη διοίκηση».*

3.2. Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ)

Η πληροφορία που παράγει ή διαχειρίζεται ένας οργανισμός κατά την λειτουργία του, είναι ένα αντικείμενο ζωτικής σημασίας. Σήμερα, οι πληροφορίες θεωρούνται ως προϊόντα με επιχειρησιακή αξία, χρησιμότητα και σημασία. Αξίζει να σημειωθεί πως αυτό ισχύει για όλα τα είδη και μεγέθη των επιχειρήσεων. Για τον λόγο αυτό η αναγνώριση της επιχειρησιακής αξίας των πληροφοριών είναι μέγιστης σπουδαιότητας σε όλους τους οργανισμούς [5].

Η πληροφορία λαμβάνει διάφορες μορφές όπως, έντυπη ή χειρόγραφη σε χαρτί, σε ηλεκτρονική μορφή, αποθηκευμένη σε συστήματα υπολογιστών, σε βάσεις δεδομένων ή διακινούμενη σε δίκτυα κάθε είδους, μέσω ηλεκτρονικού ταχυδρομείου ή άλλων υπηρεσιών. Επίσης, η πληροφορία μπορεί να επιδεικνύεται σε παρουσιάσεις με διάφορα οπτικά μέσα, ή ακόμη να παράγεται σε προφορική μορφή κατά την διάρκεια συζητήσεων η τηλεφωνικών συνδιαλέξεων.

Δεδομένου ότι οι πληροφορίες αυξάνονται στον όγκο, την πολυπλοκότητα, και την κρισιμότητά τους, και καθώς η πρόσβαση στις πληροφορίες διευρύνεται, είναι όλο και περισσότερο τρωτές. Περισσότεροι άνθρωποι μπορούν να έχουν πρόσβαση σε περισσότερα στοιχεία όσο ποτέ άλλοτε. Συνεπώς η ασφάλεια των ευαίσθητων πληροφοριών επιχείρησης καθίσταται μια απόλυτη ανάγκη για τους οργανισμούς.

Οι σύγχρονες επιχειρησιακές απειλές που αντιμετωπίζουν οι επιχειρήσεις σε καθημερινή βάση από την ραγδαία εξέλιξη της τεχνολογίας προκαλούν τεράστιες ανησυχίες, σε βαθμό που θεωρείται αναγκαία η εφαρμογή ενός συστήματος που να διαχειρίζεται την ασφάλεια των πληροφοριών. Ένα τέτοιο σύστημα ασφάλειας πληροφοριών προσφέρει αποτελεσματική προστασία από τις διάφορες αρνητικές επιδράσεις συμπεριλαμβανομένων οικονομικών συνεπειών, αδυναμίας στην προστασία της πνευματικής ιδιοκτησίας του οργανισμού, απώλειας μεριδίου αγοράς, ή ακόμη και απώλειας φήμης.

Για τον σκοπό αυτό απαιτείται η ανάπτυξη και ενσωμάτωση στην λειτουργία του οργανισμού, ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών, το οποίο να επικεντρώνεται στις διαδικασίες που λαμβάνουν χώρα στο πλαίσιο του οργανισμού. Για τη διαχείριση της ασφάλειας πληροφοριών υπάρχουν πολλές διαφορετικές μεθοδολογίες που χρησιμοποιούν ή στηρίζονται σε κάποιο από τα πολλά και διαφορετικά πρότυπα που έχουν αναπτυχθεί, όπως [10]:

- OCTAVE από τον οργανισμό CERT (Carnegie Mellon University)

- COBIT από τον οργανισμό ISACA. Βασίζεται στον κύκλο: Govern → Direct → Control → Implement → Measure → Evaluate →Report
- FIRM από το Information Security Forum
- Μεθοδολογία του οργανισμού NIST. Βασίζεται στον κύκλο: System Characterization → Threat Identification → Vulnerability Identification → Control Analysis → Likelihood Determination → Impact Analysis → Risk Determination → Control Recommendations → Results Documentation

Μια μέθοδος ιδιαίτερα διαδεδομένη για τον έλεγχο και τη βελτίωση των διαδικασιών κατά την ανάπτυξη ενός ΣΔΑΠ είναι η μέθοδος Plan-Do-Check-Act (PDCA) η οποία αποτελείται από τέσσερα επαναληπτικά βήματα:

- Σχεδιασμός (Plan), όπου αναλύεται και μελετάται η ασφάλεια πληροφοριών στον οργανισμό, θέτονται οι στόχοι και ορίζονται οι τρόποι με τους οποίους θα επιτευχθούν.
- Υλοποίηση (Do), όπου υλοποιούνται τα μέτρα τα οποία ορίστηκαν κατά τη φάση του σχεδιασμού
- Έλεγχος (Check), όπου πραγματοποιείται έλεγχος απόκλισης των αρχικών στόχων και των τελικών αποτελεσμάτων.
- Δράση (Act), όπου εφαρμόζονται ενέργειες διόρθωσης και βελτίωσης μέτρων.

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών είναι μία διεργασία η οποία δέχεται ως είσοδο τις απαιτήσεις ασφάλειας του οργανισμού και παρέχει ως έξοδο τη διαχείριση της ασφάλειας πληροφοριών.

Κατά τη φάση του σχεδιασμού, πραγματοποιείται ανάλυση και εκτίμηση επικινδυνότητας και διαμορφώνονται και υλοποιούνται τα εξής:

- Έγκριση από τη διοίκηση του οργανισμού
- Καθορισμός του πεδίου εφαρμογής (υπολογιστικά συστήματα, δεδομένα κλπ.)
- Μελέτη ανάλυσης και αποτίμησης επικινδυνότητας
- Καθορισμός απαιτήσεων ασφάλειας
- Δημιουργία Πολιτικής Ασφάλειας

Είναι πρωταρχικής σημασίας για έναν οργανισμό ο καθορισμός των απαιτήσεων του σε θέματα ασφάλειας. Μερικές βασικές πηγές άντλησης πληροφοριών για απαιτήσεις ασφάλειας είναι:

- Η αποτίμηση επικινδυνότητας (Risk Assessment) που αντιμετωπίζει ο οργανισμός. Μέσω αυτής της διαδικασίας αναγνωρίζονται οι πιθανές απειλές προς τους πόρους του οργανισμού. Επιπλέον, εκτιμάται η συνολική ευπάθεια (vulnerability) του οργανισμού στις συγκεκριμένες απειλές, η πιθανότητα υλοποιήσεων τους, καθώς και το κόστος που θα έχουν οι επιπτώσεις για τον οργανισμό από πιθανές επιθέσεις.
- Το νομικό και κανονιστικό πλαίσιο, καθώς και οι συμβατικές υποχρεώσεις του οργανισμού απέναντι στο κράτος, το προσωπικό και τους συνεργάτες του.
- Το σύνολο των αρχών, των απαιτήσεων και των στόχων που ορίζει ο ίδιος ο οργανισμός σχετικά με την επεξεργασία των πληροφοριών που είναι απαραίτητες για τη λειτουργία του.

Στη φάση της υλοποίησης και με βάση τα αποτελέσματα της αποτίμησης, ακολουθεί νέα μελέτη που αποσκοπεί στη μείωση της επικινδυνότητας με την επιλογή και υλοποίηση των κατάλληλων μέτρων προστασίας. Αναλυτικότερα, διαμορφώνονται και υλοποιούνται μεταξύ άλλων τα εξής:

- Σχέδιο Διαχείρισης Επικινδυνότητας
- Κατανομή ρόλων και αρμοδιοτήτων
- Υλοποίηση μέτρων ασφαλείας
- Δράσεις ενημέρωσης και κατάρτισης του προσωπικού
- Υλοποίηση διαδικασιών έγκαιρης ανίχνευσης και αντιμετώπισης περιστατικών ασφαλείας

Κατά τον έλεγχο, πραγματοποιείται μια αξιολόγηση των αποτελεσμάτων σε σχέση με τους αρχικούς στόχους που είχαν τεθεί και διαμορφώνεται μια αναφορά αξιολόγησης προς τη διοίκηση του οργανισμού. Η διαδικασία του ελέγχου είναι επαναληπτική και πραγματοποιείται ανά τακτά χρονικά διαστήματα, συνήθως από το αρμόδιο τμήμα εσωτερικού ελέγχου του οργανισμού.

Τέλος, στα στάδιο της δράσης εκτελούνται όλες εκείνες οι απαραίτητες ενέργειες, οι οποίες κρίθηκε ότι απαιτούνται προκειμένου να βελτιωθεί η συνολική διεργασία της διαχείρισης ασφάλειας πληροφοριών. Πραγματοποιείται ενημέρωση της διοίκησης και

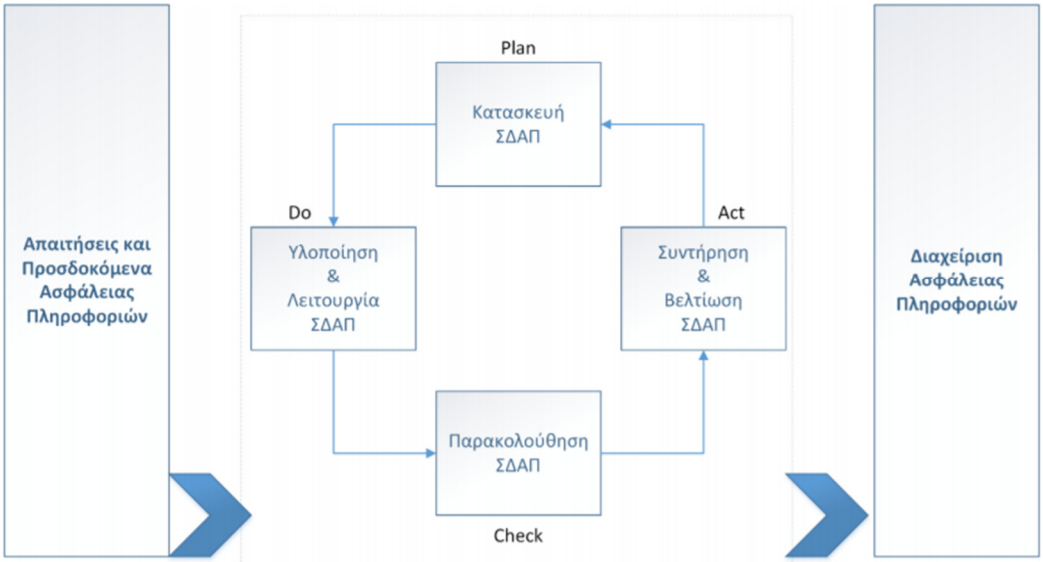
παράλληλα ελέγχεται και αξιολογείται και η ίδια η διαδικασία βελτίωσης των μέτρων προστασίας.

Συνοπτικά, τα οφέλη για έναν οργανισμό από την υιοθέτηση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών είναι σημαντικά και πολλαπλά. Ενδεικτικά αναφέρονται τα εξής:

- διαβεβαιώνει τα ενδιαφερόμενα μέρη ότι η επιχείρηση συμμορφώνεται με την υπάρχουσα νομοθεσία
- βελτιώνει την αξιοπιστία και ενισχύει την εμπιστοσύνη πελατών
- αποδεικνύει τη δέσμευση της ανώτερης διοίκησης για την ασφάλεια των πληροφοριών ενός οργανισμού
- δέσμευση του προσωπικού και βελτίωση της κουλτούρας ασφάλειας των πληροφοριών στην εργασία
- παρέχει την ευκαιρία για τη συνεχή βελτίωση μέσω των συστηματικών επιθεωρήσεων
- εξασφάλιση της αποτελεσματικής ολοκλήρωσης των θεμάτων διαχείρισης της ασφάλειας των πληροφοριών με άλλα διαχειριστικά συστήματα (π.χ. ISO 9001)
- μείωση του κόστους – από άμεσα κόστη π.χ. κλοπή φορητού υπολογιστή, και από έμμεσα κόστη π.χ. φήμη, νομικές απώλειες
- παροχή ανταγωνιστικού πλεονεκτήματος και αναβάθμιση της εικόνας του οργανισμού.

3.3. Πρότυπο ISO/IEC 27001

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System–ISMS) κατά ISO/IEC 27001, το οποίο συνιστά μια συνολική και συστηματική προσέγγιση του οργανισμού στην διαχείριση της ευαίσθητης πληροφορίας του και των κινδύνων που την απειλούν, έτσι ώστε η πληροφορία να παραμένει ασφαλής, συνδυάζει τα τέσσερα βήματα της μεθοδολογία PDCA.



Εικόνα 8: Διαχείριση Ασφάλειας Πληροφοριών κατά ISO/IEC 27001

Πηγή: Μαυρίδης Ιωάννης (2015), *Ασφάλεια Πληροφοριών στο Διαδίκτυο*, Σύνδεσμος Ελληνικών και Ακαδημαϊκών Βιβλιοθηκών (ΣΕΑΒ)

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) κατά το ISO/IEC 27001 είναι ένα σύνολο μέτρων και εταιρικών διαδικασιών με στόχο την προστασία των δεδομένων από τους πλέον πιθανούς και σοβαρούς κινδύνους, ώστε να ελαχιστοποιήσουμε τις πιθανότητες:

- να χαθούν και να μη μπορούμε να δουλέψουμε και να εξυπηρετήσουμε τους πελάτες μας
- να διαρρεύσουν σε τρίτους που μπορούν να μας βλάψουν
- να αλλοιωθούν προκαλώντας μας ζημιά.

Τα μέτρα ασφάλειας και οι εταιρικές διαδικασίες αφορούν την τεχνολογική προστασία της εταιρείας (back-up, firewalls, κρυπτογράφηση, κλπ.), τις επιχειρησιακές λειτουργίες (φυσική ασφάλεια, πρόσβαση προσωπικού σε δεδομένα, διαχείριση προσωπικού και υπεργολάβων, κλπ.) και τις πρακτικές των χρηστών (κωδικοί, δικαιώματα, κλπ.).

Το ISO/IEC 27001 είναι το διεθνές πρότυπο που αποτελεί τον αδιαμφισβήτητο οδηγό για κάθε επιχείρηση που επιθυμεί να ελέγξει και να βελτιστοποιήσει τα μέτρα ασφάλειας και τις εταιρικές διαδικασίες της ως προς όλες τις πλευρές της ασφάλειας πληροφοριών. Περιλαμβάνει 114 περιοχές ελέγχου και σε συνδυασμό με το ερμηνευτικό πρότυπο ISO/IEC 27002 αποτελούν το πλέον διαδεδομένο πλαίσιο αναφοράς στον

κόσμο για την ασφάλεια πληροφοριών. Πρωτοεμφανίσθηκε ως ISO 17799 το 2000, βασιζόμενο στο βρετανικό BS 7799 του 1995, και στη συνέχεια βγήκε η πρώτη έκδοση του ISO/IEC 27001 το 2005, η οποία αναθεωρήθηκε το 2013 [4].

3.4. Διαχείριση κινδύνων

3.4.1. Εισαγωγή

Καθώς το ψηφιακό λειτουργικό περιβάλλον κάθε οργανισμού μεγαλώνει συνεχώς σε όγκο και νέα πληροφοριακά συστήματα ενσωματώνονται στο περιβάλλον αυτό για να υποστηρίξουν τις λειτουργίες του οργανισμού, οι κίνδυνοι οι οποίοι μπορούν να εισέλθουν μέσα στον οργανισμό αυξάνονται συνεχώς.

Η πληροφορία, σε οποιαδήποτε μορφή και αν αυτή υφίσταται, αποτελεί σημαντικό περιουσιακό στοιχείο και διαδραματίζει πρωταρχικό ρόλο στην επίτευξη των επιχειρησιακών στόχων κάθε οργανισμού, δημιουργώντας την ανάγκη ύπαρξης ενός επαρκούς συστήματος προστασίας για τη διασφάλιση της αξιοπιστίας της.

Ως *Διαχείριση Κινδύνων* ορίζεται η διαδικασία κατά την οποία αναγνωρίζονται, αναλύονται, αξιολογούνται, κοινοποιούνται και περιορίζονται οι εκάστοτε κίνδυνοι. Η διαχείριση της οποιασδήποτε μορφής κινδύνων είναι μία διαρκής διαδικασία, η οποία περιλαμβάνει στάδια, κατά τα οποία οι κίνδυνοι προσδιορίζονται και αξιολογούνται και στη συνέχεια υλοποιούνται οι κατάλληλες δικλείδες ασφαλείας, προκειμένου να μειωθούν οι κίνδυνοι και κατ' επέκταση η αρνητική επίπτωση που έχουν. Μέρος της διαδικασίας αποτελεί και η ενημέρωση του προσωπικού για θέματα που αφορούν στη μείωση των κινδύνων. Η διαδικασία ολοκληρώνεται με το συνεχή έλεγχο της τήρησης και επάρκειας των δικλείδων ασφαλείας.

3.4.2. Κίνδυνος

Ο κίνδυνος είναι συνυφασμένος με τις έννοιες των απειλών και των αδυναμιών ασφάλειας πληροφοριών.

Συγκεκριμένα, ο *κίνδυνος* που αφορά στην ασφάλεια πληροφοριών προσδιορίζεται από το γινόμενο της πιθανότητας εκδήλωσης μιας απειλής και της επίδρασης της απειλής στον οργανισμό [14].

Κίνδυνος = (Πιθανότητα εκδήλωσης Απειλής Ασφάλειας) Χ (Επίδραση της Απειλής)

Στο σημείο αυτό θα αναλύσουμε τους ορισμούς που χρησιμοποιούνται στην ανάλυση κινδύνων:

3.4.3. Απειλή

Απειλή είναι ένα μη επιθυμητό γεγονός που μπορεί να προκαλέσει μη διαθεσιμότητα του συστήματος και των υπηρεσιών, τυχαία ή με πρόθεση μετατροπή των δεδομένων, καταστροφή των δεδομένων ή του συστήματος και τέλος μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών. Με άλλα λόγια είναι η δυνατότητα πρόκλησης ζημιάς σε έναν πληροφοριακό πόρο και κατά συνέπεια στον οργανισμό.

Ως κυριότερες κατηγορίες απειλών ασφάλειας πληροφοριών μπορούμε να θεωρήσουμε τις ακόλουθες [15]:

- Απώλεια Εμπιστευτικότητας των πληροφοριών που διακινούνται, καθώς και των πληροφοριών που αφορούν στα προσωπικά δεδομένα πελατών & συνεργατών.
- Απώλεια Ακεραιότητας των πληροφοριών κατά τη διακίνησή τους, με πιθανό αποτέλεσμα τη μη εξουσιοδοτημένη τροποποίησή τους (π.χ. τροποποίηση χρηματικών ποσών ή ποσοτήτων παραγγελιών, καθώς και τροποποίηση των αποδεκτών κάποιων πληρωμών).
- Απώλεια Διαθεσιμότητας λόγω (ακούσιας ή ηθελημένης) δυσλειτουργίας των δικτύων επικοινωνίας ή λόγω ηθελημένης ενέργειας, με σκοπό τη διακοπή παροχής των συγκεκριμένων υπηρεσιών. Αποτέλεσμα μιας τέτοιας απειλής είναι πιθανή αδυναμία λειτουργίας των παρεχόμενων υπηρεσιών, καθώς και αδυναμία αναζήτησης δεδομένων που αφορούν κάποιες συναλλαγές.

- Επανάληψη της διενέργειας προηγούμενης συναλλαγής, χρησιμοποιώντας τα ίδια ακριβώς δεδομένα (διπλές καταχωρήσεις, διπλές εγγραφές).
- Άρνηση κάποιου από τα συναλλασσόμενα μέρη ότι διενέργησε ή συμμετείχε σε συναλλαγή.
- Εξαπάτηση του Οργανισμού μέσω πλαστοπροσωπίας.
- Απάτη μέσω εκμετάλλευσης διαφόρων αδυναμιών ασφάλειας, με αποτέλεσμα την εξαπάτηση συνεργατών ή πελατών από τρίτους ή την εξαπάτηση του Οργανισμού από άτομα του περιβάλλοντός του.

Οι απειλές διακρίνονται σε εσωτερικές οι οποίες προέρχονται από το εσωτερικό περιβάλλον του οργανισμού και εξωτερικές οι οποίες προέρχονται από το εξωτερικό περιβάλλον του.

3.4.4. Ευπάθεια

Ευπάθεια είναι η αδυναμία ή σχεδιαστική ατέλεια σε ένα σύστημα, στην εφαρμογή ή στην υποδομή που μπορεί να γίνει αιτία για την παραβίαση της ασφάλειας και της ακεραιότητας του συστήματος. Η ευπάθεια μπορεί να οριστεί και με την εξής συνάρτηση:

Ευπάθεια = (Πιθανότητα να συμβεί μια απειλή) Χ (Πιθανότητα να είναι επιτυχής)

Όλα τα πληροφοριακά συστήματα έχουν ευπάθειες που μπορούν να τύχουν εκμετάλλευσης από απειλές με σημαντικές συνέπειες στη λειτουργία ενός οργανισμού, την κερδοφορία, την αξία και την μακροπρόθεσμη επιβίωση του.

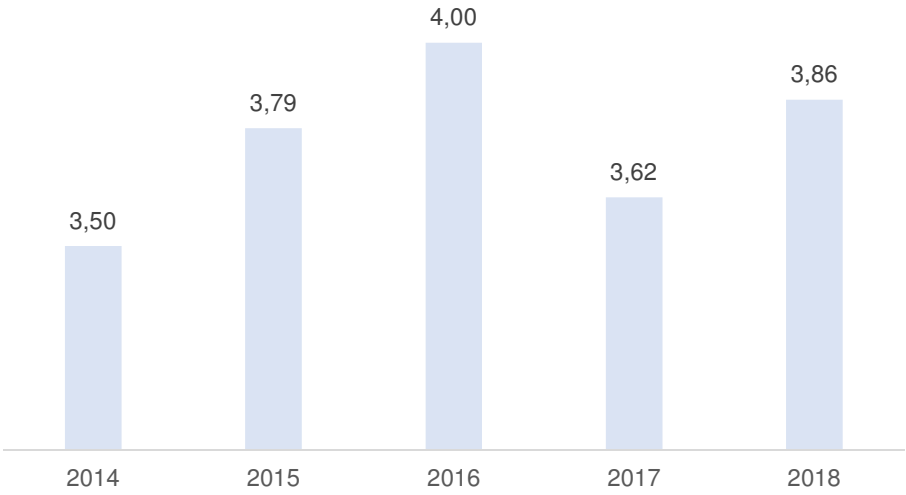
3.4.5. Περιστατικό ασφαλείας

Περιστατικό ασφαλείας είναι οτιδήποτε αποκλίνει από την κανονική λειτουργία των συστημάτων και διαδικασιών. Είναι προφανές ότι κάθε περιστατικό ασφαλείας

μπορεί να έχει αρνητικές συνέπειες είτε με άμεσο τρόπο (απώλεια χρημάτων) ή με έμμεσο (πλήγμα στην αξιοπιστία και τη φήμη του οργανισμού).

Τις οικονομικές επιπτώσεις που έχουν τα περιστατικά ασφαλείας τις παρουσιάζει σε ετήσια βάση η έρευνα του Ponemon Institute το οποίο διενεργεί μελέτες σε παγκόσμιο επίπεδο.

Σύμφωνα με την τελευταία έρευνα του 2018, το μέσο συνολικό κόστος των περιστατικών ασφαλείας φτάνει τα 3,86 εκατομμύρια δολάρια (αύξηση κατά 6,4% σε σχέση με το 2017) [16].



Εικόνα 9: Μέσο συνολικό κόστος περιστατικών ασφαλείας (σε εκατομμύρια $)

(Πηγή: Ponemon Institute, 2018 Cost of a Data Breach Study)

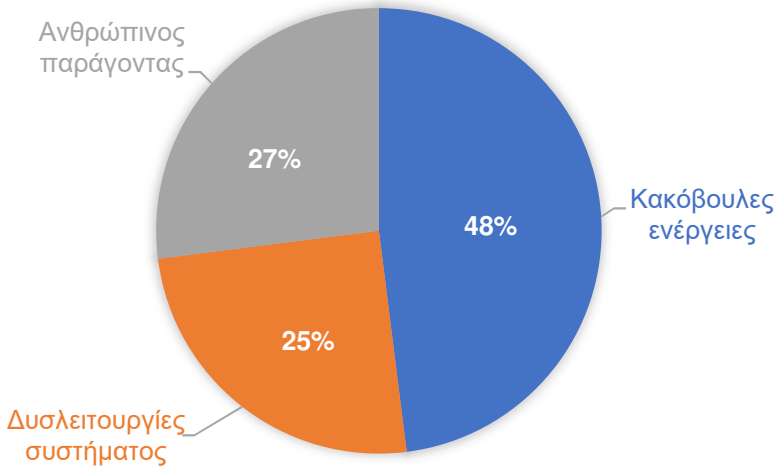
Το μέσο κατά κεφαλήν κόστος για κάθε περιστατικό ασφαλείας υπολογίζεται στα 148 δολάρια. Οι χώρες με το μεγαλύτερο μέσο κατά κεφαλήν κόστος είναι οι ΗΠΑ, ο Καναδάς, η Γερμανία, η Γαλλία και το Μεξικό.

Σημειώνεται ότι με τον όρο «κατά κεφαλήν κόστος» (“per capita cost”) ορίζεται το συνολικό κόστος ενός μεμονωμένου περιστατικού διαιρεμένου με το πλήθος των εγγραφών των δεδομένων που διέρρευσαν ή χάθηκαν.

Στη συνέχεια, παρουσιάζεται η διερεύνηση των αιτιών των περιστατικών ασφαλείας και αν αυτά προέρχονται από:

- Κακόβουλες ενέργειες όπως εισαγωγή ιομορφικού λογισμικού (malware), επιθέσεις εκ των έσω (insider attacks), μεθόδων κοινωνικής μηχανικής (phishing/social engineering) και δικτυακών επιθέσεων (SQL injection, XXS)
- Δυσλειτουργία συστημάτων η οποία μπορεί να διακόψει τη ροή εργασιών της μηχανογράφησης και συνεπώς του business
- Ανθρώπινους παράγοντες όπως αμέλεια καθηκόντων ή άγνοια κινδύνου

Τα αποτελέσματα της έρευνας για το 2018 δείχνουν ότι το 48% των περιστατικών ασφαλείας προέρχονται από κακόβουλες ενέργειες, ενώ ιδιαίτερα αυξημένο είναι και το ποσοστό του ανθρώπινου παράγοντα το οποία ανέρχεται στο 27%, επισημαίνοντας την ανάγκη για εκπαίδευση και ενημέρωση του προσωπικού σε ό,τι αφορά τη διαχείριση των πληροφοριών εντός του οργανισμού.



Εικόνα 10: Αίτια περιστατικών ασφαλείας

(Πηγή: Ponemon Institute, 2018 Cost of a Data Breach Study)

3.4.6. Ανάλυση επικινδυνότητας

Η διαδικασία της Διαχείρισης Κινδύνων θα οδηγήσει στην αποτίμηση των κινδύνων και στους τρόπους αντιμετώπισης τους. Για το λόγο αυτό κατά την έναρξη της διαδικασίας πρέπει να προσδιοριστούν τα παρακάτω [14]:

- Τεκμηρίωση μεθοδολογίας αξιολόγησης κινδύνων, η οποία θα περιλαμβάνει τα βήματα που πρέπει να ακολουθηθούν, ποιοι πρέπει να εμπλακούν σε κάθε βήμα, αλλά και ποιος ο τρόπος υπολογισμού του κινδύνου.

- Προσδιορισμός του εύρους που εντάσσεται στην εν λόγω διαδικασία. Το εύρος περιλαμβάνει όλο το περιβάλλον στο οποίο λειτουργούν οι τεχνικές υποδομές (ανθρώπινο δυναμικό, διαδικασίες, τεχνολογικό περιβάλλον).

- Κριτήρια αποδοχής κινδύνου – προσδιορισμός των περιστάσεων – περιπτώσεων κατά τις οποίες ο οργανισμός αποδέχεται τον κίνδυνο. Για παράδειγμα, η εταιρεία μπορεί να ορίσει ότι κατά τη διάρκεια ανάπτυξης ενός πολύ σημαντικού project θα υπάρχει μεγαλύτερη ανεκτικότητα που αφορά στην αποδοχή συγκεκριμένων κινδύνων.

- Ανεκτό επίπεδο κινδύνου – προσδιορισμός του επιπέδου κινδύνου, το οποίο ο οργανισμός μπορεί να αποδεχθεί. Η συγκεκριμένη απόφαση είναι απόφαση της διοίκησης της εταιρείας.

Η αξιολόγηση κινδύνων ασφάλειας πληροφοριών είναι η διαδικασία κατά την οποία αναγνωρίζονται οι κίνδυνοι που αφορούν στους πληροφοριακούς πόρους του οργανισμού, ενώ ταυτόχρονα προσδιορίζεται η πιθανότητα εκδήλωσης του κινδύνου, η αρνητική επίδραση που θα επιφέρει και οι δικλείδες ασφάλειας οι οποίες πρέπει να εφαρμοστούν, ώστε τόσο να ελαχιστοποιηθεί ο κίνδυνος στο επιθυμητό επίπεδο, όσο και η αρνητική επίδρασή του σε περίπτωση που εκδηλωθεί.

Κατά τη διαδικασία αξιολόγησης κινδύνων, συλλέγονται πληροφορίες σχετικά με τα δεδομένα (τα οποία αποτελούν μέρος των περιουσιακών στοιχείων της εταιρείας) και τους πληροφοριακούς πόρους στους οποίους αυτά αποθηκεύονται και επεξεργάζονται. Οι πληροφορίες αφορούν στην κρισιμότητα των δεδομένων για τη λειτουργία της

εταιρείας και στις απειλές στις οποίες εκτίθενται. Ο συνδυασμός και η ανάλυση των παραπάνω πληροφοριών, έχει σαν στόχο τον προσδιορισμό και την αξιολόγηση του κινδύνου στον οποίο εκτίθεται η εταιρεία, τόσο κατά την καθημερινή της λειτουργία, όσο και στο πλαίσιο ανάπτυξης ενός έργου ή κατά τη φάση υλοποίησης και σχεδιασμού νέων υπηρεσιών και δραστηριοτήτων.

Τα προσδοκώμενα αποτελέσματα της αξιολόγησης κινδύνων είναι τα ακόλουθα:

- Προσδιορισμός των απειλών και αδυναμιών ασφάλειας, που αφορούν στις επιχειρησιακές πληροφορίες
- Εκτίμηση κινδύνου και επιχειρησιακής επίδρασης
- Προσδιορισμός των κατάλληλων δικλείδων ασφαλείας για την ελαχιστοποίηση των κινδύνων.

Τα βασικά βήματα της διαδικασίας για την αξιολόγηση κινδύνων είναι τα ακόλουθα:

- Προσδιορισμός πληροφοριών και της αξίας τους για τον οργανισμό
- Προσδιορισμός αδυναμιών ασφάλειας και απειλών
- Εκτίμηση κινδύνου
- Σχέδιο δράσης για την ελαχιστοποίηση των κινδύνων

Στον παρακάτω πίνακα παρατίθενται ενδεικτικές περιοχές ελέγχου, οι οποίες κατ' ελάχιστο θα πρέπει να αποτελούν μέρος της αξιολόγησης κινδύνων:

Πίνακας 1: Περιοχές ελέγχου της αξιολόγησης κινδύνων

Περιοχές Ελέγχου	**Υπό αξιολόγηση δικλείδες ασφαλείας**
Διαχείριση Ασφάλειας Πληροφοριών	• Πολιτική ασφάλειας • Διαδικασίες και πρότυπα • Αξιολόγηση & Διαχείριση Κινδύνων • Ρόλοι και αρμοδιότητες
Δικλείδες Ασφαλείας που αφορούν στη Λειτουργία των Πληροφοριακών Συστημάτων	• Ασφάλεια Προσωπικού • Φυσική Ασφάλεια • Εξωτερικοί συνεργάτες

	• Σχέδιο επιχειρηματικής συνέχειας • Διαμόρφωση συστημάτων • Διαχείριση περιστατικών ασφάλειας • Διαχείριση αλλαγών • Ενημέρωση, εκπαίδευση • Ακεραιότητα συστημάτων και δεδομένων • Προστασία αποθηκευτικών μέσων
Τεχνικές δικλείδες ασφαλείας	• Πιστοποίηση ταυτότητας χρηστών • Έλεγχος πρόσβασης • Accountability • Log files • Κρυπτογράφηση • Δικλείδες ασφαλείας εφαρμογών • Ασφάλεια δικτύου • Προστασία από κακόβουλο λογισμικό

Έχοντας ολοκληρώσει τους ελέγχους, απομένει η αξιολόγηση των αποτελεσμάτων και ο προσδιορισμός του κινδύνου για κάθε μία από τις αδυναμίες ασφάλειας που εντοπίσθηκαν.

- Αξιολόγηση αποτελεσμάτων και εκτίμηση του κινδύνου – Εκτίμηση του επιπέδου κινδύνου για κάθε ζεύγος απειλής και αδυναμίας ασφάλειας, που έχει προκύψει από το προηγούμενο στάδιο.

- Προσδιορισμός δικλείδων ασφαλείας και διορθωτικών ενεργειών – Οι διορθωτικές ενέργειες αφορούν στον προσδιορισμό νέων δικλείδων ασφαλείας ή στη βελτιστοποίηση της αποτελεσματικότητας αυτών που υπάρχουν, με στόχο την ελαχιστοποίηση ή την εξάλειψη των κινδύνων που έχουν προσδιορισθεί.

Κύριος στόχος των διορθωτικών ενεργειών είναι ο περιορισμός του κινδύνου σε επίπεδο το οποίο να είναι αποδεκτό για την εταιρεία. Αυτό σημαίνει ότι οι προτεινόμενες διορθωτικές ενέργειες είναι ικανές να διαμορφώσουν επίπεδο ασφάλειας ανάλογο της

κρισιμότητας των δεδομένων στα οποία απευθύνονται και να περιορίσουν τον υφιστάμενο κίνδυνο σε επίπεδο ανεκτό για τη λειτουργία της εταιρείας και την επίτευξη των επιχειρησιακών της στόχων

Έχοντας ολοκληρώσει τον προσδιορισμό και την αξιολόγηση των κινδύνων, χρειάζεται να προσδιοριστεί και ο τρόπος διαχείρισης των κινδύνων. Ο αποτελεσματικότερος τρόπος για να γίνει αυτό, είναι να τεκμηριωθεί συγκεκριμένο Σχέδιο Διαχείρισης των Κινδύνων, στο οποίο θα περιγράφεται ο τρόπος αντιμετώπισης των κινδύνων, η σειρά αντιμετώπισής τους, ποιος θα είναι ο υπεύθυνος υλοποίησης των διορθωτικών ενεργειών και ποιος ο χρόνος υλοποίησης αυτών.

Τα περιεχόμενα Σχεδίου Διαχείρισης Κινδύνων είναι τουλάχιστον τα ακόλουθα:

- Τρόπος διαχείρισης κινδύνων – για κάθε κίνδυνο που έχει προσδιορισθεί και αξιολογηθεί, χρειάζεται να προσδιορισθεί ο τρόπος διαχείρισής του. Η αντιμετώπιση ενός κινδύνου εμπίπτει σε μία από τις παρακάτω περιπτώσεις: Αντιμετώπιση (υλοποίηση συγκεκριμένων διορθωτικών ενεργειών), Αποδοχή (σύμφωνα με κριτήρια για την αποδοχή του κινδύνου και το ανεκτό επίπεδο κινδύνου), Αποφυγή, Μεταβίβαση κινδύνων (σε τρίτα μέρη και συνεργάτες).

- Προσδιορισμός προτεραιοτήτων για υλοποίηση, προσδιορισμός της σειράς υλοποίησης των διορθωτικών ενεργειών με βάση την κρισιμότητα του αλλά και τις απαιτήσεις σε πόρους και χρόνο.

- Χρονοδιάγραμμα υλοποίησης, στόχοι, συμφωνημένος χρόνος υλοποίησης – όλα αυτά θα πρέπει να συμφωνούνται με τους εκάστοτε υπεύθυνους για την υλοποίηση.

- Προσδιορισμός απαιτούμενων πόρων, εξοικονόμηση πόρων.

- Διαδικασία ελέγχου τρόπου και χρόνου υλοποίησης – Επανέλεγχος για την υλοποίηση των διορθωτικών ενεργειών με το συμφωνημένο τρόπο και στο συμφωνημένο χρονικό πλαίσιο.

- Εναπομένων κίνδυνος – Υπολογισμός του επιπέδου κινδύνου, το οποίο συνεχίζει να υφίσταται και μετά την υλοποίηση των διορθωτικών ενεργειών. Πολύ σημαντική ενέργεια, διότι ενημερώνει τη διοίκηση για την πραγματική διάσταση των κινδύνων.

Η αποτελεσματικότητα του σχεδίου διαχείρισης των κινδύνων εξαρτάται και επηρεάζεται από διάφορους παράγοντες, οι οποίοι χρήζουν διαφορετικής αντιμετώπισης, ανάλογα με το λειτουργικό περιβάλλον στο οποίο αναφέρονται.

Οι εν λόγω παράγοντες, είναι οι ακόλουθοι:

- Ευκολία/δυσκολία υλοποίησης των προτεινόμενων διορθωτικών ενεργειών. Η γνώμη των τεχνικών πρέπει να λαμβάνεται σοβαρά υπόψη, αναφορικά με την εφαρμοσιμότητα των προτεινόμενων διορθωτικών ενεργειών.

- Διαθεσιμότητα πόρων στο δεδομένο χρονικό διάστημα

- Εσωτερική επικοινωνία και κουλτούρα της εταιρείας

- Επιχειρηματικές – τεχνολογικές προτεραιότητες της εταιρείας

Η αποτελεσματική διαχείριση των κινδύνων ολοκληρώνεται με το συνεχή έλεγχο, τόσο της υλοποίησης των διορθωτικών ενεργειών που έχουν προκύψει, αλλά και με τον έλεγχο της αποτελεσματικής λειτουργίας των υφιστάμενων δικλείδων ασφάλειας. Για το λόγο αυτό, κρίνεται επιβεβλημένη η υιοθέτηση ενός πλαισίου συνεχούς ελέγχου, το οποίο περιλαμβάνει τα έξης:

- Έλεγχος αποτελεσματικής λειτουργίας υφιστάμενων δικλείδων ασφαλείας ανά τακτά χρονικά διαστήματα. Προτεραιότητα δίδεται στις δικλείδες ασφαλείας που αφορούν στις κρίσιμες επιχειρηματικές διεργασίες.

- Επιθεώρηση υλοποίησης του σχεδίου διαχείρισης κινδύνων.

- Αξιολόγηση κινδύνων ασφάλειας στις νέες τεχνολογίες που πρόκειται να χρησιμοποιηθούν.

- Ανεξάρτητος έλεγχος για το υφιστάμενο επίπεδο ασφάλειας πληροφοριών.

- Δημιουργία αναφορών, κοινοποίηση αποτελεσμάτων, ενημέρωση διοίκησης.

- Διαδικασία συνεχών ελέγχων, μέτρηση αποτελεσματικής λειτουργίας δικλείδων ασφαλείας.

3.5. Πολιτική Ασφάλειας Πληροφοριών

3.5.1. Εισαγωγή

Η Πολιτική Ασφάλειας Πληροφοριών είναι ένα σύνολο κειμένων στα οποία αναφέρονται οι κρίσιμοι πληροφοριακοί πόροι του οργανισμού ή της επιχείρησης και περιγράφονται οι τρόποι που αυτοί μπορούν και πρέπει να προστατευτούν. Για το σκοπό αυτό προσδιορίζονται διαδικασίες, οδηγίες και πρακτικές οι οποίες διαμορφώνουν και διαχειρίζονται το περιβάλλον ασφάλειας του οργανισμού. Η Πολιτική Ασφάλειας πρέπει να εκφράζει τη γενικότερη φιλοσοφία του οργανισμού, καθώς και τις απαιτήσεις για την διασφάλιση των πληροφοριακών πόρων [8].

Ο πρωταρχικός σκοπός της Πολιτικής Ασφάλειας είναι η προστασία των δεδομένων της επιχείρησης, ορίζοντας διαδικασίες για τη διαμόρφωση και διαχείριση της ασφάλειας στο επιχειρηματικό περιβάλλον. Αν όμως η επιχείρηση κατορθώσει να εφαρμόσει με επιτυχία μια σαφή και ρεαλιστική Πολιτική Ασφάλειας, τα οφέλη θα είναι πολλαπλά. Καταρχήν, θα είναι σίγουρο ότι έχουν εντοπιστεί τρωτά σημεία στα πληροφοριακά συστήματα και έχουν ληφθεί μέτρα για την κάλυψή τους. Έτσι κατοχυρώνεται η επιχειρησιακή συνέχεια και ενισχύεται η πληροφοριακή υποδομή. Επίσης, αν οι εργαζόμενοι ακολουθούν την Πολιτική Ασφάλειας στις καθημερινές τους συναλλαγές με συναδέλφους, πελάτες και συνεργάτες, διασφαλίζεται ότι οι πληροφορίες ανταλλάσσονται με ασφαλή τρόπο και έτσι μειώνονται οι επιχειρηματικοί κίνδυνοι. Και τελευταίο, αλλά πολύ σημαντικό στοιχείο, είναι η επίγνωση των κινδύνων που αποκτά ο καθένας εργαζόμενος στην επιχείρηση όταν υπάρχει και εφαρμόζεται η πολιτική ασφάλειας, αυξάνοντας έτσι την πιθανότητα συμμόρφωσής του με τους κανόνες της.

Το κλειδί για την επιτυχία του έργου δημιουργίας αποτελεσματικής Πολιτικής Ασφάλειας είναι η δέσμευση και η έγκριση της διοίκησης. Οι εργαζόμενοι πρέπει να αισθάνονται ότι η διοίκηση υποστηρίζει αυτή την προσπάθεια, ώστε να συμμετέχουν ενεργά στην υλοποίηση και την εφαρμογή της. Το επόμενο στάδιο είναι η δημιουργία της ομάδας που θα καταρτίσει την πολιτική και η οποία πρέπει να έχει «πολυφυλετικό» χαρακτήρα. Εκτός από τους κατεξοχήν συμμετέχοντες – υπεύθυνοι ασφάλειας, τεχνικοί επικοινωνιών και γενικά ειδικοί στην Πληροφορική – η ομάδα πρέπει να απαρτίζεται και από εκπροσώπους της διοίκησης, της οργάνωσης, του ανθρώπινου δυναμικού, της νομικής υπηρεσίας, της επικοινωνίας, της εκπαίδευσης και του εσωτερικού ελέγχου. Ο στόχος δεν είναι απλά να δημιουργηθεί μια Πολιτική Ασφάλειας, αλλά αυτή να είναι

κατανοητή από τους εργαζόμενους, χωρίς ασάφειες και κενά, εύκολη στην εφαρμογή της, συμβατή με νόμους και κανονισμούς και σύμφωνη με τη θέση της διοίκησης αναφορικά με την ασφάλεια των πληροφοριακών πόρων.

3.5.2. Περιεχόμενα Πολιτικής Ασφάλειας

Το κείμενο της Πολιτικής Ασφάλειας μιας εταιρείας θα πρέπει να περιλαμβάνει σκοπό, πεδίο εφαρμογής, πρότυπα και διεργασίες [34].

Σκοπός

Αναγράφεται μια σύντομη δήλωση με το γιατί αναπτύχθηκε η πολιτική και τι πρέπει να προστατευτεί.

Πεδίο Εφαρμογής

Περιγράφει το πεδίο εφαρμογής της πολιτικής. Αν η επιχείρηση είναι γεωγραφικά διάσπαρτη ή είναι πολυεθνική, εδώ πρέπει να περιγράφονται με λεπτομέρεια οι μονάδες της στις οποίες πρέπει να εφαρμόζεται η πολιτική. Το ίδιο τμήμα πρέπει, επίσης, να περιέχει μια περιγραφή των τύπων της πληροφορίας, τους απαραίτητους ορισμούς, καθώς και μια δήλωση περί του τι καλύπτει η πολιτική. Το ίδιο τμήμα μπορεί επίσης να περιγράφει τις τεχνικές πλατφόρμες στις οποίες έχει εφαρμογή η πολιτική, ανάλογα, για παράδειγμα, με το λειτουργικό σύστημα ή την πλατφόρμα υλικού.

Κανόνες, Πρότυπα και Διαδικασίες

Ανεξάρτητα από το πώς θα δομηθεί η πληροφορία που σχετίζεται με τους κανόνες, τα πρότυπα και τις διαδικασίες, τα σχετικά τμήματα της Πολιτικής Ασφάλειας πρέπει να περιλαμβάνουν κανόνες, πρότυπα και διαδικασίες για:

- Την αγορά υπολογιστικού εξοπλισμού, όπου θα καθορίζονται τα απαιτούμενα ή επιθυμητά χαρακτηριστικά ασφάλειας.

- Τη διαφύλαξη της προσωπικής ζωής, όπου θα καθορίζονται τα όρια της προσωπικής ζωής σε σχέση με την επιχείρηση και θα κανονίζονται ζητήματα

όπως η παρακολούθηση του ηλεκτρονικού ταχυδρομείου, η καταγραφή δακτυλισμών και η πρόσβαση σε αρχεία χρηστών.

- Την πρόσβαση σε υπολογιστικά συστήματα, όπου θα καθορίζονται τα δικαιώματα πρόσβασης του προσωπικού στους πόρους του συστήματος. Το τμήμα αυτό θα πρέπει να καλύπτει εξωτερικές συνδέσεις, επικοινωνίες δεδομένων, σύνδεση συσκευών σε δίκτυα και πρόσθεση νέου λογισμικού.

