ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«ΑΣΦΑΛΕΙΑ ERP ΣΥΣΤΗΜΑΤΩΝ»

Της φοιτήτριας:
Παρασκευαΐδου Ελισάβετ
Αρ. Μητρώου: 185445

Επιβλέπων
Ονοματεπώνυμο: Ηλιούδης Χρήστος
Βαθμίδα Καθηγητής

Ημερομηνία Μάϊος 2023

Τίτλος Ασφάλεια ERP συστημάτων
Κωδικός 23127
Ονοματεπώνυμο φοιτητή: Παρασκευαΐδου Ελισάβετ
Ονοματεπώνυμο εισηγητή: Ηλιούδης Χρήστος
Ημερομηνία ανάληψης 07/03/2023
Ημερομηνία περάτωσης Δ.Ε. 24/5/2023

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Η παρούσα διπλωματική εργασία εκπονήθηκε κατά την περίοδο του θερινού Ακαδημαϊκού εξαμήνου 2023 και ο λόγος της επιλογής του παρόντος θέματος ήταν η ραγδαία αύξηση των κυβερνοεπιθέσεων στις εταιρείες και η ανάγκη προστασίας των προσωπικών δεδομένων που αυτές διαχειρίζονται κυρίως με τα ERP λογισμικά. Αντικείμενο μελέτης είναι η λειτουργία των ERP λογισμικών, η ασφάλεια τους και η καταγραφή των ευάλωτων σημείων τους. Επιπλέον, η εργασία αυτή καταγράφει μερικές δηλωμένες επιθέσεις που έχουν πραγματοποιηθεί σε αυτά. Περιλαμβάνεται επίσης ο τρόπος με τον οποίο μπορεί να πραγματοποιηθεί μια επίθεση με σκοπό την πληρέστερη κατανόηση των απειλών. Στόχος της παρούσας εργασίας είναι η κατανόηση όλων των παραπάνω έτσι ώστε να μπορούν να εφαρμοστούν τα κατάλληλα μέτρα για την προστασία του ERP συστήματος.

Περίληψη

Τα ERP συστήματα είναι ένα λογισμικό το οποίο βρίσκει ολοένα και μεγαλύτερη αναγνώριση από όλους τους επιχειρηματικούς κλάδους. Μαζί με τα ERP όμως, ραγδαία εξέλιξη εμφανίζουν και οι κυβερνοεπιθέσεις σε αυτά. Γνωρίζοντας ότι τα ERP είναι συστήματα που διαχειρίζονται πολλών ειδών ευαίσθητες πληροφορίες, είναι ζωτικής σημασίας να εφαρμοστούν τα αναγκαία μέτρα προστασίας του συστήματος από όλους τους οργανισμούς και τις επιχειρήσεις. Έχοντας ως στόχο την σωστή εφαρμογή αυτών των μέτρων, στην παρούσα διπλωματική θα αναφερθούμε στην έννοια του ERP καθώς και στο πώς αυτό δουλεύει, στην σημασία της προστασίας των δεδομένων, στην έννοια της κυβερνοεπίθεσης και στους τρόπους που αυτή πραγματοποιείται ανάλογα με τον τύπο της. Επιπλέον, θα αναφερθούμε σε δηλωμένες επιθέσεις που έχουν λάβει χώρα σε αυτά τα λογισμικά. Τέλος αφού αναφέρουμε τα βασικότερα βήματα για την προστασία του ERP συστήματος θα αναλύσουμε ένα πλαίσιο με στόχο την κατανόηση της σημασίας της χαρτογράφησης της επιχείρησης και την ακόλουθη εφαρμογή των μέτρων προστασίας.

«Security in ERP Systems»

«Elizabeth Paraskevaidou»

Abstract

ERP systems are a software that is finding more and more recognition from all business sectors. Along with ERPs, however, cyber-attacks on them are also showing rapid development. We know that ERP are systems that manage a lot of sensitive information, it is vital for all organizations and businesses to implement the necessary system protection measures. Aiming at the correct implementation of these measures, in this diplomacy we will refer to the concept of ERP as well as how it works, the importance of data protection, the concept of cyber attack and the ways in which it is carried out depending on its type. In addition, we will refer to reported attacks that have taken place on these softwares. Finally, after mentioning the most basic steps for the protection of the ERP system, we will analyze a framework with the aim of understanding the importance of business mapping and the following application of protection measures.