- Την ανάθεση αρμοδιοτήτων και υποχρεώσεων, όπου θα καθορίζονται οι αρμοδιότητες και οι υποχρεώσεις του προσωπικού. Το τμήμα αυτό θα πρέπει να καθορίζει επίσης τα σχετικά με τον έλεγχο (audit) του συστήματος.

- Την αυθεντικοποίηση χρηστών, όπου θα καθορίζονται τα σχετικά με τα συνθηματικά ή με άλλους, συμπληρωματικούς ή εναλλακτικούς, μηχανισμούς αυθεντικοποίησης.

- Τη διαφύλαξη της διαθεσιμότητας, όπου θα καθορίζονται, αφενός, τα αναμενόμενα από τους χρήστες ποσοστά διαθεσιμότητας των πόρων του συστήματος και, αφετέρου, ζητήματα σχετικά με την πολλαπλότητα πόρων και την ανάκαμψη, τις ώρες λειτουργίας και τις περιόδους μη λειτουργίας λόγω συντήρησης.

- Τη συντήρηση του υπολογιστικού συστήματος, όπου θα καθορίζονται τα καθήκοντα τόσο των εσωτερικών όσο και των εξωτερικών συντηρητών, η δυνατότητα ή απαγόρευση της από απόσταση συντήρησης και, στην περίπτωση όπου αυτή επιτρέπεται, ο τρόπος ελέγχου της πρόσβασης αυτής. Επίσης, εδώ αναφέρονται όλα τα σχετικά με την ανάθεση εργασιών σε τρίτους.

- Το χειρισμό των περιστατικών, όπου θα καθορίζονται ποιοι τύποι περιστατικών και σε ποιον πρέπει να αναφέρονται.

Οι οδηγίες και τα μέτρα προστασίας που καθορίζει η Πολιτική Ασφάλειας πληροφοριακών συστημάτων θα πρέπει να καλύπτουν τις ακόλουθες κατηγορίες απαιτήσεων ασφάλειας:

- Ζητήματα προσωπικού

- Φυσική ασφάλεια
- Έλεγχος πρόσβασης στο πληροφοριακό σύστημα
- Διαχείριση υλικών και λογισμικών
- Νομικές υποχρεώσεις
- Διαχείριση της πολιτικής ασφάλειας
- Οργανωτική δομή
- Σχέδιο συνέχισης λειτουργίας

3.5.3. Εμπλεκόμενοι στην Πολιτική Ασφάλειας

Η Πολιτική Ασφάλειας αφορά την καταγραφή όλων των απαιτήσεων ασφάλειας μιας επιχείρησης οι οποίες θα οδηγήσουν στο σχέδιο ασφάλειας το οποίο θα προσδιορίζει τους τρόπους αντιμετώπισης τους. Γίνεται, συνεπώς, παραπάνω από προφανές ότι οι εμπλεκόμενοι οι οποίοι θα προσδιορίσουν τις απαιτήσεις ασφάλειας είναι:

- Ο υπεύθυνος ασφάλειας της επιχείρησης
- Οι υπεύθυνοι και οι διαχειριστές του δικτύου
- Οι υπεύθυνοι των τμημάτων που θα εφαρμόσουν την Πολιτική Ασφάλειας στα τμήματα τους
- Οι πελάτες της επιχείρησης
- Η διοίκηση και οι αντιπρόσωποι της των οποίων τα προσωπικά δεδομένα αποθηκεύονται στα πληροφοριακά συστήματα της επιχείρησης
- Οι νομικοί σύμβουλοι οι οποίοι έχουν τη γνώση του νομικού και ρυθμιστικού πλαισίου στο οποίο λειτουργεί η επιχείρηση

3.5.4. Σχέδιο επιχειρησιακής συνέχειας

Η διαχείριση της επιχειρησιακής συνέχειας είναι η διαδικασία με την οποία ένας οργανισμός προετοιμάζεται για μελλοντικά περιστατικά που θα μπορούσαν να θέσουν σε κίνδυνο τους στόχους, την αποστολή και τη μακροπρόθεσμη βιωσιμότητά του [35].

Ο στόχος του σχεδίου επιχειρησιακής συνέχειας (Business Continuity Plan) είναι να δώσει τη δυνατότητα στον οργανισμό για αποκατάσταση των κρίσιμων επιχειρηματικών διεργασιών του, μετά την εκδήλωση ενός κρίσιμου περιστατικού. Το σχέδιο επιχειρησιακής συνέχειας αφορά στη διαχείριση του κινδύνου και στη διαμόρφωση ενός πλαισίου επιχειρηματικής συνέχειας, αναλόγως των πιθανών κινδύνων αλλά και της επιχειρηματικής αξίας του οργανισμού.

Για την ανάπτυξη ενός αποτελεσματικού σχεδίου επιχειρησιακής συνέχειας χρειάζεται να ακολουθηθεί μια εξίσου αποτελεσματική προσέγγιση, οι βασικές φάσεις ανάπτυξης της οποίας περιγράφονται στη συνέχεια:

Φάση 1: Προσδιορισμός των λεπτομερών απαιτήσεων

Έχοντας ορίσει το πεδίο εφαρμογής του σχεδίου επιχειρησιακής συνέχειας, χρειάζεται μια λεπτομερής ανάλυση των εξειδικευμένων απαιτήσεων της επιχειρησιακής συνέχειας για τον κάθε οργανισμό. Αυτό γίνεται για να κατανοήσουμε τη ροή των εργασιών που αφορούν στις κρίσιμες επιχειρηματικές διεργασίες της κάθε επιχειρηματικής μονάδας. Ταυτόχρονα προσδιορίζεται ο στόχος χρονικής αποκατάστασης των κρίσιμων πόρων και διεργασιών της κάθε επιχειρησιακής μονάδας.

Φάση 2: Ανάπτυξη της στρατηγικής αποκατάστασης

Ο στόχος της συγκεκριμένης φάσης είναι ο σχεδιασμός των απαραίτητων λύσεων (διαχειριστικές, τεχνολογικές) προκειμένου να διασφαλισθεί το απαραίτητο επίπεδο διαθεσιμότητας και δυνατότητας ανάκτησης των επιχειρηματικών διαδικασιών. Η διαδικασία επιλογής στρατηγικής ασχολείται με θέματα όπως ο προσδιορισμός των κρίσιμων πόρων για τους οποίους δεν υπάρχει πρόβλεψη αυξημένης διαθεσιμότητας (π.χ. ένα κτίριο παραγωγής, εξάρτηση από έναν και μοναδικό προμηθευτή, ένα τηλεφωνικό κέντρο κ.λπ.). Εξετάζονται επίσης οι κίνδυνοι που αφορούν σε ευρύτερες περιβαλλοντικές απειλές (π.χ. πολιτική αστάθεια, φυσικά φαινόμενα). Στο πλαίσιο της στρατηγικής προσδιορίζονται οι επιχειρηματικές ανάγκες συναρτήσει της ανάλυσης των επιχειρηματικών επιπτώσεων, όπως η προστασία της αξιοπιστίας του οργανισμού και η πρόληψη ή η μείωση του χρόνου διακοπής της επιχειρηματικής δραστηριότητας.

Φάση 3: Ανάπτυξη των σχεδίων αντιμετώπισης

Ένα σχέδιο επιχειρησιακής συνέχειας αποτελείται από ένα σύνολο επιμέρους σχεδίων αντιμετώπισης κρίσιμων περιστατικών (διαδικασίες και πληροφορίες για τους σχετικούς πόρους), τα οποία χρησιμοποιούνται για την ανάκτηση των επιχειρηματικών διεργασιών από ένα γεγονός το οποίο έχει προκαλέσει μερική ή ολική διακοπή σε μία ή περισσότερες επιχειρηματικές δραστηριότητες. Το σχέδιο αντιμετώπισης απαντά στα βασικά ερωτήματα ενός σχεδίου, όπως: ποιος (ποιος εκτελεί την ανάκτηση), τι (τι θα γίνει), πότε (η σειρά των διαδικασιών ανάκτησης), πού (πού θα λάβει χώρα η ανάκαμψη) και πώς (η ενσωμάτωση και ο συντονισμός εταιρικών πόρων, συνεργατών και πελατών).

Φάση 4: Ενσωμάτωση του σχεδίου επιχειρηματικής συνέχειας στην κουλτούρα και το περιβάλλον του Οργανισμού

Αυτή είναι μία από τις πιο σημαντικές πτυχές του σχεδίου επιχειρηματικής συνέχειας. Η αποτελεσματικότητά της εξαρτάται σε μεγάλο βαθμό από την ενσωμάτωση και το βαθμό επικοινωνίας του σχεδίου επιχειρηματικής συνέχειας σε όλο τον οργανισμό. Για το λόγο αυτό είναι απαραίτητη η ανάπτυξη:

- Προγραμμάτων και υλικού εκπαίδευσης
- Εκπαίδευσης της ομάδας διαχείρισης κρίσεων
- Εκπαίδευσης της βασικής ομάδας υλοποίησης του σχεδίου επιχειρηματικής συνέχειας
- Δημιουργίας και προγραμματισμού συνεχούς εκπαίδευσης και ευαισθητοποίησης

Φάση 5: Δοκιμές & Συντήρηση του σχεδίου επιχειρηματικής συνέχειας

Οι δοκιμές καταδεικνύουν εάν τα τεκμηριωμένα σχέδια και η στρατηγική αποκατάστασης είναι επαρκή και μπορούν αποτελεσματικά να ανακτήσουν τις κρίσιμες επιχειρηματικές λειτουργίες εντός των προβλεπόμενων χρονικών στόχων. Οι δοκιμές επικυρώνουν το σχεδιασμό του σχεδίου επιχειρηματικής συνέχειας και προσδιορίζουν τις τυχόν αδυναμίες του.

ΚΕΦΑΛΑΙΟ 4:

ΨΗΦΙΑΚΟΙ ΚΙΝΔΥΝΟΙ & ΑΠΕΙΛΕΣ

4.1. Εισαγωγή

Πριν από τριάντα χρόνια, εμφανίστηκε ο πρώτος ιός υπολογιστών, ο Elk Cloner, παρουσιάζοντας ένα σύντομο μήνυμα σε μορφή ποιήματος όταν ένας μολυσμένος υπολογιστής εκκινούσε για 50ή φορά. Από τότε, οι κυβερνοεγκληματίες έχουν δημιουργήσει εκατομμύρια ιούς και άλλους ιούς (malwares), δούρειους ίππους (trojans), σκουλήκια στο Διαδίκτυο (worms), καταγραφείς πληκτρολόγησης (spyware) που πολλοί από αυτούς εξαπλώνονται σε όλον τον κόσμο και γίνονται πρωτοσέλιδα [18].

Πολλοί άνθρωποι έχουν ακούσει για ιούς που γεμίζουν την οθόνη του υπολογιστή με σκουπίδια ή διαγράφουν αρχεία. Για τον περισσότερο κόσμο το κακόβουλο λογισμικό εξακολουθεί να σημαίνει φάρσα ή σαμποτάζ. Στις αρχές της δεκαετίας του 1990 παρατηρήθηκε παγκόσμιος πανικός για τον ιό Michelangelo. Στη δεκαετία του 2000, όταν εκατομμύρια υπολογιστές είχαν μολυνθεί από τον ιό SoBig-F και είχαν προετοιμαστεί να μεταμορφώσουν άγνωστα προγράμματα από το Διαδίκτυο σε καθορισμένο χρόνο, οι εταιρείες προστασίας από ιούς πάσχισαν για να πείσουν τους παρόχους υπηρεσιών διαδικτύου να κλείσουν τους διακομιστές τους για να αποφύγουν ένα κρίσιμο σενάριο. Οι κινηματογραφικές ταινίες του Χόλυγουντ, όπως η «Ημέρα Ανεξαρτησίας» ενίσχυσαν αυτή την αντίληψη με επιθέσεις από ιούς που σηματοδοτούνται από οθόνες που αναβοσβήνουν και συναγερμούς.

Ωστόσο, τα παραπάνω απέχουν πολύ από την αλήθεια σήμερα. Οι απειλές δεν είναι λιγότερο πραγματικές τώρα, αλλά είναι χαμηλού προφίλ, καλά στοχευμένες και είναι πιθανότερο να γίνονται για να ζητήσουν χρήματα παρά για να δημιουργήσουν χάος.

Σήμερα το κακόβουλο λογισμικό είναι απίθανο να διαγράψει τον σκληρό δίσκο, να καταστρέψει το υπολογιστικό φύλλο ή να εμφανίσει ένα μήνυμα. Αυτός ο κυβερνοβανδαλισμός έδωσε τη θέση του σε πιο επικερδείς εκμεταλλεύσεις. Οι σημερινοί ιοί ενδέχεται να κρυπτογραφήσουν όλα τα αρχεία και να ζητήσουν λύτρα. Ή ένας χάκερ μπορεί να εκβιάσει μία μεγάλη εταιρεία απειλώντας να ξεκινήσει μία επίθεση άρνησης

της υπηρεσίας η οποία εμποδίζει τους πελάτες να έχουν πρόσβαση στην ιστοσελίδα της εταιρείας.

Συνηθέστερα οι ιοί δεν προκαλούν καμία φαινομενική βλάβη ούτε ανακοινώνουν την παρουσίας τους. Αντ' αυτού, ένας ιός μπορεί να εγκαταστήσει σιωπηλά έναν καταγραφέα πληκτρολόγησης, ο οποίος περιμένει έως ότου το θύμα να επισκεφθεί έναν τραπεζικό λογαριασμό και, στη συνέχεια, καταγράφει τα στοιχεία του λογαριασμού του χρήστη και τον κωδικό πρόσβασης και τα διαβιβάζει σε έναν χάκερ μέσω του Διαδικτύου. Ο χάκερ είναι ένας κλέφτης ταυτότητας χρησιμοποιώντας αυτές τις λεπτομέρειες για να κλωνοποιήσει πιστωτικές κάρτες ή να λεηλατήσει τραπεζικούς λογαριασμούς. Το θύμα δε γνωρίζει καν ότι ο υπολογιστής έχει μολυνθεί, μόλις ο ιός κάνει τη δουλειά του μπορεί να διαγραφεί για να αποφευχθεί η ανίχνευση.

Μία άλλη τάση είναι το κακόβουλο λογισμικό να αναλάβει τον υπολογιστή ενός χρήστη μετατρέποντάς του σε τηλεχειριζόμενο ζόμπι. Χρησιμοποιεί τον υπολογιστή του χρήστη χωρίς τη γνώση του για να αναμεταδίδει εκατομμύρια κερδοσκοπικά μηνύματα spam ή μπορεί να εκκινήσει άλλες επιθέσεις malware σε ανυποψίαστους χρήστες υπολογιστών.

Καθώς τα κοινωνικά δίκτυα όπως το Facebook και το Twitter έχουν εξελιχθεί σε δημοτικότητα, οι χάκερ και οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται αυτά τα συστήματα για να βρουν νέους τρόπους μόλυνσης υπολογιστών και κλοπής ταυτότητας.

Οι χάκερ πλέον μπορούν να μην στοχεύουν έναν μεγάλο αριθμό θυμάτων, καθώς τέτοιες επιθέσεις υψηλής ορατότητας φέρνουν ανεπιθύμητη προσοχή και οι εταιρείες προστασίας από ιούς μπορούν σύντομα να εξουδετερώσουν το κακόβουλο λογισμικό. Επιπλέον, μεγάλης κλίμακας εκμεταλλεύσεις μπορούν να φέρουν στους χάκερ περισσότερα κλεμμένα δεδομένα από όσα μπορούν να χειριστούν. Εξαιτίας αυτού οι απειλές γίνονται πιο προσεκτικά εστιασμένες.

Το Spearphishing είναι ένα παράδειγμα. Αρχικά, το ηλεκτρονικό «ψάρεμα» περιλάμβανε την αποστολή μηνυμάτων μαζικής αλληλογραφίας που φαινόταν να προέρχονται από τράπεζες, ζητώντας από τους πελάτες να επανεγγράψουν εμπιστευτικά στοιχεία τα οποία, στη συνέχεια, θα μπορούσαν κα κλαπούν. Το Spearphishing, αντίθετα, περιορίζεται σε ένα μικρό αριθμό ατόμων, συνήθως μέσα σε έναν οργανισμό. Το μήνυμα φαίνεται να προέρχεται από συναδέλφους σε αξιόπιστα τμήματα ζητώντας πληροφορίες σχετικά με τον κωδικό πρόσβασης. Η αρχή είναι ίδια αλλά η επίθεση είναι πιο πιθανό να πετύχει διότι το θύμα πιστεύει ότι το μήνυμα είναι εσωτερικό.

Στέρεες, μικρής κλίμακας και καλά στοχευμένες. Αυτός φαίνεται να είναι τώρα ο τρόπος με τον οποίο προχωράνε οι απειλές για την ασφάλεια. Η πρόβλεψη του πώς θα αναπτυχθούν οι απειλές ασφάλειας είναι σχεδόν αδύνατη. Ορισμένοι σχολιαστές υπολόγισαν ότι δε θα υπάρξουν περισσότεροι από μερικές εκατοντάδες ιοί και ο Bill Gates της Microsoft δήλωσε ότι το spam δε θα είναι πια πρόβλημα μέχρι το 2006. Δεν είναι σαφές από που θα προέρχονται οι μελλοντικές απειλές ή πόσο σοβαρές θα είναι αυτές. Αυτό που είναι σαφές είναι ότι κάθε φορά που θα υπάρχει μία ευκαιρία για οικονομικό όφελος οι χάκερ και οι εγκληματίες θα προσπαθήσουν να έχουν πρόσβαση και να κάνουν κατάχρηση δεδομένων.

4.2. Ιοί υπολογιστών

4.2.1. Ορισμός

Ένας ιός υπολογιστών είναι ένα κακόβουλο πρόγραμμα υπολογιστή, το οποίο μπορεί να αντιγραφεί χωρίς παρέμβαση του χρήστη και να «μολύνει» τον υπολογιστή χωρίς τη γνώση ή την άδεια του χρήστη του. Ο αρχικός ιός μπορεί να τροποποιήσει τα αντίγραφά του ή τα ίδια τα αντίγραφα μπορούν να υποστούν από μόνα τους τροποποίηση, όπως συμβαίνει σε έναν μεταμορφικό ιό. Ένας ιός μπορεί να διαδοθεί από έναν υπολογιστή σε άλλους, παραδείγματος χάριν από ένα χρήστη που στέλνει τον ιό μέσω δικτύου ή του Διαδικτύου, ή με τη μεταφορά του σε ένα φορητό μέσο αποθήκευσης, όπως δισκέτα, οπτικό δίσκο ή μνήμη flash USB [19].

Αποτελείται από δύο τμήματα:

- Τον κώδικα αναπαραγωγής: αποτελεί απαραίτητο στοιχείο του ιού καθώς μέσω αυτού ο ιός εξαπλώνεται.
- Τον κώδικα εκτέλεσης: εκτελεί μία συγκεκριμένη λειτουργία ανάλογα με το τι έχει αποφασίσει ο δημιουργός του ιού.

Ένας ιός εισάγεται σε έναν υπολογιστή μέσω μίας ποικιλίας ενεργειών. Για τους χρήστες του διαδικτύου αυτό μπορεί να συμβεί με το κατέβασμα αρχείων με FTP (File Transfer Protocol) με τη λήψη ενός ηλεκτρονικού μηνύματος ή και απλά με περιήγηση

στο Διαδίκτυο. Παλαιότερα οι ιοί διαδίδονταν με τις δισκέτες. Όταν ένας ιός εισαχθεί σε έναν υπολογιστή προσκολλάται ή αντικαθιστά ένα υπάρχον πρόγραμμα. Έτσι, όταν ο χρήστης εκτελεί το μολυσμένο πρόγραμμα, εκτελείται και ο ιός. Αυτό συνήθως συμβαίνει χωρίς να το αντιλαμβάνεται ο χρήστης [20].

4.2.2. Τύποι ιών

Υπάρχουν πολλοί τύποι ιών, από τους οποίους οι πιο διαδεδομένοι είναι:

- *Ιοί περιοχής εκκίνησης:* Αυτοί οι ιοί μολύνουν δισκέτες και σκληρούς δίσκους. Ο ιός φορτώνεται πριν από το λειτουργικό σύστημα. Ήταν οι πρώτοι ιοί που εμφανίστηκαν.

- *Ιοί αρχείων:* Σε αυτή τη κατηγορία ανήκει η πλειοψηφία των ιών και η πιο εύκολα αντιμετωπίσιμη κατηγορία. Είναι μικρά εκτελέσιμα αρχεία. Προσκολλώνται σε ένα αρχείο, συνήθως αρχείο εφαρμογής. Το βασικό γνώρισμα των ιών είναι ότι δημιουργούν αντίγραφα του εαυτού τους μέσα σε άλλα αρχεία. Τα αρχεία αυτά είναι εκτελέσιμα ή αρχεία βιβλιοθηκών. Οι ιοί είτε αντικαθιστούν κάποιο τμήμα του κώδικα του αρχείου (χωρίς να μεταβάλλουν το μέγεθός του) είτε προσκολλώνται σε αυτό.

- *Ιοί σκουλήκια (worms):* Έχουν την ικανότητα αναπαραγωγής χωρίς να χρησιμοποιούν άλλα αρχεία. Ο τρόπος διάδοσης τους είναι το Διαδίκτυο με τη βοήθεια των δικτυακών πρωτοκόλλων, εκμεταλλευόμενοι τα προβλήματα ασφαλείας των λειτουργικών συστημάτων ή με τη βοήθεια των μηνυμάτων του ηλεκτρονικού ταχυδρομείου. Οι ιοί σκουλήκια αποκτούν προσπέλαση στο βιβλίο διευθύνσεων του υπολογιστή (όπου κρατούνται οι διευθύνσεις ηλεκτρονικού ταχυδρομείου με τις οποίες επικοινωνεί ο χρήστης του υπολογιστή) και αποστέλλει μολυσμένα μηνύματα. Αρκετές φορές χρησιμοποιούν σαν αποστολέα ένα όνομα από το βιβλίο διευθύνσεων. Όσοι παραλήπτες ανοίξουν το ηλεκτρονικό μήνυμα μολύνονται. Η διάδοση των ιών worm με αυτή τη μέθοδο είναι αστραπιαία.

- *Δούρειος ίππος (horse trojan):* Αυτοί οι ιοί δρουν αθόρυβα. Μολύνουν τον υπολογιστή και αναμένουν κάποιο γεγονός ανάλογα με το προγραμματισμό τους.

Συνήθως δεν πολλαπλασιάζονται και δεν εξαπλώνονται σε άλλους υπολογιστές. Για να μολυνθεί ένας υπολογιστής ο χρήστης του πρέπει να κατεβάσει και να εκτελέσει τον ιό. Αυτό γίνεται συνήθως με ένα ηλεκτρονικό μήνυμα όπου ο ιός είναι συνημμένος και ο χρήστης πείθεται να τον εκτελέσει. Όταν ο ιός δούρειος ίππος εγκατασταθεί στέλνει μέσω Διαδικτύου τις κατάλληλες πληροφορίες στο δημιουργό του ώστε αυτός να πάρει τον έλεγχο του υπολογιστή και να χρησιμοποιηθεί σε διάφορες παράνομες και επιβλαβείς ενέργειες.

- *Ιός τύπου Ransomware:* Ο ιός τύπου Ransomware είναι τύπος κακόβουλου λογισμικού (γνωστό και ως malware) που έχει σχεδιαστεί να μπλοκάρει την πρόσβαση του χρήστη-θύματος σε αρχεία ή μέρη του συστήματος του υπολογιστή του ζητώντας κάποιο ποσό ως λύτρα. Το ύψος του ποσού, η αιτιολογία, αλλά και η τακτική, ποικίλει από ιό σε ιό. Ορισμένες εκδόσεις ιών τύπου ransomware υποστηρίζουν ότι η πληρωμή των λύτρων πρέπει να γίνει ως μορφή τιμωρίας από κάποια κυβερνητική αρχή (συνήθως, FBI ή κάποια άλλη παρόμοια υπηρεσία), άλλες εκδόσεις υποστηρίζουν ότι η πληρωμή των λύτρων αποτελεί τη μοναδική λύση για αποκρυπτογράφηση των κρυπτογραφημένων αρχείων. Επιπρόσθετη συμπεριφορά των περισσότερων παράσιτων τύπου ransomware είναι η υποκλοπή – καταγραφή - προώθηση σε τρίτους ευαίσθητων/απόρρητων προσωπικών δεδομένων, τερματισμός νόμιμων προγραμμάτων ασφάλειας (anti-virus, anti-spyware, κτλ.), εμφάνιση παραπλανητικών ερευνών, διαγωνισμών, διαφημίσεων, κλπ. Οι πρώτες εκδόσεις αυτού του είδους ιών δημιουργήθηκαν στη Ρωσία. Έκτοτε, εμφανίζονται σχεδόν σε όλα τα μήκη και πλάτη του κόσμου [21].

4.3. Adware (Ανεπιθύμητο λογισμικό εμφάνισης διαφημίσεων)

Το Adware είναι είδος ανεπιθύμητου λογισμικού που εμφανίζει επιχορηγούμενες, εκνευριστικές και παραπλανητικές διαφημίσεις τρίτων. Από τη στιγμή που θα καταφέρει να διεισδύσει και να εγκατασταθεί στο σύστημα-στόχο, αρχίζει να εμφανίζει προωθητικό/διαφημιστικό περιεχόμενο με διάφορες μορφές, συμπεριλαμβανομένων αναδυόμενων διαφημίσεων, διαφημίσεων κειμένου, κτλ. Σκοπός αυτών των διαφημίσεων είναι η μόχλευση ροών επισκεψιμότητας προς συγκεκριμένους ιστότοπους

συνεργαζόμενων τρίτων (βλ. affiliate websites) ώστε να βελτιωθεί η διαδικτυακή τους κατάταξη ή να μεγιστοποιηθούν οι δυνητικές πωλήσεις και τα έσοδα από τις πωλήσεις αυτές.

Εκτός από αυτή την λειτουργία, τα ανεπιθύμητα προγράμματα τύπου adware χρησιμοποιούνται ευρέως και στη συλλογή-καταγραφή-προώθηση σε τρίτους, κατόπιν αμοιβής, πληροφοριών που σχετίζονται με τις διαδικτυακές δραστηριότητες και προτιμήσεις των χρηστών-θυμάτων. Αυτό συμβαίνει από την πρώτη στιγμή που θα προσκολληθούν στον web browser του χρήστη.

4.4. Ψευδές/παραπλανητικό Anti-Spyware

Ψευδές/παραπλανητικό anti-spyware είναι ένας όρος που χρησιμοποιείται για να προσδιορίσει ένα «μαϊμού» anti-spyware λογισμικό.

Τα προγράμματα που ανήκουν σε αυτή την κατηγορία μπορούν επίσης να προσδιοριστούν ως ιοί. Ο κύριος σκοπός των περισσότερων ψευδών/παραπλανητικών anti-spywares είναι να μολύνουν συστήματα-στόχους, κατόπιν να «πλημμυρίζουν» την οθόνη του υπολογιστή με ψευδείς/παραπλανητικές ειδοποιήσεις ασφάλειας, και με το τρόπο αυτό να τρομοκρατούν τους χρήστες-θύματα κάνοντας τους να πιστεύουν ότι ο υπολογιστής τους έχει μολυνθεί από δεκάδες ανεπιθύμητα και κακόβουλα προγράμματα/αρχεία. Απώτερος σκοπός είναι ο χρήστης-θύμα να αναγκαστεί να προβεί σε αγορά της πλήρους έκδοσης του ψευδούς/παραπλανητικού anti-spyware το οποίο, υποτίθεται, θα εντοπίσει και θα αφαιρέσει ολοκληρωτικά οποιαδήποτε κυβερνοαπειλή κατάφερε να διεισδύσει και να μολύνει το σύστημα του υπολογιστή. Σε αυτή την περίπτωση, αυτό που θα πρέπει να αφαιρεθεί άμεσα κι ολοκληρωτικά είναι το ίδιο το ψευδές/παραπλανητικό anti-spyware λογισμικό.

4.5. Ιός κερκόπορτας (Backdoor)

Ως backdoor χαρακτηρίζεται ένα κακόβουλο πρόγραμμα που χρησιμοποιείται για την απόκτηση αυθαίρετης απομακρυσμένης πρόσβασης του κυβερνοεγκληματία (βλ. hacker, spammer) στο σύστημα-στόχο. Η απομακρυσμένη αυτή πρόσβαση επιτυγχάνεται μέσω εκμετάλλευσης «τρωτών» σημείων στην ασφάλεια του συστήματος-στόχου ή λογισμικών με τα οποία έχει συνδεθεί ή κατεβάσει ο χρήστης-θύμα.

Το Backdoor, όπως άλλωστε υποδηλώνει και το όνομά του, δουλεύει κρυφά στο παρασκήνιο του συστήματος-στόχου. Έχει πολλά κοινά χαρακτηριστικά με άλλα κακόβουλα προγράμματα (βλ. malware viruses, ιοί) και ως επί το πλείστον ο εντοπισμός του, κι άρα η ολοκληρωτική αφαίρεσή του, είναι ένα αρκετά δύσκολο και περίπλοκο ζήτημα. Αξίζει να σημειωθεί ότι τα κακόβουλα προγράμματα τύπου backdoor αποτελούν ένα από τα πλέον επικίνδυνα είδη διαδικτυακών παρασίτων, καθώς παρέχουν, μέσω της απομακρυσμένης πρόσβασης, τη δυνατότητα στους κυβερνοεγκληματίες να ελέγχουν την λειτουργία και ρυθμίσεις του συστήματος-στόχου.

Αναλυτικότερα, με τη βοήθεια ενός backdoor οι κυβερνοεγκληματίες μπορούν να κατασκοπεύουν τον χρήστη-θύμα, να διαχειρίζονται όπως επιθυμούν τα αρχεία και δεδομένα του, να εγκαθιστούν κρυφά κι αυθαίρετα PUPs (Potentially Unwanted Programs, δηλαδή δυνητικά ανεπιθύμητα προγράμματα) και κακόβουλα προγράμματα malware, να ελέγχουν απομακρυσμένα όλες τις λειτουργίες του συστήματος-στόχου, και μέσω του μολυσμένου υπολογιστή να εξαπλώνονται διαδικτυακά και να μολύνουν περαιτέρω κι άλλα συστήματα υπολογιστών με τα οποία συνδέεται το μολυσμένο σύστημα.

Επιπρόσθετα, ένα κακόβουλο πρόγραμμα τύπου backdoor έχει ευρύ φάσμα κακόβουλων και καταστροφικών για το σύστημα και τον χρήστη δραστηριοτήτων, όπως πχ. καταγραφή και υποκλοπή πληκτρολογήσεων (keystroke logging), αυθαίρετη λήψη στιγμιότυπων οθόνης (screenshot capture), μολύνσεις και κρυπτογραφήσεις αρχείων/εγγράφων, κλπ. Εν ολίγοις, η παρουσία ενός κακόβουλου προγράμματος τύπου backdoor στο σύστημα του υπολογιστή είναι πολύ κακά μαντάτα για τον χρήστη.

4.6. Cryptojacking

Για να κατανοήσουμε τον όρο «cryptojacking», θα εξηγήσουμε αρχικά τι είναι το cryptomining («εξόρυξη» κρυπτονομισμάτων) [26].

Το cryptomining μοιάζει πολύ με την εξόρυξη του χρυσού, και επομένως, όπως και με τα κοιτάσματα χρυσού, υπάρχουν εκατομμύρια κρυπτονομίσματα που όμως δεν είναι ακόμα διαθέσιμα. Αυτό που κάνουν οι «miners» είναι να τα εξορύξουν, χρησιμοποιώντας πολλές φορές την συνδυαστική επεξεργαστική ισχύ ενδεχομένως πολλών, αλλά λιγότερο ισχυρών υπολογιστών, για να επιλύσουν σύνθετους αλγόριθμους. Μόλις επαληθευτούν οι αλγόριθμοι, οι miners ανταμείβονται αναλόγως. Όμως όταν η εξόρυξη κρυπτονομισμάτων γίνεται χωρίς εξουσιοδότηση ονομάζεται «cryptojacking» και είναι παράνομη.

Το cryptojacking είναι η διαδικασία εκμετάλλευσης υπολογιστικών πόρων χωρίς εξουσιοδότηση για την εξόρυξη κρυπτονομισμάτων.

Για την εξόρυξη απαιτούνται σημαντική πόροι σε επεξεργαστική ισχύ και κατανάλωση ρεύματος. Ορισμένοι επιτήδειοι χρησιμοποιώντας κακόβουλα προγράμματα (malware) ή εφαρμογές ιστού, μολύνουν υπολογιστές ιδιωτών ή ιδρυμάτων και εταιρειών για να «κλέψουν» στην ουσία τους πόρους τους και να απολαμβάνουν οι ίδιοι τα κέρδη. Η διαδικασία καθιστά τους επιτήδειους πρακτικά αόρατους, και το χειρότερο είναι ότι οι απλοί χρήστες σπάνια μπορούν να αντιληφθούν ότι κάποιος εκμεταλλεύεται την ισχύ του υπολογιστή τους αφού ο μοναδικός αντίκτυπος είναι η επιβράδυνση του συστήματός τους που θα μπορούσε πολύ εύκολα να αποδοθεί σε άλλους παράγοντες.

Το cryptojacking μπορεί να πραγματοποιηθεί με δύο διαφορετικούς τρόπους. Μέσω in-browser προσέγγισης που στην ουσία εκχύνει το script στον browser του καταναλωτή και χρησιμοποιεί τους πόρους του επεξεργαστή για την εξόρυξη κρυπτονομισμάτων. Άλλος τρόπος είναι η παράκαμψη του browser και η εγκατάσταση απευθείας τοπικά στο μηχάνημα του καταναλωτή ενός cryptominer μέσω ενός παραπλανητικού συνδέσμου.

4.7. Επιθέσεις άρνησης εξυπηρέτησης

Επιθέσεις άρνησης εξυπηρέτησης DDos (Df-service attack, DoS attack) ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες. Υπάρχουν γενικά δύο μορφές αυτής της επίθεσης. Η μία είναι η επίθεση κατά την οποία η υπηρεσία αναγκάζεται να καταρρεύσει και να πρέπει να επανεκκινηθεί και η άλλη είναι η αποστολή υπερβολικά μεγάλου αριθμού ψεύτικων αιτήσεων για εξυπηρέτηση με αποτέλεσμα η υπηρεσία να μην μπορεί να εξυπηρετήσει αυτούς που πραγματικά θέλουν την υπηρεσία.

Σε μια επίθεση DoS, ο εισβολέας προκαλεί συμφόρηση στη διεύθυνση IP της συσκευής που στοχεύει (υπολογιστής-server) με εξωτερικές, περιττές αιτήσεις επικοινωνίας (στέλνονται αιτήματα συνέχεια απο τον εισβολέα στον server για να είναι συνέχεια »απασχολημένος»), καθιστώντας έτσι αδύνατη τη σύνδεση της συσκευής στο Internet. Η επίθεση κατευθύνεται προς το τη διεύθυνση IP της στοχευόμενης συσκευής.

Σε μια επίθεση DDoS, ο εισβολέας χρησιμοποιεί κακόβουλο λογισμικό που εγκαθίσταται σε πολλούς υπολογιστές προκειμένου να εντοπίσουν και να επιτεθούν στη στοχευόμενη συσκευή. Οι εισβολείς που ξεκινούν μια επίθεση DDoS επιλέγουν αυτό το είδος επίθεσης για να επιτύχουν μεγαλύτερο πλήγμα στη στοχευόμενη συσκευή σε σχέση με μια επίθεση DoS που ξεκινά από μία μόνο συσκευή [22].

4.8. Απάτες και επιθέσεις μέσω email

Μία από τις μεγαλύτερες προκλήσεις που αντιμετωπίζουν οι οργανισμοί για την ασφάλεια τους είναι η προστασία της ηλεκτρονικής τους επικοινωνίας μέσω email [29].

Η ασφάλεια των email αντιμετωπίζει δύο μεγάλες προκλήσεις: η μία αφορά τις απάτες μέσω email που στοχεύουν στους ανθρώπους και η άλλη σε αυτά τα email που περιλαμβάνουν malware τα οποία εγκαθίστανται στους υπολογιστές και διευκολύνουν τις ψηφιακές επιθέσεις.

Η απάτη μέσω email είναι μία απλή επίθεση που όμως μπορεί να δημιουργήσει σύγχυση και σοβαρά προβλήματα ακόμα και στις πιο εξελιγμένες τεχνολογικά εταιρείες στον κόσμο. Αντίθετα από άλλες κυβερνοεπιθέσεις, τα email που χρησιμοποιούνται για απάτες δεν περιέχουν κάποιο κακόβουλο λογισμικό ή URL, αλλά εκμεταλλεύονται το social engineering, καθώς στοχεύουν ανθρώπους. Χρησιμοποιώντας μια τεχνική που λέγεται spoofing, οι ηλεκτρονικοί απατεώνες ξεγελούν τους υπαλλήλους ώστε να νομίζουν ότι έλαβαν email από κάποιον προϊστάμενο, συνάδελφο ή συνεργάτη. Ο απατεώνας ζητά μεταφορές χρημάτων, φορολογικά στοιχεία και άλλα ευαίσθητα δεδομένα. Αυτού του είδους οι επιθέσεις πετυχαίνουν γιατί περιλαμβάνουν emails που είναι εξαιρετικά όμοια με νόμιμα μηνύματα.

Οι πιο κοινές απάτες μέσω email είναι:

- *Spoofed Name:* Αυτή η εκδοχή αντιπροσωπεύει το 75% των επιθέσεων. Χρησιμοποιεί το όνομα του spoofed στελέχους στο πεδίο «from». Όμως, η διεύθυνση email προέρχεται από εξωτερική υπηρεσία, όπως το Gmail, και ανήκει στον επιτιθέμενο.

- *Reply-To-Spoofing:* Αυτή η τεχνική χρησιμοποιεί το πραγματικό όνομα και email του αποστολέα που πλαστοπροσωπείται. Το όνομα στο «Reply-to» χρησιμοποιεί επίσης το όνομα του πλαστοπροσωποποιημένου αποστολέα. Όμως η διεύθυνση «απάντηση σε», όπου στέλνονται οι απαντήσεις, ανήκει στον επιτιθέμενο.

- *Spoofed Sender (with No reply-to Address):* Αυτή η μορφή απάτης μέσω email χρησιμοποιεί το όνομα και το email του spoofed στελέχους. Όμως το μήνυμα δεν περιλαμβάνει διεύθυνση «απάντηση σε», οπότε είναι αδύνατη η αμφίδρομη αλληλογραφία. Το μήνυμα συχνά περιλαμβάνει οδηγίες μεταφοράς χρημάτων, που καταργούν την ανάγκη για περεταίρω διευκρινίσεις.

- *Lookalike Domain:* Σε αυτή τη μορφή απάτης μέσω email, η διεύθυνση «Από» του επιτιθέμενου έχει παρόμοια εμφάνιση με αυτή του πλαστοπροσωποποιημένου στελέχους. Το παρόμοιο domain μπορεί να διαφέρει μόνο προς ένα γράμμα από το πραγματικό.

4.9. Παραβίαση δεδομένων

4.9.1. Ορισμός

Οι ηλεκτρονικοί και διαδικτυακοί κίνδυνοι αποτελούν μία πραγματικότητα στον κόσμο των πληροφοριών και των πληροφοριακών συστημάτων. Κάθε εταιρεία που ασχολείται με ηλεκτρονικά δεδομένα, ανεξάρτητα από το εάν αυτά βρίσκονται σε υπολογιστές, διακομιστές ή το διαδίκτυο, μπορεί να βρεθεί αντιμέτωπη με αντίστοιχες περιπτώσεις [36].

Οι κίνδυνοι μπορεί να αφορούν είτε απώλεια (διαρροή δεδομένων από εσωτερικές ή εξωτερικές «επιθέσεις»), ή αμέλεια στην χρήση. Μπορεί να προέρχονται από ένα μεμονωμένο υπολογιστή, ή μία επίθεση σε μονάδες αποθήκευσης, data warehouses, routers, private ή common servers.

Η ραγδαία εξέλιξη της τεχνολογίας, η ανάπτυξη της πληροφορικής και η ευρύτατη χρήση του διαδικτύου έχουν επιφέρει επαναστατικές αλλαγές στο σύνολο των καθημερινών δραστηριοτήτων μιας επιχείρησης. Οι επιχειρήσεις βασίζονται για τη λειτουργία τους ολοένα και περισσότερο στη συλλογή, συγκέντρωση, ανάλυση, φύλαξη, χρήση και διάδοση ηλεκτρονικών δεδομένων, παράγοντες που ευνοούν την έκθεσή τους σε μια σειρά από κινδύνους.

Παραβίαση δεδομένων επέρχεται όταν σημειώνεται συμβάν ασφαλείας σε σχέση με τα δεδομένα για τα οποία ευθύνεται η εταιρεία ή ο οργανισμός, το οποίο έχει ως αποτέλεσμα την παραβίαση του απορρήτου, της διαθεσιμότητας ή της ακεραιότητας. Εάν αυτό συμβεί, και είναι πιθανό η παραβίαση να θέτει σε κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικού προσώπου, η εταιρεία ή ο οργανισμός πρέπει να ειδοποιήσει την εποπτική αρχή χωρίς αδικαιολόγητη καθυστέρηση και το αργότερο εντός 72 ωρών αφού αντιληφθεί την παραβίαση. Εάν η εταιρεία ή ο οργανισμός είναι ο εκτελών την επεξεργασία, πρέπει να ενημερώνει τον υπεύθυνο επεξεργασίας δεδομένων για κάθε παραβίαση δεδομένων [37].

Εάν η παραβίαση δεδομένων θέτει σε υψηλό κίνδυνο τα φυσικά πρόσωπα που επηρεάζονται, τότε πρέπει επίσης να ενημερωθεί το καθένα εξ αυτών, εκτός εάν έχουν τεθεί σε εφαρμογή αποτελεσματικά τεχνικά και οργανωτικά μέτρα προστασίας ή άλλα μέτρα που διασφαλίζουν ότι ο κίνδυνος δεν είναι πλέον πιθανό να προκύψει.

Ως οργανισμός, είναι ζωτικής σημασίας να εφαρμόζονται τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την αποφυγή ενδεχόμενων παραβιάσεων δεδομένων.

4.9.2. Οι σημαντικότερες υποθέσεις παραβίασης προσωπικών δεδομένων

Τα τελευταία χρόνια έχουν πραγματοποιηθεί εκατομμύρια μικρές και μεγάλες κυβερνοεπιθέσεις ανά τον κόσμο. Υπάρχουν, ωστόσο, ορισμένες που λόγω ιδιαίτερων συνθηκών ή λόγω του όγκου των δεδομένων που κλάπηκαν ή υφαρπάχτηκαν, συγκλόνισαν τον πλανήτη. Οι διαρροές αυτές αποδεικνύουν, παράλληλα, πόσο μεγάλη σημασία έχει η προστασία των προσωπικών δεδομένων [17].

- <u>Cambridge Analytica</u>

Ένα σκάνδαλο μεγατόνων, με «θύματα» δεκάδες εκατομμύρια χρήστες: Η Cambridge Analytica ήταν μία βρετανική εταιρεία που ασχολείται με την ανάλυση δεδομένων. Η εταιρεία συνέλεγε τεράστιους όγκους δεδομένων από διάφορες πηγές – μεταξύ αυτών, δικές του δημοσκοπήσεις, social media και πλατφόρμες όπως το Facebook που, με τη συνδρομή της Συμπεριφορικής Επιστήμης, στήνει το ψυχολογικό προφίλ των χρηστών, προβλέποντας και επηρεάζοντας τις επιλογές τους.

Όπως κατήγγειλε προ μηνών ο Κρις Γουάιλι, πρώην εργαζόμενος, η Cambridge Analytica συνέλεξε και επεξεργάστηκε τα δεδομένα 75 εκατομμυρίων χρηστών του Facebook εν αγνοία τους. Εκμαίευε, χωρίς τη συγκατάθεσή τους, πληροφορίες σχετικά με τους φίλους, τα likes, την κατοικία, τις επιλογές και, στη συνέχεια, βάσει του «ψυχογραφήματος, τους «σφυροκοπούσε» με συγκεκριμένες πολιτικές διαφημίσεις.

Συμμετέχοντας στο φαινομενικά «αθώο» αυτό-κουίζ, οι χρήστες δεν «πουλούσαν» εν αγνοία μόνο τα δικά τους δεδομένα αλλά κι εκείνα των διαδικτυακών φίλων τους. Το σκάνδαλο αυτό προκάλεσε «σεισμό» σε ΗΠΑ και Ευρώπη, με τον ιδρυτή του κοινωνικού δικτύου Μαρκ Ζάκερμπεργκ να εμφανίζεται ενώπιον του Κογκρέσου αλλά και του Ευρωπαϊκού Κοινοβουλίου για να δώσει εξηγήσεις.

- Yahoo

Τον Σεπτέμβριο 2016, ο τότε γίγαντας στην παροχή διαδικτυακών υπηρεσιών Yahoo αποκάλυψε ότι το 2014 υπέστη την μεγαλύτερη παραβίαση δεδομένων χρηστών στην ιστορία, πιθανώς από χάκερ που έχαιρε κυβερνητικής στήριξης.