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

2FA	Two-factor Authentication
AES	Advances Encryption Standard
ALARP	As Low As Reasonably Practicable
ASAP	Accelerated Systems, Applications and Products in Data Processing
CCTV	Closed Circuit Television
CD	Compact Disc
COBIT	Control Objectives for Information and Related Technologies
CPU	Central Processing Unit
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerabilities and Exposures
DAC	Digital (to) Analog Converter
DDoS	Distributed Denial-of-Service
DEM	Dynamic Enterprise Modeler
DNS	Domain Name System
DVD	Digital Video Disc
ERP	Enterprise Resource Planning
GDPR	General Data Protection Regulation
GUI	Graphical User Interface
ISO	International Organization for Standardization
MAC	Media Access Control
MD5	Message-Digest Algorithm
MFA	Multifactor Authentication
NIST	National Institute of Standards and Technology
RBAC	Role-based access control
SAP	Systems, Applications and Products in Data Processing
SHA	Secure Hash Algorithms
SMB	Server Message Block
SMS	Short Message Service
SQL	Structured Query Language
SSH	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
VPD	Virtual Private Database table

VPN	Virtual Private Network
WIDS	Wireless Intrusion Detection System
WPA	Wireless Protected Access
ΑΠΕΔ	Αρχή Πιστοποίησης Ελληνικού Δημοσίου

Κεφάλαιο 1: Εισαγωγή

ERP συστήματα, είναι όλα εκείνα τα λογισμικά τα οποία αποτελούνται από ένα σύνολο λειτουργειών που αποσκοπούν στην υποστήριξη των εταιρειών, προσφέροντας τους όλους τους απαραίτητους επιχειρηματικούς μηχανισμούς που χρειάζονται, ομαδοποιημένους σε ένα ενιαίο σύστημα. Τα συστήματα αυτά, πρωτοεμφανίστηκαν την δεκαετία του 60 και κατάφεραν να εξελιχθούν σε ένα σχετικά γρήγορο χρονικό διάστημα. Για την ακρίβεια το πρώτο ολοκληρωμένο ERP εμφανίστηκε στις αρχές του 90 και λειτουργούσε μόνο σε τοπικές (*on-premise*) εγκαταστάσεις. Έξι χρόνια αργότερα δημιουργήθηκε από την Oracle το πρώτο ERP που λειτουργούσε σε "σύννεφο" (*cloud*) μορφή. Αυτή η μορφή ήταν που οδήγησε όλα τα επιχειρησιακά λειτουργικά συστήματα σε ραγδαία εξέλιξη στη σημερινή εποχή. Με την cloud εγκατάσταση το κόστος του συστήματος μειώθηκε σημαντικά και πλέον μπορούν ακόμη περισσότερες μικρομεσαίες επιχειρήσεις να εντάξουν ένα επιχειρησιακό λειτουργικό σύστημα στην επιχείρησή τους.

Με άλλα λόγια, τα ERP είναι ένα εργαλείο που λύνει τα χέρια σε όλους τους επιχειρηματίες, σε όλους τους επιχειρησιακούς κλάδους, που διαχειρίζονται οικονομικά στοιχεία, στοιχεία αποθήκης, στοιχεία πελατών/προμηθευτών/εργαζομένων και πολλά άλλα. Μπορεί να χρησιμοποιηθεί στον βιομηχανικό κλάδο, στον κλάδο τις ναυτιλίας, στον ξενοδοχειακό κλάδο, στον κλάδο της ιατρικής, στον στρατιωτικό κλάδο αλλά και σε όλους εκείνους τους κλάδους που χρειάζονται μια ομαδοποιημένη και σύγχρονη λύση για την καλύτερη επίβλεψη των αναγκών τους.

Οι λειτουργίες που περιέχουν τα επιχειρησιακά λογισμικά, αποθηκεύουν και διαχειρίζονται κρίσιμα δεδομένα για την κάθε επιχείρηση τα οποία εάν υποκλαπούν μπορούν να προκαλέσουν μεγάλη ζημιά. Οι πληροφορίες που διαχειρίζονται είναι είτε προσωπικά στοιχεία εργαζομένων ή και γενικές πληροφορίες των ανθρώπων που συναναστρέφονται με την επιχείρηση, είτε ακόμη και οικονομικά στοιχεία. Τα τελευταία χρόνια, λόγο της ραγδαίας αύξησης των ERP συστημάτων, οι χάκερς, γνωρίζοντας την σημαντικότητα που έχουν αυτά τα συστήματα για την εταιρεία, επιτίθονται ολοένα και περισσότερο. Επιπλέον, το γεγονός ότι τα συστήματα αυτά, για μεγαλύτερη διευκόλυνση προς τους πελάτες, είναι πλέον διαθέσιμα και σε cloud μορφή τα καθιστά ακόμη πιο ευάλωτα σε πιθανές επιθέσεις.

Ξέροντας ότι τα επιχειρησιακά λογισμικά δεν αγοράζονται μόνο από μικρομεσαίες και μεγάλες επιχειρήσεις αλλά και από κρατικές υπηρεσίες όπως είναι ο στρατός, είναι σημαντικό να δώσουμε μεγάλη βαρύτητα στους μηχανισμούς και στα μέσα για την προστασία αυτών των συστημάτων από πιθανές επιθέσεις. Είναι ζωτικής σημασίας η συνεχής ενημέρωση των χρηστών αλλά και η τεχνολογική εξέλιξη στον τομέα της ασφάλειας για να επιτευχθεί όσο τον δυνατόν γίνεται η ασφάλεια των ERP συστημάτων.

1.1 Σκοπός – Στόχοι

Ο σκοπός και οι στόχοι αυτής της διπλωματικής εργασίας είναι η μελέτη και καταγραφή των θεμάτων ασφαλείας στα ERP συστήματα. Αναλυτικότερα, στόχος της είναι η αξιολόγηση των καταγεγραμμένων ευπαθειών που έχουν εμφανισθεί στα ERP, να καταγράψει τις τεχνολογίες και τους μηχανισμούς ασφαλείας που εφαρμόζονται στα συστήματα αυτά, να αναλύσει το πλαίσιο και τις καλές πρακτικές ασφαλείας των συστημάτων αυτών και τέλος να παρουσιάσει μια μελέτη περίπτωσης και εφαρμογής.

1.2 Επιτεύγματα

Στην παρούσα διπλωματική αφού αναλύσαμε τα βασικά χαρακτηριστικά των ERP συστημάτων και εξηγήσαμε τον λόγο για τον οποίο είναι χρήσιμο ένα τέτοιο λογισμικό, εξηγήσαμε την σημαντικότητα των πληροφοριών που αυτό διαχειρίζεται καθώς και τους λόγους για τους οποίους είναι ζωτικής σημασίας η προστασία αυτών των δεδομένων. Έπειτα, σειρά είχε η καταγραφή των μέτρων ασφαλείας που χρησιμοποιούν μέχρι και σήμερα οι εταιρείας παραγωγής ERP λογισμικού αλλά και τις αδυναμίες που έχουν τα ERP και τα καθιστούν ευάλωτα σε κυβερνοεπιθέσεις. Στην συνέχεια έγινε μια εκτενής καταγραφή μερικών κυβερνοεπιθέσεων που έλαβαν χώρα σε διάφορα ERP λογισμικά ανά τον κόσμο. Σειρά έχει η ανάλυση των σταδίων για την πραγματοποίηση μια επίθεσης, οι τύποι των επιθέσεων που υπάρχουν καθώς και οι επιπτώσεις που δέχεται μια εταιρεία στην περίπτωση που πέσει θύμα κυβερνοεπίθεσης. Επιπλέον, έγινε αξιολόγηση των επιθέσεων στις πέντε κορυφαίες εταιρείες παραγωγής ERP λογισμικού ανά έτος και ανά τύπο επίθεσης. Επίσης, έγινε μια πλήρης καταγραφή των απαραίτητων μέτρων ασφαλείας που θα πρέπει να τηρούν οι εταιρείες προκυμμένου να κρατήσουν ασφαλής το σύστημα τους και κατά συνέπεια το ERP λογισμικό τους από κυβερνοεπιθέσεις καθώς επίσης αναλύθηκε ένα πλαίσιο για την επιτυχής ένταξη των μέτρων ασφαλείας στην εταιρεία. Τέλος, μελετήθηκε η περίπτωση ασφαλείας των e-invoicing και προτάθηκαν κάποια μέτρα για την ασφάλεια τους.