Στην πρώτη της δήλωση, η εταιρεία ανακοίνωσε ότι η διαδικτυακή αυτή επίθεση επηρέασε 500 εκατομμύρια χρήστες και πως κατά την διάρκειά της εκτέθηκαν ονόματα, email, ημερομηνίες γέννησης και τηλέφωνα. Παρόλα αυτά, έσπευσε να καθησυχάσεις τους χρήστες ότι η πλειονότητα των κωδικών είχαν προστατευτεί μέσω της χρήσης του αλγόριθμου bcrypt.

Τρεις μήνες αργότερα, η Yahoo εξέδωσε νέα ανακοίνωση και παραδέχτηκε ότι το 2013 μια άλλη ομάδα χάκερ εξασφάλισε πρόσβαση στα δεδομένα 1 δισ. χρηστών, τα οποία περιλάμβαναν όχι μόνο ονόματα, email, ημερομηνίες γέννησης και κωδικούς πρόσβασης αλλά και ερωτήσεις ασφαλείας των χρηστών με τις αντίστοιχες απαντήσεις. Τον Οκτώβριο του 2017, η ίδια εταιρεία παραδέχτηκε ότι στην πραγματικότητα κατά την κυβερνοεπίθεση αυτή διέρρευσαν τα δεδομένα 3 δισ. χρηστών της πλατφόρμας.

Κατά την περίοδο της πρώτης αποκάλυψης το 2016, η Yahoo βρισκόταν εν μέσω διαπραγματεύσεων με την Verizon, η οποία προσπαθούσε να την αγοράσει. Το σκάνδαλο υπολογίζεται ότι μείωσε την αξία της Yahoo κατά 350 εκατομμύρια δολάρια και, μετά την πώλησή της στην Verizon, η Yahoo μετονομάστηκε σε Altaba, Inc.

- Adult Friend Finder

Τον Οκτώβριο 2016, μία παραβίαση δεδομένων επηρέασε πάνω από 412,2 εκατομμύρια χρήστες το δίκτυο FriendFinder, στο οποίο περιλαμβάνονται ιστοσελίδες για ευκαιριακές σεξουαλικές συνευρέσεις αλλά και πορνογραφικού υλικού, όπως για παράδειγμα το Adult Friend Finder και το Penthouse.com.

Οι χάκερ κατόρθωσαν να συλλέξουν δεδομένα 20 ετών, συμπεριλαμβανομένων ονομάτων, email και κωδικών πρόσβασης, εκμεταλλευόμενοι την αδυναμία τοπικής ενσωμάτωσης αρχείων (Local file inclusion vulnerability) του λογισμικού. Οι περισσότεροι κωδικοί πρόσβασης προστατεύονταν από τον αδύναμο αλγόριθμο SHA-1, κάτι που είχε ως συνέπεια το 99% αυτών να έχουν αποκρυπτογραφηθεί πριν η

LeakedSource.com εκδώσει την πλήρη ανάλυση δεδομένων της επίθεσης στα μέσα στου Νοεμβρίου.

Η αδυναμία αποκαλύφθηκε από έναν ερευνητή ο οποίος εμφανίζεται ως χρήστης 1x0123 στο Twitter και με το όνομα Revolver σε άλλους κύκλους, ο οποίος και εξέθεσε την αδυναμία τοπικής ενσωμάτωσης δεδομένων μέσω φωτογραφιών που ανάρτησε.

Μετά την δημοσίευση της παραβίασης, η αντιπρόεδρος της εταιρείας δήλωσε ότι η αδυναμία του συστήματος που επέτρεψε πρόσβαση στον πηγαίο κώδικα εντοπίστηκε και διορθώθηκε.

- eBay

Και το eBay, η γνωστή ιστοσελίδα δημοπρασιών, έπεσε θύμα χάκερ τον Μάιο του 2014, με αποτέλεσμα να επηρεαστούν 145 εκατ. χρηστών.

Στην διάρκεια της παραβίασης, χάκερ χρησιμοποίησαν τα πιστοποιητικά στοιχεία τριών υπαλλήλων, τα οποία τους εξασφάλισαν πλήρη πρόσβαση στο σύστημα του eBay για 229 μέρες. Στη διάρκεια της περιόδου αυτής, προσκόμισαν ονόματα, διευθύνσεις, ημερομηνίες γέννησης και κρυπτογραφημένους κωδικούς πρόσβασης. Το eBay καθησύχασε τους χρήστες ότι οι πληροφορίες πληρωμής των χρηστών φυλάσσονται χωριστά και δεν είχαν εκτεθεί στη διάρκεια της επίθεσης στον κυβερνοχώρο του. Ωστόσο, προέτρεψε τους χρήστες να αλλάξουν τους κωδικούς τους. Το eBay δέχτηκε, επίσης, σφοδρή κριτική λόγω του ότι δεν είχε μια πιο προληπτικής φύσεως πολιτική ανανέωσης κωδικών για τους χρήστες της.

Παρότι η επίθεση μείωσε λίγο την δραστηριότητα των χρηστών, το eBay δεν υπέστη μόνιμη ζημιά, καθώς το επόμενο τρίμηνο τόσο τα έσοδα όσο και τα κέρδη της εταιρείας αυξήθηκαν όπως είχαν προβλέψει αναλυτές πριν την επίθεση.

- Equifax

Η Equifax είναι ένα από τα μεγαλύτερα πιστωτικά γραφεία των ΗΠΑ, που ανακάλυψε τον Ιούλιο του 2017 μία επίθεση στον κυβερνοχώρο της με «θύματα» 147,9 εκατομμυρίων χρηστών.

Στα δεδομένα αυτά περιλαμβάνονταν αριθμοί κοινωνικής ασφάλισης, ημερομηνίες γέννησης, διευθύνσεις και σε κάποιες περιπτώσεις αριθμοί αδειών οδήγησης και στοιχεία πιστωτικών καρτών.

Παρότι η εταιρεία ανακάλυψε την διαρροή δεδομένων τον Ιούλιο, δήλωσε ότι, κατά τις εκτιμήσεις τους, το χτύπημα μπορεί να είχε ξεκινήσει από τα μέσα Μαΐου.

- Uber

Στο τέλος του 2016 η εταιρεία ανακάλυψε ότι χάκερ είχαν διαρρήξει το σύστημα ασφαλείας της ηλεκτρονικής πλατφόρμας της και είχαν πρόσβαση στα δεδομένα 57 εκατομμυρίων χρηστών καθώς και 600.000 οδηγών. Στα δεδομένα περιλαμβάνονταν τα ονόματα, email, και τηλέφωνα των χρηστών και οι αριθμοί αδείας των οδηγών.

Η Uber αρχικά απέκρυψε την παραβίαση από τους χρήστες της, απέλυσε τον διευθυντή ασφαλείας της και πλήρωσε τους χάκερ 100.000 δολάρια για να καταστρέψουν τα δεδομένα, χωρίς όμως να έχει τρόπο να διαπιστώσει αν πράγματι καταστράφηκαν. Δημοσιοποίησε την παραβίαση έναν ολόκληρο χρόνο αργότερα και υπέστη σοβαρό πλήγμα τόσο στη φήμη όσο και στα έσοδά της.

Την περίοδο που αποκαλύφθηκε το σκάνδαλο, η Uber ήταν εν μέσω διαδικασιών να πουλήσει μέρος των μετοχών της στην Softbank. Η αξία της εταιρείας μειώθηκε από 68 σε 48 δισ. δολάρια όταν έκλεισε η συμφωνία και, παρότι υπήρξαν και άλλοι παράγοντες που επηρέασαν την πτώση αυτή στη μετοχή της, ειδικοί θεωρούν ότι το σκάνδαλο αυτό έπαιξε κομβικό ρόλο.

- Sony's PlayStation Network

Τον Απρίλιο του 2011, επίθεση στη Sony εξέθεσε τα δεδομένα 77 εκατομμυρίων λογαριασμών και κόστισε τουλάχιστον 171 εκατομμύρια δολάρια λόγω του γεγονότος ότι η υπηρεσία ήταν ανενεργή για περίοδο ενός μήνα. Οι 12 από τους 77 εκατομμύρια χρήστες είχαν μη αποκρυπτογραφημένα δεδομένα πιστωτικών καρτών και, ως αποτέλεσμα, οι χάκερ εξασφάλισαν πρόσβαση σε ονοματεπώνυμα, κωδικούς πρόσβασης, email, διευθύνσεις, ιστορικό αγορών, στοιχεία πιστωτικών καρτών καθώς και στοιχεία πρόσβασης στο δίκτυο PlayStation/Qriocity.

Το 2014, η Sony δέχτηκε να πληρώσει περί τα 15 εκατομμύρια δολάρια μετά από ομαδική αγωγή σε βάρος της.

- Adobe

Ο blogger σε θέματα ασφαλείας Μπράιαν Κρεμπς ήταν ο πρώτος που γνωστοποίησε την παραβίαση δεδομένων στο σύστημα της Adobe τον Οκτώβριο του 2013, αλλά χρειάστηκαν εβδομάδες ανάλυσης προκειμένου να διαπιστωθεί η πλήρης κλίμακα της ζημιάς.

Σε αρχική της δήλωση η Adobe εκτίμησε ότι τα θύματα ανέρχονταν στα 3 εκατομμύρια. Παράλληλα, αποκάλυψαν ότι επηρεάστηκε αριθμός χρηστών –άγνωστο ακριβώς πόσοι- τα αποκρυπτογραφημένα στοιχεία πιστωτικών καρτών των οποίων είχαν επίσης εκτεθεί. Η Adobe διόρθωσε την δήλωσή της τον ίδιο μήνα εκτιμώντας ότι οι χάκερ είχαν πρόσβαση στοιχεία πρόσβασης 38 εκατομμυρίων «ενεργών χρηστών». Ο Κρεμπς όμως δήλωσε ότι το αρχείο που είχε αναρτηθεί μερικές μέρες νωρίτερα περιλάμβανε πάνω από 150 στοιχεία πρόσβασης, τον πηγαίο κώδικα για πολλά από τα προϊόντα της Adobe όπως και τα ονόματα, στοιχεία πρόσβασης και στοιχεία πιστωτικών και χρεωστικών καρτών των χρηστών της Adobe.

Η εταιρεία αναγκάστηκε να πληρώσει 1,1 εκατ. δολάρια σε νομικά έξοδα και άγνωστο ποσό σε αποζημιώσεις χρηστών.

- Stuxnet

Το Stuxnet, ένα κακοήθες «σκουλήκι» είχε ως σκοπό του μολύνει υπολογιστές ανά τον κόσμο. Αν και το «σκουλήκι» αυτό εντοπίστηκε το 2010, ειδικοί υπολογίζουν ότι η εφεύρεσή του χρονολογείται γύρω στο 2005.

Η δημιουργία του θεωρείται ότι έγινε μέσω της συνεργασίας των ΗΠΑ και του Ισραήλ στο πρόγραμμα «Επιχείρηση Ολυμπιακοί Αγώνες» (Operation Olympic Games), η οποία ξεκίνησε υπό την ηγεσία του Προέδρου Τζορτζ Μπους και συνέχισε κατά την διάρκεια της θητείας του Προέδρου Μπαράκ Ομπάμα.

Ο στόχος του Stuxnet ήταν να διακόψει, ή τουλάχιστον να καθυστερήσει την ανάπτυξη του πυρηνικού προγράμματος του Ιράν. Παρότι ο σκοπός του ήταν να στοχοποιήσει αποκλειστικά το πυρηνικό πρόγραμμα του Ισραήλ, το «σκουλήκι» ξέφυγε στο διαδίκτυο λόγω της επιθετικής του φύσης και μόλυνε πληθώρα υπολογιστών εκτός του ιρανικού συστήματος, χωρίς όμως να προκαλέσει ιδιαίτερη ζημιά στους περισσότερους από αυτούς.

Θεωρείται ότι θα τελέσει ως πρότυπο για μελλοντικές απόπειρες με στόχο πραγματικές επιθέσεις όπως για παράδειγμα επιθέσεις σε παροχές νερού ή ηλεκτρικού, καθώς και σε δίκτυα μέσων μαζικής μεταφοράς.

- <u>JP Morgan Chase</u>

Τον Ιούλιο του 2014 η επίθεση στα αρχεία της JP Morgan Chase, της μεγαλύτερης τράπεζας των ΗΠΑ, κλόνισε τη χώρα. Η παραβίαση έπληξε πάνω από 50% των Αμερικάνικων νοικοκυριών (76 εκατομμύρια) καθώς επίσης και 7 εκατομμύρια μικρές επιχειρήσεις.

Στην επίθεση αυτή εκτέθηκαν ονόματα, διευθύνσεις, email και αριθμοί τηλεφώνου καθώς και οι εσωτερικές πληροφορίες της τράπεζας για τους πελάτες αυτούς. Σύμφωνα με δήλωση της τράπεζας, δεν κλάπηκαν χρήματα από τους λογαριασμούς των χρηστών και δεν υπήρχε λόγος να πιστέψει κανείς ότι εκτέθηκαν πληροφορίες όπως αριθμοί λογαριασμών, κωδικοί πρόσβασης, ονόματα χρηστών, ημερομηνίες γέννησης ή Αριθμοί Κοινωνικής Ασφάλισης. Παρόλα αυτά, οι χάκερ είχαν πρόσβαση στους διακομιστές της τράπεζας, κάτι που θα τους έδινε προνόμια να μεταφέρουν κεφάλαια ή να κλείσουν λογαριασμούς.

Τον Νοέμβριο του 2015 οι αρχές παρέπεμψαν τέσσερις άνδρες σε δίκη (τρείς εκ των οποίων έχουν ταυτοποιηθεί ως οι Τζέρι Σάλον, Τζόσουα Σάμιουελ Άαρον και Ζιβ Όρενσταϊν) για εγκλήματα συνολικής αξίας $100 εκατομμυρίων. Ο τέταρτος χάκερ δεν ταυτοποιήθηκε.

ΚΕΦΑΛΑΙΟ 5:

ΑΝΤΙΜΕΤΩΠΙΣΗ ΨΗΦΙΑΚΩΝ ΚΙΝΔΥΝΩΝ & ΑΠΕΙΛΩΝ – ΠΡΟΣΤΑΣΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

5.1. Εισαγωγή

Όπως αναφέραμε στα προηγούμενα κεφάλαια, το ζήτημα της ασφάλειας από πιθανές επιθέσεις στο δίκτυο ή στην ιστοσελίδα ενός οργανισμού πρέπει να αποτελεί προτεραιότητα της διοίκησης. Η σπουδαιότητα της ασφάλειας δεν έγκειται μόνο στο γεγονός ότι μέσω μιας πιθανής επίθεσης θα κλονιστεί η φήμη του οργανισμού και θα αποδειχθεί η αδυναμία συμμόρφωσης του στους ευρωπαϊκούς κανονισμούς, αλλά και στο κόστος της επίθεσης το οποίο είναι πολύ σημαντικό.

Στο κεφάλαιο αυτό θα παρουσιάσουμε τα συστήματα ασφάλειας πληροφοριακών συστημάτων που μπορεί να εγκαταστήσει μία εταιρεία ώστε να παραμείνει ασφαλής απέναντι στις επιθέσεις. Σε κάθε περίπτωση θα πρέπει να τονίσουμε ότι οι εφαρμογές λύσεων πληροφορικής από μόνες τους δεν αρκούν για να θεωρήσει μία εταιρεία ότι είναι προστατευμένη.

Πολύ σημαντικός και κρίσιμος παράγοντας είναι και ο ανθρώπινος. Όπως έχουμε αναφέρει, ο ανθρώπινος παράγοντας αποτελεί το ¼ περίπου των αιτιών των περιστατικών ασφαλείας. Για το λόγο αυτό οι εταιρείες θα πρέπει να αφιερώνουν ένα μεγάλο μέρος από το χρόνο και το κόστος που προορίζεται στην ασφάλεια των πληροφοριακών υποδομών τους στην εκπαίδευση των χρηστών.

5.2. Εκπαίδευση χρηστών

Όσο τέλεια κι αν είναι η Πολιτική Ασφάλειας μιας εταιρείας, ποτέ δε θα μπορέσει να αποδειχθεί αποτελεσματική αν οι χρήστες του δικτύου της εταιρείας δεν έχουν την κατάλληλη εκπαίδευση σε θέματα ασφάλειας.

Η εκπαίδευση για την αύξηση της ενημερότητας και της ευαισθητοποίησης σε θέματα που αφορούν την ασφάλεια πληροφοριών πρέπει να αποτελεί συνεχή διαδικασία μιας εταιρείας.

Το «ψάρεμα» είναι ο συχνότερος τρόπος που πολλές απειλές περνούν μέσα στο περιβάλλον μιας επιχείρησης. Το ηλεκτρονικό ταχυδρομείο είναι μία από τις πλέον προβληματικές πηγές μόλυνσης και οι χάκερ εκμεταλλευόμενοι το ανθρώπινο στοιχείο των επιχειρήσεων καταφέρνουν να δημιουργούν διάφορα προβλήματα κλέβοντας συνθηματικά, στοιχεία λογαριασμών κτλ. [23]

Είναι πολύ εύκολο κάποιος εργαζόμενος να παρασυρθεί και να κάνει κλικ σε ένα κακόβουλο email. Συνεπώς, κάθε οργανισμός θα πρέπει να δημιουργήσει μία κουλτούρα όπου η πρώτη σκέψη ή το ένστικτο του κάθε χρήστη θα ήταν να σκεφτεί δύο φορές πριν κάνει κλικ σε συνδέσμους, πριν κατεβάσει συνημμένα αρχεία ή τρέξει λογισμικό που έφτασε στον υπολογιστή του μέσω email.

Υπάρχουν πολλά προγράμματα - προσομοιωτές επιθέσεων phishing («ψαρέματος») μέσω των οποίων οι εταιρείες μπορούν να οργανώνουν εκστρατείες που θα βοηθήσουν τους χρήστες να μάθουν να εντοπίζουν phishing links, επικίνδυνα συνημμένα αρχεία, καθώς και κακόβουλα scripts που δημιουργήθηκαν για να προκαλέσουν ζημιά στην εταιρεία.

Σε τακτά χρονικά διαστήματα μέσα στην εταιρεία μπορεί να τρέχει ένα τέτοιο προσομοιωμένο μήνυμα phishing και να αξιολογείται η ετοιμότητα των χρηστών απέναντι στα πραγματικά περιστατικά phishing που μπορεί να συμβούν.

5.3. Δικτυακή προστασία

Η δικτυακή προστασία αφορά όλα τα δικτυακά συστήματα περιμέτρου που προστατεύουν μία εταιρεία και μέσω των συστημάτων δικτυακής προστασίας προστατεύονται όλοι οι υπολογιστές, οι φορητές συσκευές και οι διακομιστές σε ένα δίκτυο, υποκαταστήματα και απομακρυσμένοι χρήστες που είναι συνδεδεμένοι με VPN, συστήματα ηλεκτρονικής αλληλογραφίας, διακομιστές Web και ασύρματοι χρήστες.

Η λέξη «περίμετρος, ίσως να θυμίζει ένα φράκτη, ένα τείχος ή μια ένοπλη στρατιωτική περιπολία. Όταν αναφερόμαστε σε ένα δίκτυο, ως περίμετρο μπορούμε, αντίστοιχα, να θεωρήσουμε κάθε συσκευή, πραγματική ή εικονική, που διαχωρίζει το δίκτυο αναφοράς από όλα τα υπόλοιπα δίκτυα που το περιβάλλουν και, φυσικά, το ίδιο το Διαδίκτυο. Ως δίκτυο αναφοράς, σε σχέση με την περίμετρο, νοείται το εσωτερικό δίκτυο του οποίου τους πόρους επιθυμούμε να προστατεύσουμε. Για την επίτευξη της προστασίας αυτής χρησιμοποιούνται, σε συνδυασμό ή ξεχωριστά, διατάξεις τείχους προστασίας (firewall) και συστημάτων ανίχνευσης εισβολών (IDS) [10].

Τα συστήματα ασφάλειας πληροφοριακών συστημάτων σε δικτυακό επίπεδο προσφέρουν την απόλυτη προστασία και πλήρη έλεγχο σχετικά με γνωστές ή άγνωστες επιθέσεις, ιούς και ανεπιθύμητα προγράμματα (malware).

Τα συστήματα αυτά είναι:

5.3.1. Τοίχος προστασίας (Firewall)

Η κύρια λειτουργία ενός firewall είναι η ρύθμιση της κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα υπολογιστών. Συνήθως τα δύο αυτά δίκτυα είναι το Διαδίκτυο και το τοπικό/εταιρικό δίκτυο. Ένα firewall παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης (low level of trust), ενώ το εταιρικό δίκτυο ή το οικιακό δίκτυο διαθέτουν τον μέγιστο βαθμό εμπιστοσύνης. Ένα περιμετρικό δίκτυο (perimeter network) ή μία Demilitarized Zone (DMZ) διαθέτουν μεσαίο επίπεδο εμπιστοσύνης. Ο σκοπός της τοποθέτησης ενός firewall είναι η πρόληψη επιθέσεων στο τοπικό δίκτυο και η αντιμετώπισή τους.

Τα firewalls μπορεί να ενσωματώνουν όλες τις υπηρεσίες Antivirus, URL Filtering, Antispam, τοίχου προστασίας εφαρμογών Web, συστήματος πρόληψης

εισβολής (IPS) κλπ. καθότι μπορούν να περιλαμβάνουν πλήθος των χαρακτηριστικών ασφάλειας τους σε ένα σύνολο που ονομάζεται UTM (Unified Threat Management).

Τα firewalls προσφέρουν κεντρικό έλεγχο μέσα από ένα web interface πολύ εύκολο στη χρήση, δίνοντας όλες τις επιλογές που πρέπει να εφαρμοστούν για την ολοκληρωμένη διαχείριση της περιμετρικής ασφάλειας, προκειμένου να διαχειριστούν όλες οι απαραίτητες πολιτικές ασφάλειας για τον αποτελεσματικό έλεγχο των κινδύνων στο κυβερνοχώρο.

5.3.2. Σύστημα ανίχνευσης εισβολών (Intrusion Detection System – IDS)

Η ανίχνευση εισβολών στοχεύει στην ανακάλυψη κακόβουλων ενεργειών μέσω της ανάλυσης καταγραφών (auditing) και του εντοπισμού ύποπτης συμπεριφοράς ενός επιτιθέμενου που έχει καταφέρει να αποκτήσει πρόσβαση στο σύστημα. Η αρχή της λειτουργίας της βασίζεται στην υπόθεση πως ο επιτιθέμενος θα συμπεριφερθεί διαφορετικά σε σχέση με ένα νόμιμο χρήστη του συστήματος. Καθώς η ανάλυση των καταγραφών από το διαχειριστή είναι εργασία επίπονη και χρονοβόρα, έχουν αναπτυχθεί συστήματα τα οποία είναι επιφορτισμένα με την ανάλυση αυτή σε πραγματικό χρόνο, τα οποία είναι γνωστά ως Intrusion Detection Systems (IDS).

5.3.3. Ασφάλεια διακομιστή περιήγησης ιστοσελίδων (Secure Web Gateway)

Σκοπός ενός συστήματος Secure Web Gateway είναι να καθιστά την περιήγηση στο web ασφαλή και να παρέχει προηγμένη προστασία από εξελιγμένα κακόβουλα λογισμικά που κυκλοφορούν στο web, ταχύτατα χωρίς να επιβραδύνει τους χρήστες που εργάζονται. Επίσης, παρέχει πλήρη έλεγχο και πληροφόρηση σχετικά με τη δραστηριότητα του web στο δίκτυο.

5.3.4. Ασφάλεια διακομιστή ηλεκτρονικής αλληλογραφίας (Secure Email Gateway)

Το σύστημα Secure Email Gateway είναι μία λύση όλα-σε-ένα για την ασφάλεια του ηλεκτρονικού ταχυδρομείου, κρυπτογράφησης, DLP, anti-spam και την προστασία έναντι απειλών, παρέχοντας προηγμένη προστασία από εξελιγμένες επιθέσεις phishing

και δίνοντας πλήρη έλεγχο των δεδομένων που διακινούνται από μία επιχείρηση μέσω του ηλεκτρονικού ταχυδρομείου.

5.3.5. Ασφάλεια ασύρματης δικτύωσης (Secure Wi-Fi)

Το σύστημα Secure Wi-Fi εξασφαλίζει την αξιόπιστη ασύρματη πρόσβαση όλων των χρηστών σε ένα δίκτυο με κεντρική διαχείριση και μεγάλη ασφάλεια. Τα σημεία ασύρματης πρόσβασης (access points) παρέχουν πλήρη προστασία για τους ασύρματους χρήστες που διασυνδέουν.

5.4. Προστασία χρηστών

Η θωράκιση των χρηστών με συστήματα για προστασία από ιούς, κρυπτογράφηση δεδομένων και έλεγχο κινητών συσκευών είναι το επόμενο βήμα για μία εταιρεία ώστε να ενισχύσει την ασφάλεια της πέρα από την περίμετρο.

5.4.1. Προστασία τελικού σημείου (Endpoint protection)

Πλέον μία λύση προστασίας στον τελικό χρήστη είναι κάτι παραπάνω από ένα απλό λογισμικό antivirus ενάντια στους ιούς. Η νέα εποχή προστασίας τερματικών συσκευών από προηγμένες απειλές περιλαμβάνει τεχνολογίες signature-less, anti-hacker, anti-ransomware και anti-exploit που προσφέρουν root-cause analysis, προηγμένη σάρωση antivirus και καθαρισμό malware ώστε να το απομακρύνει από το σύστημα του χρήστη.

Κάθε τερματική συσκευή πρέπει να προστατεύεται με μία τέτοια λύση ενάντια στην μάστιγα του ransomware η οποία να είναι ικανή να τα σταματήσει εν τη γενέσει τους, από όπου και αν προέρχονται όπως πχ. usb sticks και όσο σύγχρονα και να είναι, ενώ να μπορεί να επαναφέρει τυχόν κατεστραμμένα αρχεία σε μία πρωτύτερα γνωστή και ασφαλή κατάσταση τους. Επίσης, να μπορεί να σταματάει τις απειλές zero-day χωρίς την ανάγκη παραδοσιακής σάρωσης των αρχείων, χάρη στην προηγμένη τεχνολογία anti-exploit που ενσωματώνει και χωρίς την ανάγκη ενημέρωσης των υπογραφών

(signatures), κάτι που κάνουν τα παραδοσιακά antivirus. Επίσης, να μπορεί να προσφέρει αυτόματα ειδικές αναφορές, για την πηγή προέλευσης των επιθέσεων (root cause analysis), την επισήμανση τυχόν πρόσθετων σημείων μόλυνσης, ενώ να παρέχει και οδηγίες για την ενίσχυση της ασφάλειας της επιχείρησης ή του οργανισμού.

Συνεπώς, η Προστασία Τερματικών Συσκευών είναι μία αποδεδειγμένη λύση για επιτραπέζιους και φορητούς υπολογιστές που τρέχουν σε Windows, Mac, Linux. Ο πυρήνας υψηλής απόδοσης του συστήματος (endpoint agent) μπορεί να παρέχει αποτελεσματική προστασία που περιλαμβάνει έλεγχο εφαρμογών και διαχείριση εξωτερικών συσκευών (device control), έλεγχο περιήγησης ιστοσελίδων για κακόβουλο ή ακατάλληλο περιεχόμενο (web protection) με ενσωματωμένο έλεγχο για ανίχνευση επικίνδυνων προγραμμάτων (malware).

5.4.2. Ασφάλεια και έλεγχος φορητών συσκευών (Mobile security & control)

Με την έκρηξη της χρήσης των φορητών συσκευών σε εταιρείες και επιχειρήσεις έρχεται και ο αναπόφευκτος πονοκέφαλος της εξασφάλισης ότι όλα τα ευαίσθητα και εμπιστευτικά εταιρικά δεδομένα και πληροφορίες παραμένουν ασφαλείς. Κανονισμοί για την προστασία των δεδομένων, θα πρέπει να τηρούνται πολιτικές ασφαλείας ενώ και η πνευματική ιδιοκτησία θα πρέπει να παραμείνει ασφαλής και εμπιστευτική.

Μέσω της Προστασίας Φορητών Συσκευών (Mobile Control) οι εταιρείες μπορούν να ασφαλίζουν αποτελεσματικά φορητές συσκευές με iOS, Android και Windows Phone 8 έτσι ώστε τα ευαίσθητα δεδομένα τους να διακινούνται με πλήρη ασφάλεια μέσω συσκευών που ανήκουν στην εταιρία ή στους εργαζόμενους (BYOD-Bring Your Own Device). Μία λύση Προστασίας Φορητών Συσκευών διαχειρίζεται όλες τις συσκευές από την αρχική παραμετροποίησή τους και την εγγραφή στο σύστημα, έως τον παροπλισμό της συσκευής αν αυτό κριθεί αναγκαίο.

5.4.3. Προστασία διακομιστών (Server protection)

Οι διακομιστές αποτελούν τα βασικά εργαλεία κάθε επιχείρησης ή οργανισμού για την αποθήκευση ευαίσθητων δεδομένων, για την διευκόλυνση των επικοινωνιών και για την εκτέλεση διάφορων επιχειρησιακών διαδικασιών, οπότε η προστασία τους αποτελεί κλειδί για την προστασία ολόκληρου του οργανισμού.

Είτε πρόκειται για ένα βασικό διακομιστή διάθεσης αρχείων με Windows ή ένα εξελιγμένο διακομιστή εφαρμογών με Linux, η ουσιαστική προστασία από ιούς είναι απολύτως απαραίτητη, χωρίς να καταναλώνονται πολύτιμοι πόροι του συστήματος.

5.5. Κρυπτογράφηση (Encryption)

Ένα εξελιγμένο πρόγραμμα ασφαλείας δεν θα πρέπει να περιορίζεται στην ασφάλεια σε επίπεδο firewall ή σε επίπεδο endpoint. Τα αρχεία χρειάζονται προστασία, επίσης, όπου και αν βρίσκονται, ανά πάσα στιγμή.

Ένα σύστημα κρυπτογράφησης που μπορεί να εγκαταστήσει μία εταιρεία στις συσκευές των χρηστών της είναι μία πλήρως επεκτάσιμη λύση ελέγχου και προστασίας των πληροφοριών, που επιβάλλει την πολιτική ασφάλειας για επιτραπέζιους και φορητούς υπολογιστές, μετακινούμενα μέσα (removable media) σε ετερογενή περιβάλλοντα, δικτυακά αποθηκευτικά μέσα και υπηρεσίες αποθήκευσης στο Cloud. Το σύστημα επιτρέπει στις εταιρείες να προστατεύουν αποτελεσματικά τις εμπιστευτικές τους πληροφορίες και στόχους, πάντα σύμφωνα με τις αποφάσεις που έχουν πάρει για την ασφάλεια τους.

Η κρυπτογράφηση ολόκληρου του δίσκου, το full-disk encryption είναι μία ζωτικής σημασίας πρώτη γραμμή άμυνας σε περιπτώσεις που κάποιος υπολογιστής κλαπεί, χαθεί ή ξεχαστεί οπουδήποτε εκτός εταιρείας και πρέπει να χρησιμοποιείται σε όλους τους υπολογιστές μίας επιχείρησης.

5.6. Προστασία προνομιακών λογαριασμών

Το πρώτο, και ενδεχομένως κρισιμότερο βήμα για την εφαρμογή και ενεργοποίηση αποτελεσματικής άμυνας ενάντια στην κλοπή δεδομένων και κάθε είδους επίθεση, που προέρχεται από έξω ή ακόμα και από κακόβουλους χρήστες εντός της επιχείρησής, είναι η προστασία των προνομιακών λογαριασμών όλων των τερματικών συσκευών, των εγκαταστάσεων, των διακομιστών ή των υποδομών στο σύννεφο.

Οι τύποι προνομιακών λογαριασμών που συνήθως υπάρχουν σε ένα επιχειρηματικό περιβάλλον είναι [27]:

- *Οι λογαριασμοί διαχείρισης σε τοπικό επίπεδο* είναι μη προσωπικοί λογαριασμοί που παρέχουν πρόσβαση διαχειριστή μόνο στον τοπικό κεντρικό υπολογιστή ή σε ένα instance. Οι τοπικοί λογαριασμοί διαχείρισης χρησιμοποιούνται συνήθως από το προσωπικό πληροφορικής για τη συντήρηση των σταθμών εργασίας, των διακομιστών, των συσκευών δικτύου, των βάσεων δεδομένων, των κεντρικών υπολογιστών κλπ. Συχνά έχουν τον ίδιο κωδικό πρόσβασης σε ολόκληρη την πλατφόρμα ή στον οργανισμό για ευκολία χρήσης. Αυτός ο κοινόχρηστος κωδικός πρόσβασης σε δεκάδες, εκατοντάδες ή και χιλιάδες υπολογιστές αποτελεί εύκολο στόχο και οι προηγμένες απειλές έχουν δημιουργηθεί για να εκμεταλλεύονται συστηματικά.

- *Οι προνομιακοί λογαριασμοί χρηστών* είναι ονομαστικά διαπιστευτήρια στα οποία έχουν χορηγηθεί δικαιώματα διαχειριστή σε ένα ή περισσότερα συστήματα. Αυτή είναι συνήθως μια από τις πιο κοινές μορφές λογαριασμού προνομιακής πρόσβασης που παρέχεται σε ένα επιχειρηματικό δίκτυο, επιτρέποντας σε χρήστες να έχουν δικαιώματα διαχείρισης, όπως για παράδειγμα, σε τοπικούς επιτραπέζιους υπολογιστές ή σε συστήματα που διαχειρίζονται. Συχνά αυτοί οι λογαριασμοί έχουν μοναδικούς και σύνθετους κωδικούς πρόσβασης και η δύναμη που έχουν πάνω στα συστήματα που διαχειρίζονται είναι τέτοια που καθιστά απαραίτητη τη συνεχή παρακολούθηση της χρήσης τους.

- *Οι λογαριασμοί διαχείρισης τομέα (Domain)* έχουν προνομιακή διοικητική πρόσβαση σε όλους τους σταθμούς εργασίας και διακομιστές εντός domain. Ενώ αυτοί οι λογαριασμοί είναι λίγοι σε αριθμό, παρέχουν την πιο εκτεταμένη και ισχυρή πρόσβαση σε όλο το δίκτυο. Με πλήρη έλεγχο σε όλους τους domain controllers και με δυνατότητα ακόμα και τροποποίησης της ιδιότητας μέλους κάθε διαχειριστικού λογαριασμού εντός του τομέα, η κλοπή αυτών των διαπιστευτηρίων αποτελεί συχνά το χειρότερο σενάριο για κάθε οργανισμό.

- *Οι λογαριασμοί έκτακτης ανάγκης* παρέχουν σε μη προνομιούχους λογαριασμούς χρηστών δυνατότητα πρόσβασης διαχειριστή σε περιπτώσεις έκτακτης ανάγκης και για αυτό μερικές φορές αναφέρονται ως λογαριασμοί «firecall» ή «breakglass». Και ενώ η πρόσβαση σε αυτούς τους λογαριασμούς συνήθως απαιτεί έγκριση από τη

διαχείριση για λόγους ασφαλείας, πρόκειται συνήθως για μία χειροκίνητη διαδικασία που είναι αναποτελεσματική και στερείται οποιουδήποτε ελέγχου.

- *Οι υπηρεσιακοί λογαριασμοί* μπορούν να είναι προνομιούχοι τοπικοί λογαριασμοί ή λογαριασμοί τομέα (domain) που χρησιμοποιούνται από μια εφαρμογή ή μια υπηρεσία για να αλληλοεπιδρούν με το λειτουργικό σύστημα. Σε ορισμένες περιπτώσεις, αυτοί οι λογαριασμοί υπηρεσιών έχουν δικαιώματα διαχείρισης τομέα ανάλογα με τις απαιτήσεις της εφαρμογής για την οποία χρησιμοποιούνται. Οι τοπικοί υπηρεσιακοί λογαριασμοί μπορούν να αλληλοεπιδρούν με διάφορα στοιχεία των Windows, γεγονός που καθιστά δύσκολο τον συντονισμό των αλλαγών σε κωδικούς πρόσβασης.

- *Οι αλλαγές στον κωδικό πρόσβασης λογαριασμού Active Directory ή domain service* μπορεί να είναι ακόμα πιο δύσκολες καθώς απαιτούν το συντονισμό μεταξύ πολλών συστημάτων. Αυτή η πρόκληση συχνά οδηγεί στη κοινή πρακτική της σπάνιας αλλαγής των κωδικών πρόσβασης υπηρεσιακών λογαριασμών κάτι που αντιπροσωπεύει σημαντικό κίνδυνο για μια επιχείρηση.

- *Οι λογαριασμοί εφαρμογών* είναι λογαριασμοί που χρησιμοποιούνται από εφαρμογές για πρόσβαση σε βάσεις δεδομένων, για εκτέλεση εργασιών ή ενεργειών μαζικά ή για να παρέχουν πρόσβαση σε άλλες εφαρμογές. Αυτοί οι προνομιακοί λογαριασμοί έχουν συνήθως ευρεία πρόσβαση σε βασικές πληροφορίες της επιχείρησης και σε εταιρικά δεδομένα που βρίσκονται σε εφαρμογές και βάσεις δεδομένων. Οι κωδικοί πρόσβασης για αυτούς τους λογαριασμούς ενσωματώνονται συχνά και αποθηκεύονται σε μη κρυπτογραφημένα αρχεία κειμένου, ένα θέμα ευπάθειας που αναπαράγεται σε πολλούς διακομιστές και αντιπροσωπεύει σημαντικό κίνδυνο για έναν οργανισμό, επειδή οι εφαρμογές συχνά φιλοξενούν τα συγκεκριμένα δεδομένα που αποτελούν και στόχο των προηγμένων επίμονων απειλών (APTs).

Οι προνομιακοί λογαριασμοί αντιπροσωπεύουν τη μεγαλύτερη ευπάθεια στην ασφάλεια που έχει να αντιμετωπίσει σήμερα ένας σύγχρονος οργανισμός. Στα χέρια ενός εξωτερικού εισβολέα ή ενός κακόβουλου ατόμου από το εσωτερικό μίας εταιρείας, οι προνομιακοί λογαριασμοί επιτρέπουν σε επιτιθέμενους να αναλάβουν τον πλήρη έλεγχο της υποδομής IT ενός οργανισμού, να απενεργοποιήσουν ρουτίνες ελέγχου ασφαλείας, να κλέψουν εμπιστευτικές πληροφορίες, να διαπράξουν οικονομικές απάτες και να

διαταράξουν την λειτουργία της επιχείρησης γενικότερα. Σχεδόν σε όλες τις παραβιάσεις, προηγείται κλοπή και κατάχρηση διαπιστευτηρίων. Με αυτή την ολοένα αυξανόμενη απειλή, οι οργανισμοί και οι εταιρείες πρέπει να τοποθετούν συστήματα ελέγχου για την προληπτική τους προστασία, τα οποία ανιχνεύουν και απαντούν σε εν εξελίξει κυβερνοεπιθέσεις προτού χτυπήσουν ζωτικής σημασίας συστήματα και θέσουν σε κίνδυνο ευαίσθητα δεδομένα.

Ένα σύστημα προστασίας προνομιακών λογαριασμών (Privileged Accounts Security) αποτελείται από επιμέρους υποσυστήματα τα οποία προσφέρουν σε μία ενιαία αρχιτεκτονική ευελιξία και επεκτασιμότητα ώστε να μπορούν να ταιριάξουν και να προσαρμοστούν σε κάθε επιχειρησιακό περιβάλλον.

Αρχικά, ένα τέτοιο σύστημα αποτελείται από την Ασφαλή Τράπεζα Πληροφοριών (Secure Vault) η οποία ανακαλύπτει, ασφαλίζει, ανανεώνει ανά τακτά χρονικά διαστήματα και ελέγχει την πρόσβαση σε κωδικούς πρόσβασης προνομιακών λογαριασμών που χρησιμοποιούνται σε συστήματα πρόσβασης κατά μήκος του περιβάλλοντος IT στην επιχείρηση. Η λύση επιτρέπει σε οργανισμούς να κατανοήσουν τα ρίσκα που συνοδεύουν τους προνομιακούς λογαριασμούς τους και να τοποθετήσουν ελέγχους για τον μετριασμό των συγκεκριμένων κινδύνων. Ευέλικτες πολιτικές επιτρέπουν σε οργανισμούς και εταιρείες να επιβάλλουν λεπτομερείς ελέγχους προνομιακής πρόσβασης, να αυτοματοποιήσουν τις ροές εργασιών και να αλλάζουν διαρκώς τους κωδικούς πρόσβασης ανά συγκεκριμένα χρονικά διαστήματα χωρίς να απαιτείται κάποια χειροκίνητη προσπάθεια από το τμήμα IT. Για λόγους συμμόρφωσης, οι οργανισμοί και οι εταιρείες μπορούν εύκολα να δημιουργήσουν αναφορές σχετικά με το ποιοι χρήστες είχαν πρόσβαση σε συγκεκριμένους προνομιούχους λογαριασμούς, πότε είχαν πρόσβαση και για πιο σκοπό συγκεκριμένα.

Στη συνέχεια μία εταιρεία μπορεί να εγκαταστήσει έναν Διαχειριστή Κλειδιών SSH (SSH Key Manager) για να αποθηκεύει με ασφάλεια, να ανανεώνει ανά τακτά χρονικά διαστήματα και να ελέγχει την πρόσβαση στα κλειδιά SSH για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε προνομιακούς λογαριασμούς.

Ένα ακόμη υποσύστημα είναι ο Διαχειριστής Προνομιακών Συνεδριών (Privileged Session Manager) ο οποίος επιτρέπει σε εταιρείες και οργανισμούς να απομονώνουν, να παρακολουθούν, να καταγράφουν και να ελέγχουν τις προνομιακές συνεδρίες σε κρίσιμης σημασίας συστήματα υπολογιστών, συμπεριλαμβανομένων συστημάτων Unix και Windows καθώς και βάσεων δεδομένων και εικονικών μηχανών. Το σύστημα ενεργεί ως jump server και ως μοναδικό σημείο ελέγχου πρόσβασης, εμποδίζοντας σε οποιοδήποτε κακόβουλο λογισμικό να μεταπηδήσει στο σύστημα-

στόχο, παρακολουθώντας διαρκώς μέσω καταγραφής τόσο των πληκτρολογήσεων που γίνονται όσο και των εντολών που δίνονται στα συστήματα. Οι λεπτομερείς καταγραφές των συνεδριών που προκύπτουν καθώς και τα διάφορα αρχεία καταγραφής συμβάντων χρησιμοποιούνται για την απλούστευση των ελέγχων συμμόρφωσης και την επιτάχυνση των εγκληματολογικών ερευνών που ενδέχεται να προκύψουν.

Το υποσύστημα Threat Analytics Προνομιακών Λογαριασμών (Privileged Threat Analytics) είναι ένα σύστημα πληροφοριών ασφαλείας που επιτρέπει στους οργανισμούς να ανιχνεύουν, να ειδοποιούν και να αντιμετωπίζουν κυβερνοεπιθέσεις που έχουν στόχο προνομιακούς λογαριασμούς. Η λύση σχεδιάστηκε για να ανιχνεύει και να εντοπίζει μια επίθεση σε πραγματικό χρόνο και να ανταποκρίνεται αυτόματα αποτρέποντας τον εισβολέα από το να συνεχίσει να εξελίσσει την επίθεση. Στον πυρήνα της συγκεκριμένης λύσης, η μηχανή analytics εκτελεί ένα εξελιγμένο σύνολο αλγορίθμων που έχει αναπτυχθεί συμπεριλαμβανομένων αλγορίθμων βεβαιότητας ή συμπεριφοράς (deterministic / behavioral) πάνω σε χρήστες, οντότητες αλλά και πάνω στη δικτυακή κίνηση για την ανίχνευση τυχόν ενδείξεων μόλυνσης ή παραβίασης στα αρχικά στάδια μίας επίθεσης. Με τον εντοπισμό των εισβολέων στα αρχικά στάδια μίας επίθεσης, οι ομάδες ασφαλείας IT έχουν στη διάθεση τους περισσότερο χρόνο για να βρουν τον τρόπο να σταματήσουν την επίθεση, προτού μπει σε κίνδυνο η λειτουργία της επιχείρησης.

Τέλος, ο Διαχειριστής Ταυτότητας Εφαρμογών (Application Identity Manager) δίνει την δυνατότητα σε οργανισμούς και επιχειρήσεις να προστατεύουν κρίσιμης σημασίας συστήματα της επιχείρησης με το να εξαλείφει hard-coded διαπιστευτήρια που έχουν καταγραφεί εντός scripts εφαρμογών, σε αρχεία ρυθμίσεων ή σε κώδικα λογισμικού, καθώς και να αφαιρεί κλειδιά SSH από διακομιστές όταν αυτά χρησιμοποιούνται από εφαρμογές και scripts.

5.7. Διαχείριση ευαίσθητων πληροφοριών

Στο σημερινό δυναμικό επιχειρησιακό περιβάλλον, που περιλαμβάνει αλληλεπιδράσεις μεταξύ του Cloud αλλά και των φορητών συσκευών, οι χρήστες απαιτούν αξιόπιστη πρόσβαση σε πληροφορίες και δεδομένα οπουδήποτε και οποτεδήποτε χρειαστεί. Η δυνατότητα ανταλλαγής πληροφοριών μεταξύ χρηστών και συστημάτων έχει γίνει πλέον μία θεμελιώδης απαίτηση για τις σύγχρονες επιχειρήσεις.

Ο διαμοιρασμός των πληροφοριών δίνει τη δυνατότητα στους χρήστες να είναι περισσότερο παραγωγικοί, διευκολύνει την συνεργασία μεταξύ των ομάδων και βοηθάει τις διάφορες εταιρείες να προσφέρουν πολύ καλύτερα αποτελέσματα στους πελάτες τους. Παρόλα αυτά, καθώς οι επιχειρήσεις διαμοιράζονται όλο και περισσότερες ευαίσθητες πληροφορίες, είναι απολύτως απαραίτητο να εξασφαλιστεί ότι οι συγκεκριμένες ευαίσθητες πληροφορίες και τα κρίσιμα δεδομένα θα παραμείνουν ασφαλή.

Για να διατηρηθεί η παραγωγικότητα των χρηστών σε υψηλά επίπεδα, χωρίς να μπει σε κίνδυνο η ασφάλεια υπάρχει μία απαίτηση κρίσιμης σημασίας. Αυτό επιτυγχάνεται δίνοντας τη δυνατότητα στους χρήστες να μοιράζονται με ασφαλή τρόπο αρχεία, εσωτερικά και εξωτερικά, καθώς και να υπάρχει ασφαλής παρακολούθηση των διαπιστευτηρίων σύνδεσης σε ένα ολοένα αυξανόμενο αριθμό επιχειρηματικών εφαρμογών. Ταυτόχρονα, οι ομάδες πληροφορικής και ασφαλείας είναι επιφορτισμένες με την ασφάλεια των διάφορων ευαίσθητων πληροφοριών που διαμοιράζονται σε αυτοματοποιημένες επιχειρησιακές διαδικασίες, ενώ παράλληλα τα κόστη πρέπει να μειώνονται για να εξασφαλιστεί η αποδοτικότητα της επιχείρησης.

Η Λύση Διαχείρισης Ευαίσθητων Πληροφοριών (Sensitive Information Management Solution) είναι μια ολοκληρωμένη πλατφόρμα για την ασφαλή αποθήκευση, την κοινή χρήση και την ασφαλή διανομή πληροφοριών μεταξύ των χρηστών και των συστημάτων. Δίνει τη δυνατότητα σε άτομα να αποθηκεύουν με ασφάλεια, να μοιράζονται ευαίσθητα αρχεία και επιχειρησιακούς κωδικούς πρόσβασης καθώς και να αυτοματοποιούν επιχειρησιακές διαδικασίες για την ασφαλή συλλογή, πρόσβαση και διανομή ευαίσθητων πληροφοριών και δεδομένων.

5.8. Ταξινόμηση δεδομένων

Κάθε μέρα οι επιχειρήσεις παράγουν όλο και περισσότερα δεδομένα. Τα δεδομένα αποθηκεύονται, οι εργαζόμενοι προχωρούν με τη δουλειά τους, τα δεδομένα ξεχνιούνται και, αναπόφευκτα πολλές φορές, χάνονται. Πολύτιμες πληροφορίες που βρίσκονται σε διακομιστές αρχείων και σε “αποθήκες” εγγράφων δεν προστατεύονται και μερικές φορές είναι ακατόρθωτο να ανακτηθούν, επειδή πολύ απλά δεν μπορούν να εντοπιστούν. Ωστόσο, χάρη στην ταξινόμηση δεδομένων (Data Classification) οι

επιχειρήσεις μπορούν να ανακτήσουν ευκολότερα και να προσδιορίσουν με μεγαλύτερη ακρίβεια ποια είναι τα δεδομένα που πρέπει να προστατευθούν. Η ταξινόμηση των δεδομένων μπορεί να μειώσει τον κίνδυνο της διαρροής δεδομένων και παράλληλα να αυξήσει την αποδοτικότητα της επιχείρησης.

Επίσης, η ταξινόμηση δεδομένων αποτελεί βασικό συστατικό κάθε επιτυχημένης στρατηγικής πρόληψης απώλειας δεδομένων (DLP). Η ταξινόμηση είναι επομένως ένα βασικό δομικό στοιχείο μιας συνεκτικής και συνεχώς εξελισσόμενης στρατηγικής διαχείρισης κινδύνου, δεδομένων και συμμόρφωσης για τις επιχειρήσεις που έχουν μπροστά τους CUI, HIPAA, NYCRR PART 500, συμμόρφωση GDPR και άλλα πολλά [24].

Η ταξινόμηση δεδομένων μπορεί να βοηθήσει την επιχείρηση να ανακτήσει τον έλεγχο όλων των μη δομημένων και ταξινομημένων/κατηγοριοποιημένων δεδομένων. Με τη συμμετοχή των χρηστών στη ταξινόμηση δεδομένων, αυτομάτως καθίστανται περισσότερο ενημερωμένοι για τα δεδομένα, και κατανοούν καλύτερα τις πολιτικές της εταιρείας, καθώς και την αξία των δεδομένων του οργανισμού.

Μία λύση ταξινόμησης δεδομένων περιλαμβάνει ένα σύνολο προϊόντων ταξινόμησης που συνδυάζονται για να προσφέρουν μέγιστη αξία στις κοινότητες των χρηστών της επιχείρησης. Τα προϊόντα αυτά είναι:

- *Ταξινομητής Email:* Επιτρέπει στους χρήστες του Outlook να ταξινομούν τα μηνύματα ηλεκτρονικού ταχυδρομείου τους. Μόλις επισημανθούν, τα δεδομένα είναι πια υπό έλεγχο, για να εξασφαλιστεί ότι τα email και τα αρχεία αποστέλλονται μόνο σε όσους οι χρήστες θέλουν να τα λάβουν, προστατεύοντας τις πολύτιμες πληροφορίες από κάποια τυχαία απώλεια.

- *Ταξινομητής Σημειώσεων:* Δίνει την δυνατότητα στους χρήστες να επιλέξουν τον τρόπο ταξινόμησης των μηνυμάτων τους και στη συνέχεια να εφαρμόσουν κανόνες έτσι ώστε τα δεδομένα να μπορούν να μαρκάρονται (επισημαίνονται) και να ελέγχονται με βάση το πόσο ευαίσθητα ή κρίσιμης σημασίας είναι. Αυτοί οι κανόνες συμπεριλαμβάνουν έλεγχο πάνω στα δεδομένα που διαμοιράζονται με άτομα εκτός του οργανισμού.

- *Ταξινομητής Κινητών Συσκευών:* Επιτρέπει τους χρήστες να διαχωρίζουν τα προσωπικά δεδομένα από εκείνα της επιχείρησης, διασφαλίζοντας ότι οι χρήστες ταξινομούν σωστά τα επιχειρηματικά δεδομένα, ώστε να διευκολυνθεί η διαχείριση και προστασία τους.

- *Ταξινομητής OWA:* Καθώς αυξάνεται η επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, η απώλεια δεδομένων οφείλεται περισσότερο σε σφάλματα χρηστών. Χρησιμοποιώντας τον OWA Classifier, όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται από το Microsoft Outlook Web App μπορούν να ταξινομηθούν και να ελεγχθούν σύμφωνα με την πολιτική ασφαλείας δεδομένων της επιχείρησής. Το Add-In του Classifier Mail for OWA σχεδιάστηκε για να λειτουργεί με το OWA 2013/16 ή το Office 365.

- *Ταξινομητής Office:* Λειτουργεί μέσα από το Microsoft Office, υποστηρίζοντας κάθε χρήστη στη ταξινόμηση εγγράφων που δημιουργούνται ή τροποποιούνται, εφαρμόζοντας οπτικές σημάνσεις για να διασφαλιστεί η ευαισθητοποίηση τους σχετικά με τις ευθύνες τους στη διαφύλαξη δεδομένων.

- *Ταξινομητής Sharepoint:* Για την ταξινόμηση δεδομένων που βρίσκονται αποθηκευμένα εντός του Microsoft δίνοντας τη δυνατότητα ταξινόμησης μεγάλων όγκων εγγράφων καθώς φορτώνονται στο SharePoint γρήγορα και αποτελεσματικά.

- *Ταξινομητής CAD:* Για την ταξινόμηση δεδομένων σε βασικά έγγραφα που αφορούν στη σχεδίαση και σε εφαρμογές CAD. Σε συνδυασμό με τον Ταξινομητή Email, ο CAD Classifier μπορεί επίσης να διασφαλίσει ότι τα έγγραφα αυτά αποστέλλονται μόνο στα κατάλληλα τμήματα του οργανισμού και μόνο στους κατάλληλους εξωτερικούς οργανισμούς.

- *Ταξινομητής Mac:* Για την ταξινόμηση δεδομένων σε οργανισμούς που χρησιμοποιούν συσκευές Mac, υποστηρίζοντας κάθε χρήστη πάνω στη σωστή ταξινόμηση των εγγράφων και των μηνυμάτων ηλεκτρονικού ταχυδρομείου καθώς επεξεργάζονται μέσα από τις εφαρμογές του Microsoft Office για Mac.

5.9. Σάρωση ασφάλειας εφαρμογών ιστού

Οι επιχειρήσεις βασίζονται σε εφαρμογές ιστού για να επιτρέπουν στους υπαλλήλους τους να έχουν πρόσβαση σε κρίσιμης σημασίας εταιρικά δεδομένα από

οπουδήποτε και ανά πάσα στιγμή, επιτρέποντάς τους να συνεργάζονται με επιχειρηματικούς εταίρους όποτε είναι απαραίτητο και παράλληλα να είναι παραγωγικότεροι. Σαν αποτέλεσμα πολλές επιχειρήσεις έχουν μεταφέρει τις περισσότερες δραστηριότητές τους στο Διαδίκτυο, έτσι ώστε οι εργαζόμενοι και οι επιχειρηματικοί συνεργάτες από απομακρυσμένα γραφεία και από διαφορετικές χώρες αντίστοιχα να μπορούν να μοιράζονται ευαίσθητα δεδομένα σε πραγματικό χρόνο και να συνεργάζονται για έναν κοινό στόχο.

Οι εταιρικές και business-focused εφαρμογές ιστού του είδους τείνουν να είναι ευαίσθητες σε ευπάθειες που μπορούν να ανιχνευθούν αυτόματα και να πέσουν θύματα εκμετάλλευσης εύκολα. Οι στατιστικές και οι αναφορές από αξιόπιστες πηγές δείχνουν μια σταθερή ανοδική τάση στις επιτυχείς επιθέσεις από χάκερ.

Η λύση για τις επιχειρήσεις είναι να προσδιορίσουν και να διορθώσουν ευπάθειες στις εφαρμογές ιστού πριν εντοπιστούν τυχόν “exploits” και πέσουν θύματα εκμετάλλευσης από χάκερ. Με αυτοματοποιημένους σαρωτές ασφαλείας για εφαρμογές ιστού οι επιχειρήσεις και οι οργανισμού μπορούν να εντοπίσουν αυτόματα τις εκμεταλλεύσιμες ευπάθειες και άλλα κενά ασφαλείας και ελαττώματα που θα μπορούσαν να τις αφήσουν εκτεθειμένες.

Στο σημείο αυτό θα αναφερθούμε σε δύο διαδικασίες που χρησιμοποιούνται για την ανίχνευση πιθανόν κινδύνων και απειλών, την αξιολόγηση ευπάθειας και την δοκιμή διείσδυσης [25].

- **Αξιολόγηση ευπάθειας**

Η αξιολόγηση ευπάθειας (vulnerability assessment) περιλαμβάνει τη διεξαγωγή μιας σειράς πολλαπλών δοκιμών ενάντια σε ορισμένες ιστοσελίδες, σε εφαρμογές ιστού, σε διευθύνσεις IP και σε εύρη IP, χρησιμοποιώντας μια γνωστή λίστα ευπαθειών και τρωτών σημείων σαν αυτά που περιλαμβάνονται στη λίστα Top 10 του OWASP[1] (Open Web Application Security Project), μία online κοινότητα που παράγει ελεύθερα διαθέσιμα άρθρα, μεθοδολογίες, τεκμηρίωση, εργαλεία και τεχνολογίες στον τομέα της ασφάλειας εφαρμογών ιστού.

Οι αξιολογήσεις ευπάθειας τείνουν να περιλαμβάνουν τα ακόλουθα στάδια:

1. Προσδιορισμός όλων των πόρων, και των συνδεδεμένων πόρων, των συστημάτων πληροφορικής στο εσωτερικό ενός οργανισμού

2. Αντιστοίχιση κάποιας τιμής ή προτεραιότητας σε κάθε έναν από αυτούς
3. Διεξαγωγή αξιολόγησης μίας λίστας γνωστών τρωτών σημείων κατά μήκος ενός μεγάλου αριθμού επιφανειών επίθεσης (από login screens έως παραμέτρους διευθύνσεων URL και μέχρι διακομιστές ηλεκτρονικής αλληλογραφίας)
4. Καθορισμός των πιο κρίσιμων τρωτών σημείων και λήψη αποφάσεων σχετικά με τον τρόπο αντιμετώπισης των υπολοίπων

- **Δοκιμή διείσδυσης**

Η δοκιμή διείσδυσης (penetration test) περιλαμβάνει την αναπαραγωγή ενός συγκεκριμένου τύπου επίθεσης που μπορεί να εκτελεστεί από κάποιον χάκερ. Κάποιος που πραγματοποιεί δοκιμές διείσδυσης θα εξερευνήσει διεξοδικά τα συστήματα μέχρι να εντοπίσει κάποια ευπάθεια. Ενδεχομένως να χρησιμοποιήσει ακόμα και κάποιο εργαλείο αξιολόγησης ευπάθειας για να αποκαλυφθεί μία ευπάθεια. Μόλις εντοπιστεί κάτι τότε θα γίνει προσπάθεια εκμετάλλευσης για να καθοριστεί αν είναι δυνατό για έναν χάκερ να επιτύχει ένα συγκεκριμένο στόχο (πρόσβαση, αλλαγή ή διαγραφή δεδομένων).

Συχνά, ενώ πραγματοποιείται η δοκιμή διείσδυσης, μπορεί να συναντήσει ο ειδικός που τρέχει την δοκιμή τυχαία άλλες αδυναμίες και να τις ακολουθήσει εκεί που οδηγούν. Όποιος κάνει, επίσης, τη δοκιμή μπορεί να χρησιμοποιήσει κάποιο αυτοματοποιημένο εργαλείο σε αυτό το σημείο για να εκτελέσει μια σειρά από exploits ενάντια στην ευπάθεια.

Ορισμένες δοκιμές διείσδυσης αναφέρονται ως «white box» για να υποδείξουν ότι ο δοκιμαστής διείσδυσης έχει δώσει λεπτομερείς πληροφορίες για το περιβάλλον, όπως έναν κατάλογο περιουσιακών στοιχείων που ανήκουν στον οργανισμό, πηγαίο κώδικα, ονόματα υπαλλήλων και διευθύνσεις ηλεκτρονικού ταχυδρομείου κτλ. Όταν οι δοκιμές αναφέρονται ως «black box», με αυτό τον τρόπο υποδεικνύεται ότι οι δοκιμές διείσδυσης διεξήχθησαν ή διεξάγονται χωρίς προηγούμενη πληροφόρηση σχετικά με την εσωτερική δομή του οργανισμού, χωρίς πρόσβαση σε πηγαίο κώδικα κλπ. Αυτό το είδος δοκιμής διείσδυσης μπορεί να μοιάζει περισσότερο με τις δραστηριότητες ενός κακόβουλου χάκερ, όμως μπορεί επίσης να οδηγήσει σε μικρότερη κάλυψη των δυνητικά ευάλωτων περιουσιακών στοιχείων κάποιας επιχείρησης ή οργανισμού.

[1] Διαθέσιμη στο: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

Τόσο οι αξιολογήσεις ευπάθειας όσο και οι δοκιμές διείσδυσης πρέπει να πραγματοποιούνται ενάντια σε συσκευές δικτύου και ενάντια σε εσωτερικούς και εξωτερικούς διακομιστές. Είναι σημαντικό να καθοριστεί αν μια επίθεση μπορεί να γίνει από το εξωτερικό (για παράδειγμα, από έναν κακόβουλο εισβολέα που στοχεύει σε διαθέσιμες στο κοινό επιφάνειες στόχων στο διαδίκτυο) ή από το εσωτερικό (για παράδειγμα, από έναν δυσαρεστημένο υπάλληλο ή παλιό συνεργάτη, κάποιον χρήστη με δικαιώματα που δεν θα έπρεπε να έχει ή από κάποιον υπολογιστή που έχει μολυνθεί στο εσωτερικό δίκτυο).

Οι αξιολογήσεις ευπάθειας βοηθούν τις επιχειρήσεις να είναι συνεπείς με τη συμμόρφωση τους σε πρότυπα, ενώ οι δοκιμές διείσδυσης βοηθούν όλους τους οργανισμούς να μένουν μπροστά από τους χάκερ.

Το κόστος των αξιολογήσεων ευπάθειας και των δοκιμών διείσδυσης εξαρτάται στην ουσία από το μέγεθος της επιχείρησης. Για τις μικρές εταιρείες, η τιμή θα είναι σημαντικά χαμηλότερη από ό,τι είναι για μια μεγάλη εταιρεία με χιλιάδες δυνητικά ευάλωτες συσκευές και υπολογιστές, IPs και παρόχους Internet.

Ανεξάρτητα από το κόστος, οι εκτιμήσεις ευπαθειών συνεισφέρουν στην καλύτερη απόδοση της επένδυσής. Ενώ μια δοκιμή διείσδυσης μπορεί να προσφέρει μία αρκετά καλή και βαθιά εικόνα για το πόσο ασφαλή είναι τα συστήματά μιας εταιρείας, στην πραγματικότητα αποκαλύπτει μόνο ένα πράγμα και προς μία κατεύθυνση. Από την άλλη, με τις αξιολογήσεις ευπαθειών και επενδύοντας σε χρόνο και πόρους στην ανάπτυξη συστημάτων και διαδικασιών η εταιρεία θα έχει ένα σταθερό επίπεδο ασφάλειας πάνω στο οποίο θα αναπτυχθούν περαιτέρω τα συστήματά της και θα ενσωματωθούν νέα εξαρτήματα.

5.10. Διαχείριση δικαιωμάτων εγγράφων

Μία λύση διαχείρισης δικαιωμάτων εγγράφων (IRM / Information Rights Management) μπορεί να προστατεύσει τα έγγραφα και τα αρχεία μιας επιχείρησης ή ενός οργανισμού οπουδήποτε και αν βρίσκονται, ενώ παράλληλα επιτρέπει τον εύκολο και ασφαλή διαμοιρασμό τους.

Μία τέτοια λύση προσφέρει τον πλήρη έλεγχο των δικαιωμάτων των εγγράφων σε πραγματικό χρόνο, ακόμα και μετά τον διαμοιρασμό τους εντός ή εκτός της επιχείρησης ή του οργανισμού. Τα έγγραφά προστατεύονται όπου και αν βρίσκονται αφού επιτρέπεται η αλλαγή των δικαιωμάτων ενός εγγράφου ακόμα και αν αυτό έχει αποσταλεί ή προωθηθεί σε κάποιον μέσω ηλεκτρονικής αλληλογραφίας ή έχει εγγραφεί σε κάποιο ηλεκτρονικό μέσο αποθήκευσης. Επιπλέον, δίνεται η δυνατότητα να οριστούν περιορισμοί σε όσα μπορούν να γίνουν με τα έγγραφα και να παρακολουθείται ποιος και πότε βλέπει τις πληροφορίες και τα δεδομένα με αναφορές και στατιστικά.

Η λύση Διαχείρισης Δικαιωμάτων Εγγράφων είναι ιδανική για ομάδες και εταιρείες που απαιτούν ευέλικτη, απλή και ασφαλή ανταλλαγή εγγράφων για την επιχείρηση τους. Κάθε εταιρεία που απαιτεί ιδιωτική ανταλλαγή εγγράφων, μπορεί να επωφεληθεί, κυρίως στον νομικό κλάδο, στον κλάδο του βιομηχανικού σχεδιασμού και των ευρεσιτεχνιών, στον κλάδο της βιοτεχνολογίας και της έρευνας και στον χρηματοπιστωτικό κλάδο μεταξύ άλλων.

5.11. Διαχείριση πληροφοριών και συμβάντων ασφάλειας

Ένα σύστημα διαχείρισης πληροφοριών και συμβάντων ασφάλειας (SIEM - Security Information and Event Management) επιτρέπει το συσχετισμό των γεγονότων και την δημιουργία αναφορών σχετικά με τις κρίσιμες λειτουργίες των συστημάτων. Αυτό επιτρέπει στις επιχειρήσεις να συγκεντρώνουν δεδομένα κατανοώντας τί ακριβώς βρίσκεται πίσω από τις πολλαπλές καταγραφές που δημιουργούνται καθημερινά από όλα τα συστήματα υποδομών και τις επιχειρησιακές εφαρμογές.

Ένα τέτοιο σύστημα μπορεί να παρέχει μια πλούσια πλατφόρμα ανάλυσης με προκαθορισμένες αναφορές σε πραγματικό χρόνο για τις υποδομές και τις κρίσιμες επιχειρησιακές εφαρμογές, επιτρέποντας την αποτελεσματική διαχείριση και συνεχή αξιολόγηση της ασφάλειας των επιχειρήσεων αλλά και της συμμόρφωσής τους σε πρότυπα ποιότητας. Επίσης, ένα σύστημα SIEM μπορεί να διασυνδεθεί με συστήματα ERP, βάσεις δεδομένων και συστήματα ανθρωπίνων πόρων. Συνεπώς, ξεκινά από τη συλλογή δεδομένων από το δίκτυο και τις συσκευές ασφάλειας, τους διακομιστές και τις εφαρμογές, γεφυρώνοντας έτσι το χάσμα μεταξύ των εφαρμογών, των επιχειρήσεων και των υποδομών, αφού είναι εφικτό να ανιχνεύσει μέχρι την πιο πολύπλοκη απειλή.

Ενώ η ασφάλεια των πληροφοριών είναι μία πολύπλοκη διαδικασία, η λήψη και ανάλυση των στοιχείων αυτών πρέπει να είναι απρόσκοπτη και απλή. Για να εξασφαλιστεί αυτό, ένα σύστημα SIEM δημιουργεί λεπτομερή αλλά περιεκτικά στατιστικά στοιχεία και ειδοποιήσεις. Το σύστημα παράγει συνεχείς αναφορές για συγκεκριμένο χρονικό διάστημα ή σε πραγματικό χρόνο μέσω ειδικών πινάκων κατάστασης (dashboard) παρέχοντας σαφή επισκόπηση όλων των πληροφοριών ασφάλειας. Αυτό εξασφαλίζει ότι μία κακόβουλη δραστηριότητα μπορεί να ανακαλυφθεί αλλά και να αντιμετωπιστεί άμεσα πριν ζημιωθεί στην πραγματικότητα η επιχείρηση.

5.12. Άμυνα πρώτης γραμμής

Οι σημερινές επιχειρήσεις εξαρτώνται πραγματικά από την online παρουσία τους στο Διαδίκτυο, είτε αν αυτή βασίζεται στη δημιουργία εσόδων, στη διασφάλιση της υψηλής αποδοτικότητας των υπαλλήλων τους, ή για να προσφέρουν υπηρεσίες υψηλού επιπέδου. Η πανταχού πρόσβαση στο Διαδίκτυο καθιστά μία online επιχείρηση ευπαθή σε κυβερνοεπιθέσεις όπως είναι οι επιθέσεις DDoS από οπουδήποτε στον κόσμο. Τυχόν διακοπές στη λειτουργία των υπηρεσιών τους (downtimes) ενδέχεται να οδηγήσουν τα συστήματά τους για μεγάλα χρονικά διαστήματα εκτός λειτουργίας, κάτι εξαιρετικά δαπανηρό, απώλεια παραγωγικότητας και συμβάλουν στην δυσφήμιση του ονόματος της εταιρείας επηρεάζοντας αρνητικά τους νόμιμους χρήστες.

Δυστυχώς, οι παραδοσιακές λύσεις ασφάλειας όπως είναι τα firewall και οι συσκευές IPS δεν είναι αποτελεσματικές λύσεις ενάντια σε εξελιγμένες κυβερνοαπειλές και πολλές φορές αποτελούν οι ίδιες στόχο για επιθέσεις. Αυτό που απαιτούν οι σύγχρονες επιχειρήσεις είναι μία λύση Άμυνας Πρώτης Γραμμής (First Line of Defence), η οποία έχει κατασκευαστεί για να αποκρούει και να αντέχει στις μοντέρνες κυβερνοαπειλές, όπως είναι οι επιθέσεις DDoS για την διασφάλιση της αδιάλειπτης λειτουργίας της επιχείρησης και των διαδικτυακών υπηρεσιών και των εφαρμογών της.

5.13. Αντίγραφα ασφαλείας

Μία από τις βασικές πτυχές του κανονισμού GDPR είναι ότι απαιτεί οι εταιρείες να έχουν συγκεκριμένο πλάνο αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων. Αυτό επιβάλει τη χρήση συστημάτων αντιγράφων ασφαλείας σε πολλαπλά επίπεδα, που θα πρέπει να διασφαλίζει την ακεραιότητα των δεδομένων σε περίπτωση ανάγκης ανάκτησης ή αποκατάστασης δεδομένων σε περιπτώσεις οποιασδήποτε μορφής έλλειψης διαθεσιμότητας ή καταστροφής.

Ένα Σύστημα Αντιγράφων Ασφαλείας (Backup System) μπορεί να προσφέρει εξειδικευμένα αντίγραφα ασφαλείας για συστήματα όπως τα Microsoft Exchange Server, Groupwise, Lotus Domino Server, Zarafa, Dovecot IMAP, Cyrus IMAP, Courier IMAP, openLDAP, Microsoft SharePoint και άλλα.

5.14. Ψηφιακά πιστοποιητικά

Οι λύσεις ταυτότητας και ασφαλείας επιτρέπουν σε εταιρείες και μεγάλες επιχειρήσεις, σε cloud-based παρόχους υπηρεσιών και σε όσους καινοτομούν στον χώρο του Διαδικτύου των Πραγμάτων (Internet Of Things) σε όλο τον κόσμο να διεξάγουν ασφαλείς ηλεκτρονικές επικοινωνίες, να διαχειριστούν εκατομμύρια εξακριβωμένες ψηφιακές ταυτότητες, να αυτοματοποιήσουν τον έλεγχο ταυτότητας και την κρυπτογράφηση.

Τα πιστοποιητικά SSL προσφέρουν ισχυρή κρυπτογράφηση και χαρακτηριστικά που προσθέτουν επιπλέον αξία για να εξασφαλίσουν ότι η ιστοσελίδα της εταιρείας προστατεύεται και ικανοποιεί τις απαιτήσεις των σημερινών μοντέρνων ιστοσελίδων. Οι πελάτες και οι επισκέπτες της ιστοσελίδας γνωρίζουν ότι η περίοδος περιήγησης τους στον ιστότοπο είναι ασφαλής και πως όλες οι λεπτομέρειες που αφορούν σε στοιχεία πληρωμής και προσωπικά δεδομένα παραμένουν ασφαλείς και είναι κρυπτογραφημένες.

Εκτός από τα ψηφιακά πιστοποιητικά SSL, μία εταιρεία μπορεί να χρησιμοποιεί ψηφιακές ταυτότητες οι οποίες μπορούν να χρησιμοποιηθούν για λειτουργίες ασφαλούς επικοινωνίας, συμπεριλαμβανομένων ασφαλούς ηλεκτρονικού ταχυδρομείου (S/MIME),

ταυτοποίηση σε online υπηρεσίες, καθώς και ψηφιακές υπογραφές για το Microsoft Office και άλλων ηλεκτρονικών εγγράφων, για την προστασία της ακεραιότητας του εγγράφου αφού πιστοποιεί την «πατρότητα» του εγγράφου στους αποδέκτες.

Τέλος, τα Πιστοποιητικά Υπογραφής Κώδικα (Code Signing Certificates) χρησιμοποιούνται από προγραμματιστές σε όλες τις πλατφόρμες για να υπογράψουν ψηφιακά τις εφαρμογές και το λογισμικό που διανέμουν μέσω του Διαδικτύου. Η υπογραφή κώδικα αποδεικνύει ότι το υπογεγραμμένο λογισμικό είναι νόμιμο, προέρχεται από γνωστό προμηθευτή λογισμικού και ότι ο κώδικας δεν έχει αλλοιωθεί από την ώρα που δημοσιεύτηκε. Η υπογραφή κώδικα εμποδίζει τους χρήστες να εγκαταλείψουν την εγκατάσταση μιας εφαρμογής λόγω προειδοποιητικών μηνυμάτων ασφαλείας, εμποδίζει τις κακόβουλες αλλαγές στο νόμιμο κώδικα, καθώς και την κλοπή της ταυτότητας της εταιρείας που δημιούργησε και πουλάει νόμιμα την εφαρμογή.

5.15. Ασφάλεια βάσεων δεδομένων

Καθώς η παραγωγή ψηφιακών πληροφοριών αυξάνεται με ρυθμούς ρεκόρ, οι σχεσιακές βάσεις δεδομένων και τα big data θα γίνουν όλο και περισσότερο αναπόσπαστα από έναν οργανισμό. Αυτά τα αποθετήρια, τα οποία συχνά περιέχουν την ψυχή της επιχείρησης, πρέπει να προστατεύονται για να αποτραπεί οποιαδήποτε μη εγκεκριμένη ή ανάρμοστη πρόσβαση με στόχο τη διαρροή ή την αποκάλυψη ευαίσθητων δεδομένων.

Η ποσότητα των ψηφιακών πληροφοριών στον κόσμο αυξάνεται με υψηλούς ρυθμούς. Αυτή η αύξηση προωθείται από το ηλεκτρονικό ταχυδρομείο, τα πολυμέσα, τα μέσα κοινωνικής δικτύωσης και τις ηλεκτρονικές πληρωμές μέσω κινητού τηλεφώνου. Αυτό συμβαίνει όλο και περισσότερο καθώς οι θεμελιώδεις περιπτώσεις επιχειρηματικής χρήσης απαιτούν τη διατήρηση μεγάλου εύρους δομημένων και μη δομημένων δεδομένων.

Σε πολλές περιπτώσεις, αυτά τα δεδομένα που αποθηκεύονται σε παραδοσιακές σχεσιακές βάσεις δεδομένων ή σε πιο σύγχρονες πλατφόρμες big data είναι εμπιστευτικές και κρίσιμης σημασίας. Ως αποτέλεσμα, χρειάζονται ειδική προστασία (Database Security), ξεχωριστή από τις λύσεις ασφαλείας και τις προστασίες δικτύου ή εφαρμογών.

5.16. Έλεγχος πρόσβασης δικτύου

Μία λύση ελέγχου πρόσβασης δικτύου (NAC – Network Access Control) σχεδιάζεται για να προστατεύει οποιαδήποτε δικτυακή υποδομή, παρέχοντας πλήρη προστασία για όλα τα τερματικά, διαχειρίσιμα ή μη. Συνδυάζει τον agentless έλεγχο πρόσβασης δικτύου με τη πρόληψη απειλών zero-day, την αυτοματοποιημένη επιβολή πολιτικών και τη δικτυακή νοημοσύνη για να προσφέρει μία ενοποιημένη εικόνα της δραστηριότητας των τερματικών και παράλληλα μία ισχυρή ανάλυση της χρήσης και του ιστορικού του δικτύου. Όλες μαζί αυτές οι λειτουργίες παρέχουν ολοκληρωμένο έλεγχο τερματικών και προσφέρουν ελέγχους ασφαλείας καθ' όλη τη διάρκεια του κύκλου ζωής της δικτυακής πρόσβασης μιας συσκευής.

5.17. Πρόληψη απώλειας δεδομένων

Ένα σύστημα πρόληψης απώλειας δεδομένων (DLP – Data Loos Prevention) αναλύει όλες τις επικοινωνίες και τα συνημμένα αρχεία που διακινούνται στο διαδίκτυο, μεταξύ άλλων μέσω ηλεκτρονικού ταχυδρομείου, άμεσων μηνυμάτων (IM), μέσω κοινής χρήση αρχείων P2P, blogs, κοινωνικών μέσων δικτύωσης, FTP και Telnet κ.α. Μέσω του DLP υπάρχει συνεχής έλεγχος για παραβιάσεις στη διακυβέρνηση ενός οργανισμού, διασφαλίζοντας τη κανονιστική συμμόρφωση στις πολιτικές αποδεκτής χρήσης μίας επιχείρησης.

Επίσης, το DLP αποκλείει αυτόματα τις επισκέψεις που παραβιάζουν τις πολιτικές συμμόρφωσης σε μία επιχείρηση, μέσω των πρωτοκόλλων HTTP, HTTPS και FTP. Για τις επικοινωνίες ηλεκτρονικού ταχυδρομείου και τα συνημμένα αρχεία που εντοπίζονται ότι αποτελούν παραβίαση συμμόρφωσης, προσφέρεται η δυνατότητα αποκλεισμού, απομόνωσης ή αυτοεξυπηρέτησης με την παρέμβαση του χρήστη. Το DLP μπορεί να διερευνήσει τα δεδομένα μίας επιχείρησης για την εύρεση και προστασία ευαίσθητων πληροφοριών που διαμένουν σε αποθηκευτικά μέσα. Η ανακάλυψη ευαίσθητων δεδομένων επιτρέπει στις ομάδες ασφαλείας να επικεντρώσουν τις πρωτοβουλίες τους σε συγκεκριμένους χρήστες και συστήματα και στη συνέχεια να εφαρμόσουν τα κατάλληλα μέτρα για την εκπλήρωση των απαιτήσεων συμμόρφωσης.

5.18. Φυσική ασφάλεια

Η φυσική ασφάλεια έχει άμεση σχέση με την ασφάλεια του δικτύου και των πληροφοριακών συστημάτων ώστε να εξασφαλιστούν οι βασικές απαιτήσεις της ασφάλειας πληροφοριών, δηλαδή η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα.

Τα μέτρα που υποστηρίζουν τη φυσική ασφάλεια έχουν ως κύριο στόχο την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στους χώρους των πληροφοριακών συστημάτων και της καταστροφής των αγαθών του

Η Πολιτική Ασφάλειας περιλαμβάνει, συνεπώς, και την φυσική ασφάλεια και συγκεκριμένα πρέπει να δηλώνονται ζητήματα που αφορούν την εξουσιοδοτημένη πρόσβαση των χρηστών στους χώρους που είναι εγκατεστημένα τα πληροφοριακά συστήματα, την αντιμετώπιση φυσικών απειλών όπως είναι οι πυρκαγιές, οι πλημμύρες, οι σεισμοί κτλ., την συντήρηση των ηλεκτρικών εγκαταστάσεων και του εξοπλισμού της εταιρείας.

ΚΕΦΑΛΑΙΟ 6:

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΑΝΑΠΤΥΞΗΣ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΤΑ ISO/IEC 27001:2013

6.1. Εισαγωγή

Στο κεφάλαιο αυτό θα παρουσιαστεί μια μελέτη περίπτωσης ανάπτυξης ΣΔΑΠ σε μια επιχείρηση με βάση το Πρότυπο ISO/IEC 27001:2013. Το συγκεκριμένο πρότυπο ακολουθεί την μεθοδολογία PCDA (Plan – Do – Check – Act) την οποία περιγράψαμε στο Κεφάλαιο 3. Στα πλαίσια του ΣΔΑΠ θα παρουσιαστεί η διαδικασία Εκτίμησης Κινδύνων και θα οριστούν οι Πολιτικές Ασφάλειας Πληροφοριών.

Το Πρότυπο ISO/IEC 27001:2013 περιλαμβάνει μία σειρά από μέτρα ασφαλείας όπως περιγράφονται στο Παράρτημα Α' του Προτύπου. Είναι προφανές ότι μία επιχείρηση δεν είναι απαραίτητο να επιλέξει και να αναπτύξει όλα τα μέτρα ασφαλείας του ISO/IEC 27001:2013 για να διαχειριστεί τους κινδύνους της, αλλά επιλέγει εκείνα τα μέτρα ασφαλείας σύμφωνα με του στόχους που η ίδια έχει θέσει. Για το λόγο αυτό θα πρέπει να καταρτίζεται η Δήλωση Εφαρμοσιμότητας (Statement of Applicability) όπου θα σημειώνεται ποια μέτρα εφαρμόζει η εταιρεία και ποια όχι.

Στο case study θα αναπτύξουμε την μελέτη ασφαλείας κατά ISO/IEC 27001:2013 σε μία επιχείρηση η οποία δραστηριοποιείται στο κλάδο των επιχειρηματικών συμβουλευτικών υπηρεσιών.

6.2 Στόχοι και πεδίο εφαρμογής του ΣΔΑΠ

Η Ασφάλεια Πληροφοριών αποτελεί πρωταρχική προτεραιότητα της εταιρείας προκειμένου:

- Να διασφαλίσει την ασφαλή τήρηση, την επεξεργασία και τη μετάδοση των πληροφοριών
- Να εξασφαλίσει την πλήρη συμμόρφωση της εταιρείας με τις σχετικές κείμενες νομικές και κανονιστικές απαιτήσεις
- Να προστατεύσει τα συμφέροντα της εταιρείας και όσων συναλλάσσονται με αυτή και την εμπιστεύονται για τη χρήση και διακίνηση των εμπιστευτικών δεδομένων τους
- Να διασφαλίσει τη διαθεσιμότητα, την ακεραιότητα και της εμπιστευτικότητα των πληροφοριών, που παράγονται, λαμβάνονται και διακινούνται στο πλαίσιο έργων ασφαλείας
- Να μεγιστοποιήσει την αξιοπιστία των πληροφοριακών πόρων της εταιρείας.

Η εφαρμογή του ΣΔΑΠ στοχεύει στα ακόλουθα:

- Προστασία των υπολογιστικών πόρων και της διακινούμενης πληροφορίας στις υπηρεσίες της εταιρείας από κάθε απειλή, εσωτερική ή εξωτερική, σκόπιμη ή τυχαία
- Συστηματική αποτίμηση και αξιολόγηση των κινδύνων που αφορούν στη διασφάλιση πληροφοριών, προσβλέποντας στην ορθή και έγκαιρη διαχείρισή τους
- Αρχειοθέτηση δεδομένων, αποφυγή ιών και εξωτερικών εισβολών, έλεγχο πρόσβασης στα συστήματα, καταγραφή όλων των περιστατικών ασφαλείας και διαχείριση απρόσμενων εξελίξεων
- Διαρκή ενημέρωση της διοίκησης και του προσωπικού σε θέματα ασφάλειας πληροφοριών και την διεξαγωγή εκπαιδευτικών σεμιναρίων για το προσωπικό,
- Πλήρη δέσμευση της διοίκησης της εταιρείας στην πιστή εφαρμογή και στη συνεχή βελτίωση του ΣΔΑΠ, το οποίο συμμορφώνεται με τις απαιτήσεις του προτύπου ISO/IEC 27001:2013.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών (ΥΑΠ) έχει την ευθύνη για τον έλεγχο και την παρακολούθηση της λειτουργίας του ΣΔΑΠ, καθώς και για την ενημέρωση όλου του εμπλεκόμενου προσωπικού για την Πολιτική Ασφάλειας Πληροφοριών.

6.3. Εκτίμηση κινδύνων ασφάλειας πληροφοριών

Η παρούσα διαδικασία περιγράφει τις ενέργειες του Υπευθύνου Ασφάλειας Πληροφοριών για τη συστηματική αναγνώριση των πόρων της εταιρείας, την αναγνώριση των κινδύνων που απειλούν τη διαθεσιμότητα, ακεραιότητα, και εμπιστευτικότητα αυτών καθώς και των ευπαθειών αυτών. Παρουσιάζει μια συστηματική μεθοδολογία ποσοτικοποίησης των κινδύνων.

Η διαδικασία αφορά όλους τους πόρους που εμπίπτουν στο πεδίο εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών της εταιρείας.

6.3.1. Σύνταξη καταλόγου πληροφοριακών πόρων

Ο ΥΑΠ καταρτίζει κατάλογο όλων των πληροφοριακών πόρων της εταιρείας εντός του πεδίου εφαρμογής του ΣΔΑΠ και τον ενημερώνει ανάλογα με τις μεταβολές των πόρων. Ο κατάλογος περιέχει τα ακόλουθα είδη πόρων:

- Μηχανογραφικός εξοπλισμός:
    - Εξυπηρετητές – servers
    - Σταθμοί εργασίας – workstations – laptop
    - Εκτυπωτές, φαξ, φωτοτυπικά μηχανήματα
    - Δικτυακός εξοπλισμός – switches, routers, firewalls
    - Εξοπλισμός αποθήκευσης – SAN, NAS, RAID
    - Φορητά μέσα αποθήκευσης – εξωτερικοί σκληροί δίσκοι, CD/DVD-R
- Εφαρμογές λογισμικού
    - Συστήματα Διαχείρισης Βάσεων Δεδομένων
    - Εργαλεία ανάπτυξης
    - Λειτουργικά συστήματα
    - Άλλες εφαρμογές ιδιαίτερης κρισιμότητας
- Πληροφοριακά δεδομένα
    - Βάσεις δεδομένων
    - Άλλα ψηφιακά δεδομένα
    - Δεδομένα σε έντυπη μορφή

- Δεδομένα σε άλλη μορφή (σε οπτικά ή μαγνητικά μέσα)

- Βοηθητικά δίκτυα:
  - Δίκτυο Παροχής Ηλεκτρικού Ρεύματος
  - τηλεπικοινωνίες
  - κλιματισμός
- Ανθρώπινοι πόροι: εργαζόμενοι των οποίων η απώλεια είναι σημαντική λόγω εξειδίκευσης, ειδικών προσόντων και εμπειρίας.

Η πλήρης λίστα των πόρων αποτελεί ελεγχόμενο αρχείο και περιέχει επαρκή αναγνωριστικά στοιχεία για κάθε πόρο, καθώς και τον «ιδιοκτήτη» αυτού, δηλαδή τον εργαζόμενο ή την ομάδα εργαζομένων που είναι αρμόδιοι για την καλή λειτουργία καθώς και τη χρήση του.

6.3.2. Αναγνώριση κινδύνων – ευπαθειών

Ο ΥΑΠ καταρτίζει καταλόγους των κινδύνων που απειλούν τους ανωτέρω πόρους καθώς και των ευπαθειών αυτών. Ενημερώνει τους καταλόγους όποτε υπάρχει αλλαγή στον εξοπλισμό, τους χώρους ή τις δραστηριότητες της εταιρείας.

Για την αναγνώριση των κινδύνων και των ευπαθειών εξετάζονται:

- Οι χρησιμοποιούμενες πληροφοριακές διατάξεις
- Τα χρησιμοποιούμενα μέσα εργασίας
- Η οργάνωση εργασίας
- Η χωροταξική διάταξη των μηχανημάτων και των θέσεων εργασίας

Εντοπίζονται, επίσης, οι κανονικές αλλά και οι έκτακτες καταστάσεις στις οποίες μπορεί να βρεθεί το σύστημα εργασίας και η μορφή που μπορεί να λάβουν τα στοιχεία που το αποτελούν (π.χ. προβλέψιμες βλάβες του τεχνολογικού συστήματος, εργασία υπό χρονική πίεση, κλπ.)

Οι κίνδυνοι εντάσσονται γενικά στις εξής ομάδες:

- Σκόπιμες κακόβουλες ενέργειες ανθρώπων
- Φυσικά φαινόμενα
- Λανθασμένες ενέργειες ανθρώπων – χωρίς δόλο

- Αστοχία υλικού/λογισμικού/διαδικασιών

Οι ευπάθειες ομαδοποιούνται στις εξής κατηγορίες:

- Περιβάλλον
- Υλικό
- Λογισμικό
- Επικοινωνίες
- Αρχεία
- Προσωπικό
- Διαδικασίες

Η πλήρης λίστα των κινδύνων και των ευπαθειών που εντοπίζεται καταγράφονται στα ελεγχόμενα αρχεία Κινδύνων και Ευπαθειών αντίστοιχα.

6.3.3. Κατάλογος κινδύνων ασφάλειας πληροφοριών

Στον παρακάτω πίνακα παρουσιάζονται οι πιθανοί κίνδυνοι που απειλούν τα πληροφοριακά συστημάτα και τον εξοπλισμό της εταιρείας.