1.3 Διάρθρωση της μελέτης

Η διπλωματική εργασία χωρίζεται σε πέντε κεφάλαια.

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στο θέμα της παρούσας διπλωματικής, όπου επισημαίνεται ο στόχος της διπλωματικής και αναλύονται οι ανάγκες που οδήγησαν στην σύνταξή της.

Στο δεύτερο κεφάλαιο γίνεται η καταγραφή των βασικών χαρακτηριστικών των ERP συστημάτων. Στα χαρακτηριστικά αυτά εντάσσεται, η αρχιτεκτονική, το μοντέλο εφαρμογής, οι τρόποι εγκατάστασης, τα πλεονεκτήματα που έχει η κάθε εγκατάσταση και σχετίζονται με την παρούσα διπλωματική, τα γενικότερα πλεονεκτήματα και μειονεκτήματα των ERP και τέλος τα κριτήρια για την σωστή επιλογή ενός ERP λογισμικού.

Έπειτα, στο κεφάλαιο τρία γίνεται αναφορά στην ασφάλεια των δεδομένων και στους λόγους για τους οποίους είναι ζωτικής σημασίας η ασφάλεια στα ERP συστήματα. Επίσης, αναφέρονται οι μηχανισμοί ασφαλείας που χρησιμοποιούν μέχρι και σήμερα οι εταιρείες παραγωγής ERP λογισμικού καθώς και οι αδυναμίες που υπάρχουν σε αυτά τα συστήματα και οδηγούν σε κυβερνοεπιθέσεις. Επιπλέον, καταγράφονται μερικές κυβερνοεπιθέσεις που έχουν πραγματοποιηθεί σε ERP λογισμικά ανά τον κόσμο και στην συνέχεια περιγράφονται τα στάδια για την ολοκλήρωση μια επίθεσης, οι τύποι των επιθέσεων που υπάρχουν μέχρι στιγμής καθώς και οι επιπτώσεις που δέχονται οι εταιρείες σε περίπτωση που πέσουν θύμα κυβερνοεπίθεσης.

Συνεχίζοντας, στο κεφάλαιο τέσσερα, γίνεται αξιολόγηση των επιθέσεων στις πέντε κορυφαίες εταιρείες παραγωγής ERP λογισμικού ανά έτος και ανά τύπο επίθεσης. Συγκεκριμένα, η αξιολόγηση χωρίζεται σε δύο μέρη τα οποία περιλαμβάνουν αντιστοίχως ένα γράφημα ανά έτος και ένα γράφημα ανά τύπο επίθεσης. Η πρώτο μέρος αναφέρεται στις επιθέσεις και στους τύπους επιθέσεων που έλαβαν χώρα από το 2017 έως και το 2022 ενώ το δεύτερο αναφέρεται στις επιθέσεις και στους τύπους επιθέσεων που έλαβαν χώρα κατά την διάρκεια της πανδημίας (έτος 2020-2022). Τέλος γίνεται σύγκριση των δύο μερών ανά γράφημα αντίστοιχα.

Στο πέμπτο κεφάλαιο, καταγράφονται τα απαραίτητα μέτρα προστασίας που πρέπει να λάβουν υπόψιν τους οι εταιρείες εφόσον θέλουν να διατηρήσουν ασφαλές το σύστημα τους και κατά συνέπεια το ERP λογισμικό τους από κυβερνοεπιθέσεις καθώς επίσης αναλύεται και ένα πλαίσιο για την επιτυχής ένταξη των μέτρων ασφαλείας στην εταιρεία.

Στο έκτο και προτελευταίο κεφάλαιο επικεντρωνόμαστε στην ασφάλεια της ηλεκτρονικής τιμολόγησης. Συγκεκριμένα αφού περιγράφουμε την έννοια της ηλεκτρονικής τιμολόγησης και τους λόγους για τους οποίους είναι απαραίτητη η προστασία, αναφερόμαστε σε κάποια βασικά θέματα ασφαλείας που υπάρχουν σε αυτά, στις απαιτήσεις ασφαλείας και τέλος καταγράφουμε μερικά μέτρα προστασίας που προτείνουμε για την διασφάλιση της μέγιστης ασφάλειας.