Πίνακας 2: Πιθανοί κίνδυνοι πληροφοριακών συστημάτων

ΚΙΝΔΥΝΟΣ	ΠΕΡΙΓΡΑΦΗ ΚΙΝΔΥΝΟΥ
Αστοχία κλιματισμού	Σε περίπτωση διακοπής λειτουργίας των κλιματιστικών μπορεί να προκληθεί υπερθέρμανση του εξοπλισμού
Βομβιστική επίθεση	Έκρηξη βόμβας θα προκαλέσει καταστροφή του εξοπλισμού
Τηλεπικοινωνιακές υποκλοπές	Σύνδεση μηχανισμών υποκλοπής θα οδηγήσει σε διαρροή δεδομένων
Φθορά αγωγών	Γήρανση των αγωγών ρεύματος ή δεδομένων μπορεί να προκαλέσει βραχυκύκλωμα, διακοπή ή απώλεια πληροφορίας.
Γήρανση μέσων αποθήκευσης	Μπορεί να προκαλέσει απώλεια δεδομένων και αδυναμία ανάκτησης δεδομένων

ΚΙΝΔΥΝΟΣ	ΠΕΡΙΓΡΑΦΗ ΚΙΝΔΥΝΟΥ
Σκόνη	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού και δυσλειτουργία των συστημάτων
Σεισμός	Μπορεί να προκληθεί καταστροφή εξοπλισμού
Παράνομη ακρόαση	Μπορεί να οδηγήσει σε διαρροή δεδομένων
Ηλεκτρομαγνητική ακτινοβολία	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού και δυσλειτουργία των συστημάτων
Ηλεκτροστατικά φορτία	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού και δυσλειτουργία των συστημάτων
Ακραία θερμοκρασία/υγρασία	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού και δυσλειτουργία των συστημάτων
Αστοχία τηλεπικοινωνιών	Μπορεί να προκαλέσει σφάλμα μετάδοσης πληροφοριών, απώλεια και δυσλειτουργία των συστημάτων
Διακοπή ρεύματος	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού και δυσλειτουργία των συστημάτων
Διακοπή νερού	Μπορεί να οδηγήσει σε αδυναμία λειτουργία των συστημάτων πυρόσβεσης
Πυρκαγιά	Μπορεί να προκληθεί καταστροφή εξοπλισμού
Πλημμύρα	Μπορεί να προκληθεί καταστροφή εξοπλισμού
Αστοχία υλικού	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού και δυσλειτουργία των συστημάτων
Τυφώνας	Μπορεί να προκληθεί καταστροφή εξοπλισμού
Παράνομη εισαγωγή/εξαγωγή λογισμικού	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Παράνομη χρήση λογισμικού	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Απεργία	Μπορεί να οδηγήσει σε μη επίβλεψη των χώρων και των συστημάτων καθώς και δυσλειτουργία των συστημάτων

ΚΙΝΔΥΝΟΣ	ΠΕΡΙΓΡΑΦΗ ΚΙΝΔΥΝΟΥ
Κεραυνός	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού και δυσλειτουργία των συστημάτων
Σφάλμα συντήρησης	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού και δυσλειτουργία των συστημάτων
Κακόβουλο λογισμικό	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Παραποίηση ταυτότητας	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Ανακατεύθυνση μηνυμάτων	Μπορεί να προκαλέσει διαρροή δεδομένων
Μη εξουσιοδοτημένη πρόσβαση στο δίκτυο	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Λάθος χειρισμού	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Διακύμανση τάσης	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού και δυσλειτουργία των συστημάτων
Αστοχία λογισμικού	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Έλλειψη προσωπικού	Μπορεί να οδηγήσει σε μη επίβλεψη των χώρων και των συστημάτων
Κλοπή	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων και εξοπλισμού
Ανάλυση κίνησης δικτύου	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Υπερφόρτωση δικτύου	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Σφάλμα μετάδοσης	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Μη εξουσιοδοτημένη χρήση αποθηκευτικών μέσων	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων

ΚΙΝΔΥΝΟΣ	ΠΕΡΙΓΡΑΦΗ ΚΙΝΔΥΝΟΥ
Χρήση όπλων	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού
Μη εξουσιοδοτημένη χρήση λογισμικού	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Χρήση λογισμικού από μη εξουσιοδοτημένους χρήστες	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Σφάλμα χρήσης	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Ηθελημένη φθορά	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων και εξοπλισμού
Χάκερ δικτύου	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων καθώς και δυσλειτουργία των συστημάτων
Εγκληματίες δικτύου	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων καθώς και δυσλειτουργία των συστημάτων
Τρομοκρατική επίθεση	Μπορεί να προκαλέσει καταστροφή του εξοπλισμού
Βιομηχανική κατασκοπία	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων
Κακόβουλοι εργαζόμενοι	Μπορεί να προκαλέσει καταστροφή η διαρροή δεδομένων και εξοπλισμού

6.3.4. Κατάλογος ευπαθειών ασφάλειας πληροφοριών

Στον παρακάτω πίνακα παρουσιάζονται οι πιθανές ευπάθειες των πληροφοριακών συστημάτων και του εξοπλισμού της εταιρείας.

Πίνακας 3: Πιθανές ευπάθειες πληροφοριακών συστημάτων

ΚΑΤΗΓΟΡΙΑ	ΕΥΠΑΘΕΙΑ
Περιβάλλον	Πυρκαγιά
Περιβάλλον	Έλλειψη φυσική προστασίας του χώρου (πόρτες, παράθυρα)
Περιβάλλον	Ανεπαρκής έλεγχος φυσικής πρόσβασης στο χώρο
Περιβάλλον	Αστάθεια ηλεκτρικού ρεύματος
Περιβάλλον	Έλλειψη προστασίας από πλημμύρα
Υλικό	Μη περιοδική αντικατάσταση
Υλικό	Ευπάθεια σε διακυμάνσεις τάσης
Υλικό	Ευπάθεια σε διακυμάνσεις θερμοκρασίας
Υλικό	Ευπάθεια στην υγρασία, τη σκόνη, τη βρωμιά
Υλικό	Ευπάθεια στην ηλεκτρομαγνητική ακτινοβολία
Υλικό	Ελλιπής/λανθασμένη συντήρηση
Υλικό	Ελλιπής έλεγχος αλλαγών ρυθμίσεων
Λογισμικό	Ασαφείς ή ελλιπείς προδιαγραφές για τους προγραμματιστές
Λογισμικό	Ελλιπής έλεγχος του λογισμικού
Λογισμικό	Δύσχρηστο περιβάλλον χρήσης
Λογισμικό	Έλλειψη μηχανισμών ταυτοποίησης χρήστη
Λογισμικό	Έλλειψη αρχείου ενεργειών

ΚΑΤΗΓΟΡΙΑ	ΕΥΠΑΘΕΙΑ
Λογισμικό	Γνωστά σφάλματα του λογισμικού
Λογισμικό	Μη κρυπτογραφημένα συνθηματικά
Λογισμικό	Κακή διαχείριση συνθηματικών
Λογισμικό	Κακή ανάθεση δικαιωμάτων χρήσης
Λογισμικό	Ανεξέλεγκτη εγκατάσταση και χρήση λογισμικού
Λογισμικό	Μη κλείδωμα του υπολογιστή κατά την απομάκρυνση του χρήστη
Λογισμικό	Έλλειψη αρχείου και ελέγχου αλλαγών
Λογισμικό	Έλλειψη τεκμηρίωσης
Λογισμικό	Έλλειψη αρχείων ασφαλείας
Λογισμικό	Απόρριψη ή επανάχρηση μέσων αποθήκευσης χωρίς πλήρη διαγραφή
Λογισμικό	Ενεργοποίηση μη απαραίτητων υπηρεσιών
Λογισμικό	Χρήση μη ώριμου λογισμικού
Λογισμικό	Χρήση λογισμικού με μεγάλη διανομή
Επικοινωνίες	Γραμμές επικοινωνίας χωρίς προστασία
Επικοινωνίες	Κακή σύνδεση γραμμών επικοινωνίας
Επικοινωνίες	Έλλειψη ταυτοποίησης αποστολέα/δέκτη
Επικοινωνίες	Μεταφορά συνθηματικών χωρίς κρυπτογράφηση
Επικοινωνίες	Έλλειψη επιβεβαίωσης αποστολής/λήψης
Επικοινωνίες	Γραμμές dial-up πρόσβασης
Επικοινωνίες	Μεταφορά ευαίσθητης πληροφορίας χωρίς κρυπτογράφηση
Επικοινωνίες	Ελλιπής διαχείριση δικτύου
Επικοινωνίες	Μη προστατευμένη σύνδεση με το εξωτερικό δίκτυο

ΚΑΤΗΓΟΡΙΑ	ΕΥΠΑΘΕΙΑ
Επικοινωνίες	Ανασφαλής αρχιτεκτονική δικτύου
Αρχεία	Μη προστατευμένη αποθήκευση
Αρχεία	Απόρριψη χωρίς προσοχή
Αρχεία	Ανεξέλεγκτη αντιγραφή
Προσωπικό	Απουσία προσωπικού
Προσωπικό	Μη εποπτευόμενη εργασία από εξωτερικό προσωπικό
Προσωπικό	Ανεπαρκής εκπαίδευση σε θέματα ασφαλείας
Προσωπικό	Ελλιπής επίγνωση κινδύνων ασφαλείας
Προσωπικό	Λανθασμένη χρήση λογισμικού και υλικού
Προσωπικό	Έλλειψη μηχανισμών παρακολούθησης
Προσωπικό	Έλλειψη πολιτικής χρήσης μέσων επικοινωνίας
Προσωπικό	Ανεπαρκείς διαδικασίες πρόσληψης
Διαδικασίες	Έλλειψη τυπικής διαδικασίας έγκρισης υλικού προς δημοσίευση
Διαδικασίες	Έλλειψη τυπικής διαδικασίας ελέγχου δικαιωμάτων χρήσης
Διαδικασίες	Έλλειψη πολιτικής χρήσης φορητών υπολογιστών
Διαδικασίες	Έλλειψη τυπικής διαδικασίας ενεργοποίησης/απενεργοποίησης κωδικών χρηστών
Διαδικασίες	Ελλιπής έλεγχος υλικού που εξέρχεται των εγκαταστάσεων
Διαδικασίες	Έλλειψη συμβάσεων συντήρησης SLA
Διαδικασίες	Μη εφαρμογή της αρχής "Κενό Γραφείο" & "Κενή Οθόνη"
Διαδικασίες	Έλλειψη όρων ασφαλείας στις συμβάσεις με πελάτες και προμηθευτές
Διαδικασίες	Έλλειψη όρων ασφαλείας στις συμβάσεις προσωπικού
Διαδικασίες	Έλλειψη σχεδίου εφεδρείας

ΚΑΤΗΓΟΡΙΑ	ΕΥΠΑΘΕΙΑ
Διαδικασίες	Έλλειψη/Κακή ανάθεση ευθυνών ασφάλειας πληροφορίας
Διαδικασίες	Έλλειψη πολιτική χρήσης e-mail
Διαδικασίες	Έλλειψη διαδικασιών αναγνώρισης και εκτίμησης κινδύνων
Διαδικασίες	Έλλειψη διαδικασιών χειρισμού διαβαθμισμένης πληροφορίας
Διαδικασίες	Έλλειψη διαδικασίας ελέγχου πνευματικών δικαιωμάτων προμηθειών
Διαδικασίες	Έλλειψη διαδικασίας αναφοράς κινδύνων ασφαλείας
Διαδικασίες	Έλλειψη τυπικής διαδικασίας εγκατάστασης λογισμικού
Διαδικασίες	Έλλειψη διαδικασίας παρακολούθησης χώρων επεξεργασίας πληροφορίας
Διαδικασίες	Έλλειψη τακτικών ελέγχων και επιτόπιων επιθεωρήσεων
Διαδικασίες	Έλλειψη διοικητικών ελέγχων
Διαδικασίες	Έλλειψη μηχανισμών παρακολούθησης παραβάσεων ασφαλείας
Διαδικασίες	Έλλειψη απαιτήσεων ασφαλείας στις ευθύνες εργασίας του προσωπικού
Διαδικασίες	Έλλειψη αρχείων ενεργειών των διαχειριστών και χειριστών
Διαδικασίες	Έλλειψη καταγραφών προβλημάτων/λαθών στα αρχεία ενεργειών των διαχειριστών/χειριστών
Διαδικασίες	Έλλειψη καθορισμένης πειθαρχικής διαδικασίας για το χειρισμό περιστατικών ασφαλείας
Άλλα	Μοναδικό σημείο αστοχίας
Άλλα	Ανεπαρκής απόκριση συντήρησης/επισκευής

6.3.5. Εκτίμηση επικινδυνότητας

Για κάθε πόρο εντοπίζονται οι κίνδυνοι που διατρέχει:

- Κατά την κανονική ροή της εργασίας
- Όταν η ροή της εργασίας αποκλίνει από το κανονικό και όταν συμβούν έκτακτα αλλά πιθανά γεγονότα.

Η επικινδυνότητα καθορίζεται με βάση:

- Τη βαρύτητα των συνεπειών εμφάνισης του κινδύνου στην επιχειρησιακή συνέχεια της εταιρείας και στη διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα των πληροφοριών, όπως εκφράζεται από την αξία του πόρου
- Τη στατιστική πιθανότητα εμφάνισης του κινδύνου
- Το βαθμό ευπάθειας του πόρου απέναντι στον κίνδυνο

Για την ποσοτικοποίηση της αξίας των πόρων γίνεται αξιολόγηση με κλίμακα 5 επιπέδων, στην οποία το 0 παριστάνει την ελάχιστη αξία και το 4 τη μέγιστη. Η αξιολόγηση γίνεται από τον ΥΑΠ αλλά και μέσω συνέντευξης με τους εργαζομένους που εμπλέκονται άμεσα με τους αντίστοιχους πόρους.

Κατά την αξιολόγηση εξετάζεται η χειρότερη περίπτωση που θα μπορούσε να προκύψει λόγω διαρροής, τροποποίησης, καταστροφής ή μη διαθεσιμότητας των πόρων, τόσο των άυλων, δηλαδή της διακινούμενης πληροφορίας, όσο και των υλικών, δηλαδή του ίδιου του πληροφορικού εξοπλισμού καθώς και του λοιπού τεχνικού εξοπλισμού που στηρίζει τη λειτουργία του πληροφοριακού συστήματος.

Η αντιστοίχιση με τις πραγματικές αξίες είναι η εξής:

Πίνακας 4: Ποσοτικοποίηση της αξίας των πόρων

Αξία	Υλική (χρηματική)	Άυλη (υποκειμενική)
0	< 1.000€	Αμελητέα
1	< 2.000€	Μικρή
2	< 10.000€	Μέτρια

3	< 100.000€	Μεγάλη
4	> 100.000€	Ανυπολόγιστη

Για κάθε πόρο επιλέγεται η μεγαλύτερη αξία μεταξύ της υλικής και της άυλης, δηλαδή:

- Αν ένας πόρος έχει χαμηλή χρηματική αξία αλλά περιέχει πληροφορίες μεγάλης άυλης αξίας, επιλέγεται η άυλη αξία
- Αν ένας πόρος περιέχει πληροφορίες χαμηλής άυλης αξίας (ή δεν περιέχει πληροφορίες) αλλά η υλική του αξία είναι μεγάλη και επομένως η απώλειά του επηρεάζει αρνητικά την επιχειρησιακή συνέχεια της εταιρείας (π.χ. συγκρινόμενη με το τζίρο αυτής) επιλέγεται η υλική αξία.

Το μέγεθος κάθε απειλής, δηλαδή η στατιστική πιθανότητα εμφάνισής της κωδικοποιείται σύμφωνα με τον παρακάτω πίνακα:

Πίνακας 5: Κωδικοποίηση μεγέθους απειλής

Μέγεθος απειλής	**Πιθανότητα εμφάνισης**	**Συχνότητα εμφάνισης**
0	Χαμηλή	Πρακτικά μικρή, 1 φορά στα 10 έτη
1	Μέση	Σημαντική, 1 φορά στα 5 έτη
2	Υψηλή	Μεγάλη, 1 φορά το έτος ή λιγότερο

Ο βαθμός ευπάθειας, δηλαδή ο βαθμός που ο πόρος επηρεάζεται από την ευπάθεια κωδικοποιείται σύμφωνα με τον παρακάτω πίνακα:

Πίνακας 6: Κωδικοποίηση βαθμού ευπάθειας πόρου

Βαθμός ευπάθειας	Ευαισθησία στοιχείου	Επιπτώσεις ευπάθειας
0	Χαμηλή	Ελάχιστες, μικρή επίπτωση στη λειτουργία
1	Μέση	Σημαντικές, μερική απώλεια διαθεσιμότητας
2	Υψηλή	Μεγάλες, πλήρης απώλεια διαθεσιμότητας

Μετά τον χαρακτηρισμό όλων των κινδύνων για κάθε στοιχείο σύμφωνα με την κωδικοποίηση που αναφέρθηκε στις παραπάνω παραγράφους, ακολουθεί ο υπολογισμός του μεγέθους του κινδύνου, εκφρασμένου σε κλίμακα από 0 έως 10. Το μέγεθος κάθε κινδύνου αποτελεί ποσοτικοποίηση της ανάγκης αντιμετώπισης του. Για τον υπολογισμό χρησιμοποιείται ο ακόλουθος πίνακας:

Πίνακας 7: Υπολογισμός μεγέθους κινδύνου

Αύξηση αξίας

		Απειλή			*Χαμηλή*			*Μέση*			*Υψηλή*		
	Ευπάθεια	***X***	***M***	***Y***	***X***	***M***	***Y***	***X***	***M***	***Y***			
Αξία	0	0	1	2	2	3	4	4	5	6			
	1	1	2	3	3	4	5	5	6	7			
	2	2	3	4	4	5	6	6	7	8			
	3	3	4	5	5	6	7	7	8	9			
	4	4	5	5	6	6	7	8	9	10			

Ανάλογα με το μέγεθος του κινδύνου διακρίνουμε τις εξής περιπτώσεις:

- Μέγεθος 8, 9, 10: Απαιτείται άμεση αντιμετώπιση
- Μέγεθος 6, 7: Προτείνεται η αντιμετώπιση σε εύλογο χρονικό διάστημα
- Μέγεθος 4, 5: Προτείνεται η λήψη μέτρων, ωστόσο δεν είναι αναγκαία
- Μέγεθος 0-3: Δεν απαιτείται αντιμετώπιση

Η Εκτίμηση Κινδύνων Ασφάλειας Πληροφοριών συντάσσεται με ευθύνη του ΥΑΠ και περιλαμβάνει:

- Τους κινδύνους ανά πόρο Πληροφοριών
- Την εκτίμηση της επικινδυνότητας

6.4. Πολιτικές Ασφάλειας Πληροφοριών

6.4.1. Κατεύθυνση της διοίκησης για την ασφάλεια πληροφοριών

Η Πολιτική Ασφάλειας Πληροφοριών τηρείται σαν ιδιαίτερο έγγραφο του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Υπογράφεται από τη διοίκηση της εταιρείας και κοινοποιείται σε όλους τους εργαζομένους της εταιρείας μέσω εσωτερικής διανομής.

Το επίπεδο ασφάλειας πληροφοριών καθορίζεται από:

- ΝΟΜΟΣ 3471/2006 Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν. 2472/1997

- ΝΟΜΟΣ 2472/1997 Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα με ενσωματωμένες τις τροποποιήσεις

- ΝΟΜΟΣ 2251/1994 Προστασία των καταναλωτών, όπως ισχύει μετά τις τροποποιήσεις

- ΝΟΜΟΣ 2121/1993 περί προστασίας Πνευματικών Δικαιωμάτων

- Των στόχων που έχει θέσει η εταιρεία

- Των αποφάσεων του Συμβουλίου Ανασκόπησης.

- Των εξελίξεων στον τεχνολογικό τομέα και την υιοθέτησή τους από ανταγωνιστές που δραστηριοποιούνται στο τομέα.

- Τις απαιτήσεις από τα Διεθνή Στάνταρ Ασφάλειας Πληροφοριών

- Τις συμβατικές απαιτήσεις των πελατών

- Την ανατροφοδότηση που δέχεται η εταιρεία, σε θέματα ασφάλειας πληροφοριών, από τους εργαζόμενους, τους προμηθευτές και τους πελάτες της

- Το αντικείμενο εργασιών της εταιρείας που σχετίζεται με παροχή υπηρεσιών και προϊόντων Ασφάλειας Πληροφοριών

Η εταιρεία έχει ως σκοπό την συνεχή αύξηση του επιπέδου της Ασφάλειας Πληροφοριών μέσω της συνεχούς βελτίωσης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.

6.4.2. Οργάνωση της ασφάλειας πληροφορίας

6.4.2.1. Εσωτερική οργάνωση

Ο συντονισμός και η εφαρμογή του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) γίνεται από την Υπεύθυνο Ασφάλειας Πληροφοριών της εταιρείας.

Οι ευθύνες του προσωπικού της εταιρείας ως προς το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών ορίζονται μέσω:

- της αναλυτικής λίστας πόρων και των υπευθύνων για τον καθένα
- των δικαιωμάτων πρόσβασης και της αντίστοιχης λίστας
- των διαδικασιών που περιγράφονται στο παρόν έγγραφο
- των διαδικασιών που διανέμονται στο προσωπικό

Ο Υπεύθυνος Ασφάλειας Πληροφοριών διατηρεί κατάλογο με τους αρμόδιους φορείς και υπηρεσίες που ενδέχεται να απαιτηθούν για το χειρισμό Περιστατικού Ασφάλειας Πληροφοριών.

Ο κατάλογος επικοινωνίας περιέχει τουλάχιστον τους ακόλουθους:

- Πλησιέστερο Αστυνομικό Τμήμα
- Υπηρεσία Δίωξης Ηλεκτρονικού Εγκλήματος
- Τμήμα Πυροσβεστικής
- Αρχή Προστασίας Προσωπικών Δεδομένων
- Ιδιωτική εταιρεία φύλαξης

Επίσης, διατηρεί κατάλογο με βασικά πρόσωπα επικοινωνίας στους παρόχους υπηρεσιών που στηρίζουν τα πληροφοριακά συστήματα της εταιρείας, όπως:

- ΔΕΗ
- Πάροχοι τηλεφωνίας & Internet
- Τεχνικοί Ηλεκτρομηχανολογικών Εγκαταστάσεων & Συστημάτων Κλιματισμού

Επιπλέον, ο Υπεύθυνος Ασφάλειας Πληροφοριών σε τακτική βάση ενημερώνεται από τις ιστοσελίδες και τις κοινότητες συζήτησης του Internet για εξελίξεις σε θέματα ασφάλειας (vulnerabilities, exploits, service packs) ώστε να λάβει τα απαραίτητα μέτρα εκσυγχρονισμού των εγκαταστάσεων, όπως:

- http://www.exploit-db.com/
- http://www.securityfocus.com/
- https://isc.sans.edu/

Για την αποφυγή επικάλυψης καθηκόντων, όλες οι διαχειριστικές αρμοδιότητες των πληροφοριακών συστημάτων της εταιρείας ανατίθενται στο διαχειριστή των συστημάτων, ενώ η έγκριση, η παρακολούθηση και ο έλεγχος αυτών ανατίθενται στον Υπεύθυνο Ασφάλειας Πληροφοριών.

Κατά την ανάπτυξη-υλοποίηση νέων έργων (projects) συμμετέχει και ο Υπεύθυνος Ασφάλειας Πληροφοριών ο οποίος φροντίζει από τη φάση της σχεδίασης στους στόχους να συμπεριλαμβάνονται και στόχοι που αφορούν την ασφάλεια. Στα πρώτα στάδια της ανάπτυξης μάλιστα γίνεται μία εκτίμηση κινδύνων (risk assessment)

ώστε να μπορούν να εντοπιστούν τα σημεία που επηρεάζουν την ασφάλεια του έργου και στα οποία πρέπει να δοθεί μεγαλύτερη προσοχή. Κατά τη διάρκεια της υλοποίησης του έργου τίθενται κάποια σημεία στα οποία θα πρέπει να γίνει εκ' νέου εκτίμηση κινδύνων προκειμένου να εξακριβωθεί η ασφαλής ανάπτυξη-υλοποίηση αυτού.

6.4.2.2. Φορητές συσκευές και τηλεργασία

Για την περίπτωση φορητού εξοπλισμού, ο οποίος μπορεί να μεταφερθεί εκτός εταιρείας, ο Διαχειριστής του συστήματος τηρεί τις ακόλουθες πρόσθετες απαιτήσεις Ασφάλειας:

- Όλοι οι ηλεκτρονικοί φάκελοι που περιέχουν ευαίσθητα αρχεία είναι προστατευμένοι και είναι προσπελάσιμοι μόνο από εξουσιοδοτημένους χρήστες.
- Είναι πλήρως ενημερωμένα ως προς το λογισμικό και τις διορθώσεις ασφάλειας των εφαρμογών.
- Η χρήση τους καθορίζεται σαφώς κατά την παραλαβή τους.
- Απαγορεύεται η χρήση του εξοπλισμού από άτομα πέραν των εξουσιοδοτημένων (π.χ. οικογένεια, φίλοι, κοκ).
- Η πρόσβαση σε υπηρεσίες και συστήματα της εταιρείας γίνεται μόνο μέσω κρυπτογραφημένων πρωτοκόλλων και VPN.
- Γίνεται σχετική εκπαίδευση των χρηστών για όλους τους κινδύνους που υφίστανται καθώς και για τις διαδικασίες ασφαλούς πρόσβασης στα ευαίσθητα δεδομένα.
- Τηρείται λεπτομερής κατάλογος του διαθέσιμου εξοπλισμού που μπορεί να μεταφερθεί
- Οι συσκευές που μπορούν να βγουν εκτός εταιρείας και περιέχουν διαβαθμισμένη πληροφορία είναι κρυπτογραφημένες.

Στην περίπτωση εξοπλισμού που μεταφέρεται εκτός εταιρείας (π.χ. φορητοί υπολογιστές), το προσωπικό ενημερώνεται προκειμένου να:

- μην αφήνει τον εξοπλισμό χωρίς επίβλεψη και να τον κλειδώνει όποτε είναι δυνατό (π.χ. χρήση ειδικών κλειδαριών για φορητούς υπολογιστές).

- να τηρεί τις απαιτήσεις ασφάλειας του κατασκευαστή (π.χ. να μη τον εκθέτει σε ισχυρά ηλεκτρομαγνητικά πεδία)
- μην συνδέεται με υπηρεσίες της εταιρείας χωρίς τη χρήση πρωτοκόλλων Ασφάλειας (π.χ. SSL, TLS) ή μηχανισμών VPN και σε καμία περίπτωση να μην εισάγει προσωπικούς κωδικούς σε μη ασφαλείς σελίδες ή email.

Η απομακρυσμένη πρόσβαση στα συστήματα της εταιρείας γίνεται μόνο από εξουσιοδοτημένο προσωπικό.

6.4.3. Ασφάλεια ανθρώπινων πόρων

6.4.3.1. Πριν την εργασία

Ένα από τα πλέον ευαίσθητα σημεία για τη διαφύλαξη της ασφάλειας της διακινούμενης πληροφορίας είναι η ακεραιότητα και ο επαγγελματισμός του προσωπικού που τη χειρίζεται. Η πρόσληψη νέου προσωπικού διέπεται από κανόνες και κριτήρια που σχετίζονται και με την αξιοπιστία του προσλαμβανομένου.

Οι έλεγχοι που γίνονται από τη διοίκηση της εταιρείας (ανάλογα με τις ευθύνες και τη σοβαρότητα της θέσης) είναι οι εξής:

- Ακρίβεια βιογραφικού σημειώματος ως προς τις προηγούμενες εργασίες, ημερομηνίες
- Ύπαρξη γραπτών συστάσεων που να επιβεβαιώνουν τόσο τις επαγγελματικές δεξιότητες όσο και την ακεραιότητα του χαρακτήρα
- Επιβεβαίωση επαγγελματικών και ακαδημαϊκών προσόντων με τους αντίστοιχους τίτλους και βεβαιώσεις
- Επιβεβαίωση της ταυτότητας με έλεγχο αριθμού δελτίου ταυτότητας και ΑΦΜ.

Οι παραπάνω έλεγχοι θα γίνονται με ιδιαίτερη εμπιστευτικότητα και τα αποτελέσματά τους δε θα πρέπει να κοινοποιούνται πέραν του εξουσιοδοτημένου προσωπικού.

Κατά την πρόσληψη θα υπογράφεται κείμενο:

- ανάληψης νομικών ευθυνών έναντι διαρροής δεδομένων και υποβάθμισης της ασφάλειας του συστήματος
- προστασίας προσωπικών δεδομένων των πελατών και των πνευματικών δικαιωμάτων του χρησιμοποιούμενου υλικού.

Ο προσληφθείς θα εκπαιδεύεται – ενημερώνεται για όλα τα τηρούμενα πρωτόκολλα Ασφάλειας πληροφοριών, ενώ θα καταγράφεται σαφώς ο ρόλος του, ο εξοπλισμός και οι υπηρεσίες που δικαιούται να χρησιμοποιεί είτε εντός, είτε εκτός του χώρου της εταιρείας.

Τα παραπάνω ισχύουν τόσο για το προσωπικό της εταιρείας όσο και για εξωτερικούς συνεργάτες (εταιρείες καθαρισμού, υπηρεσιών, συμβούλων κοκ.) που προσλαμβάνονται άμεσα ή μέσω τρίτων. Η εταιρεία αναλαμβάνει την ενημέρωση των εξωτερικών συνεργατών περί των επιταγών των προτύπων ποιότητας και την υπογραφή των συμφώνων εμπιστευτικότητας.

6.4.3.2. Κατά τη διάρκεια της εργασίας

Ο Υπεύθυνος Ασφάλειας Πληροφοριών σε συνεχή βάση επιθεωρεί και επιβεβαιώνει την καλή εφαρμογή της Πολιτικής Ασφάλειας Πληροφοριών από όλο το προσωπικό καθώς και τους εξωτερικούς συνεργάτες.

Σε τακτά χρονικά διαστήματα, όποτε διαπιστώνει παρεκκλίσεις ή όποτε τροποποιείται η Πολιτική Ασφάλειας Πληροφοριών προβαίνει σε διαδικασίες εκπαίδευσης και επιμόρφωσης σχετικά με τις απαιτήσεις Ασφάλειας της ασφάλειας πληροφορίας καθώς και όλες τις διαδικασίες του Συστήματος Διαχείρισης Ασφάλειας Πληροφορίας. Ο Υπεύθυνος Ασφάλειας Πληροφοριών εκπαιδεύει κάθε νέο συνεργάτη που αναλαμβάνει εργασία για την εταιρεία.

Η διοίκηση της εταιρείας στα συμβούλια ανασκόπησης ελέγχει την ορθή τήρηση των προβλεπόμενων διαδικασιών Ασφάλειας και ενημερώνεται από τον Υπεύθυνο Ασφάλειας Πληροφοριών για τις λεπτομέρειες του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών. Επιπλέον, παρέχει όλους τους απαιτούμενους πόρους για την καλή λειτουργία του Συστήματος, συνεπής προς την Πολιτική Ασφάλειας Πληροφοριών και οι σχετικές αποφάσεις επικυρώνονται στο συμβούλιο ανασκόπησης.

Σε περίπτωση επιβεβαιωμένης παραβίασης των κανονισμών Ασφάλειας, διενεργείται διερευνητική διαδικασία στην οποία λαμβάνονται υπόψη:

- η σοβαρότητα της παραβίασης
- αν πρόκειται για μεμονωμένο περιστατικό ή επαναλαμβανόμενο
- αν είχε γίνει η απαραίτητη εκπαίδευση
- οι επιπτώσεις της παραβίασης στη λειτουργία της εταιρείας.

Σε περίπτωση που η παραβίαση δεν έχει προκαλέσει σημαντική ζημιά, θα γίνεται προφορική σύσταση στο χρήστη. Για επαναλαμβανόμενη παραβίαση ή σημαντικές επιπτώσεις θα γίνεται γραπτή σύσταση στο χρήστη και προειδοποίηση σχετικά με τις επόμενες κυρώσεις. Σε νέα υποτροπή θα κινούνται οι διαδικασίες λήξης της συνεργασίας με το χρήστη. Στην περίπτωση που κριθεί απαραίτητο, θα αφαιρούνται τα δικαιώματα χρήσης του παραβάτη και θα κινούνται οι προβλεπόμενες νόμιμες διαδικασίες. Σε κάθε περίπτωση, θα λαμβάνονται τα απαραίτητα μέτρα ανάκαμψης από το κενό Ασφάλειας που δημιουργείται.

6.4.3.3. Διακοπή/αλλαγή εργασίας

Ο Υπεύθυνος Ασφάλειας Πληροφοριών ενημερώνεται άμεσα για κάθε περίπτωση απόλυσης ή αποχώρησης προσωπικού ή λήξης συνεργασίας με κάποιο εργολάβο, ώστε να προβεί άμεσα στις απαραίτητες ενέργειες.

Επιπλέον, ο υπάλληλος ή ο εργολάβος θα ενημερώνεται από τη διοίκηση της εταιρείας για τις υποχρεώσεις που απορρέουν από τις συμβάσεις εμπιστευτικότητας και Ασφάλειας καθώς για τη χρονική περίοδο που δεσμεύεται από αυτές. Σε περίπτωση που δεδομένα της εταιρείας βρίσκονται αποθηκευμένα σε μέσα του εργαζομένου, θα πρέπει να απαιτείται η άμεση απαλοιφή τους.

Τα παραπάνω έχουν εφαρμογή και σε περίπτωση αλλαγής της θέσης εργασίας μέσα στην εταιρεία, οπότε θα πρέπει να προσαρμοστούν ανάλογα τα δικαιώματα πρόσβασης σε χώρους και δεδομένα, καθώς και να ενημερωθούν όλα τα σχετικά αρχεία.

6.4.4. Διαχείριση πόρων

6.4.4.1. Ευθύνη για τους πόρους

Ο Υπεύθυνος Ασφάλειας Πληροφοριών διατηρεί κατάλογο των πληροφοριακών πόρων της εταιρείας, τον οποίο τηρεί πάντοτε ενημερωμένο. Στον κατάλογο αυτό περιλαμβάνονται οι πόροι που συμμετέχουν στον κύκλο ζωής της πληροφορίας (δηλ. τη δημιουργία, την επεξεργασία, την αποθήκευση, τη μετάδοση, τη διαγραφή και την καταστροφή της). Ο κατάλογος περιέχει τα ακόλουθα στοιχεία:

- **Πληροφορίες:** βάσεις δεδομένων, αρχεία δεδομένων, συμβάσεις, τεκμηρίωση λογισμικού κοκ.
- **Λογισμικό**: εφαρμογές, λειτουργικά συστήματα, εργαλεία ανάπτυξης και βοηθητικές εφαρμογές
- **Υλικό**: υπολογιστές, τηλεπικοινωνιακές υποδομές, αφαιρούμενα μέσα αποθήκευσης, άλλος εξοπλισμός
- **Βοηθητικά δίκτυα**: ηλεκτρικό ρεύμα, τηλεπικοινωνίες, κλιματισμός
- **Φυσικό αρχείο**: εκτυπώσεις, πρωτότυπα έγγραφα, κλπ.
- **Ανθρώπινοι πόροι**: εργαζόμενοι των οποίων η απώλεια είναι σημαντική λόγω εξειδίκευσης, ειδικών προσόντων και εμπειρίας.

Για κάθε πόρο καταγράφονται τα εξής στοιχεία:

- Περιγραφή (όνομα, τύπος, σειριακός αριθμός)
- Θέση
- Προμηθευτής
- Πρόγραμμα συντήρησης
- Ιδιοκτήτης
- Διαβάθμιση Ασφάλειας
- Προσωπικό εξουσιοδοτημένο για τη χρήση του και τα δικαιώματα χρήσης αυτού

- Αξία του πόρου

Ο υπεύθυνος «ιδιοκτήτης» ορίζεται ως το άτομο ή το τμήμα της εταιρείας που έχει την ευθύνη για την παραγωγή, ανάπτυξη, συντήρηση, χρήση και ασφάλεια του πόρου. Με άλλα λόγια, οι πληροφοριακοί πόροι της εταιρείας δεν αποτελούν ιδιοκτησία των εργαζομένων που τους χρησιμοποιούν, αλλά υπευθυνότητα τους.

Οι προσφερόμενες υπηρεσίες από την εταιρεία όπως ηλεκτρονική αλληλογραφία (email), πρόσβαση στο Internet, φορητά υπολογιστικά μέσα, κινητά τηλέφωνα κλπ. διατίθενται αποκλειστικά και μόνο για χρήση στα πλαίσια της εργασίας και απαγορεύεται κάθε άλλη χρήση τους.

Κατά την απόλυση / αποχώρηση ενός εργαζομένου ή τη λήξη της συνεργασίας με κάποιο εργολάβο, επιστρέφονται όλοι οι πόροι της εταιρίας. Έτσι καταχωρούνται στο σύστημα εκτός των άλλων και:

- Στοιχεία που επιστράφηκαν (π.χ. φορητοί υπολογιστές, κινητά τηλέφωνα, κλειδιά, κάρτες εισόδου) και αντιπαραβολή αυτών με τα στοιχεία που του είχαν παραχωρηθεί.

Επίσης, γίνεται άμεσα ανάκληση των δικαιωμάτων από προσβάσεις που είχε σε συστήματα και έγγραφα, καθώς και σε αρμοδιότητες που είχαν δοθεί κατά τη διάρκεια υλοποίησης του έργου. Έτσι, αποφεύγεται η πιθανότητα να αντιγραφούν ευαίσθητα δεδομένα που σχετίζονται με το έργο ή την εταιρεία, με σκοπό την κλοπή.

6.4.4.2. Διαβάθμιση πληροφοριών

Στα πλαίσια της διασφάλισης της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων της εταιρείας, εφαρμόζεται το ακόλουθο σύστημα διαβάθμισης της διακινούμενης πληροφορίας:

1. **Εσωτερικό / Αδιαβάθμητο**

Περιγραφή: Κάθε πληροφορία που αφορά την εσωτερική λειτουργία της εταιρείας χωρίς να αφορά δεδομένα πελατών και χωρίς να επηρεάζει την καλή λειτουργία της εταιρείας

Συνέπειες διαρροής: Καμία

Παραδείγματα: Συνήθη εσωτερικά σημειώματα, αναφορές, αρχεία

Σήμανση εγγράφου: Δεν απαιτείται σήμανση, όλα τα έγγραφα χωρίς σήμανση θεωρούνται εσωτερικά

Ηλεκτρονική αποθήκευση: Στον εξυπηρετητή αρχείων στις προβλεπόμενες θέσεις αποθήκευσης, σε κάθε υπολογιστή που απαιτείται και σε φορητά μέσα αποθήκευσης και υπολογιστές. Για τα αρχεία που αποθηκεύονται εκτός δικτύου της εταιρείας, σε περίπτωση καταστροφής του αρχείου ή δυσλειτουργίας του πόρου, την ευθύνη φέρουν οι ίδιοι οι χρήστες

Φυσική αποθήκευση: Σε συνήθη φάκελο χωρίς ιδιαίτερη σήμανση

Ηλεκτρονική διανομή: Δεν απαιτείται ιδιαίτερη προστασία, μπορεί να σταλεί με e-mail, fax

Φυσική διανομή: Δεν απαιτείται ιδιαίτερη προστασία, μέσω απλού ταχυδρομείου

Καταστροφή: Τα φυσικά αρχεία μπορούν να απορριφθούν σε συνήθεις κάδους άχρηστων ή να ανακυκλωθούν. Τα ηλεκτρονικά αρχεία και e-mail μπορούν να διαγραφούν χωρίς έλεγχο.

2. Εμπιστευτικό

Περιγραφή: Κάθε πληροφορία που απαγορεύεται να διακινείται ελεύθερα, χωρίς να αφορά δεδομένα πελατών

Συνέπειες διαρροής: Ελάχιστη ζημιά στην εικόνα της εταιρείας

Παραδείγματα: Έγγραφα σχεδιασμού των υπηρεσιών, οικονομικά στοιχεία, στοιχεία που αφορούν πελάτες της εταιρείας

Σήμανση εγγράφου: ΕΜΠΙΣΤΕΥΤΙΚΟ στην κορυφή του εγγράφου

Ηλεκτρονική αποθήκευση: Στον εξυπηρετητή αρχείων σε φακέλους που έχει πρόσβαση μόνο εξουσιοδοτημένο προσωπικό

Φυσική αποθήκευση: Σε κλειδωμένα συρτάρια ή ερμάρια

Ηλεκτρονική διανομή: Μπορεί να σταλεί με e-mail ή φαξ, με επισήμανση του εμπιστευτικού χαρακτήρα στο θέμα του mail ή στην κορυφή του εγγράφου.

Φυσική διανομή: Με φακέλους που σφραγίζονται από το συντάκτη τους, μέσω απλού ταχυδρομείου αν απαιτείται.

Καταστροφή: Τα φυσικά αρχεία θα πρέπει να καταστρέφονται με χρήση καταστροφέα εγγράφων. Τα ηλεκτρονικά αρχεία θα πρέπει να διαγράφονται και να αφαιρούνται από τον «Κάδο Ανακύκλωσης».

Η διαβάθμιση του εμπιστευτικού θα πρέπει να κοινοποιείται και να τηρείται και από κάθε τρίτο που στα πλαίσια συμβατικής συνεργασίας του με την εταιρεία έρχεται σε γνώση δεδομένων της εταιρείας.

Σε περίπτωση διανομής πληροφορίας (μέσω εγγράφων, CD, κλπ.) θα υπάρχει σήμανση εμπιστευτικότητας και αποκλειστικής χρήσης μόνο από τα μέλη της λίστας κοινοποίησης με βάση την διαβάθμιση.

Ο χειρισμός των μέσων αποθήκευσης που περιέχουν διαβαθμισμένα δεδομένα θα γίνεται σύμφωνα με τη διαβάθμισή τους (όπως αυτή αναφέρεται παραπάνω) και από το προσωπικό με εξουσιοδότηση χειρισμού της αντίστοιχης διαβάθμισης.

Κατά τη σύναψη συμβάσεων με τρίτους θα ενημερώνονται για τις διαβαθμίσεις που έχει η εταιρεία και θα συμφωνείτε ο τρόπος χειρισμού ευαίσθητων πληροφοριών.

6.4.4.3. Χειρισμός μέσων

Η παραβίαση του συστήματος μπορεί να γίνει όχι μόνο αποκτώντας πρόσβαση στα δεδομένα όσο αυτά διακινούνται μέσα στο πληροφοριακό σύστημα, αλλά ακόμα πιο εύκολα όταν βρίσκονται εκτός αυτού.

Οποιαδήποτε αποθήκευση πληροφοριών του συστήματος σε εξωτερικά μέσα αποθήκευσης αναιρεί κάθε μέσο ελέγχου πρόσβασης σε αυτά. Ταυτόχρονα, η σύνδεση τέτοιων μέσων μπορεί να εισαγάγει ανεπιθύμητο λογισμικό στο σύστημα. Για το σκοπό αυτό ακολουθούνται οι παρακάτω διαδικασίες:

1. Φορητά μέσα μαζικής αποθήκευσης
Παραδείγματα: Εξωτερικοί σκληροί δίσκοι, USB Flash Disk, Εξωτερικά CD/DVD RW

Χρήση: Επιτρέπεται η χρήση τους από το προσωπικό εντός των εργασιακών τους υποχρεώσεων.
Αποθήκευση δεδομένων: Απαγορεύεται αυστηρά η αποθήκευση δεδομένων πελατών ή δεδομένων που έχουν διαβάθμιση «εμπιστευτικό» σε φορητά μέσα μαζικής αποθήκευσης εάν αυτά δεν είναι κρυπτογραφημένα.
Φυσική αποθήκευση: Τα φορητά μέσα αποθηκεύονται από τους χρήστες στα γραφεία τους πλην αυτών που φέρουν διαβαθμισμένη πληροφορία και φυλάσσονται σε χώρους που ασφαλίζουν. Σε κάθε περίπτωση ο χώρος όπου αποθηκεύονται τα φορητά μέσα αποθήκευσης θα πρέπει να πληροί τις προδιαγραφές που ορίζει ο κατασκευαστής.
Διακίνηση: Επιτρέπεται η διακίνηση εντός των εργασιακών υποχρεώσεων του προσωπικού.
Διαγραφή: πλήρης διαγραφή/φορμάρισμα/wipe
Καταστροφή: Γίνεται καταστροφή του μέσου με μηχανικό τρόπο.

2. Αποθηκευτικά μέσα
Παραδείγματα: CD, DVD, Δισκέτες, Κασέτες
Χρήση: Επιτρέπεται η χρήση τους από το προσωπικό εντός των εργασιακών τους υποχρεώσεων.
Αποθήκευση δεδομένων: Απαγορεύεται αυστηρά η αποθήκευση δεδομένων πελατών ή δεδομένων που έχουν διαβάθμιση «εμπιστευτικό» σε φορητά μέσα μαζικής αποθήκευσης εάν αυτά δεν είναι κρυπτογραφημένα.
Φυσική αποθήκευση: Τα αποθηκευτικά μέσα αποθηκεύονται από τους χρήστες στους σε κλειδωμένες θέσεις (συρτάρια, ερμάρια). Σε κάθε περίπτωση ο χώρος όπου αποθηκεύονται τα φορητά μέσα αποθήκευσης θα πρέπει να πληροί τις προδιαγραφές που ορίζει ο κατασκευαστής.
Διακίνηση: Επιτρέπεται η διακίνηση εντός των εργασιακών υποχρεώσεων του προσωπικού.
Καταστροφή: Γίνεται καταστροφή με χρήση καταστροφέα για CD/DVD και πλήρης διαγραφή/φορμάρισμα/wipe/ φυσική καταστροφή σε περίπτωση μαγνητικού μέσου.

3. Έντυπα μέσα
Παραδείγματα: Εκτυπώσεις
Χρήση: Η εκτύπωση δεδομένων επιτρέπεται μόνο για τις ανάγκες των εργασιών της εταιρείας και μόνο όταν υπάρχει ανάγκη, στα πλαίσια προστασίας του περιβάλλοντος.
Αποθήκευση δεδομένων: Επιτρέπεται η εκτύπωση δεδομένων μόνο για τις ανάγκες εκτέλεσης των εργασιών της εταιρείας.
Φυσική αποθήκευση: Οι εκτυπώσεις ευαίσθητων δεδομένων αποθηκεύονται από το εξουσιοδοτημένο προσωπικό σε καθορισμένες και κλειδωμένες θέσεις. Για τις θέσεις αυτές είναι ενήμερος ο Υπεύθυνος Ασφάλειας Πληροφορίας.
Διακίνηση: Απαγορεύεται η διακίνηση εκτός του χώρου της εταιρείας.
Καταστροφή: Γίνεται καταστροφή με χρήση καταστροφέα χαρτιού (shredder).

Διαγράμματα και διαδικασίες που αφορούν τη λειτουργία του συστήματος (διάγραμμα δικτύου, δικλείδες Ασφάλειας, εγχειρίδια συστήματος, μηχανισμοί ελέγχου) θα αποθηκεύονται σε θέση διαφορετική από τα υπόλοιπα αρχεία του συστήματος, μη προσβάσιμη από τους μη εξουσιοδοτημένους χρήστες. Η έντυπη μορφή τους φυλάσσεται στο γραφείο του Υπευθύνου Ασφάλειας Πληροφοριών.

6.4.5. Έλεγχος πρόσβασης

6.4.5.1. Επιχειρησιακές απαιτήσεις ελέγχου πρόσβασης

Ο έλεγχος πρόσβασης είναι το βασικό εργαλείο εφαρμογής της Πολιτικής Ασφάλειας Πληροφορίας. Τα μέσα ελέγχου πρόσβασης είναι τόσο λογικά (σε επίπεδο λειτουργικού συστήματος, δικτύου και εφαρμογών) όσο και φυσικά (αποκλεισμός φυσικής πρόσβασης).

Οι βασικές αρχές της πολιτικής πρόσβασης για την εταιρεία είναι οι εξής:

- Η πληροφορία που διακινείται στην εταιρεία διαβαθμίζεται με βάση τους κανόνες της παραγράφου 6.4.4.2.

- Όλη η πληροφορία που αφορά τους πελάτες είναι εμπιστευτική και απαγορεύεται να κοινοποιείται σε μη εξουσιοδοτημένους χρήστες. Ο Υπεύθυνος Ασφάλειας Πληροφοριών τηρεί κατάλογο με τις θέσεις αποθήκευσης και το είδος των ευαίσθητων δεδομένων που είναι αποθηκευμένα.
- Η εταιρεία δεσμεύεται από τη σχετική νομοθεσία για την προστασία των προσωπικών δεδομένων καθώς και των πνευματικών δικαιωμάτων.
- Η ιεραρχία του προσωπικού μεταφέρεται στα δικαιώματα χρήσης του πληροφοριακού εξοπλισμού. Κάθε κρίσιμη ενέργεια των χρηστών θα πρέπει να εγκρίνεται και να εποπτεύεται από τον υπεύθυνο / προϊστάμενο. Οι εργαζόμενοι εντάσσονται σε ομάδες ασφάλειας (security groups) βάσει των οποίων τους ανατίθενται δικαιώματα χρήσης των συστημάτων και πρόσβασης των πληροφοριών, σε αντιστοιχία με τη διαβάθμιση αυτών.
- Ο Υπεύθυνος Ασφάλειας Πληροφοριών διατηρεί κατάλογο των χρηστών του συστήματος και των δικαιωμάτων πρόσβασης που τους έχουν ανατεθεί σε εξοπλισμό και πληροφοριακά συστήματα.
- Τα δικαιώματα πρόσβασης σχετίζονται άμεσα με την εργασία και τη θέση του εργαζομένου στην εταιρεία. Αλλαγή θέσης ή λήξη της συνεργασίας συνεπάγεται την άμεση τροποποίηση ή/και αφαίρεση των δικαιωμάτων.
- Εφαρμόζεται η γενική αρχή «*κάθε ενέργεια απαγορεύεται εκτός αν έχει ρητά επιτραπεί*».
- Τα δικαιώματα και οι προσβάσεις των χρηστών δίνονται με βάση τις αρχές:
    - Ανάγκη γνώσης (Need to know)
    - Ανάγκη χρήσης (Need to use)

Η σύνδεση με το εξωτερικό δίκτυο διέρχεται μέσω συστημάτων Ασφάλειας Firewall με access lists καθώς και σύγχρονων routers και switches έτσι ώστε να ελαχιστοποιείται ο κίνδυνος παράνομης εισόδου ή διακοπής της πρόσβασης λόγω βλάβης. Οι κανόνες πρόσβασης και δρομολόγησης του firewall και του router θα εγκρίνονται από τον Υπεύθυνο Ασφάλειας Πληροφοριών και θα τηρούνται και σε αρχείο εκτός του firewall/router. Κάθε αλλαγή θα απαιτεί έγκριση και αιτιολόγηση. Η συνολική αρχιτεκτονική του δικτύου της εταιρείας τηρείται σε ηλεκτρονικό αρχείο.

Δεν επιτρέπεται η χωρίς έλεγχο ύπαρξη συνδέσεων τύπου tunnel VPN προς το δίκτυο της εταιρείας. Στην περίπτωση που απαιτούνται εισερχόμενες συνδέσεις προς το δίκτυο της εταιρείας (π.χ. από εργαζομένους που δουλεύουν εκτός του κτηρίου ή από προσωπικό που εκτελεί διαδικασίες συντήρησης), αυτές θα υλοποιούνται με χρήση VPN και θα καταγράφονται. Στην περίπτωση αυτή η πρόσβαση θα περιορίζεται σε

συγκεκριμένη διεύθυνση IP, με κωδικό πρόσβασης και για συγκεκριμένο χρονικό διάστημα.

Όλα τα συνδεδεμένα στο δίκτυο μηχανήματα θα είναι αναγνωρίσιμα από το δικτυακό όνομα τους.

Η πολιτική απόδοσης ονομάτων στους πληροφοριακούς πόρους γίνεται σύμφωνα με τη χρήση του εκάστοτε συστήματος.

Τηρείται ενημερωμένο αρχείο του ενεργού, του ανενεργού και του προς καταστροφή εξοπλισμού.

Στους εξυπηρετητές της εταιρείας θα είναι ανοικτές μόνον οι δικτυακές θύρες που απαιτούνται για την εξυπηρέτηση των συστημάτων της εταιρείας. Όλες οι διαγνωστικές και ρυθμιστικές θύρες θα είναι απενεργοποιημένες, εκτός από τις περιπτώσεις που απαιτείται παραμετροποίηση του εξοπλισμού. Ομοίως, όλες οι φυσικές θύρες διασύνδεσης που χρησιμοποιούνται για ρύθμιση του εξοπλισμού θα είναι αποσυνδεδεμένες και θα χρησιμοποιούνται μόνο από εγκεκριμένο προσωπικό. Σε περίπτωση λογισμικού που επιτρέπει την απομακρυσμένη αλλαγή ρυθμίσεων των συστημάτων (web configuration), θα είναι προσβάσιμο μόνο για εξουσιοδοτημένους χρήστες και αν δεν απαιτείται σε συνεχή βάση, θα απενεργοποιείται

6.4.5.2. Διαχείριση πρόσβασης χρηστών

Κάθε χρήστης των συστημάτων της εταιρείας έχει μοναδικό προσωπικό κωδικό πρόσβασης που του αποδίδεται κατά την πρόσληψη και απενεργοποιείται κατά τη λήξη της εργασίας του στην εταιρεία. Μέσω του κωδικού αυτού αναγνωρίζονται και καταγράφονται όλες οι ενέργειες του που αφορούν τα δεδομένα των πληροφοριακών συστημάτων της εταιρείας και του εκχωρούνται τα δικαιώματα πρόσβασης που απαιτούνται για την εκτέλεση των καθορισμένων του εργασιών και μόνον αυτών.

Η χρήση του κωδικού πρόσβασης εκφράζει την πλήρη αποδοχή όλων των όρων που διέπουν το πληροφοριακό σύστημα και το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών της εταιρείας. Ο κωδικός και τα δικαιώματα που έχουν ανατεθεί καταγράφονται στο σχετικό αρχείο που τηρεί ο Υπεύθυνος Ασφάλειας Πληροφοριών καθώς και στο αρχείο Έναρξης – Λήξης Συνεργασίας. Η υπογραφή της σύμβασης συνεργασίας καθώς και του συμφώνου εμπιστευτικότητας υποδηλώνουν τη σαφή αποδοχή όλων των όρων που διέπουν το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.

Κάθε κωδικός χρήστη συνοδεύεται από μυστικό συνθηματικό (password) το οποίο ο χρήστης δεσμεύεται και φέρει την πλήρη ευθύνη να διατηρεί μυστικό. Όλα τα συνθηματικά θα πρέπει να διατηρούνται στη μνήμη των χρηστών και σε καμία περίπτωση να καταγράφονται σε έγγραφα τα οποία βρίσκονται γύρω από τον σταθμό εργασίας, ηλεκτρονικές συσκευές ή άλλα μέσα αποθήκευσης.

Κατά την απόλυση / αποχώρηση ή κατά την αλλαγή θέσης εργασίας γίνονται τα εξής:

- Αναίρεση δικαιωμάτων χρήσης:
    - Κωδικός χρήστη
    - Προσωπικοί φάκελοι αποθήκευσης – θα μεταφέρονται στον έλεγχο του διαχειριστή και θα αρχειοθετούνται ή θα διαγράφονται. Σε περίπτωση που οι φάκελοι περιέχουν εταιρική πληροφορία, ο φάκελος μεταφέρεται και στον έλεγχο της Διοίκησης.
    - Email – η αλληλογραφία θα αρχειοθετείται και το e-mail θα προωθείτε σε λογαριασμό e-mail της διοίκησης
- Υπηρεσίες στις οποίες ο υπάλληλος είχε πρόσβαση. Θα γίνεται η αλλαγή του συνθηματικού χρήσης αυτών, σε περίπτωση που ο εργαζόμενος δεν διέθετε προσωπικό κωδικό.

6.4.5.3. Ευθύνες χρηστών

Η διαχείριση των συνθηματικών των χρηστών υπακούει στις ακόλουθες απαιτήσεις:

- Δε θα γράφονται ευαίσθητα δεδομένα όπως συνθηματικά σε έγγραφα τα οποία βρίσκονται στην περιοχή γύρω από το σταθμό εργασίας ούτε θα μένουν μέσα αποθήκευσης εκτεθειμένα σε κοινή θέα.
- Οι χρήστες δε θα μοιράζονται κωδικούς χρήσης και συνθηματικά μεταξύ τους.
- Σε καμία περίπτωση δε θα υπάρχουν μηχανήματα και πληροφοριακά συστήματα με κενά συνθηματικά και δε θα χρησιμοποιείται το ίδιο συνθηματικό σε πάνω από ένα μηχανήματα.

- Το σύστημα θα επιτρέπει την επιλογή συνθηματικών επαρκούς ασφάλειας και μόνο. Προτείνεται να έχουν μήκος τουλάχιστον **8 χαρακτήρων**, να περιέχουν πεζά και κεφαλαία γράμματα, αριθμούς και σύμβολα.
- Όλα τα συνθηματικά των Windows θα αλλάζουν υποχρεωτικά **τουλάχιστον κάθε 6 μήνες.** Οι χρήστες ενημερώνονται για την αναγκαιότητα της αλλαγής του κωδικού πρόσβασης 5 ημέρες νωρίτερα. Ο χρήστης δεν θα μπορεί να χρησιμοποιήσει τα 3 τελευταία συνθηματικά. Μετά την λάθος εισαγωγή για 5 φορές του συνθηματικού θα κλειδώνεται ο λογαριασμός του για 15 λεπτά. Σε περίπτωση που υπάρχει υποψία διαρροής του συνθηματικού, τότε η αλλαγή γίνεται άμεσα. Ο χρήστης θα πρέπει να επιλέγει το συνθηματικό κατά τρόπο ώστε:
    - Να το θυμάται εύκολα
    - Να μην μπορεί να προσδιοριστεί από άλλα προσωπικά του στοιχεία (πχ. Όνομα, διεύθυνση, συγγενικά πρόσωπα) και να μην είναι κανονική λέξη της ελληνικής ή άλλης γλώσσας.
    - Να μην περιέχει διαδοχικά ίδια γράμματα ή αριθμούς.
    - Να μην είναι το ίδιο με ένα από τα **3** προηγούμενα συνθηματικά του
    - Να μην ταυτίζεται με συνθηματικά που χρησιμοποιεί για προσωπικές χρήσεις.
- Συγκεκριμένα, για το email ακολουθούνται τα παρακάτω:
    - μήκος συνθηματικών τουλάχιστον **6 χαρακτήρων,**
    - τα συνθηματικά περιέχουν πεζά και κεφαλαία γράμματα, αριθμούς και σύμβολα,
    - τα συνθηματικά αλλάζουν υποχρεωτικά **κάθε 6 μήνες.**

Οι διαχειριστές θα πρέπει να αλλάζουν τα συνθηματικά τους τουλάχιστον κάθε 6 μήνες.

6.4.5.4. Έλεγχος πρόσβασης σε συστήματα και εφαρμογές

Η πρόσβαση των χρηστών της εταιρείας τόσο στις εφαρμογές λογισμικού όσο και στα δεδομένα που αποθηκεύονται στους servers γίνεται μόνο με χρήση προσωπικού κωδικού και συνθηματικού και με δικαιώματα πρόσβασης και ελέγχου που καθορίζονται από την ομάδα Ασφάλειας του χρήστη.

Συγκεκριμένα οι χρήστες των πληροφοριακών συστημάτων επιτρέπεται να κάνουν μόνο τις ενέργειες που είναι καθορισμένες για την ομάδα Ασφάλειας τους. Αντίστοιχα, η πρόσβαση καθώς και το δικαίωμα read/write στους φακέλους αποθήκευσης των εξυπηρετητών αρχείων προσδιορίζεται από την ομάδα Ασφάλειας του χρήστη. Η παροχή/αφαίρεση δικαιωμάτων ενός χρήστη γίνεται έπειτα από αίτημα προς τον Υπεύθυνο Ασφάλειας Πληροφοριών.

Τα δικαιώματα των χρηστών τηρούνται σε αρχείο από τον Υπεύθυνο Ασφάλειας Πληροφοριών.

Οι εφαρμογές που χρησιμοποιούνται στους σταθμούς εργασίας διαθέτουν φιλικά περιβάλλοντα χρήσης όπου οι επιτρεπτές ενέργειες θα είναι προσβάσιμες μέσω μενού και πλήκτρων ελέγχου, προκειμένου να ελαχιστοποιείται η πιθανότητα λανθασμένου χειρισμού.

Η είσοδος στο περιβάλλον εργασίας θα γίνεται μόνο μετά την επιτυχή εισαγωγή του προσωπικού τους κωδικού και συνθηματικού ή μέσω άλλης ασφαλούς διαδικασίας. Σε καμία περίπτωση τα συνθηματικά δε θα εμφανίζονται στην οθόνη παρά μόνον ως άστρα ή άλλο σύμβολο και δε θα μεταδίδονται ως απλό κείμενο μέσω δικτύου. Τα συνθηματικά χρήσης διέπονται από τις απαιτήσεις της παραγράφου 6.4.5.3.

Σε περίπτωση εισαγωγής εσφαλμένου συνθηματικού στους υπολογιστές της εταιρείας για 5 συνεχόμενες φορές, ο λογαριασμός θα κλειδώνει και θα ξεκλειδώνει μετά την παρέλευση διαστήματος 15 λεπτών. Ο Υπεύθυνος Ασφάλειας Πληροφοριών ελέγχει σε εβδομαδιαία βάση τα logs για κλείδωμα λογαριασμών. Επιπλέον οι εφαρμογές δεν μεταδίδουν ποτέ το συνθηματικό του χρήστη σε μορφή απλού κειμένου, αλλά κρυπτογραφημένο ή με άλλο ασφαλή τρόπο (π.χ. hash).

Οι χρήστες θα έχουν δικαιώματα ανάλογα με την ομάδα Ασφάλειας που ανήκουν. Εκτός των καταγεγραμμένων εξαιρέσεων, η πλειοψηφία θα έχει δικαιώματα τοπικού χρήστη στον τοπικό υπολογιστή όπου εργάζεται. Δε θα έχουν δικαίωμα τροποποίησης των ρυθμίσεων του λειτουργικού συστήματος. Επιπλέον δε θα επιτρέπεται η εκτέλεση βοηθητικών εφαρμογών – πέραν των εγκεκριμένων – με τις οποίες ενδέχεται να παρακαμφθούν οι μηχανισμοί Ασφάλειας των συστημάτων. Ο Υπεύθυνος Ασφάλειας Πληροφοριών στις επιθεωρήσεις του θα ελέγχει για την ύπαρξη και χρήση τέτοιου λογισμικού και ο διαχειριστής του συστήματος θα το απεγκαθιστά έπειτα από έγκριση του Υπευθύνου Ασφάλειας Πληροφοριών.

6.4.6. Κρυπτογραφία

6.4.6.1. Κρυπτογραφικά εργαλεία

Για τη διασφάλιση της προστασίας και της αυθεντικότητας της διακινούμενης πληροφορίας, η εταιρεία χρησιμοποιεί:

• τεχνολογικά υπογεγραμμένων και αξιόπιστων πιστοποιητικών κατά την επικοινωνία της με email (S-MIME signed emails) για ορισμένα πρόσωπα από τη Διοίκηση, καθώς και στο δικτυακό της τόπο (https – SSL).

• σύστημα κρυπτογράφησης που επιτρέπει την κρυπτογράφηση χωρίς να απαιτείται η έκδοση προσωπικών πιστοποιητικών.

Τα πιστοποιητικά εκδίδονται από αξιόπιστο προμηθευτή, κατόπιν σχετικής έγκρισης και ταυτοποίησης της εταιρείας και των χρηστών με ευθύνη της διοίκησης της εταιρείας και είναι τεχνολογίας RSA. Τα ιδιωτικά κλειδιά (private keys) αποθηκεύονται:

- για τα ατομικά πιστοποιητικά των εργαζομένων σε ασφαλείς θέσεις προσβάσιμες μόνο από κάθε εργαζόμενο

- για τα εταιρικά πιστοποιητικά σε ασφαλή θέση του server, στην οποία έχει πρόσβαση μόνο η διοίκηση της εταιρείας.

Σε περίπτωση απώλειας ή διαρροής ιδιωτικού κλειδιού γίνεται άμεση ανάκληση του πιστοποιητικού και έκδοση νέου, ενώ καταγράφεται περιστατικό ασφαλείας σύμφωνα με τη σχετική διαδικασία.

6.4.7. Φυσική και περιβαλλοντική ασφάλεια

6.4.7.1. Ασφαλείς περιοχές

Κατά την είσοδο επισκεπτών στα γραφεία της εταιρείας, τα στοιχεία τους καταχωρούνται από τη γραμματεία στο αρχείο επισκεπτών και σημειώνεται η ημερομηνία και η ώρα εισόδου και εξόδου, το ονοματεπώνυμο και το στέλεχος της εταιρείας που επισκέπτονται. Οι επισκέπτες θα ενημερώνονται ότι εισέρχονται σε

ελεγχόμενο χώρο, και θα είναι συνεχώς υπό την επίβλεψη ενός εργαζομένου της εταιρείας. Οι είσοδοι των γραφείων της εταιρείας ελέγχονται μέσω κλειστού κυκλώματος καταγραφής εικόνας, το οποίο διατηρεί αρχείο για τουλάχιστον 15 ημέρες.

Κατά την απομάκρυνση του προσωπικού από τα γραφεία του, φροντίζει ώστε οι ντουλάπες και τα συρτάρια που έχουν διαβαθμισμένη πληροφορία να είναι κλειδωμένα και τα κλειδιά αυτών να είναι ασφαλισμένα. Μετά τη λήξη της εργασίας τους οι εργαζόμενοι ασφαλίζουν τους χώρους τους.

Ιδιαίτερη έμφαση δίνεται στο server room όπου η πρόσβαση είναι εκτός από ελεγχόμενη και καταγραφόμενη μέσω κλειστού κυκλώματος καμερών. Η είσοδος γίνεται μόνο με χρήση κλειδιών, τα οποία έχουν διανεμηθεί σε συγκεκριμένα άτομα της εταιρείας. Δεν υπάρχει πρόσβαση στο server room, εκτός της κύριας εισόδου.

Το προσωπικό που είναι εξουσιοδοτημένο να εισέρχεται και να εργάζεται σε ασφαλισμένες περιοχές είναι καταγεγραμμένο σε ειδική λίστα και θα ενημερώνεται για τις ευθύνες και τις υποχρεώσεις που απορρέουν από αυτό. Ιδιαίτερα, το προσωπικό αυτό φέρει την πλήρη ευθύνη για τη μη εισαγωγή τρίτων στους χώρους αυτούς και την ασφάλισή τους μετά την έξοδό του. Επιπλέον, φέρει την ευθύνη να ελέγχει τουλάχιστον μια φορά την ημέρα τις ασφαλισμένες περιοχές και να εξασφαλίζει ότι είναι κλειδωμένες όταν δεν εργάζεται κάποιος σε αυτές.

Για την αποφυγή και αντιμετώπιση ζημιών λόγω πυρκαγιάς ή άλλης καταστροφής έχουν εγκατασταθεί συσκευές πυρανίχνευσης σε όλους τους ασφαλισμένους χώρους ενώ δε θα γίνεται αποθήκευση εύφλεκτου και επικίνδυνου υλικού κοντά σε αυτούς (π.χ. είδη γραφείου, χαρτικά κλπ.).

Το προσωπικό που εργάζεται σε ασφαλείς περιοχές απαγορεύεται να τρώει, να πίνει ή να καπνίζει για την αποφυγή ατυχημάτων. Κατά τη διάρκεια επίσης της εργασίας του στις περιοχές αυτές απαγορεύεται η χρήση συσκευών με δυνατότητα λήψης φωτογραφιών (π.χ. κινητά τηλέφωνα, φωτογραφικές μηχανές κ.λπ.).

6.4.7.2. Εξοπλισμός

Δεδομένου ότι η εύρυθμη λειτουργία του πληροφοριακού συστήματος βασίζεται στην ομαλή συνδεσιμότητα μεταξύ των σταθμών εργασίας και των εξυπηρετητών, έχει ληφθεί μέριμνα ώστε όλα τα σχετικά μέσα επικοινωνίας να λειτουργούν σωστά και χωρίς διακοπές.

Οι χώροι ελέγχου του δικτύου ηλεκτρικού ρεύματος, κλιματισμού και πυρασφάλειας είναι προστατευόμενοι. Δολιοφθορά στο δίκτυο τροφοδοσίας θα προκαλέσει διακοπή της εύρυθμης λειτουργίας της εταιρείας και ενδεχομένως ζημίες στον εξοπλισμό και απώλεια δεδομένων.

- Παντού η καλωδίωση είναι δομημένη και δεν υπάρχουν ελεύθερα καλώδια, των οποίων η διαδρομή και η σύνδεση είναι άγνωστη.

- Κάθε καλώδιο και κάθε πρίζα δικτύου είναι αναγνωρίσιμη με σχετική κωδικοποίηση. Οι πίνακες συνδέσεων (patch panels) κλειδώνονται.

- Σε περίπτωση υποψίας φθοράς καλωδίου, γίνεται άμεση αντικατάσταση για την αποφυγή καταστροφής δεδομένων.

- Ο σχεδιασμός του δικτύου απομονώνει ευαίσθητα υποδίκτυα και δεν επιτρέπει διείσδυση από το εξωτερικό δίκτυο καθώς και μη εξουσιοδοτημένη πρόσβαση από το εσωτερικό δίκτυο.

- Όλος ο ευαίσθητος εξοπλισμός, δηλαδή ο εξοπλισμός που έχει μεγάλη αξία, περιέχει ευαίσθητα δεδομένα, εκτυπώνει ευαίσθητα δεδομένα ή δεν είναι δυνατόν να προστατευθεί επαρκώς μέσω λογισμικού και τεχνικών μεθόδων Ασφάλειας βρίσκεται σε χώρους με ελεγχόμενη πρόσβαση. Εφόσον δεν απαιτείται αποκόπτεται η σύνδεση με το δίκτυο ευαίσθητου εξοπλισμού.

- Οι υπολογιστές του προσωπικού εγκαθίστανται σε θέσεις όπου το κοινό δεν έχει οπτική πρόσβαση στην οθόνη και το πληκτρολόγιο ώστε να μην έχει τη δυνατότητα θέασης στοιχείων ή κωδικών πρόσβασης.

Όλος ο κρίσιμος εξοπλισμός του Computer Room είναι συνδεδεμένος πάνω σε σύστημα αδιάλειπτης παροχής ενέργειας UPS και σε σύστημα H/Z με γεννήτρια πετρελαίου για τη διαφύλαξη της απρόσκοπτης λειτουργίας τους. Αντίστοιχα, το server room διαθέτει αυτόνομο σύστημα κλιματισμού.

Επισημαίνεται ότι οι χώροι λειτουργίας των εξυπηρετητών (server room) τροφοδοτούνται από ιδιαίτερη ηλεκτρική γραμμή. Επιπλέον, παρέχει την απαραίτητη ενέργεια που απαιτεί η ομαλή λειτουργία των μηχανημάτων χωρίς να προκαλείται υπερφόρτωση των γραμμών.

Η θερμοκρασία και η υγρασία σε 3 σημεία, η ύπαρξη νερού (πλημμύρα) και καπνού στο χώρο του server room ελέγχεται μέσω ειδικού εργαλείου επίβλεψης περιβαλλοντικών συνθηκών, ενώ τηρείται πρόγραμμα συντηρήσεων. Σε περίπτωση βλάβης γίνεται άμεση επισκευή.

Όλος ο κρίσιμος εξοπλισμός της εταιρείας καλύπτεται από συμβάσεις συντήρησης, στις οποίες έχουν προστεθεί οι απαιτήσεις Ασφάλειας, ή εγγύηση λειτουργίας και τεχνικής. Σε περίπτωση βλάβης του εξοπλισμού η επισκευή του θα γίνεται μόνο από τον εξουσιοδοτημένο πάροχο και το εξουσιοδοτημένο προσωπικό. Στην περίπτωση που ο εξοπλισμός προς συντήρηση μεταφέρεται εκτός της εταιρείας ή ενδέχεται να υποστεί χειρισμό από προσωπικό άγνωστο προς την εταιρεία, θα πρέπει να μεταφέρονται, να κρυπτογραφούνται ή να διαγράφονται ευαίσθητα δεδομένα από αυτόν. Τέλος, εφόσον ο εξοπλισμός κριθεί απορριπτέος, πριν τη διάθεσή του θα πρέπει να διαγράφουν όλα τα δεδομένα από αυτόν και να καταστεί μη χρησιμοποιήσιμος.

Στα πλαίσια των παραπάνω το προσωπικό οφείλει να μην καταγράφει και αποθηκεύει ευαίσθητα δεδομένα και σε κάθε άλλο μέσο αποθήκευσης όπως εξωτερικοί σκληροί δίσκοι, USB Flash Disks, CD καθώς και κινητά τηλεφώνα ή προσωπικές σημειώσεις και organizer. Σε περίπτωση που αυτό είναι απαραίτητο, η αποθήκευση θα πρέπει να γίνεται με κρυπτογράφηση.

Η κλοπή αποτελεί μια από τις πλέον κοινές απειλές και θέτει σε κίνδυνο τη διαθεσιμότητα της πληροφορίας αλλά και του πληροφοριακού εξοπλισμού. Για την αντιμετώπιση κρουσμάτων κλοπής υλοποιούνται τα ακόλουθα μέτρα:

- Φυσικά μέτρα: έλεγχος πρόσβασης στους χώρους του κτηρίου καθώς και αποτρεπτικά μέσα όπως πρόσδεση εξοπλισμού, εγκατάσταση συναγερμού, καταγραφή με κλειστό κύκλωμα καμερών.

- Έλεγχος προσωπικού: νομικά κείμενα που δεσμεύουν τους εργαζομένους έναντι της κλοπής καθώς και αντίστοιχες δεσμεύσεις και ρήτρες για τους εξωτερικούς συνεργάτες αποθαρρύνουν από την κλοπή.

- Ασφάλιση μέσων αποθήκευσης: κάθε στοιχείο που περιέχει ευαίσθητη πληροφορία (χαρτί, δίσκος, CD, δισκέτα) φυλάσσεται σε ασφαλή τοποθεσία.

- Επιπλέον απαγορεύεται η απομάκρυνση εξοπλισμού από την (προ)καθορισμένη του θέση χωρίς γραπτή άδεια και εξουσιοδότηση από τον Υπεύθυνο Ασφάλειας Πληροφορίας.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών εξουσιοδοτείται να πραγματοποιεί έκτακτους ελέγχους προκειμένου να διαπιστώσει αν ο εξοπλισμός βρίσκεται στην προβλεπόμενη θέση καθώς και αν έχει εισαχθεί και εγκατασταθεί μη εγκεκριμένος εξοπλισμός από το προσωπικό.

Επιπλέον όλοι οι εργαζόμενοι θα πρέπει να εφαρμόζουν την πολιτική καθαρού γραφείου – καθαρής οθόνης:

- Η οθόνη του χρήστη δε θα είναι ορατή από τρίτους και ο χρήστης δε θα εισάγει συνθηματικά ενώ παρακολουθείται από τρίτους

- Ο υπολογιστής θα κλειδώνει αυτόματα μετά τη παρέλευση 10 λεπτών.

- Ο υπολογιστής θα κλειδώνει αυτόματα μετά τη παρέλευση 10 λεπτών.

- Ο χρήστης θα αποσυνδέεται από το σύστημα και θα τακτοποιεί το γραφείο του όποτε εγκαταλείπει την εργασία του.

- Δε θα καταγράφεται ευαίσθητη πληροφορία σε χαρτιά ή άλλα μέσα αποθήκευσης τα οποία βρίσκονται εκτεθειμένα πάνω στο γραφείο του χρήστη. Μετά τη λήξη της εργασίας, όλα τα έντυπα θα τακτοποιούνται και θα κλειδώνονται ασφαλώς, σύμφωνα με την κατηγορία διαβάθμισής τους.

- Όλα τα έντυπα θα απομακρύνονται από τους εκτυπωτές, τα φαξ και τα φωτοαντιγραφικά μηχανήματα.

6.4.8. Επιχειρησιακή ασφάλεια

6.4.8.1. Επιχειρησιακές διαδικασίες και αρμοδιότητες

Κατά την πρόσληψή του, το προσωπικό θα ενημερώνεται για τις διαδικασίες χειρισμού του πληροφοριακού εξοπλισμού όπως:

- έναρξης και λήξης λειτουργίας υπολογιστών
- αποθήκευσης και χρήσης αρχείων
- αρχειοθέτησης που αφορά το προσωπικό
- χειρισμός σφαλμάτων και δυσλειτουργιών του εξοπλισμού
- χειρισμός μέσων αποθήκευσης
- χειρισμός λογισμικού.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών εγκρίνει κάθε αλλαγή στις υποδομές και τις υπηρεσίες της εταιρείας. Πριν από την υλοποίηση κάθε αλλαγής θα γίνεται εκτίμηση των πιθανών επιπτώσεων, τόσο από πλευράς Ασφάλειας όσο και ως προς τις πιθανές

επιπτώσεις στην εργασία του προσωπικού. Επιπλέον, θα καταρτίζεται σχέδιο ανάκαμψης σε περίπτωση αποτυχίας της αλλαγής. Ειδικά σε περίπτωση βασικής αλλαγής του συστήματος θα πρέπει να γίνεται αρχικά πλήρης δοκιμή σε πραγματικές συνθήκες (staging) και στη συνέχεια μετάβαση σε επιχειρησιακή λειτουργία (production).

Όλοι οι υπολογιστικοί πόροι της εταιρείας ελέγχονται από το Διαχειριστή του Συστήματος και η λειτουργία τους εγκρίνεται από τον Υπεύθυνο Ασφάλειας Πληροφοριών. Κάθε τροποποίηση του εξοπλισμού καθώς και η προμήθεια και εγκατάσταση νέου περνάει από την έγκριση του Υπευθύνου Ασφάλειας Πληροφοριών.

Επιπλέον, λαμβάνεται και η έγκριση της διοίκησης. Πριν την υλοποίηση κάθε αλλαγής, συμπληρώνεται το αρχείο έγκρισης αλλαγής και ενημερώνεται όλο το εμπλεκόμενο προσωπικό.

Για την αποφυγή αστοχιών των υποδομών της εταιρείας, θα γίνεται προσεκτικός σχεδιασμός των συστημάτων που υλοποιούνται και εγκαθίστανται. Κατά την ανάλυση απαιτήσεων προς τον προμηθευτή θα λαμβάνεται υπ' όψη η πρόβλεψη των μελλοντικών απαιτήσεων και αναγκών. Επιπλέον, θα ζητείται η ρύθμιση και πλήρης προσαρμογή των νέων συστημάτων και υπηρεσιών προς τις υπάρχουσες ώστε να βελτιστοποιείται η απόδοση της εργασίας και να μην υπάρχουν ασυμβατότητες.

Ο Διαχειριστής συστημάτων ελέγχει σε εβδομαδιαία βάση ότι η επάρκεια των πληροφοριακών υποδομών της εταιρείας είναι σε αποδεκτό επίπεδο, εξετάζοντας στους κρίσιμους εξυπηρετητές:

- Στοιχεία χρήσης CPU και μνήμης
- Στοιχεία χρήσης μέσων αποθήκευσης – διαθέσιμος ελεύθερος χώρος και ρυθμός αύξησης.
- Καταγραφές και logs που ενδέχεται να υποδηλώνουν προβλήματα επάρκειας.

Σε περίπτωση οριακής χρήσης γίνονται οι εξής ενέργειες:

- Διαγραφή άχρηστων δεδομένων (για εξοικονόμηση χώρου).
- Απενεργοποίηση εφαρμογών, συστημάτων, βάσεων δεδομένων ή ολόκληρων περιβαλλόντων.
- Βελτιστοποίηση των διαδικασιών batch καθώς και του προγραμματισμού.
- Βελτιστοποίηση της λογικής των εφαρμογών και των ερωτημάτων στις βάσεις δεδομένων.

- Άρνηση ή περιορισμός στην εξυπηρέτηση διαδικασιών (services) που δεν είναι κρίσιμες για την εταιρία και οι οποίες καταναλώνουν μεγάλο εύρος ζώνης (bandwidth).

Σε περίπτωση αποτυχίας των παραπάνω γίνεται αναβάθμιση των συστημάτων.

Επιπλέον μέσω αυτοματοποιημένου λογισμικού παρακολούθησης γίνεται συνεχής έλεγχος της επάρκειας και διαθεσιμότητας των συστημάτων και ενημερώνεται άμεσα ο Διαχειριστής για οποιοδήποτε συμβάν.

Κάθε ανάπτυξη γίνεται σε περιβάλλον εκτός παραγωγής το οποίο θα πρέπει να προσομοιάζει το πραγματικό, χωρίς όμως να φέρει πραγματικά στοιχεία πελατών. Μόνο όταν εξασφαλιστεί ή πλήρης λειτουργικότητα των εφαρμογών εγκρίνεται η μεταφορά τους στους υπολογιστές της παραγωγής. Η απαίτηση αυτή ισχύει τόσο για εσωτερική ανάπτυξη της εταιρείας όσο και εξωτερικούς συνεργάτες και υπεργολάβους.

6.4.8.2. Προστασία από κακόβουλο λογισμικό

Στα πλαίσια προστασίας από κακόβουλο και μη ελέγξιμο λογισμικό, οι χρήστες απαγορεύεται να εγκαθιστούν και να χρησιμοποιούν λογισμικό που δεν έχει εγκριθεί και αγοραστεί νόμιμα από την εταιρεία. Επιπλέον κάθε υπολογιστής εκτελεί λογισμικό που προστατεύει από ιούς και κακόβουλο κώδικα (antivirus, anti-spyware, κλπ.), το οποίο μάλιστα ενημερώνεται συχνά και αυτομάτως. Το λογισμικό αυτό ελέγχει όλα τα εισερχόμενα και εξερχόμενα αρχεία από τον υπολογιστή, είτε αυτά διακινούνται μέσω δικτύου, Internet, ιστοσελίδων, e-mail ή φορητών μέσων αποθήκευσης. Επιπλέον, έχει εγκατασταθεί κονσόλα κεντρικής διαχείρισης του λογισμικού που προστατεύει από ιούς, μέσω του οποίου ελέγχεται η συχνή ενημέρωση των εκδόσεων στους επιμέρους υπολογιστές και τηρείται αρχείο των ιών που έχουν εντοπιστεί.

6.4.8.3 Αρχειοθέτηση

Η διαδικασία της αρχειοθέτησης – λήψης αντιγράφων ασφάλειας (backup) αποτελεί αναγνωρισμένο κομβικό σημείο για τη διασφάλιση της διαθεσιμότητας της πληροφορίας και την ταχεία επαναφορά της επιχειρησιακής λειτουργίας σε περίπτωση

καταστροφής. Για το σκοπό αυτό, η εταιρεία εφαρμόζει την ακόλουθη πολιτική χειρισμού αρχείων και λήψης backup:

- Οι χρήστες δεν πρέπει να αποθηκεύουν ευαίσθητα και σημαντικά δεδομένα τους στους τοπικούς υπολογιστές αλλά σε εγκεκριμένες από τον Υπεύθυνο Ασφάλειας Πληροφορίας θέσεις στον εξυπηρετητή αρχείων. Το βέλτιστο σενάριο είναι να μην αποθηκεύεται τίποτα στον τοπικό σκληρό δίσκο, αλλά να αποθηκεύονται στο δίκτυο της εταιρείας ώστε να μην καταστραφούν τα αρχεία σε περίπτωση καταστροφής του υπολογιστή
- Τα backup εκτελούνται τις βραδινές ώρες ενώ η πλειοψηφία του προσωπικού δεν εργάζεται στους υπολογιστές του.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών τηρεί καταγεγραμμένο πρόγραμμα αρχειοθέτησης, όπου αναλύονται τα αρχεία που αρχειοθετούνται, η συχνότητα backup και τα μέσα αποθήκευσης που χρησιμοποιούνται.

Τα εβδομαδιαίο backup αποθηκεύονται στο πυρίμαχο χρηματοκιβώτιο με ευθύνη της διοίκησης. Ο διαχειριστής του συστήματος ή σε περίπτωση απουσίας του, το εξουσιοδοτημένο προσωπικό είναι υπεύθυνοι για την συνεχή αντικατάσταση των εβδομαδιαίων backup.

Τα ημερήσια backup αποθηκεύονται σε σκληρό δίσκο (Virtual Tape Library), ο οποίος βρίσκεται σε σύστημα αντιγράφων ασφαλείας (backup) εντός του computer room.

Το πρόγραμμα του backup θα πρέπει να υπάρχει εντός του Διακομιστή Αντιγράφων Ασφαλείας (Backup server).

Καθημερινά, ο Διαχειριστής του Συστήματος ενημερώνεται με email από το λογισμικό του backup για την ορθή ή μη λειτουργία του backup.

Η διαθεσιμότητα των δεδομένων που βρίσκονται αποθηκευμένα σε κάθε μέσο αποθήκευσης (σκληρός δίσκος, CD, δισκέτα, κασέτα, κοκ) δε θα πρέπει να θεωρείται δεδομένη καθώς τα μέσα σταδιακά αλλοιώνονται και καταστρέφονται. Για το λόγο αυτό:

- Θα γίνεται τακτικός έλεγχος των μέσων και των συσκευών εγγραφής για φθορά και γήρανση.
- Θα γίνεται φύλαξη τους σε θέσης χαμηλής υγρασίας και μη μεταβαλλόμενης θερμοκρασίας.
- Σε τακτική βάση θα γίνεται δοκιμή ανάκτησης των δεδομένων (restore), η οποία καταγράφεται.

6.4.8.4. Καταγραφή και παρακολούθηση

Τα αρχεία παρακολούθησης ενεργειών (event logs) αποτελούν καίριο εργαλείο στα χέρια του διαχειριστή του συστήματος και του Υπευθύνου Ασφάλειας Πληροφοριών. Τα αρχεία θα περιέχουν τις ακόλουθες πληροφορίες, όπου απαιτούνται και είναι τεχνικά εφικτό:

- Όνομα χρήστη που εκτελεί την ενέργεια
- Η ενέργεια που έγινε
- Η ημερομηνία, η ώρα και η περιγραφή της ενέργειας
- Συσκευή (π.χ. όνομα υπολογιστή) από την οποία έγινε η ενέργεια
- Οι επιτυχημένες και αποτυχημένες προσπάθειες πρόσβασης στο σύστημα και τα δεδομένα
- Οι αλλαγές στις ρυθμίσεις των συστημάτων
- Αλλαγές στα δικαιώματα των χρηστών
- Αλλαγές στις ρυθμίσεις των logs
- Κάθε λάθος (error, warning, exception) που προκύπτει από την εκτέλεση των εφαρμογών
- Κάθε συμβάν που προκύπτει από αυτοματοποιημένες διαδικασίες προστασίας (π.χ. anti-virus, firewall κλπ.).
- Οι συνδέσεις και οι ενέργειες του διαχειριστή
- Η ενεργοποίηση και η απενεργοποίηση των συστημάτων που εμπλέκονται στην ασφάλεια και την προστασία (π.χ. antivirus, IDS/IPS κλπ.)
- Καταγραφές των ενεργειών που έκαναν οι χρήστες μιας εφαρμογής.

Λόγω της πληθώρας των συλλεγόμενων πληροφοριών, τα αρχεία ενεργειών αποτελούν και αυτά ευαίσθητα δεδομένα και έτσι θα πρέπει να είναι προσβάσιμα μόνο από το διαχειριστή του συστήματος και τον Υπεύθυνο Ασφάλειας Πληροφοριών. Επιπλέον, απαγορεύεται να απενεργοποιούνται ακόμα και από το διαχειριστή του συστήματος, ενώ θα αρχειοθετούνται για διάστημα τουλάχιστον 12 μηνών.

Τα logs συγκεντρώνονται σε σύστημα SIEM (Security Information & Event Management), ελέγχονται σε συνεχή βάση, αναλύονται και εντοπίζονται όλα τα καταγεγραμμένα σφάλματα καθώς και κάθε «ύποπτη» δραστηριότητα. Κάθε σφάλμα θα πρέπει να υφίσταται την απαραίτητη αντιμετώπιση, ενώ κάθε περιστατικό (ή παρ' ολίγον

περιστατικό) ασφάλειας καταγράφεται σύμφωνα με τη σχετική διαδικασία και λαμβάνονται οι απαραίτητες διορθωτικές και προληπτικές ενέργειες.

Ο χρόνος τήρησης των Logs είναι 365 ημέρες στο storage.

Τηρούνται τοπικά στα μηχανήματα και συγκεντρώνονται στον SIEM server.

Ο ΥΑΠ σε 3μηνιαία βάση επιθεωρεί τα logs ή όποτε παραστεί ανάγκη διερεύνησης κάποιου συμβάντος.

Προκειμένου να αποφευχθούν δικτυακές επιθέσεις (π.χ. τύπου replay) στους υπολογιστές του δικτύου, τα ρολόγια όλων των υπολογιστών είναι πάντα συγχρονισμένα, είτε με χρήση της διαδικασία του Microsoft Active Directory (όπου συγχρονίζονται με τον Domain Controller), καθώς και με NTP Proxy της εταιρείας.

6.4.8.5. Έλεγχος του επιχειρησιακού λογισμικού

Δεδομένου ότι το λειτουργικό σύστημα αποτελεί τον πυρήνα λειτουργίας κάθε υπολογιστή, απαιτείται η προστασία του από μη εξουσιοδοτημένες ή μη σχεδιασμένες αλλαγές. Το ίδιο ισχύει και για τα υπόλοιπα λογισμικά που χρησιμοποιεί η εταιρία. Σύμφωνα με την Πολιτική Ασφαλείας της εταιρείας, δικαίωμα εγκατάστασης νέων εφαρμογών έχει μόνο ο διαχειριστής των συστημάτων.

Ο διαχειριστής πριν από κάθε σημαντική αλλαγή στα συστήματα καταστρώνει στρατηγική επαναφοράς του συστήματος, σε περίπτωση που αυτή αποτύχει.

Ο διαχειριστής μαζί με τον Υπεύθυνο Ασφάλειας Πληροφοριών, παρακολουθεί τυχόν ενημερώσεις που ανακοινώνουν οι κατασκευαστές των λογισμικών που χρησιμοποιεί η εταιρία. Η πρόσβαση (φυσική ή λογική) που δίνεται στους ανθρώπους που υποστηρίζουν συγκεκριμένα λογισμικά είναι απολύτως ελεγχόμενη και καταγραφόμενη μέσω logs. Αν λήξει η υποστήριξη κάποιας έκδοσης λογισμικού από τον κατασκευαστή του, γίνεται πρόταση στη διοίκηση για αναβάθμισή του στην επόμενη έκδοση.

6.4.8.6. Διαχείριση τεχνικών αδυναμιών

Χάρη στους πίνακες πόρων, αδυναμιών και κινδύνων ο Υπεύθυνος Ασφάλειας Πληροφοριών μπορεί να προβεί στον εντοπισμό τεχνικών αδυναμιών που ενδέχεται να εμφανιστούν και να υποβαθμίσουν τις απαιτήσεις Ασφάλειας του ΣΔΑΠ. Για τη διαχείριση των τεχνικών αδυναμιών, μετά τον εντοπισμό και την αξιολόγησή τους, θα προγραμματίζεται η απαραίτητη διορθωτική ενέργεια. Μετά την υλοποίηση αυτής, ο Υπεύθυνος Ασφάλειας Πληροφοριών θα επανεκτιμά αν και κατά πόσον ο κίνδυνος έχει αντιμετωπιστεί επιτυχώς ή αν θα πρέπει να γίνει αποδεκτός.