Τέλος η παρούσα διπλωματική ολοκληρώνεται με το έβδομο κεφάλαιο το οποίο περιλαμβάνει τα συμπεράσματα που πάρθηκαν μετά το πέρας της συγγραφής καθώς και τις μελλοντικές επεκτάσεις που προτείνουμε και αφορούν την χρήση του blockchain.

1.4 Επίλογος

Έχοντας ολοκληρώσει την παρούσα μελέτη καταλήγουμε στα συμπέρασμα ότι οι ασφάλεια των δεδομένων που διαχειρίζεται μια εταιρεία στο ERP λογισμικό της είναι ζωτικής σημασίας. Οι συνέπειες που θα δεχτεί σε περίπτωση κυβερνοεπίθεσης είναι πολύ μεγάλες. Πέραν των χρηματικών ποσών που θα χάσει, αυτομάτως μειώνει και την εμπιστοσύνης της προς τους πελάτης και τους προμηθευτές της. Για τον λόγο αυτό και κυρίως λόγο της ραγδαίας αύξησης των κυβερνοεπιθέσεων τα τελευταία χρόνια, έχουν αναπτυχθεί κάποια πρότυπα για την ασφάλεια των συστημάτων και την σωστή εφαρμογή των μέτρων που περιέχουν αυτά τα πρότυπα. Είναι σημαντικό όλες οι εταιρείες που νοιάζονται για τους ανθρώπους με τους οποίους συναναστρέφονται να τηρούν τα πρότυπα για την ασφάλεια του συστήματος από κυβερνοεπιθέσεις.

Κεφάλαιο 2ο : Χαρακτηριστικά των ERP συστημάτων

2.1 Ορισμός

Τα συστήματα ERP είναι λογισμικό που βοηθά τους επιχειρηματίες να οργανώσουν και να διαχειριστούν τις εγκαταστάσεις τους. Πλέον το μεγαλύτερο ποσοστό των εταιρειών σε παγκόσμιο επίπεδο χρησιμοποιεί κάποιο ERP λογισμικό για την βέλτιστη επίβλεψη της εταιρείας τους. Το ERP λογισμικό παρέχει μια πλήρη σουίτα λειτουργιών, περιλαμβανομένης της οικονομικής διαχείρισης της εταιρείας (όπως η γενική λογιστική, η λογιστική κόστους και η διαχείριση των παγίων των περιουσιακών στοιχείων), των διεθνών λογιστικών πρότυπων, της διοικητικής λογιστικής του προϋπολογισμού και του ελέγχου, της εμπορικής και πιστωτικής πολιτικής, της διαχείριση της χρηματοοικονομικής κατάστασης, της χρηματορροής των εισπρακτέων και των πληρωτέων της επιχείρησης, των αποθεμάτων και των αποθηκών, των πωλήσεων και των διανομών, των αγορών και των προμηθειών, της παραγωγής αλλά και της διαχείριση των έργων. Με άλλα λόγια ένα ERP σύστημα καλύπτει όλες τις ανάγκες που μπορεί να έχει ένας επιχειρηματίας και τον βοηθάει να έχει μια ολοκληρωμένη εικόνα των επιχειρήσεων του.

Σχήμα 2.1: Ενότητες που υποστηρίζουν τα ERP

2.2 Η αξία του περιεχομένου και των διαδικασιών

Όπως ήδη αναφέρθηκε, στόχος των ERP είναι η διευκόλυνση της λειτουργίας μιας εταιρείας. Για να επιτευχθεί αυτό με τον καλύτερο δυνατό τρόπο, είναι απαραίτητο το ERP σύστημα να διαχειρίζεται σημαντικές πληροφορίες μιας επιχείρησης με πολύ καλά σχεδιασμένες και οργανωμένες διαδικασίες. Οι σωστά αναπτυγμένες διαδικασίες των ERP μπορούν να διασφαλίσουν την αποτροπή τυχόν λαθών του χρήστη και συνεπώς να προστατεύσουν τις πληροφορίες της επιχείρησης από ακούσια έκθεση σε λάθος άτομα.

2.3 Αρχιτεκτονική υλοποίησης ERP συστήματος

Η αρχιτεκτονική υλοποίηση ενός ERP συστήματος είναι η διαδικασία κατά την οποία συνδυάζονται οι καλύτερες πρακτικές για να δημιουργηθεί ένα άριστο και πλήρως αποδοτικό σύστημα για τον τελικό χρήστη. Μερικές από αυτές τις πρακτικές είναι η εμφάνιση, η δομή αλλά και η γενική συμπεριφορά του συστήματος. Υπάρχουν πολλά μοντέλα αρχιτεκτονικής για την υλοποίηση ενός ERP

αλλά το πιο διαδεδομένο και το πιο συχνά χρησιμοποιούμε μοντέλο είναι αυτό των τριών επιπέδων (*The 3 Landscape Architecture*). Ένα από τα πιο γνωστά ERP στην Ελλάδα της εταιρείας "SoftOne" είναι και αυτή ένα από τα πολλά συστήματα που χρησιμοποιούν αυτό το μοντέλο αρχιτεκτονικής για την ανάπτυξη της εφαρμογής του ERP.

2.3.1 Μοντέλο τριών επιπέδων

Το μοντέλο αυτό, όπως λέει και το όνομα του χωρίζεται σε τρία επίπεδα (*layers*), τη βάση δεδομένων (Database Server), τον διακομιστή εφαρμογής (*Application Server*) και το λογισμικό (*Client*).

Βάση δεδομένων - Database Server

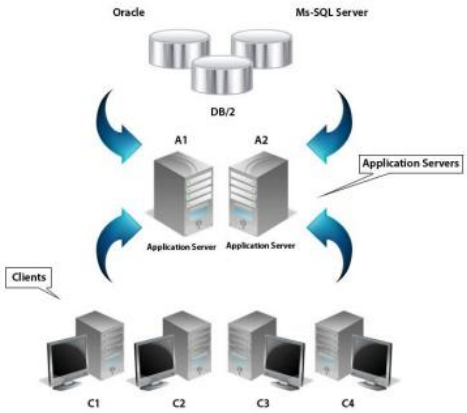
Αυτό το επίπεδο είναι υπεύθυνο για την διαχείριση και την αλληλεπίδραση των δεδομένων (*data*) που υπάρχουν στο σύστημα. Εδώ γίνεται η αποθήκευση, η διαγραφή, η δημιουργία ή ενημέρωση, η ανάκτηση αλλά και η συντήρηση των δεδομένων. Όλα τα παραπάνω, πραγματοποιούνται, χρησιμοποιώντας την Δομημένη Γλώσσα Ερωτημάτων ή αλλιώς SQL, που είναι ιδανική για την διαχείριση δεδομένων. Επιπλέον σε αυτό το επίπεδο υπάρχουν όλοι οι απαραίτητοι μηχανισμοί για την ακεραιότητα των δεδομένων.

Διακομιστής εφαρμογής - Application Server

Αποτελεί το κύριο κομμάτι του λογισμικού και για τον λόγο αυτό πολλοί το θεωρούν την «καρδία» του ERP συστήματος. Εδώ εκτελούνται οι περισσότερες λειτουργίες, εκτός των λειτουργιών που αφορούν τη διαμόρφωση των οθονών εργασίας. Μερικές από τις λειτουργίες αυτές είναι η ανταλλαγή των δεδομένων από και προς το database server, η μοντελοποίηση και η εκτέλεση της επιχειρηματικής λογικής. Η ταυτόχρονη όμως χρήση αυτών των λειτουργιών επιβαρύνουν το σύστημα και για αυτό δίνεται η δυνατότητα εγκατάστασης του Application Server παραπάνω από μία φορά, σε διαφορετικό server. Αυτό εξυπηρετεί στη μέγιστη αξιοποίηση της υπολογιστικής ισχύος και στην βελτίωση της ανταπόκρισης, της αξιοπιστίας και της επεκτασιμότητας των αποτελεσμάτων.