Για την έγκαιρη αντιμετώπιση των αδυναμιών που εντοπίζονται σε υπολογιστές με λειτουργικά συστήματα Windows, η εταιρεία έχει εγκαταστήσει Windows Services Update Server, μέσω του οποίου όλα τα τερματικά λαμβάνουν άμεσα και εγκαίρως όλες τις ενημερώσεις που εκδίδονται από τη Microsoft και εγκρίνονται από το Διαχειριστή των συστημάτων. Κρίσιμα συστήματα και εξυπηρετητές ρυθμίζονται ώστε να μην εγκαθιστούν αυτόματα τις ενημερώσεις αλλά κατόπιν ελέγχου τους από το Διαχειριστή των συστημάτων.

6.4.9. Ασφάλεια επικοινωνιών

6.4.9.1. Διαχείριση ασφάλειας δικτύου

Η εκτενής χρήση εσωτερικής δικτύωση μέσα στην εταιρεία αλλά και η ανάγκη διασύνδεσης με το Internet καθιστούν επιτακτική την ανάγκη υψηλού βαθμού ελέγχου της διακινούμενης πληροφορίας και τη λήψη όλων των απαραίτητων μέτρων Ασφάλειας. Η σύνδεση με το εξωτερικό δίκτυο διέρχεται μέσω συστημάτων Ασφάλειας UTM Firewall με access lists καθώς και σύγχρονων routers και switches έτσι ώστε να ελαχιστοποιείται ο κίνδυνος παράνομης εισόδου ή διακοπής της πρόσβασης λόγω βλάβης.

Για το σκοπό αυτό η εταιρεία έχει προμηθευτεί τελευταίας τεχνολογίας συστήματα firewall και έχει οργανώσει το δίκτυό της σε διάταξη ζωνών (εσωτερική ζώνη, ζώνη επισκεπτών, DMZ και άλλες). Τέλος, λειτουργεί ειδικό λογισμικό και υλικό ανάλυσης της κίνησης του δικτύου και ανίχνευσης πιθανών επιθέσεων και κενών Ασφάλειας.

Οι ισχύουσες ρυθμίσεις του firewall τηρούνται και σε αρχείο εκτός του μηχανήματος και τροποποιούνται μόνο κατόπιν ελέγχου και έγκρισης του Υπευθύνου Ασφάλειας Πληροφοριών. Επιπλέον, τηρούνται και οι παλαιότερες ρυθμίσεις σε έντυπη μορφή και φέρουν τη σήμανση ΑΚΥΡΟ.

Οι προσφερόμενες δικτυακές υπηρεσίες (π.χ. email, διασύνδεση χρηστών εκτός εταιρείας) γίνεται με χρήση κρυπτογραφημένων πρωτοκόλλων SSL, τεχνολογιών VPN και username/ password για την αποφυγή μετάδοσης μη κρυπτογραφημένης πληροφορίας). Όλες οι συνδέσεις των χρηστών καταγράφονται σε αρχεία (logs) και υφίστανται περιοδικό έλεγχο. Καμία σύνδεση VPN δεν παραμένει ανοιχτή, εκτός αυτή του Υπευθύνου Ασφάλειας Πληροφορίας. Η πρόσβαση ανοίγει έπειτα από αίτημα του συνεργάτη και έγκριση από τον Υπεύθυνο Ασφάλειας Πληροφορίας.

6.4.9.2. Διακίνηση πληροφοριών

- **Ηλεκτρονικό ταχυδρομείο (email)**

Το email αποτελεί εργαλείο δουλειάς για ανταλλαγή μη ευαίσθητων δεδομένων μόνο μεταξύ εμπορικά συναλλασσόμενων μερών και σε καμία περίπτωση δεν αποτελεί εργαλείο προσωπικής χρήσης ή ασφαλές μέσον επικοινωνίας. Απαγορεύεται αυστηρά η χρήση του για ανταλλαγή πληροφοριών που δε σχετίζονται με τη λειτουργία της εταιρείας.

Το email διέπεται από όρους χρήσης τους οποίους

- Αποδέχεται ο χρήστης κατά την πρόσληψη του
- Αποδέχεται κατά τη χρήση της υπηρεσίας
- Αναγράφει στη διακινούμενη πληροφορία (π.χ. υπογραφή email, fax).

Τα δεδομένα που αποστέλλονται μέσω ηλεκτρονικού ταχυδρομείου είναι εκείνα για τα οποία επιτρέπεται η ηλεκτρονική διακίνηση.

- **Fax, φωτοτύπηση, εκτύπωση**

Οι συσκευές τηλεομοιοτυπίας, εκτύπωσης και παραγωγής φωτοαντιγράφων, θα πρέπει να βρίσκονται σε ελεγχόμενους χώρους, προσβάσιμους από εξουσιοδοτημένο προσωπικό. Η εκτύπωση, σήμανση και διακίνηση έντυπου υλικού βασίζεται στους κανόνες διαβάθμισης της παραγράφου 6.4.4.2.

Τα πρωτότυπα έγγραφα δε θα πρέπει να μένουν στα μηχανήματα. Επίσης, τα εκτυπωμένα έγγραφα θα πρέπει να απομακρύνονται σε συνεχή βάση. Οι όροι χρήσης του εξοπλισμού θα πρέπει να βρίσκονται αναρτημένοι παραπλεύρως από κάθε σχετική συσκευή. Ο Υπεύθυνος Ασφάλειας Πληροφοριών θα επιθεωρεί τακτικά τα σχετικά μηχανήματα και θα εκπαιδεύει το προσωπικό.

Ειδικά για τις συσκευές φαξ, λόγω του κινδύνου επανεκτύπωσης του απεσταλμένου υλικού από τη μνήμη αποθήκευσης και τη σημαντική πιθανότητα λάθους πληκτρολόγησης του αριθμού του αποστολέα θα πρέπει να γίνεται περιορισμένη χρήση και πάντα αποστολή εγγράφων χαμηλής διαβάθμισης. Επίσης, επισημαίνεται ότι σε περίπτωση αποτυχίας μετάδοσης, πολλές συσκευές εκτυπώνουν αντίγραφο του πρωτότυπου εγγράφου.

Καταστροφείς εγγράφων βρίσκονται εγκατεστημένοι σε καθορισμένες θέσεις πλησίον των συσκευών αναπαραγωγής εντύπων.

- **Τηλεφωνική επικοινωνία**

Η τηλεφωνική επικοινωνία αποτελεί ανταλλαγή δεδομένων και μάλιστα πάνω από μη προστατευμένα κανάλια. Το προσωπικό θα πρέπει να μην αποκαλύπτει προστατευμένα δεδομένα στο τηλέφωνο καθώς:

- η ταυτότητα του συνομιλητή δεν μπορεί να διασφαλιστεί
- υπάρχει πιθανότητα υποκλοπής της συνομιλίας
- υπάρχει πιθανότητα συνακρόασης από προσωπικό ή πελάτες που βρίσκονται κοντά στον ομιλητή.

Επιπλέον, δε θα πρέπει να αφήνει μηνύματα με ευαίσθητες πληροφορίες σε υπηρεσίες τηλεφωνητή.

- **Web/Instant Messaging**

Η πρόσβαση στο Web καθώς και όλες τις άλλες διαδικτυακές υπηρεσίες επιτρέπεται μόνο στα πλαίσια των εταιρικών υποχρεώσεων του προσωπικού. Απαγορεύεται η χρήση της για προσωπικούς λόγους. Δεδομένου ότι πολλές ιστοσελίδες

επιτρέπουν την ανταλλαγή ηλεκτρονικής πληροφορίας (ανέβασμα / κατέβασμα αρχείων) ισχύουν τα προβλεπόμενα από την παράγραφο 6.4.4.2. για τη διαβαθμισμένη πληροφορία.

Η χρήση ιστοσελίδων κοινωνικής δικτύωσης (π.χ. facebook) και υπηρεσιών streaming (audio/video) επιτρέπεται μόνο στα πλαίσια των εταιρικών υποχρεώσεων του προσωπικού.

- **Διασύνδεση με τρίτα συστήματα**

Τέλος, σε περίπτωση που υφίσταται ή πρόκειται να υλοποιηθεί διασύνδεση των πληροφοριακών συστημάτων της εταιρείας με τρίτα συστήματα θα γίνεται συνεχής έλεγχος της διακινούμενης πληροφορίας μέσω αρχείων (logs) και θα διασφαλίζεται η συμμόρφωση των διασυνδεμένων μελών με τις απαιτήσεις της Πολιτικής Ασφάλειας της εταιρείας. Οι υπεύθυνοι λειτουργίας των τρίτων συστημάτων θα ενημερώνονται εκ των προτέρων για την Πολιτική Ασφάλειας Πληροφοριών της εταιρείας από τον Υπεύθυνο Ασφάλειας Πληροφοριών.

6.4.10. Προμήθεια, ανάπτυξη και συντήρηση πληροφοριακών συστημάτων

6.4.10.1. Απαιτήσεις ασφάλειας πληροφοριακών συστημάτων

Για κάθε νέο έργο, ο Υπεύθυνος Ασφάλειας Πληροφοριών θα ενημερώνει τους εμπλεκόμενους για την ισχύουσα Πολιτική Ασφάλειας Πληροφοριών και θα εξετάζει ότι αυτή καλύπτεται πλήρως από τις σχεδιαστικές απαιτήσεις και την αρχιτεκτονική των συστημάτων. Για κάθε προσφερόμενη υπηρεσία τηρούνται τεκμηριωμένες λειτουργικές και τεχνικές προδιαγραφές, οι οποίες περιλαμβάνουν τις απαιτήσεις Ασφάλειας Πληροφοριών που διέπουν την υπηρεσία.

Κατά την προμήθεια τυποποιημένου λογισμικού και υλικού (Commercial Off-The-Shelf / COTS) θα γίνεται έλεγχος καταλληλότητας και συμμόρφωσης με τις απαιτήσεις Ασφάλειας πληροφορίας της εταιρείας.

Η πρόσβαση στις ηλεκτρονικές υπηρεσίες που παρέχει η εταιρεία γίνεται μόνο από εξουσιοδοτημένους χρήστες/ πελάτες στους οποίους έχει δοθεί προσωπικός

κωδικός πρόσβασης. Η χρήση των υπηρεσιών γίνεται μέσα από καθορισμένο και ασφαλές δικτυακό περιβάλλον (κρυπτογραφημένη ιστοσελίδα HTTPS/SSL). Οι όροι που διέπουν τη χρήση της υπηρεσίας γνωστοποιούνται στους χρήστες μέσω της σχετικής σύμβασης αδειοδότησης καθώς και κατά την πρώτη είσοδό τους στην εφαρμογή.

Το περιεχόμενο της εταιρικής ιστοσελίδας εγκρίνεται πάντοτε από τη διοίκηση και η ενημέρωση της ιστοσελίδας γίνεται από το αρμόδιο προσωπικό. Η διασφάλιση της απρόσκοπτης λειτουργίας της ιστοσελίδας διασφαλίζεται μέσω αυτοματοποιημένων ελέγχων, που επιτρέπουν την άμεση αναγνώριση αλλοιώσεων στο περιεχόμενο ή μη διαθεσιμότητας της σελίδας.

Επισημαίνεται ότι σε καμία περίπτωση δε θα δημοσιεύονται ελεγχόμενα δεδομένα και κάθε αλλαγή στο περιεχόμενο θα εγκρίνεται από τη διοίκηση της εταιρείας, είτε εγγράφως είτε με email.

6.4.10.2. Ασφάλεια στις διαδικασίες ανάπτυξης και υποστήριξης

Για κάθε εφαρμογή που σχεδιάζεται και υλοποιείται από εξωτερικούς συνεργάτες, η εταιρεία απαιτεί τα εξής, πέραν των διεθνών πρακτικών για το σχεδιασμό και την ανάλυση εφαρμογών λογισμικού θα πραγματοποιούνται τα εξής πρόσθετα βήματα:

1. Ανάλυση Επικινδυνότητας: η ομάδα προγραμματιστών σε συνεργασία με το Διαχειριστή των Συστημάτων και τον Υπεύθυνο Ασφάλειας Πληροφοριών εξετάζει τα ήδη των πληροφοριών που θα διαχειρίζεται η εφαρμογή, τις αδυναμίες που μπορεί να διαθέτει η εφαρμογή, τις εσωτερικές και εξωτερικές απειλές της εφαρμογής και το συνολικό επίπεδο έκθεσης σε κινδύνους. Στόχος είναι ο εντοπισμός των αναγκαίων μέτρων ασφαλείας που πρέπει να τεθούν σε εφαρμογή κατά την ανάπτυξη και επιχειρησιακή λειτουργία της εφαρμογής.

2. Αρχιτεκτονική Ασφάλειας: Κατά το συνολικό σχεδιασμό της εφαρμογής, η ομάδα ανάπτυξης συνεργάζεται με τον Υπεύθυνο Ασφάλειας Πληροφοριών και προβαίνει στις εξής ενέργειες:

- Μελέτη εναλλακτικών αρχιτεκτονικών ασφαλείας και προσδιορισμός δυνατών και αδύνατων σημείων
- Εκτίμηση συμβατότητας των αρχιτεκτονικών με υφιστάμενα συστήματα της εταιρείας
- Εκτίμηση του κόστους για την κάλυψη των απαιτήσεων ασφαλείας

- Τελική επιλογή αρχιτεκτονικής.

Κατά το σχεδιασμό του λογισμικού θα εξετάζονται όλα τα πιθανά σενάρια δεδομένων εισόδου με έμφαση στις λανθασμένες καταχωρήσεις που μπορεί να γίνουν είτε κατά λάθος ή τυχαία από το προσωπικό, είτε λόγω αστοχίας εξοπλισμού, είτε κακόβουλα. Θα επιβεβαιώνεται ότι υπάρχουν μηχανισμοί ελέγχου και επικύρωσης των δεδομένων εισόδου. Απαραίτητα θα ελέγχονται:

- Τιμές εκτός ορίων
- Άκυροι χαρακτήρες σε πεδία εισόδου
- Ελλιπή δεδομένα
- Μέγεθος πεδίων εκτός προδιαγραφών
- Πρόσβαση από μη εξουσιοδοτημένα μέρη.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών ελέγχει ο ίδιος ή ζητά από τους προγραμματιστές να επαληθεύουν τις διαδικασίες επεξεργασίας των πληροφοριών, να διασφαλίζουν τη σωστή λειτουργία τους ακόμα και σε περίπτωση κακής χρήσης και ότι τα αποτελέσματά τους είναι πάντοτε εντός των προδιαγραφών και σχεδιαστικών απαιτήσεων. Σε περίπτωση σφάλματος, οι εφαρμογές εμφανίζουν σχετικά ενημερωτικά μηνύματα και να καταγράφουν τις συνθήκες που οδήγησαν στο σφάλμα σε σχετικό αρχείο ενεργειών, το οποίο μελετάται από τον Υπεύθυνο Ασφάλειας Πληροφοριών.

Πριν την επιχειρησιακή λειτουργία των εφαρμογών γίνεται επικύρωση της λειτουργίας τους με έλεγχο αληθοφάνειας και εγκυρότητας των δεδομένων εξόδου και προσομοίωση με πραγματικά δεδομένα, όπου αυτό απαιτείται.

Κάθε λογισμικό που λειτουργεί εντός της εταιρείας ικανοποιεί τη θεμελιώδη απαίτηση της Πολιτικής Ασφάλειας Πληροφοριών για ιχνηλασιμότητα των εκτελούμενων διαδικασιών: κάθε πληροφορία που εισάγεται, υφίσταται επεξεργασία, τροποποιείται ή διαγράφεται θα πρέπει να φέρει το αναγνωριστικό του χρήστη που πραγματοποίησε την επεξεργασία και φυσικά να είναι προσβάσιμη και επεξεργάσιμη μόνο από εξουσιοδοτημένους χρήστες. Επιπλέον, λαμβάνονται υπόψη θέματα ταυτόχρονης πρόσβασης και επεξεργασίας από περισσότερους του ενός χρήστες.

Πριν την επιχειρησιακή λειτουργία των εφαρμογών θα γίνεται επικύρωση της λειτουργίας τους με έλεγχο αληθοφάνειας και εγκυρότητας των δεδομένων εξόδου και προσομοίωση με πραγματικά δεδομένα, όπου φυσικά αυτό απαιτείται. Οι έλεγχοι θα περιλαμβάνουν:

- Δοκιμές σε επίπεδο μονάδας κώδικα (unit testing)
- Δοκιμές συστήματος (system/ integration testing)

- Δοκιμές αποδοχής από το χρήστη (user acceptance testing).

Πριν την οριστική παραλαβή των συστημάτων και υπηρεσιών θα γίνεται επαλήθευση

- της κάλυψης της απαιτούμενης απόδοσης και δυνατοτήτων
- των διαδικασιών χειρισμού σφαλμάτων και ανάκαμψης από αυτά
- της τήρησης όλων των προβλεπόμενων διαδικασιών Ασφάλειας και της συμμόρφωσης με το ΣΔΑΠ
- της ένταξης του νέου συστήματος στο σχέδιο ανάκαμψης από καταστροφή
- της παροχής ικανής εκπαίδευση στο προσωπικό.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών θα συντάσσει σχετική έκθεση αποδοχής του συστήματος.

Μετά την ολοκλήρωση της ανάπτυξης και των προβλεπόμενων ελέγχων σε δοκιμαστικό περιβάλλον, κάθε εφαρμογή θα μεταφέρεται στο παραγωγικό σύστημα με τρόπο που να διαφυλάσσει τη διαθεσιμότητα των υπηρεσιών. Με ευθύνη των προγραμματιστών θα υπάρχει πρόβλεψη rollback σε περίπτωση αστοχίας (π.χ. με λήψη backup πριν την αλλαγή/ αναβάθμιση). Σε περίπτωση compilation/build των εφαρμογών, αυτό θα γίνεται με χρήση σταθερών και αξιόπιστων βιβλιοθηκών σε σταθερή (stable έκδοση) με αφαίρεση παραμέτρων debug σε ασφαλές σύστημα, το οποίο θα χρησιμοποιείται μόνο για το σκοπό αυτό.

Όλοι οι παραγωγικοί εξυπηρετητές θα πρέπει να διασφαλίζονται με την τήρηση των εξής ελάχιστον κανόνων ενίσχυσης (hardening):

- Θα χρησιμοποιείται η πλέον πρόσφατη σταθερή έκδοση του λειτουργικού συστήματος με ενσωμάτωση όλων των ενημερώσεων ασφαλείας (updates/ patches).

- Το σύστημα θα διαθέτει τον ελάχιστο αναγκαίο αριθμό πακέτων, βιβλιοθηκών, εφαρμογών (minimum installation χωρίς γραφικό περιβάλλον) στα οποία θα προστίθεται ακριβώς και μόνο οι πρόσθετες εφαρμογές που προσδιορίζονται από την ομάδα ανάπτυξης, στην πλέον πρόσφατη σταθερή και ελεγμένη έκδοση.

- Η ενημέρωση των συστημάτων θα γίνεται με ευθύνη του Διαχειριστή και των προγραμματιστών ως εξής:

    - Πάντοτε θα γίνεται έλεγχος των ενημερώσεων σε δοκιμαστικό σύστημα (staging/ test) πριν την εγκατάστασή τους στο παραγωγικό σύστημα.

- Οι ενημερώσεις ασφαλείας θα εγκαθίστανται με προτεραιότητα το συντομότερο δυνατό μετά την ανακοίνωσή τους από τους προμηθευτές ή κατόπιν σχετικών ενημερώσεων ασφαλείας (Security Bulletins).
- Ενημερώσεις βελτιώσεων θα εγκαθίστανται σε τριμηνιαία βάση και μόνο αφού ελεγχθεί προσεκτικά ότι δεν εισάγουν ασυμβατότητες στις λειτουργικές εφαρμογές.

Κάθε αλλαγή σε υπάρχον λογισμικό της εταιρείας (καθ' όλη τη διάρκεια του κύκλου ζωής του) θα αιτείται προς το Διαχειριστή των συστημάτων της εταιρείας. Πριν την υλοποίηση του θα γίνεται λεπτομερής ανάλυση των κινδύνων που ενδεχομένως εισάγονται από τις αλλαγές καθώς και έλεγχος για συμμόρφωση με τις υφιστάμενες απαιτήσεις της Πολιτικής Ασφάλειας Πληροφοριών. Θα ακολουθεί επίσημη έγκριση από τον Υπεύθυνο Ασφάλειας Πληροφοριών και στη συνέχεια θα γίνεται η υλοποίηση τους. Πριν την ενσωμάτωση των αλλαγών στην παραγωγική λειτουργία θα γίνεται ενδελεχής δοκιμή του συστήματος και η τελική υλοποίηση θα λαμβάνει χώρα σε χρόνο και με τρόπο που να μην επηρεάζει τη συνολική λειτουργία της εταιρείας. Μετά την ενσωμάτωση θα γίνεται νέος έλεγχος και ανασκόπηση συμμόρφωσης με τις απαιτήσεις Ασφάλειας καθώς και ενημέρωση της σχετικής τεκμηρίωσης.

Δεδομένου ότι αλλαγές σε λογισμικό που βρίσκεται ήδη σε χρήση, παρά τις διαδικασίες που αναφέρθηκαν, ενδέχεται να έχει απρόβλεπτες συνέπειες, θα καταβάλλεται κάθε προσπάθεια ώστε το λογισμικό που αγοράζεται να είναι εξαρχής επαρκές και προσαρμοσμένο κατάλληλα από τον προμηθευτή του.

Ιδιαίτερη προσοχή δίνεται σε αλλαγές που αφορούν το λειτουργικό σύστημα (ενημερώσεις – updates). Η αλλαγή γίνεται πρώτα σε δοκιμαστικό (staging) σύστημα και αφού διαπιστωθεί η σωστή λειτουργία των κρίσιμων εφαρμογών της εταιρείας και η μη δημιουργία προβλημάτων στην ασφάλεια, τότε γίνεται η εφαρμογή της αλλαγής και στο παραγωγικό σύστημα.

Στα πλαίσια αποφυγής διαρροών πληροφορίας, κάθε νέο λογισμικό που εγκαθίσταται θα τίθεται υπό παρακολούθηση για συγκεκριμένη χρονική περίοδο (1-6 μήνες ανάλογα με το είδος του) ώστε να εξασφαλιστεί ότι δεν αποστέλλει ή αποθηκεύει πληροφορίες σε μη εγκεκριμένες θέσεις.

Πριν την οριστική εγκατάσταση του λογισμικού θα διευθετούνται θέματα

- πνευματικών δικαιωμάτων και ιδιοκτησίας του πηγαίου κώδικα
- κάλυψης των ορισθέντων απαιτήσεων και εξασφάλισης ποιότητας εργασίας
- διαδικασιών χειρισμού σφαλμάτων και προβλημάτων

- ελέγχου για κακόβουλο λογισμικό

Σε περίπτωση κατάργησης εφαρμογής ή συστήματος, ο Διευθύνων Σύμβουλος αποφασίζει αν απαιτείται μερική ή ολική διατήρηση των δεδομένων που περιέχονται σε αυτό με βάση νομικές/ συμβατικές ή κανονιστικές απαιτήσεις. Ο Διαχειριστής του Συστήματος αποφασίζει το βέλτιστο τρόπο αρχειοθέτησης (σε εξυπηρετητή, σε συμπιεσμένη μορφή/ backup ή σε εξωτερικό μέσο) και προχωρά σε συνεργασία με την ομάδα προγραμματιστών στην απόσυρση του συστήματος και των δεδομένων.

Αν δεν απαιτείται, τα δεδομένα της εφαρμογής τα οποία βρίσκονται σε βάσεις δεδομένων, εξυπηρετητές, μαγνητικά ή οπτικά μέσα καταστρέφονται από το Διαχειριστή του Συστήματος και με ευθύνη του Υπεύθυνου Ασφάλειας Πληροφοριών. Η διαγραφή γίνεται σύμφωνα με τις προβλέψεις της Πολιτικής Χρήσης Μέσων Αποθήκευσης.

6.4.11. Σχέσεις με τους προμηθευτές

6.4.11.1. Ασφάλεια πληροφοριών στις σχέσεις με τους προμηθευτές

Πέραν των εσωτερικών λειτουργιών της εταιρείας, που είναι υπό τον άμεσο έλεγχο της Διοίκησης και του ΣΔΑΠ, μεγάλο μέρος των καθημερινών δραστηριοτήτων της σχετίζεται με εξωτερικά μέρη, συνεργάτες, προμηθευτές και πελάτες. Για τον έλεγχο των κινδύνων Ασφάλειας που εισάγει αυτή η αλληλεπίδραση, η εταιρεία εξετάζει με μεγάλη προσοχή, τη λαμβάνει υπόψη στη διαδικασία εκτίμησης κινδύνων Ασφάλειας Πληροφοριών και ρυθμίζει ανάλογα:

- τις εγκαταστάσεις στις οποίες έχει πρόσβαση ο εξωτερικός συνεργάτης ή πελάτης.

- το είδος της πρόσβασης που του παρέχει (φυσική, δικτυακή, λογική, απομακρυσμένη ή τοπική)

- την αξία και την ευαισθησία της πληροφορίας που εμπλέκεται

- τις διαδικασίες - εργασίες, τις απαιτήσεις καταγραφής ενεργειών και τις συμβάσεις ανάθεσης

- την εμπειρία του συνεργάτη και τις εσωτερικές του διαδικασίες για τον χειρισμό δεδομένων

- τις νομικές και ρυθμιστικές απαιτήσεις που διέπουν τη λειτουργία της
- την προστασία του συμφέροντος της εταιρείας

Χάρη στα συστήματα παρακολούθησης χώρου και ασφάλειας καθίσταται ταχεία η ανταπόκριση σε φαινόμενα κλοπής ή δολιοφθοράς.

Κάθε προμηθευτής και εξωτερικός συνεργάτης ενημερώνεται για την Πολιτική Ασφάλειας Πληροφοριών που τηρεί η εταιρεία και που οφείλει να διέπει και τη συνεργασία μεταξύ αυτού και της εταιρείας. Πριν τη σύναψη και την εκτέλεση κάθε έργου εξετάζεται από τον Υπεύθυνο Ασφάλειας Πληροφοριών η πιθανή αλληλεπίδραση του συνεργάτη με τα ελεγχόμενα δεδομένα της εταιρείας, τα αναγκαία μέτρα ελέγχου πρόσβασης και προστασίας καθώς και οι απαραίτητοι όροι στις συμβάσεις. Επιπλέον ορίζονται με σαφήνεια οι διαδικασίες παροχής των υπηρεσιών και συγκεκριμένα:

- η διαδικασία έγκρισης και υλοποίησης αλλαγών στα υπάρχοντα συστήματα
- η παροχή τεκμηρίωσης
- η αποδεδειγμένη συμβατότητα με το ΣΔΑΠ.
- τα ποσοτικά και ποιοτικά κριτήρια αξιολόγησης του παρεχόμενου έργου.
- το δικαίωμα της εταιρείας σε περιοδική επιθεώρηση και έλεγχο όλων των δραστηριοτήτων που εμπλέκουν πληροφοριακούς της πόρους
- η βιωσιμότητα των υπηρεσιών και η παροχή εγγυήσεων καλής λειτουργίας και υποστήριξης
- τα δικαιώματα χρήσης των προκυπτόντων προϊόντων και υπηρεσιών.

Τα παραπάνω αναλύονται διεξοδικά στις επιμέρους παραγράφους του παρόντος εγγράφου.

Ιδιαίτερη βαρύτητα δίνεται στην προμήθεια τηλεπικοινωνιακού εξοπλισμού και εξοπλισμού που αφορά ευαίσθητες πληροφορίες, καθώς και στις υπηρεσίες που αφορούν αυτά. Στον εξοπλισμό εκτός των ελέγχων που έχουν προαναφερθεί ελέγχονται επιπλέον:

- η αλυσίδα προμήθειας των υλικών ως προς τους όρους ασφάλειάς που έχουν επιβάλλει οι προμηθευτές μας στους δικούς τους προμηθευτές.

- η διασφάλιση ότι το προϊόν λειτουργεί όπως προδιαγράφεται, χωρίς την προσθήκη πρόσθετων ανεπιθύμητων λειτουργιών.

-η μη γνωστοποίηση από τους προμηθευτές σε τρίτους της προμήθειας του συγκεκριμένου εξοπλισμού.

6.4.11.2. Διαχείριση υπηρεσιών προσφερόμενων από προμηθευτές

Σε περίπτωση παροχής υπηρεσιών από τρίτους (εταιρείες καθαρισμού, ανάπτυξης λογισμικού, συμβούλων κοκ.) που προσλαμβάνονται άμεσα ή μέσω τρίτων, οι συμβάσεις θα περιέχουν και θα μεταφέρουν στους συνεργάτες όλες τις απαιτήσεις Ασφάλειας της εταιρείας που αφορούν τα συστήματα με τα οποία θα έρθουν σε επαφή.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών καθώς και ο επιβλέπων από την πλευρά της εταιρείας για την προσφερόμενη υπηρεσία θα παρακολουθούν σε συνεχή βάση τη συμμόρφωση του συνεργάτη με τις απαιτήσεις Ασφάλειας, θα καταγράφουν και θα χειρίζονται επιμελώς κάθε συμβάν Ασφάλειας και θα προβαίνουν σε όλες τις απαραίτητες διορθωτικές ενέργειες. Η εταιρεία έχει πλήρη επίγνωση του γεγονότος ότι ακόμα και σε περίπτωση υπεργολαβίας και υπηρεσίας προσφερόμενης από τρίτο, η τελική ευθύνη διαφύλαξης της ασφάλειας της πληροφορίας ανήκει στην εταιρεία. Για το σκοπό αυτό, ο Υπεύθυνος Ασφάλειας Πληροφοριών αναλαμβάνει επιπρόσθετα θα ενημερώνει κάθε τρίτο για νέες απαιτήσεις Ασφάλειας που προκύπτουν και να αιτείται χρήση όλων των απαιτούμενων υποστηρικτικών τεχνολογιών. Σε περίπτωση αδυναμίας του υπεργολάβου να συμμορφωθεί, η εταιρεία θα προβαίνει ακόμα και σε αλλαγή προμηθευτή για την κάλυψη των απαιτήσεων ασφάλειας.

6.4.12. Διαχείριση περιστατικών ασφάλειας πληροφοριών

Η διαδικασία περιγράφει τον εντοπισμό περιστατικών ασφαλείας από το προσωπικό της εταιρείας, την αξιολόγηση του από τον ΥΑΠ, τη συγκέντρωση σχετικών στοιχείων, τη λήψη μέτρων αντιμετώπισης καθώς και την εκτίμηση των συνεπειών αυτού.

Η διαδικασία αφορά όλους τους πόρους που εμπίπτουν στο πεδίο εφαρμογής του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών της εταιρείας.

- **Εντοπισμός περιστατικού ασφαλείας**

Όλοι οι εργαζόμενοι της εταιρείας καθώς και οι συνεργάτες – υπεργολάβοι, εφόσον εμπλέκονται σε εργασίες ή χειρίζονται πληροφορίες εντός του πεδίου εφαρμογής του ΣΔΑΠ, φέρουν την υποχρέωση να αναφέρουν άμεσα κάθε συμβάν ΑΠ ή περιστατικό ΑΠ ή άλλη αδυναμία ασφαλείας στον ΥΑΠ.

Ο ΥΑΠ ανταποκρίνεται, καταγράφοντας τα εξής στοιχεία:

- Ημερομηνία, ώρα και θέση όπου διαπιστώθηκε το συμβάν και συνθήκες εντοπισμού
- Εργαζόμενος που το ανέφερε
- Άλλοι εμπλεκόμενοι εργαζόμενοι ή τρίτοι
- Εξοπλισμός που επηρεάζεται
- Είδος συμβάντος
    - Διακοπή υπηρεσίας
    - Δυσλειτουργία υλικού/λογισμικού/επικοινωνιών
    - Σφάλμα χρήσης
    - Μη συμμόρφωση με το ΣΔΑΠ ή την Πολιτική ΑΠ
    - Παραβίαση πρόσβασης
    - Καταστροφή εξοπλισμού
    - Άλλη αδυναμία ασφαλείας

Κάθε αναφορά συμβάντος θα πρέπει να είναι χρονολογημένη και να καταγράφει ακριβώς τι συνέβη, ποιος το διαπίστωσε και αν υπήρχαν άλλοι μάρτυρες. Επίσης θα πρέπει να βεβαιώνεται η κανονική κατάσταση λειτουργίας προ του συμβάντος, στο βαθμό που αυτό είναι δυνατό.

- **Αξιολόγηση περιστατικού ασφαλείας**

Ο ΥΑΠ προβαίνει σε άμεσο έλεγχο του συμβάντος και στη λήψη όλων των απαραίτητων μέτρων για τον περιορισμό των απωλειών, τον εντοπισμό του προβλήματος και την άμεση ανάκαμψη σε κατάσταση πλήρους λειτουργίας. Επίσης ελέγχει την ακεραιότητα των δεδομένων. Αν απαιτείται, διακόπτει την κανονική

λειτουργία των προσβεβλημένων συστημάτων με στόχο τον άμεσο εντοπισμό και περιορισμό του κινδύνου. Χαρακτηρίζει το συμβάν ασφαλείας ως:

- Απλό συμβάν (μικρή σημασία)
- Εντοπισμός αδυναμίας (μέτρια σημασία)
- Περιστατικό ασφαλείας (μεγάλη σημασία – κίνδυνος διαρροής πληροφορίας)
- Άγνωστο – δεν μπορεί να κατηγοριοποιηθεί μετά από ανάλυση

Ο χαρακτηρισμός ενδέχεται να τροποποιηθεί μετά τη λεπτομερή διερεύνηση του περιστατικού.

Για τις δυο τελευταίες κατηγορίες οι οποίες χαρακτηρίζονται ως σοβαρότερες, ο ΥΑΠ συγκαλεί την Επιτροπή Διερεύνησης Περιστατικών Ασφαλείας, η οποία αποτελείται από όλα τα μέλη της διοίκησης, προκειμένου να πραγματοποιηθεί από κοινού ανασκόπηση των δεδομένων του συμβάντος. Η επιτροπή θα αποφασίσει ποιές ενέργειες πρέπει να ακολουθήσουν και από ποιούς.

- **Συλλογή αποδείξεων και στοιχείων**

Κάθε πληροφορία που αφορά το συμβάν, ένδειξη, απόδειξη ή στοιχείο εντοπίζεται και αποθηκεύεται σε ασφαλή τοποθεσία.

Στην περίπτωση έντυπων αποδείξεων τηρούνται τα πρωτότυπα αρχεία και καταγράφεται το άτομο που βρήκε το έντυπο, τη θέση και το χρόνο εύρεσης του. Στην περίπτωση ηλεκτρονικών αποδείξεων, τηρείται ακριβές αντίγραφο καθώς και όλα τα σχετικά logs. Επίσης τηρείται σε ασφαλή θέση τυχόν σχετικός ηλεκτρονικός εξοπλισμός (π.χ. σκληροί δίσκοι). Αν απαιτείται λαμβάνει φωτογραφίες από το χώρο όπου εντοπίστηκε το συμβάν.

Στην περίπτωση που υπάρχει υποψία νομικής, αστικής ή ποινικής ευθύνης για το συμβάν, ο ΥΑΠ θα πρέπει να ενημερώσει άμεσα τη διοίκηση της εταιρείας και το νομικό τμήμα και στη συνέχεια τις αστυνομικές αρχές, προκειμένου να τον καθοδηγήσουν για τη συλλογή και αποθήκευση στοιχείων και πειστηρίων που θα οδηγήσουν στη διαλεύκανση και πιθανή εκδίκαση της υπόθεσης.

- **Λήψη μέτρων αντιμετώπισης**

Ο ΥΑΠ, σε συνεργασία με στελέχη της διοίκησης της εταιρείας καθώς και τους διαχειριστές του ΣΔΑΠ αν απαιτείται, λαμβάνουν μέτρα αντιμετώπισης για τον έλεγχο και την απομόνωση του συμβάντος και την ανάκαμψη των συστημάτων στην κανονική λειτουργία.

Αν το συμβάν εμπίπτει στο πεδίο εφαρμογής των υφιστάμενων Σχεδίων Ανάκαμψης από Καταστροφή και Σχεδίων Επιχειρησιακής Συνέχειας, εφαρμόζονται οι προβλεπόμενες σε αυτά ενέργειες διερεύνησης, κλιμάκωσης και κινητοποίησης του εμπλεκόμενου προσωπικού καθώς και η ενεργοποίηση μηχανισμών και πόρων εφεδρείας.

Όλες οι ενέργειες ανάκαμψης καταγράφονται λεπτομερώς και η διοίκηση ενημερώνεται σε συνεχή βάση.

- **Αξιολόγηση αντιμετώπισης**

Μετά το πέρας των ενεργειών ανάκαμψης η ακεραιότητα του συνολικού συστήματος ελέγχεται λεπτομερώς. Επίσης συμπληρώνονται απολογιστικά τα εξής:

- Περιγραφή του συμβάντος
- Συστήματα που επηρεάστηκαν
- Διορθωτικές ενέργειες που ελήφθησαν για τον περιορισμό του συμβάντος
- Εναπομείναντες κίνδυνοι και βλάβες
- Απαραίτητες ενέργειες για την αποφυγή αντίστοιχων περιστατικών

Ο βαθμός στον οποία ακολουθήθηκαν οι προβλεπόμενες διαδικασίες του Συστήματος.

- **Ενημέρωση της διοίκησης**

Όταν και εφόσον επιβεβαιωθεί η καλή λειτουργία, οι χρήστες ενημερώνονται για να συνεχίσουν την εργασία τους. Η διοίκηση ενημερώνεται για τις συνέπειες του περιστατικού, τις ενέργειες που λήφθηκαν και ενδεχόμενες μελλοντικές ενέργειες που

απαιτούνται. Επίσης τα περιστατικά συζητούνται στο Συμβούλιο Ανασκόπησης του Συστήματος και αξιολογείται ο χειρισμός τους και τυχόν απαιτούμενες πρόσθετες διορθωτικές ενέργειες.

6.4.13. Παράμετροι ασφάλειας πληροφορίας της διαχείρισης επιχειρησιακής συνέχειας

6.4.13.1. Συνέχεια ασφάλειας πληροφοριών

Η επιχειρησιακή συνέχεια αποτελεί βασικό στόχο της εταιρείας και η επίτευξή της απαιτεί μεταξύ άλλων παραγόντων και τη διαχείριση των περιστατικών Ασφάλειας που ενδέχεται να διακόψουν ή να παρακωλύσουν την ομαλή της λειτουργία. Μέσω της εκτίμησης κινδύνων ασφάλειας πληροφοριών, η εταιρεία εντοπίζει όλους τους πιθανούς κινδύνους που μπορεί να την πλήξουν, ενώ χάρη στην καταγραφή των πληροφοριακών πόρων της έχει πλήρη εικόνα των υποδομών και του εξοπλισμού της. Κατ' αυτό τον τρόπο μπορεί να εκτιμήσει την πιθανότητα και τη σοβαρότητα περιστατικών Ασφάλειας και να προβεί στις αναγκαίες διορθωτικές ενέργειες. Μέρος αυτών αποτελεί και η παροχή των απαραίτητων οικονομικών, οργανωτικών, τεχνικών και οργανωτικών πόρων. Το αποτέλεσμα αυτής της διαδικασίας καταγράφεται στο σχέδιο επιχειρησιακής συνέχειας της εταιρείας και σε τακτά χρονικά διαστήματα δοκιμάζεται ως προς την αξιοπιστία και την ετοιμότητα εφαρμογής.

Το Σχέδιο Ανάκαμψης από Καταστροφή περιέχει ευαίσθητη πληροφορία σχετικά με τα αδύνατα σημεία της οργάνωσης της εταιρείας και γι' αυτό αποτελεί ιδιαίτερα κρίσιμο και προστατευόμενο έγγραφο. Εξ' αυτού, αντίγραφό του θα βρίσκεται και σε ασφαλή χώρο εκτός της εταιρείας ώστε σε περίπτωση σημαντικής κτηριακής καταστροφής να είναι διαθέσιμο.

Το Σχέδιο Ανάκαμψης από Καταστροφή θα έχει την ακόλουθη δομή:

- Οι συνθήκες για την ενεργοποίηση κάθε διαδικασίας του σχεδίου
- Οι διαδικασίες έκτακτης ανάγκης σε περίπτωση απειλής προς τη συνολική λειτουργία
- Οι διαδικασίες μετάπτωσης σε προσωρινές εγκαταστάσεις και διαδικασίες ώστε η εταιρεία να είναι λειτουργική παρά την απώλεια πληροφοριακών πόρων

- Οι διαδικασίες μετάβασης από την λειτουργία ανάκαμψης πίσω στην επιχειρησιακή λειτουργία.
- Οι διαδικασίες εκπαίδευσης του προσωπικού που εμπλέκεται στην εφαρμογή του σχεδίου.
- Οι ακριβείς αρμοδιότητες κάθε εμπλεκόμενου ατόμου
- Όλες οι απαραίτητες υποδομές και οι πόροι που απαιτούνται για την εφαρμογή του σχεδίου.
- Το πρόγραμμα δοκιμής και συντήρησης του Σχεδίου Ανάκαμψης

Προκειμένου να εξασφαλιστεί η αποτελεσματικότητά του Σχεδίου Ανάκαμψης τη στιγμή της κρίσης θα εφαρμόζεται το ακόλουθο πρόγραμμα επαλήθευσης:

1. Εκπαίδευση του προσωπικού και προσομοίωση των ρόλων και αρμοδιοτήτων στη φάση της ανάκαμψης (1 φορά το έτος)
2. Τεχνική εφαρμογή του σχεδίου και μερική ανάκτηση δεδομένων και λειτουργιών (1 φορά στα 2 έτη).
3. Ανάκτηση δεδομένων και μεταφορά δραστηριοτήτων σε εναλλακτική τοποθεσία (1 φορά στα 3 έτη).
4. Δοκιμή προμήθειας εξοπλισμού από τους προμηθευτές που εμπλέκονται στο Σχέδιο Ανάκαμψης (σε συνεχή βάση στα πλαίσια υλοποίησης έργων για πελάτες της εταιρείας)

Το Σχέδιο Ανάκαμψης ενημερώνεται σε συνεχή βάση με βάση και την αξιολόγηση των δοκιμών από τον Υπεύθυνο Ασφάλειας Πληροφοριών και ειδικά κάθε φορά που συμβαίνουν αλλαγές

- στο προσωπικό
- στις διευθύνσεις και στα τηλέφωνα επικοινωνίας των εμπλεκομένων
- στη στρατηγική του σχεδίου
- στις εγκαταστάσεις και τους πόρους της εταιρείας
- στη νομοθεσία
- στους προμηθευτές
- στις διαδικασίες λειτουργίας
- στους κινδύνους.

Θα πρέπει να σημειώσουμε ότι κατά την ανάκαμψη από μια καταστροφή, αν και τελικός στόχος είναι η επιστροφή στην πρότερη κατάσταση της πλήρους λειτουργίας, συχνά αυτό δεν είναι ρεαλιστικό. Στα πλαίσια του σχεδίου επιχειρησιακής συνέχειας η εταιρεία ορίζει το επιθυμητό επίπεδο λειτουργίας που θα επιδιωχθεί καθώς και τον αποδεκτό βαθμό και είδος απώλειας πληροφορίας και υπηρεσιών. Η διαδικασία ανάκαμψης, τα ακριβή βήματα καθώς και οι χρονικοί στόχοι της ανάκαμψης περιγράφονται στο Σχέδιο Ανάκαμψης από Καταστροφή. Όλο το εμπλεκόμενο προσωπικό ενημερώνεται ώστε να έχει βαθιά γνώση του και τίθεται σε δοκιμή τουλάχιστον μια φορά κάθε δυο έτη. Στόχος είναι η επιτυχής εφαρμογή του σχεδίου τόσο ως προς το εύρος της ανακτημένης πληροφορίας και λειτουργικότητας όσο και ως προς το χρόνο επίτευξης αυτής.

6.4.13.2. Εφεδρείες

Όλα τα πληροφοριακά συστήματα της εταιρείας έχουν σχεδιαστεί με στόχο την υψηλή διαθεσιμότητα και αξιοπιστία, μέσω των παρακάτω μεθόδων:

1. *Εφεδρείες σε φυσικό επίπεδο:* χρήση συστοιχιών RAID, πολλαπλά τροφοδοτικά και συστήματα ψύξης, εναλλακτική όδευση καλωδιώσεων.
2. *Εφεδρείες σε επίπεδο αρχιτεκτονικής δικτύου:* πολλαπλά φυσικά μηχανήματα, χρήση τεχνολογιών virtualization, χρήση backup τηλεπικοινωνιακών γραμμών εναλλακτικών παρόχων, εναλλακτικές διασυνδέσεις υποδικτύων, υλοποίηση υποδομής cloud.
3. *Χρήση αξιόπιστων προμηθευτών/υπεργολάβων:* υποστήριξη κρίσιμων συστημάτων με μόνιμα συμβόλαια συντήρησης, συχνά με όρους SLA (Service-level agreement).