Λογισμικό - Client

Το τρίτο και τελευταίο επίπεδο αποτελεί τη διεπαφή του χρήστη με το σύστημα. Για την επίτευξη αυτής της διεπαφής χρησιμοποιείται ένα γραφικό περιβάλλον ή αλλιώς GUI. Μέσω αυτού του περιβάλλοντος, ο τελικός χρήστης ζητάει τα δεδομένα και τις πληροφορίες που θέλει από το σύστημα αλλά και εισάγει τα δικά του δεδομένα. Η κατανάλωση της υπολογιστικής ισχύος σε αυτό το επίπεδο είναι πάρα πολύ μικρή γιατί η επικοινωνία του Λογισμικού με τον Διακομιστή εφαρμογής γίνεται με την χρήση ενός μόνο πακέτου. Επιπλέον, να σημειωθεί ότι το τρίτο επίπεδο (*client*) δεν έχει άμεση πρόσβαση με το πρώτο επίπεδο (*database server*), αλλά η επικοινωνία αυτή πραγματοποιείται μόνο μέσω του δεύτερου επιπέδου (*application server*).



Σχήμα 2.2: Αρχιτεκτονική τριών επιπέδων

2.4 Μοντέλο εφαρμογής

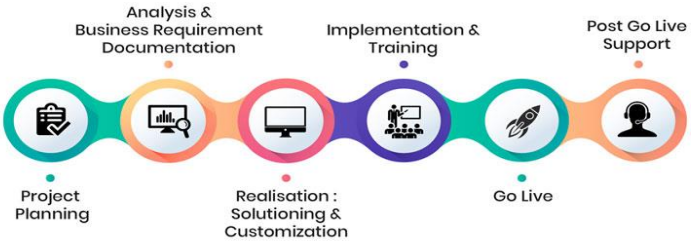
Το μοντέλο εφαρμογής είναι μια δύσκολη και απαιτητική διαδικασία γιατί βάση αυτής, ο πελάτης θα αποφασίσει ποιο ERP σύστημα και από ποιον προμηθευτή θα το αγοράσει. Τα βήματα για την υλοποίηση αυτού του μοντέλου χρήζουν μεγάλης προσοχής και οι εμπλεκόμενοι θα πρέπει να γνωρίζουν πολύ καλά τη διαδικασία. Το μοντέλο που θα συζητήσει αυτή η διπλωματική, είναι το μοντέλο "ASAP" το οποίο αποτελείται από 6 επιμέρους βήματα.

2.4.1 ASAP μοντέλο

Το ASAP μοντέλο ή αλλιώς γνωστό και ως "Accelerated SAP" είναι μια μέθοδος για την προετοιμασία και την υλοποίηση έργων που σχετίζονται με το SAP (Systems Applications and Products in Data Processing). Αυτό το μοντέλο όχι μόνο αξιολογεί το έργο αλλά είναι ικανό να διαχειρίζεται και τους κινδύνους. Ο λόγος για την δημιουργία του ASAP ήταν να βοηθήσει την ομάδα του project να προετοιμάσει και να υλοποιήσει ένα αποτελεσματικό και αποδοτικό SAP. Με άλλα λόγια, να βοηθήσει στην βελτιστοποίηση του χρόνου, του ανθρώπινου δυναμικού και των πόρων που απαιτούνται.

2.4.2 Φάσεις υλοποίησης ASAP

Στην παρακάτω εικόνα βλέπουμε τα βήματα από τα οποία αποτελείται το "ASAP" μοντέλο και τα οποία θα εξηγηθούν αναλυτικότερα.



Σχήμα 2.3: ASAP μεθοδολογία

1. **Προγραμματισμός έργου (Project Planning):** Αυτό το στάδιο, θα έλεγε κάποιος, ότι είναι ίσος και το πιο σημαντικό στάδιο διότι συγκεντρώνονται όλα τα απαραίτητα στοιχεία για την ανάπτυξη του συστήματος "ASAP". Στόχος αυτής της φάσης είναι η αρχική επικοινωνία με τον πελάτη για την συγκέντρωση πληροφοριών (αλλαγές στο σύστημα, χρονοδιάγραμμα του έργου κλπ.) και των απαιτούμενων πόρων που θα χρειαστούν. Επομένως τα μέλη που πρέπει να παρευρίσκονται σε αυτό το στάδιο είναι ο πελάτης και εργαζόμενοι από διαφορετικά τμήματα της εταιρείας (Προγραμματιστής (*programmer*), σύμβουλος IT(*Information Technology*), σύμβουλος Μάρκετινγκ κλπ.) για να γίνει μια ολοκληρωμένη καταγραφή των απαιτήσεων του πελάτη.