6.4.14. Συμμόρφωση

6.4.14.1. Συμμόρφωση με νομικές και συμβατικές απαιτήσεις

Ο Υπεύθυνος Ασφάλειας Πληροφοριών χρησιμοποιεί διάφορες πηγές πληροφόρησης με σκοπό τον εντοπισμό των σχετικών νόμων και κανονισμών. Ενδεικτικές πηγές αποτελούν οι παρακάτω δικτυακοί τόποι:

- www.europa.eu.int/eur-lex
- www.et.gr
- www.dpa.gr
- www.adae.gr

Ο Υπεύθυνος Ασφάλειας Πληροφοριών παρακολουθεί αυτές τις πηγές πληροφόρησης σε εξαμηνιαία βάση και ενημερώνει κατάλληλα τον κατάλογο ελεγχόμενων εγγράφων. Ταυτόχρονα παρακολουθεί όλες τις απαιτήσεις που προκύπτουν από τα συμβόλαια που έχει συνάψει η εταιρεία.

Ο Υπεύθυνος Ασφάλειας Πληροφοριών εξετάζει πιθανές αλλαγές στην αξιολόγηση των Κινδύνων Ασφάλειας Πληροφοριών και εάν προκύψει ανάγκη προσδιορίζει τις πιθανές αλλαγές στο ΣΔΑΠ, προκειμένου να επιτευχθεί εναρμόνιση με τους σχετικούς νόμους και κανονισμούς.

Η συμμόρφωση της εταιρείας με τις απαιτήσεις των κείμενων διατάξεων ελέγχεται τόσο σε τακτική όσο και σε έκτακτη βάση. Οι τακτικοί έλεγχοι πραγματοποιούνται μέσω των Εσωτερικών Επιθεωρήσεων.

Οι έκτακτοι έλεγχοι διενεργούνται με απόφαση του Υπευθύνου Ασφάλειας Πληροφοριών και ανάλογα με τα στοιχεία που προκύπτουν από τη διαρκή ενημέρωση της εταιρείας.

Οι έλεγχοι αυτοί διεξάγονται με επιθεώρηση των αρχείων του ΣΔΑΠ της εταιρείας. Σε περίπτωση εντοπισμού μη συμμόρφωσης κατά τους έκτακτους ελέγχους, ο Υπεύθυνος Ασφάλειας Πληροφοριών εισηγείται - εφόσον το κρίνει σκόπιμο - τη διενέργεια έκτακτης σύσκεψης για να εξεταστεί το θέμα.

Στα πλαίσια της συμμόρφωσης με τις νομικές και συμβατικές απαιτήσεις, όλοι οι πόροι της εταιρείας θεωρείται ότι εξυπηρετούν μόνον τους σκοπούς και τις ανάγκες της λειτουργίας της. Κάθε άλλη χρήση που δεν προβλέπεται και δεν ορίζεται από τη διοίκηση

της εταιρείας θεωρείται παράνομη και διώκεται με τα αναγκαία πειθαρχικά και νομικά μέσα. Κάθε εργαζόμενος θα ενημερώνεται κατά την πρόσληψή του και την εργασία για τις επιτρεπτές χρήσεις των παρεχόμενων πόρων.

6.4.14.2. Ανασκόπηση ασφάλειας πληροφοριών

Η εταιρεία μέσω των συμβούλων Ασφάλειας Πληροφοριών κατά το ISO/IEC 27001:2013 Ασφάλεια Πληροφοριών έχει σύγχρονη ενημέρωση για την καλύτερη εφαρμογή των απαιτήσεων του. Εξάλλου η εταιρεία συμμετέχει σε ομάδες ειδικού ενδιαφέροντος.

Για την επιβεβαίωση της ορθής λειτουργίας του Συστήματος Διαχείρισης Ασφάλειας Πληροφορίας, σε τακτά χρονικά διαστήματα, πέραν των Εσωτερικών Επιθεωρήσεων, καλεί εξωτερικό συνεργάτη ειδικευμένο στην ασφάλεια πληροφοριών προκειμένου να επιθεωρήσει την καλή εφαρμογή και τις δυνατότητες βελτίωσης του υφιστάμενου συστήματος. Τα αποτελέσματα της επιθεώρησης κοινοποιούνται στον Υπεύθυνο Ασφάλειας Πληροφοριών και τη διοίκηση της εταιρείας.

Ο έλεγχος συμμόρφωσης με τις τεχνικές απαιτήσεις της Πολιτικής Ασφάλειας Πληροφοριών θα γίνεται από ειδικευμένο και εξουσιοδοτημένο τεχνικό προσωπικό με χρήση κατάλληλων εργαλείων λογισμικού και υλικού. Οι μέθοδοι τεχνικού ελέγχου κατά κανόνα προσομοιώνουν συνθήκες περιστατικών Ασφάλειας και γι’ αυτό η εκτέλεσή τους θα σχεδιάζεται και θα προγραμματίζεται προσεκτικά προκειμένου να μη διαταραχθεί η ομαλή λειτουργία των συστημάτων. Ο προγραμματισμός τους θα γίνεται από το Συμβούλιο Ανασκόπησης με εισήγηση από τον Υπεύθυνο Ασφάλειας Πληροφοριών. Επιπλέον, κατά την εκτέλεση των δοκιμών ανάκτησης θα γίνεται σχετική καταγραφή στο αρχείο Δοκιμών Ανάκτησης.

ΚΕΦΑΛΑΙΟ 7:

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ ΥΠΟΛΟΓΙΣΜΟΥ ΚΟΣΤΟΥΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

7.1. Εισαγωγή

Στο κεφάλαιο αυτό θα υπολογίσουμε το κόστος για μία εταιρεία που επιθυμεί να εξασφαλίσει κάποιο επίπεδο ασφάλειας των πληροφοριακών της συστημάτων με σκοπό την προστασία των πληροφοριών και των δεδομένων που διακινούνται από και σε αυτή. Η μελέτη υπολογισμού του κόστους βασίζεται στα συστήματα ασφάλειας όπως αναπτύχθηκαν και παρουσιάστηκαν στο Κεφάλαιο 5: *Αντιμετώπιση ψηφιακών κινδύνων & απειλών – προστασία πληροφοριακών συστημάτων*.

Το κόστος αφορά δαπάνες που πραγματοποιούνται για την προστασία των πληροφοριακών συστημάτων της εταιρείας, ώστε να εναρμονιστεί με την Πολιτική Ασφαλείας και το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών που ακολουθεί.

Είναι προφανές ότι το μέγεθος της εταιρείας καθώς και ο κλάδος στον οποίο δραστηριοποιείται παίζουν πολύ σημαντικό ρόλο στο συνολικό κόστος της επένδυσης της ασφάλειας της. Για παράδειγμα, οι εταιρείες στον τραπεζικό κλάδο, στον κλάδο υγείας, οι εταιρείες τηλεπικοινωνιών κτλ. λόγω των πολύπλοκων τεχνολογικών υποδομών που χρησιμοποιούν απαιτούν και πολύπλοκα συστήματα ασφάλειας.

Στο case study μας θα εφαρμόσουμε την κοστολόγηση των συστημάτων ασφάλειας σε μία εταιρεία παροχής επιχειρηματικών συμβουλευτικών υπηρεσιών, όπως στο case study του προηγούμενου κεφαλαίου. Έχοντας, λοιπόν, ολοκληρώσει την ανάπτυξη του ΣΔΑΠ στη συγκεκριμένη εταιρεία, προχωράμε στον υπολογισμό του κόστους επένδυσης σε συστήματα ασφάλειας πληροφοριών.

Υποθέτουμε ότι στη συγκεκριμένη εταιρεία απασχολούνται 300 άτομα και όλοι οι εργαζόμενοι βρίσκονται στο ίδιο κτίριο. Η εταιρεία, επίσης, για την υποστήριξη των λειτουργιών της διαθέτει την παρακάτω υποδομή σε συστήματα πληροφορικής και επικοινωνιών:

- 300 προσωπικοί ή φορητοί υπολογιστές
- 300 κινητά τηλέφωνα
- 1 εξυπηρετητής αρχείων (file server)
- 1 εξυπηρετητής ηλεκτρονικού ταχυδρομείου (mail server)
- 1 εξυπηρετητής εκτυπωτών (print server)
- 1 εξυπηρετητής αντιγράφων ασφαλείας (backup server)
- 1 εξυπηρετητή αρχείων μέσω διαδικτύου (web server)

  Οι servers μπορεί να είναι είτε φυσικοί (hardware) ή εικονικοί (virtual). Όλοι οι servers βρίσκονται σε ειδικά διαμορφωμένο χώρο εντός της εταιρείας με ελεγχόμενη πρόσβαση (Computer room).

Προφανώς χρησιμοποιούνται επιπλέον για να υποστηρίξουν το δίκτυο της εταιρείας μεταγωγείς (switches), συστήματα αδιάλειπτης παροχής ενέργειας (UPS), δρομολογητές (routers), ίντερνετ με δίκτυο οπτικών ινών 100 Mbps.

7.2. Υπολογισμός κόστους ασφάλειας

Ο υπολογισμός του κόστους σε συστήματα ασφάλειας αφορά τις δαπάνες που θα πραγματοποιηθούν τον πρώτο χρόνο και δε περιλαμβάνουν τα κόστη συντήρησης που προκύπτουν από το δεύτερο χρόνο και μετά.

Δικτυακή προστασία

Για την προστασία του δικτύου της εταιρείας θα χρησιμοποιηθεί ένα σύστημα ενοποιημένης διαχείρισης απειλών (Unified Threat Management – UTM) το οποίο ενσωματώνει σε μία μόνο κονσόλα διαχείρισης τον τοίχο προστασίας (firewall), το σύστημα ανίχνευσης εισβολών (IDS), την ασφάλεια web για περιήγηση ιστοσελίδων και ασφάλεια email, καθώς επίσης και την ασφάλεια ασύρματης δικτύωσης.

Το κόστος ενός συστήματος UTM που περιλαμβάνει δύο συσκευές για σύνδεση υψηλής διαθεσιμότητας και το απαραίτητο λογισμικό για μια εταιρεία 300 χρηστών είναι 16.000 €.

Επίσης, θα χρησιμοποιηθούν σημεία πρόσβασης - access points (AP) για την ασύρματη πρόσβαση των χρηστών στο προστατευμένο δίκτυο. Το κόστος κάθε AP είναι 300 €. Στο σύνολο θα προστεθούν 10 συσκευές, άρα τελικό συνολικό κόστος 3.000 €.

Προστασία χρηστών

Για την προστασία των χρηστών θα αγοραστεί λογισμικό antivirus που θα εγκατασταθεί σε όλους τους υπολογιστές. Το λογισμικό θα παρέχει ενισχυμένη προστασία απέναντι στις προηγμένες απειλές τύπου ransomware και θα ενσωματώνει την έξυπνη ανίχνευση και ανταπόκριση (Endpoint Detection and Response – EDR).

Το κόστος ανέρχεται στα 50 € ανά χρήστη, οπότε συνολικά 300 x 50 € = 15.000 €.

Επίσης, θα προστεθεί προστασία των φορητών συσκευών (mobile security) σε όλα τα κινητά των εργαζομένων. Το κόστος ανά χρήστη είναι 25 €, οπότε συνολικά 300 x 25 € = 7.500 €.

Για την προστασία των εξυπηρετητών θα αγοραστεί επίσης λογισμικό με κόστος 100 € ανά τεμάχιο, οπότε σύνολο 5 x 100 € = 500 €.

Κρυπτογράφηση

Θα χρησιμοποιηθεί κρυπτογράφηση τόσο σε επίπεδο αρχείων όσο και σε επίπεδο δίσκων ώστε να προστατευτεί κάθε πληροφορία που αποθηκεύεται σε υπολογιστές που πιθανώς μπορεί να χαθούν ή να κλαπούν.

Ένα λογισμικό επιχειρησιακής κρυπτογράφησης κοστίζει 120 € ανά χρήστη, οπότε συνολικά 300 x 120 € = 36.000 €.

Προστασία προνομιακών λογαριασμών

Μία λύση διαχείρισης προνομιακών λογαριασμών σκοπό έχει να αντιμετωπίσει ίσως τη μεγαλύτερη απειλή που έχει αυτή τη στιγμή η εταιρεία, την πρόσβαση μέσω κλεμμένων κωδικών των χάκερ στα συστήματα της εταιρείας.

Το κόστος μιας τέτοιας λύσης ανέρχεται στα 23.000 € για την εταιρεία των 300 χρηστών που εξετάζουμε.

Ταξινόμηση δεδομένων

Η λύση ταξινόμησης δεδομένων θα βοηθήσει την επιχείρηση να ανακτήσει τον έλεγχο όλων των μη δομημένων και ταξινομημένων δεδομένων.

Μία πλήρη λύση, όπως παρουσιάστηκε στο Κεφάλαιο 5, περιλαμβάνει τη σουίτα και το σύνολο των προϊόντων ταξινόμησης και για 300 άτομα κοστίζει 20.000 €.

Σάρωση ασφάλειας εφαρμογών ιστού

Μία λύση σάρωσης ασφάλειας εφαρμογών ιστού εντοπίζει και αναφέρει ευπάθειες και τρωτά σημεία σε εφαρμογές ιστού. Η εταιρεία που μελετάμε επιτρέπει στους υπαλλήλους της να έχουν πρόσβαση σε εταιρικά δεδομένα μέσω τέτοιων εφαρμογών καθώς πολλοί εργάζονται εκτός εταιρείας στους χώρους των πελατών και χρειάζεται να συνδεθούν με την εταιρεία για να δουλέψουν αποτελεσματικά.

Υποθέτουμε ότι η εταιρεία μας διαθέτει το πολύ 5 τέτοιες web εφαρμογές, οπότε και το κόστος είναι περίπου 4.000 €.

Διαχείριση δικαιωμάτων εγγράφων

Η εταιρεία διακινεί έγγραφα μεταξύ των εργαζομένων και των πελατών. Τα έγγραφα αυτά αποτελούν είτε οικονομικές προσφορές ή μελέτες για τις ανάγκες των πελατών της. Είναι προφανές ότι η εταιρεία επιθυμεί να προστατεύσει τα έγγραφα αυτά μόλις βγουν από το περιβάλλον της προσθέτοντας κανόνες ασφαλείας.

Μία τέτοια λύση για 300 χρήστες κοστίζει 25.000 €.

Διαχείριση πληροφοριών και συμβάντων ασφάλειας

Ένα εξελιγμένο σύστημα διαχείρισης πληροφοριών και συμβάντων ασφάλειας (SIEM) επιτρέπει το συσχετισμό των γεγονότων και την δημιουργία αναφορών σχετικά με τις κρίσιμες λειτουργίες των συστημάτων.

Για την εταιρεία που μελετάμε η οποία διαθέτει περίπου 300 συστήματα μία λύση SIEM θα κοστίσει 30.000 €.

Αντίγραφα ασφαλείας

Για το backup των συστημάτων της και των εφαρμογών της η εταιρεία θα προσθέσει λύση αντιγράφων ασφαλείας. Το σύστημα που θα αγοραστεί θα μπορεί να κρατήσει αντίγραφα ασφαλείας έως 5 TB και έως 10 πολλαπλές ροές αντιγράφων ασφαλείας ταυτόχρονα και κοστίζει 12.500 €.

Ψηφιακά πιστοποιητικά

Για την ασφάλεια των επικοινωνιών της η εταιρεία θα εγκαταστήσει λύσεις ψηφιακής ταυτότητας, ψηφιακών υπογραφών και ψηφιακών πιστοποιητικών. Η διαχείριση τους θα γίνεται από μία ενιαία πλατφόρμα που θα προσφέρεται στην εταιρεία σαν υπηρεσία.

Το κόστος της για το μέγεθος και τις ανάγκες της εταιρείας είναι 10.000 €.

Πρόληψη απώλειας δεδομένων

Μία λύση πρόληψης απώλειας δεδομένων (Data Loss Prevention - DLP) παρακολουθεί και περιορίζει την αντιγραφή εμπιστευτικών δεδομένων σε μη κρυπτογραφημένες εξωτερικές συσκευές αποθήκευσης.

Το κόστος μιας τέτοιας λύσης για 300 χρήστες είναι 5.000 €.

Στις παραπάνω δαπάνες που αφορούν την αγορά των συστημάτων ασφάλειας θα πρέπει να προστεθούν και οι υπηρεσίες εγκατάστασης και παραμετροποίησης οι οποίες θα υλοποιηθούν από εξειδικευμένους μηχανικούς μέσω εταιρείας πληροφορικής που θα αναλάβει το έργο της ασφάλειας για λογαριασμό της εταιρείας που μελετάμε.

Θα πρέπει να επισημάνουμε ότι τέτοια μεγάλα έργα απαιτούν χρόνο, αρκετές ανθρωποώρες και σίγουρα πιο πριν θα πρέπει να διεξαχθεί για κάθε σύστημα PoC (Proof of Concept) ώστε να δοκιμασθεί στην πράξη κατά πόσο είναι εφικτό να εγκατασταθούν τα παραπάνω συστήματα στην εταιρεία. Ο χρόνος υλοποίησης των παραπάνω μπορεί να είναι από μερικούς μήνες έως και 2-3 χρόνια.

Στον παρακάτω πίνακα συνοψίζεται το συνολικό κόστος των λύσεων ασφαλείας στα πληροφοριακά συστήματα της εταιρείας:

Πίνακας 8: Συνολικό κόστος λύσεων ασφάλειας πληροφοριακών συστημάτων

Είδος ασφάλειας	Κόστος (σε €)
Δικτυακή προστασία	19.000
Προστασία χρηστών	23.000
Κρυπτογράφηση	36.000
Προστασία προνομιακών λογαριασμών	23.000
Ταξινόμηση δεδομένων	20.000

Σάρωση ασφάλειας εφαρμογών ιστού	4.000
Διαχείριση δικαιωμάτων εγγράφων	25.000
Διαχείριση πληροφοριών και συμβάντων ασφαλείας	30.000
Αντίγραφα ασφαλείας	12.500
Ψηφιακά πιστοποιητικά	10.000
Πρόληψη απώλειας δεδομένων	5.000
Σύνολο	**207.500**

Το κόστος παραμετροποίησης και εγκατάστασης των συστημάτων υπολογίζεται στο 25% του κόστους της συνολικής λύσης, δηλαδή σε περίπου 50.000 €.

Κόστος προσωπικού

Η εγκατάσταση πολλών συστημάτων που αφορούν την ασφάλεια απαιτεί και νέο προσωπικό που θα απασχολείται στο τμήμα πληροφορικής της εταιρείας και θα είναι υπεύθυνο για την ομαλή και ορθή λειτουργία των συστημάτων και την εναρμόνιση της με τις εκάστοτε πολιτικές ασφαλείας της εταιρείας.

Υπολογίζουμε ότι θα χρειαστούν τουλάχιστον 5 άτομα με μέσο ετήσιο μισθό 25.000 € ο καθένας.

Επίσης, ο κανονισμός GDPR επιβάλλει στις εταιρείες με μέγεθος 250 ατόμων και πάνω την πρόσληψη ενός Επόπτη Προστασίας Δεδομένων (Data Protection Officer) ο οποίος θα πρέπει να φροντίζει να διασφαλίζεται η συμμόρφωση του οργανισμού με τον νέο γενικό κανονισμό. Ο μισθός του υπολογίζεται ετησίως στα 35.000 €.

Γίνεται αντιληπτό ότι όσο περισσότερο επενδύει μία εταιρεία στην ασφάλεια της τόσο λιγότερες πιθανότητες έχει να αντιμετωπίσει κάποιο περιστατικό παραβίασης, διαρροή ή απώλεια δεδομένων ή μία κακόβουλη επίθεση χάκερ. Θα πρέπει να γίνει, όμως, ακόμα πιο αντιληπτό ότι ακόμα και τα πιο εξελιγμένα συστήματα ασφάλειας πληροφοριακών συστημάτων δε μπορούν να εγγυηθούν 100% προστασία.

Για το λόγο αυτό συνίσταται και η σωστή εκπαίδευση των χρηστών εντός της εταιρείας ώστε να τηρούν όλους τους κανονισμούς και να είναι ιδιαίτερα προσεκτικοί στις κρυφές απειλές όπως είναι τα email ψαρέματος, όπως έχουμε αναφέρει ήδη σε προηγούμενο κεφάλαιο.

ΚΕΦΑΛΑΙΟ 8:
ΚΟΣΤΟΣ & ΣΥΝΕΠΕΙΕΣ ΕΝΟΣ ΠΕΡΙΣΤΑΤΙΚΟΥ ΑΣΦΑΛΕΙΑΣ

8.1. Εισαγωγή

Οι σύγχρονες επιχειρήσεις δραστηριοποιούνται στον κόσμο των πληροφοριών και των πληροφοριακών συστημάτων και διαχειρίζονται ένα μεγάλο μέγεθος δεδομένων. Τα δεδομένα αυτά αποθηκεύονται σε υπολογιστές, σε διακομιστές, στο Διαδίκτυο και μπορούν ανά πάσα στιγμή να δεχτούν επίθεση από κάποιον κακόβουλο χάκερ ή να υπάρξει διαρροή τους από κάποιον εσωτερικό χρήστη λόγω αμέλειας. Οι ψηφιακοί κίνδυνοι απειλούν τις επιχειρήσεις πολύ περισσότερο απ' ότι οι φυσικοί κίνδυνοι των περιουσιακών τους στοιχείων και μπορούν να οδηγήσουν σε πολύ σοβαρά περιστατικά ασφαλείας.

Επίσης, η νομοθεσία και οι κανονισμοί που έχουν επιβληθεί από την Ευρωπαϊκή Ένωση κάνουν ακόμα πιο επιτακτική την υιοθέτηση μέτρων ασφαλείας από τις επιχειρήσεις οι οποίες είναι αντιμέτωπες με τεράστια πρόστιμα σε περίπτωση απώλειας ή παραβίασης δεδομένων.

Μια διαρροή δεδομένων μπορεί να αφορά σε κλοπή προσωπικών στοιχείων εργαζομένων και πελατών και οι συνέπειες ενός τέτοιου περιστατικού δεν περιορίζονται μόνο στο οικονομικό κόστος για την αντιμετώπιση του περιστατικού ασφαλείας, αλλά επεκτείνονται και σε μία σειρά άλλων θεμάτων που θα πρέπει να αντιμετωπίσει η επιχείρηση.

8.2. Κόστος αντιμετώπισης του περιστατικού ασφαλείας

Το κόστος αντιμετώπισης ενός περιστατικού ασφαλείας είναι και το πιο εύκολο να υπολογιστεί. Αφορά το κόστος που περιλαμβάνει την αντικατάσταση του συστήματος ή των συστημάτων που έχουν «χτυπηθεί», την εξέταση των συστημάτων από κάποιον ειδικό και την αμοιβή των υπερωριών του προσωπικού που θα εργαστεί για να επαναφέρει τα συστήματα και να αντιμετωπίσει το περιστατικό.

Αν λάβουμε υπόψη και την προθεσμία που δίνει ο κανονισμός GDPR ότι μέσα σε 72 ώρες η εταιρεία θα πρέπει να ενημερώσει τις αρχές για την παραβίαση δεδομένων με τεκμηρίωση, τότε είναι παραπάνω από προφανές ότι η εταιρεία θα χρειαστεί τόσο τις

υπερωρίες του προσωπικού της στο IT για να εντοπίσει την αιτία του περιστατικού, τη διαδρομή που ακολούθησε και το μέγεθος της καταστροφής που προκάλεσε, όσο και την συμβολή ειδικών από κάποια άλλη εταιρεία.

8.3. Δαπάνες, πρόστιμα και αποζημιώσεις

Στην κατηγορία αυτή εντάσσονται όλα τα έξοδα που θα κληθεί να κάνει η εταιρεία για την πληρωμή των προστίμων από τις ελεγκτικές αρχές, τις αποζημιώσεις των πελατών που τα προσωπικά τους δεδομένα παραβιάστηκαν και τις αμοιβές σε νομικούς συμβούλους για τις τυχόν δικαστικές διαμάχες που ακολουθήσουν [38].

Στις εταιρείες μπορούν να επιβληθούν πρόστιμα έως 4% του ετήσιου παγκόσμιου κύκλου εργασιών για παραβίαση του GDPR ή 20 εκατομμυρίων ευρώ, όποιο από τα δύο είναι μεγαλύτερο.

8.4. Κρίση εταιρικής φήμης

Στην εποχή που η πληροφορία διακινείται πολύ γρήγορα είναι προφανές ότι η είδηση ότι η εταιρεία υπέστη ένα περιστατικό ασφαλείας με αποτέλεσμα τη διαρροή δεδομένων θα εξαπλωθεί θέτοντας σε κίνδυνο της φήμη της.

Άμεση συνέπεια θα είναι η πιθανή πτώση της τιμής της μετοχής, η έλλειψη εμπιστοσύνης από την αγορά προς την επιχείρηση και, φυσικά, η απώλεια πελατών που θα επηρεάσει αρνητικά τα έσοδα της επιχείρησης.

Η εταιρεία θα κληθεί να αντιμετωπίσει κριτικές από τα μέσα μαζικής ενημέρωσης, τους συνεργάτες της, τους εργαζόμενους της και από τρίτα μέρη που έχουν άμεση ή έμμεση σχέση μαζί της.

8.5. Διακοπή εργασιών

Το κόστος από την διακοπή των εργασιών της επιχείρησης μεταφράζεται σε απώλεια εσόδων. Η εταιρεία θα πρέπει να επαναφέρει γρήγορα τα συστήματα της για την συνέχιση της λειτουργίας της. Οι εταιρείες που διαθέτουν σχέδιο επιχειρησιακής συνέχειας θα πρέπει να είναι σε θέση να το εφαρμόσουν άμεσα.

8.6. Κρίση στη διοίκηση

Ένα περιστατικό ασφαλείας που σχετίζεται με παραβίαση δεδομένων ενδέχεται να βλάψει τη φήμη των στελεχών της εταιρείας ή και να οδηγήσει ακόμα στην απώλεια της θέσης τους. Υπάρχουν πολλά παραδείγματα στελεχών όπως διευθύνοντες σύμβουλοι οι οποίοι είτε αναγκάζονται να παραιτηθούν ή απολύονται. Η αρνητική αυτή εξέλιξη μπορεί να επηρεάσει την μελλοντική τους σταδιοδρομία.

ΚΕΦΑΛΑΙΟ 9:
ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΡΟΤΑΣΕΙΣ

Οι σύγχρονες επιχειρήσεις καλούνται να δραστηριοποιηθούν σε ένα νέο παγκοσμιοποιημένο και ταυτόχρονα δικτυακά διασυνδεδεμένο περιβάλλον. Παράλληλα οι τεχνολογίες πληροφορικής και επικοινωνιών αποτελούν αναπόσπαστο κομμάτι της λειτουργίας και της οργάνωσης τους, ενώ η πρόσβαση στο Διαδίκτυο δίνει τη δυνατότητα γρήγορης επικοινωνίας και πρόσβασης σε δίκτυα διανομής και πελάτες σε όλο τον κόσμο, περιορίζοντας το κόστος και βελτιώνοντας την αποτελεσματικότητα τους και το ανταγωνιστικό τους πλεονέκτημα.

Επιπλέον, όπως αναφερθήκαμε και στην αρχή της μελέτης, η πληροφορία αποτελεί το πιο σημαντικό περιουσιακό στοιχείο μιας εταιρείας το οποίο έχει αξία και πρέπει να προστατεύεται κατάλληλα. Για την προστασία της πληροφορίας οι εταιρείες πρέπει να αναπτύξουν διαδικασίες και πολιτικές ασφάλειας για να διασφαλίσουν τις τρεις βασικές αρχές της ασφάλειας πληροφοριών: την ακεραιότητα, την εμπιστευτικότητα και την διαθεσιμότητα. Στην κατεύθυνση αυτή η ανάπτυξη ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών όπως το πρότυπο ISO/IEC 27001 συμβάλλει στην βελτιστοποίηση των επιχειρηματικών διεργασιών και βοηθά την εταιρεία να προσδιορίζει και να ελέγχει τους κινδύνους που αφορούν στην ασφάλεια των πληροφοριών.

Οι απειλές που προέρχονται από τον κυβερνοχώρο έχουν αυξηθεί κατακόρυφα τα τελευταία χρόνια και οι προκλήσεις που έχουν να αντιμετωπίσουν οι εταιρείες αφορούν σοβαρά περιστατικά ασφαλείας που οφείλονται σε hacking, σε ιούς και κακόβουλα λογισμικά όπως το ransomware, αλλά και σε απώλεια δεδομένων λόγω ανθρώπινων λαθών και κλοπή υλικού όπως κινητά τηλέφωνα και φορητοί υπολογιστές των εργαζομένων. Κι ενώ οι ψηφιακές απειλές και οι κίνδυνοι είναι μία μόνο συνιστώσα που οδηγεί τις εταιρείες να προστατεύσουν την πληροφορία και τα δεδομένα τους, η θέσπιση νέου κανονιστικού πλαισίου από την Ευρωπαϊκή Ένωση όπως ο κανονισμός GDPR και η εναρμόνιση της χώρας μας με την κοινοτική νομοθεσία επιταχύνουν ακόμα περισσότερο τις διαδικασίες για την λήψη των κατάλληλων μέτρων προστασίας για την αποφυγή υψηλών προστίμων σε περίπτωση εντοπισμού περιστατικού ασφαλείας.

Η ασφάλεια έναντι των ψηφιακών απειλών δεν περιορίζεται πλέον μόνο σε μία απλή λύση antivirus ή έναν τοίχο προστασίας (firewall). Αντιθέτως, η πολυπλοκότητα

των επιθέσεων οδηγεί σε νέους μηχανισμούς ασφάλειας και οι εταιρείες πρέπει να επενδύσουν ένα μεγάλο κεφάλαιο σε συστήματα και λογισμικό για να αυξήσουν το επίπεδο ασφαλείας τους. Όπως αναφέραμε ήδη, η σύγχρονη ψηφιακή ασφάλεια, η οποία πρέπει να συνυπάρχει με την φυσική ασφάλεια, περιλαμβάνει συστήματα για την προστασία των κινητών και φορητών συσκευών, την κρυπτογράφηση αρχείων και δίσκων, την ασφάλιση του ασύρματου δικτύου, την ταξινόμηση των δεδομένων, την άμυνα πρώτης γραμμής έναντι των κυβερνοεπιθέσεων που οδηγούν σε άρνηση παροχής υπηρεσίας (DDoS), την προστασία εγγράφων κατά τη διακίνηση τους, την πρόληψη απώλειας δεδομένων, τα αντίγραφα ασφαλείας για άμεση επαναφορά της λειτουργίας της εταιρείας και πολλά άλλα. Τονίσαμε, ακόμα, ότι η ασφάλεια των πληροφοριών δεν πρέπει να είναι μόνο ευθύνη ενός IT manager, αλλά όλου του προσωπικού της εταιρείας, το οποίο πρέπει να εκπαιδευτεί κατάλληλα ώστε να μην πέφτει θύμα απάτης.

Προσπαθώντας να κατανοήσουμε τις δυσκολίες που έχουν να αντιμετωπίσουν οι επιχειρήσεις στο νέο ψηφιακό περιβάλλον, παρουσιάσαμε μία μελέτη ανάπτυξης ενός ΣΔΑΠ κατά το πρότυπο ISO/IEC 27001:2013 και μία μελέτη επικινδυνότητας αναλύοντας όλα τα μέτρα ασφαλείας που θα πρέπει να λάβει υπόψη της μία εταιρεία. Οι διαδικασίες αυτές θα πρέπει να γίνουν αναπόσπαστο κομμάτι της καθημερινής λειτουργίας της εταιρείας και να ακολουθείται πιστά η Πολιτική Ασφαλείας που θα εγκριθεί από τη διοίκηση. Μέσα από τη μελέτη περίπτωσης που παρουσιάζεται στην συγκεκριμένη εργασία γίνεται άμεσα αντιληπτό ότι η ασφάλεια πληροφοριών είναι πολυδιάστατη καθώς περιλαμβάνει πολιτικές που αφορούν την εσωτερική οργάνωση της εταιρείας, την ασφάλεια των ανθρώπινων πόρων, την διαχείριση πόρων, την διαβάθμιση των πληροφοριών, τον έλεγχο πρόσβασης και την πρόσβαση των χρηστών σε συστήματα και εφαρμογές, τις ευθύνες των χρηστών, τις ασφαλείς περιοχές της εταιρείας, την επιχειρησιακή ασφάλεια, την ασφάλεια των επικοινωνιών, τις σχέσεις με τους προμηθευτές, τη διαχείριση των περιστατικών ασφαλείας και τη συμμόρφωση της εταιρείας σε πρότυπα, κανονισμούς και νομοθεσία.

Στη συνέχεια, αναπτύσσοντας ακόμα περισσότερο τη μελέτη περίπτωσης, υπολογίσαμε το κόστος επένδυσης σε συστήματα ασφάλειας πληροφοριακών συστημάτων με βάση τις λύσεις και τις τιμές που υπάρχουν στην αγορά. Είναι γεγονός ότι η οικονομική κρίση στη χώρα μας τα τελευταία έτη έχει επηρεάσει τις δαπάνες των εταιρειών για την ασφάλεια των πληροφοριών τους. Οι εταιρείες δρουν περισσότερο αντιδραστικά και λιγότερο προληπτικά, ενώ θα έπρεπε η στρατηγική τους για την ασφάλεια πληροφοριών να είναι άμεσα εναρμονισμένη με τους επιχειρηματικούς

στόχους και τους στόχους της διοίκησης παρά με την κατάσταση της οικονομίας. Αν συγκρίνουμε μάλιστα το ποσό που θα πρέπει να δαπανήσουν για λύσεις ασφαλείας με το κόστος που θα προκύψει μετά από ένα περιστατικό ασφαλείας και τις συνέπειες με τις οποίες θα βρεθούν αντιμέτωπες, τότε είναι προφανές ότι η επένδυση σε συστήματα ασφαλείας θα έπρεπε να είναι μονόδρομος.

Μιλώντας για συνέπειες, αυτές δε θα πρέπει να περιορίζονται μόνο στο άμεσο οικονομικό τίμημα όπως για παράδειγμα τα έξοδα για την αντιμετώπιση ενός περιστατικού ασφαλείας. Υπάρχουν συνέπειες οι οποίες θα φέρουν αρνητικά αποτελέσματα σε βάθος χρόνου τα οποία θα προκληθούν από την αρνητική φήμη της εταιρείας. Οι πελάτες, οι συνεργάτες, οι προμηθευτές και γενικά όλο το περιβάλλον της επιχείρησης θα επηρεαστεί αρνητικά από ένα γεγονός παραβίασης δεδομένων. Απώλεια εσόδων, πρόστιμα και αποζημιώσεις, έξοδα νομικής προστασίας, προβλήματα στην επιχειρησιακή της λειτουργία, απολύσεις εργαζόμενων και διευθυντικών στελεχών είναι μόνο μερικές από τις συνέπειες που πρόκειται να ακολουθήσουν. Μπροστά σε όλα αυτά τα ζητήματα μπορούμε με σιγουριά να καταλήξουμε στο συμπέρασμα ότι οι συνέπειες ενός λάθους έχουν μεγαλύτερο κόστος από το κόστος πρόληψής του.

Κι αν το παρόν φέρει προκλήσεις, το μέλλον αναμένεται να διαμορφώσει ένα ακόμα πιο συναρπαστικό περιβάλλον για τις επιχειρήσεις. Οι κινητές συσκευές, οι πρακτικές «Φέρε τη δική σου συσκευή» στον χώρο εργασίας (Bring Your Own Device – BYOD), τα μέσα κοινωνικής δικτύωσης και οι τεχνολογίες Cloud αναμένεται να υιοθετηθούν από όλες τις επιχειρήσεις ώστε να παραμείνουν ανταγωνιστικές. Δυστυχώς όμως η εξέλιξη της τεχνολογίας δίνει χώρο και στην εξέλιξη των ψηφιακών απειλών. Οι απειλές γίνονται ακόμα πιο οργανωμένες και συντονισμένες και οι χάκερ εφευρίσκουν συνεχώς νέες μεθόδους για να προσελκύουν τα θύματα τους. Ακόμα και όσες εταιρείες δεν διαθέτουν μια στρατηγική ασφάλειας πληροφοριών θα αναγκαστούν να υιοθετήσουν για να αντιμετωπίσουν αποτελεσματικά τις αναδυόμενες απειλές.

Η ασφάλεια στον κυβερνοχώρο είναι και θα είναι ακόμα περισσότερο μείζον θέμα για τις επιχειρήσεις. Για το λόγο αυτό οι αποφάσεις για την ασφάλεια πληροφοριών οφείλουν να είναι ευθύνη της διοίκησης. Ο διευθύνων σύμβουλος θα πρέπει να είναι όχι απλά ενήμερος αλλά και γνώστης των πολιτικών ασφάλειας της εταιρείας του, των συστημάτων και των υποδομών που διαθέτει. Το ζήτημα της ασφάλειας πληροφοριών δεν θα πρέπει να θεωρείται θέμα τεχνολογίας, αλλά μία κρίσιμη λειτουργία που θα πρέπει να ενταχθεί μέσα στο επιχειρησιακό πλάνο και στα επιχειρησιακά σχέδια της εταιρείας.

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΠΗΓΕΣ

[1] Επίσημη εφημερίδα της Ευρωπαϊκής Ένωσης, (2016) *ΟΔΗΓΙΑ (ΕΕ) 2016/1148 ΤΟΥ ΕΥΡΩΠΑΪΚΟΫ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ της 6ης Ιουλίου 2016 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση,*

https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016L1148

[2] Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, http://www.dpa.gr

[3] ΣΕΒ, Οικονομία & Επιχειρήσεις, Special Report, Προστασία Προσωπικών Δεδομένων, Τεύχος 23, 14 Μαρτίου 2018

[4] Priority AE, http://www.priority.com.gr/page/iso27001foryou/

[5] Κυπριακή Εταιρεία Πιστοποίησης, Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών ISO/IEC 27001, http://www.cycert.org.cy/index.php/el/2014-10-16-16-20-04/2014-10-17-16-15-03/item/31-systima-diaxeirisis-asfaleias-pliroforion-iso-iec-27001

[6] Υπουργείο Ψηφιακής Πολιτικής, Τηλεπικοινωνιών και Ενημέρωσης, Εθνική Στρατηγική Κυβερνοασφάλειας, http://mindigital.gr/index.php/kyvernoasfaleia/2055-ethniki-stratigiki-kyvernoasfaleias

[7] G Curtis, D Cobham, *Business Information Systems,* 6η έκδ., Pearson, 2008

[8] IT Security Pro, Πολιτική ασφάλειας πληροφοριών: Τα 10 μυστικά της επιτυχίας!, Ελένη Σωτηρίου [1 Μαρτίου 2009], https://www.itsecuritypro.gr/politiki-asfalias-pliroforion-ta-10-mystika-tis-epitychias/

[9] EU GDPR.ORG, https://eugdpr.org/the-regulation/gdpr-faqs/

[10] Μαυρίδης Ιωάννης (2015), *Ασφάλεια Πληροφοριών στο Διαδίκτυο*, Σύνδεσμος Ελληνικών και Ακαδημαϊκών Βιβλιοθηκών (ΣΕΑΒ)

[11] Europa.eu, Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA), https://europa.eu/european-union/about-eu/agencies/enisa_el

[12] Ευρωπαϊκό Συμβούλιο – Συμβούλιο της Ευρωπαϊκής Ένωσης, Η ΕΕ θα δημιουργήσει κοινό πλαίσιο πιστοποίησης της κυβερνοασφάλειας και θα ενισχύσει τον αντίστοιχο Οργανισμό της - καθορισμός της θέσης του Συμβουλίου, [Δελτίο τύπου 08/06/2018], http://www.consilium.europa.eu/el/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/

[13] IT Security Pro, NIS – Η νέα οδηγία για την κυβερνοασφάλεια, Ευαγγελία Βαγενά, [19 Ιουλίου 2017], https://www.itsecuritypro.gr/nis-nea-odigia-gia-tin-kyvernoasfalia/

[14] IT Security Pro, Περί κινδύνων ο λόγος... Διαχείριση και αντιμετώπιση τους, Νότης Ηλιόπουλος, [1 Σεπτεμβρίου 2008], https://www.itsecuritypro.gr/peri-kindynon-o-logos-diachirisi-ke-antimetopisi-tous-2/

[15] IT Security Pro, Διαχείριση Ασφάλειας Πληροφοριών: Η Σύγχρονη Επιχειρησιακή Αναγκαιότητα, Νότης Ηλιόπουλος, [1 Ιουλίου 2008], https://www.itsecuritypro.gr/diachirisi-asfalias-pliroforion-sygchroni-epichirisiaki-anagkeotita-2/

[16] 2018 Cost of a Data Breach Study: Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC Global Overview

[17] MSN ειδήσεις, Οι 10 υποθέσεις παραβίασης προσωπικών δεδομένων που συγκλόνισαν τον κόσμο, [25/05/2018], https://www.msn.com/el-gr/news/techandscience/οι-10-υποθέσεις-παραβίασης-προσωπικών-δεδομένων-που-συγκλόνισαν-τον-κόσμο/ar-AAxLX3m

[18] «Threatsaurus, The A-Z of computer and data security threats», 2013 Sophos in collaboration with the Center for Internet Security, Sophos Ltd

[19] https://el.wikipedia.org, Ιός υπολογιστή

[20] 2004 ΕΡΓΑΣΤΗΡΙΟ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΣΤΑ ΜΜΕ, Ιοί υπολογιστών, http://pacific.jour.auth.gr/virus/

[21] Νέα σχετικά με ασφάλεια και spyware, ioys.gr

[22] Think tech, Τι είναι η επίθεση DDoS και πως γίνεται;, [18 Ιουνίου 2015], https://thinktech.gr

[23] Sophos News, Introducing Sophos Phish Threat: the world's easiest-to-use attack simulator, Bill Lucchini, [25/01/2017], https://news.sophos.com/en-us/2017/01/25/introducing-sophos-phish-threat-the-worlds-easiest-to-use-attack-simulator/

[24] Boldon James, Driving data security awareness to transform security culture, Steve Cooper, [13/06/2018], https://www.boldonjames.com/out-of-the-box-data-classification/

[25] Netsparker blog, Vulnerability Assessments and Penetration Tests – What's the Difference?,Dawn Baird, [06/09/2018], https://www.netsparker.com/blog/web-security/difference-between-vulnerability-assessments-and-penetration-tests/

[26] Sophos News, What is… cryptojacking?, John Shier, [31/07/2018], https://news.sophos.com/en-us/2018/07/31/what-is-cryptojacking/

[27] Cyberark blog, 7 Types of Privileged Accounts You Should Know, Amy Burnis, [November 01, 2017], https://www.cyberark.com/blog/7-types-privileged-accounts-know/

[28] IT Security Pro, Το 50% των στελεχών στην Ελλάδα γνωρίζει τι προβλέπει ο GDPR, [09 Ιουλίου 218], https://www.itsecuritypro.gr/to-50-ton-stelechon-stin-ellada-gnorizei-ti-provlepei-o-gdpr/

[29] IT Security Pro, Ασφάλεια Email ..οι απάτες, οι επιθέσεις & οι τρόποι προστασίας, [16 Ιουλίου 2018], https://www.itsecuritypro.gr/asfaleia-email-oi-apates-oi-epitheseis-amp-oi-tropoi-prostasias/

[30] Kroll «Global Fraud & Risk Report, 10th Annual Edition – 2017/18»

[31] Vodafone Cyber Security Report 2017, Vodafone Group

[32] Vodafone Cyber Ready Barometer 2018, Vodafone Group

[33] IT Security Pro, Στα $133,7 δισ. οι παγκόσμιες δαπάνες για λύσεις ασφαλείας έως το 2022, [14 Οκτωβρίου 2018], https://www.itsecuritypro.gr/sta-133-7-dis-oi-pagkosmies-dapanes-gia-lyseis-asfaleias-eos-to-2022/

[34] Κάτσικας Σωκράτης (2001), *Ασφάλεια Υπολογιστών, Τόμος Α'*, ΕΑΠ, Πάτρα

[35] IT Security Pro, Διαχείριση Επιχειρησιακής Συνέχειας: Σύστημα & Στόχοι, Νότης Ηλιόπουλος, [01 Σεπτεμβρίου 2013], https://www.itsecuritypro.gr/diachirisi-epichirisiakis-synechias-systima-stochi/

[36] Real Insurance Brokers, Ηλεκτρονικοί κίνδυνοι & Κυβερνοασφάλεια, Κωνσταντίνος Κατσίφης, [02/11/2017], http://www.real-insurance.gr/el/news/electroniki-asfaleia-cybersecurity-gr

[37] Ευρωπαϊκή Επιτροπή, Τι είναι η παραβίαση δεδομένων και τι πρέπει να κάνουμε σε περίπτωση παραβίασης δεδομένων;, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_el

[38] Texnologia.net, Η ψηφιακή επιχείρηση σας απαιτείται να προστατευτεί από το hacking, Στέλιος Θεοδωρίδης, [13 Οκτωβρίου 2017], https://texnologia.net/h-psifiaki-sas-epixeirhsh-apaiteitai-na-prostateutei-apo-hacking/2017/10

[39] Ευρωπαϊκή Επιτροπή, Κατάσταση της Ένωσης 2017: Η Επιτροπή αναβαθμίζει την απόκρισή της στις κυβερνοεπιθέσεις, [Δελτίο τύπου 19 Σεπτεμβρίου 2017], http://europa.eu/rapid/press-release_MEMO-17-3194_el.htm

[40] Insurance world, Η ασφάλεια των πληροφοριών αποτελεί ευθύνη του διευθύνοντος συμβούλου και των ανώτατων στελεχών, Νίκος Γεωργόπουλος, 64-66, [Σεπτέμβριος-Οκτώβριος 2015]