2. **Ανάλυση και τεκμηρίωση επιχειρηματικών απαιτήσεων (Analysis and Business Requirement Documentation):** Μετά την ολοκλήρωση του πρώτου βήματος, σειρά έχει η ανάλυση, ο καθορισμός και η τεκμηρίωση των απαιτήσεων που καταγράφηκαν στο *project planning*. Μόλις ολοκληρωθούν οι παραπάνω διαδικασίες, αποστέλλεται στον πελάτη ένα έγγραφο το οποίο περιέχει αναλυτικά όλες τις απαιτήσεις που πρέπει να σχεδιαστούν και να υλοποιηθούν κατά την διάρκεια του κύκλου ζωής του έργου. Το επόμενο στάδιο ξεκινάει αφού πρώτα υπογραφεί από όλα τα ενδιαφερόμενα μέλη το έγγραφο.

3. **Πραγματοποίηση – Λύση και προσαρμογή (Realization - Solution and Customization):** Αφού έχουν ολοκληρωθεί με επιτυχία τα δύο προηγούμενα στάδιο, οι ειδικοί ξεκινούν την υλοποίηση του SAP συστήματος, το οποίο είναι γνωστό και ως διαμόρφωση "γραμμής βάσης" (*Baseline and Final Configuration*). Για μεγαλύτερη διευκόλυνση χωρίζουμε αυτό το στάδιο σε δύο επιμέρους φάσεις. Η πρώτη είναι η συμβουλευτική ομάδα (*consultants*) του SAP που βοηθάει στην διαμόρφωση της "γραμμής βάσης" και η δεύτερη είναι η ομάδα υλοποίησης του έργου (*project team*), η οποία είναι υπεύθυνη να τελειοποιήσει τις διαδικασίες (τις υποδομές που θα φιλοξενηθεί το σύστημα, τις διαδικασίες επιχειρηματικής διαδικασίας κλπ.) έτσι ώστε να ικανοποιήσει τόσο την επιχείρηση όσο και τον πελάτη.

4. **Εφαρμογή και εκπαίδευση:** Στο συγκεκριμένο βήμα, θα πρέπει να γίνει η εγκατάσταση του ERP στο μηχάνημα του πελάτη, έτσι ώστε να μπορέσουν να πραγματοποιηθούν δοκιμές του συστήματος και να εκπαιδευτεί ο τελικός χρήστης. Οι δοκιμές περιλαμβάνουν τον έλεγχο του φόρτου εργασίας και τη συμβατότητα με άλλα προγράμματα, προκειμένου να εντοπιστούν προβλήματα που μπορεί να μην είχαν λάβει υπόψιν τους οι προγραμματιστές αλλά και να εξασφαλιστεί μια ολοκληρωμένη εικόνα του συστήματος για τον πελάτη με σκοπό να εγκρίνει το αποτέλεσμα ή να ζητήσει αλλαγές για διαδικασίες που δεν τον εξυπηρετούν. Τέλος, αποφασίζεται μεταξύ του πελάτη και της εταιρείας η τελική ημερομηνία που θα τεθεί το σύστημα σε λειτουργία.

5. **Έναρξη λειτουργίας:** Αν όλα τα παραπάνω βήματα έχουν υλοποιηθεί και ολοκληρωθεί με τον σωστό τρόπο, τότε η διαδικασία της έναρξης λειτουργίας του ERP θα είναι εύκολη και ομαλή. Ένα πολύ σημαντικό μέρος αυτής της φάσης είναι η κατάλληλη προετοιμασία από τους υπεύθυνους αυτού του project για τυχόν απορίες που θα προκύψουν από τους τελικούς χρήστες για την λειτουργία του συστήματος.

6. **Υποστήριξη συστήματος:** Η υποστήριξη που προσφέρει μια εταιρεία στους πελάτες της είναι ζωτικής σημασίας από πολλές απόψεις. Ο πελάτης θέλει να γνωρίζει ότι οποιοδήποτε

πρόβλημα του συστήματος δημιουργηθεί ή ακόμα και μια απλή βοήθεια που μπορεί να χρειαστεί, θα μπορεί να επιλυθεί άμεσα από τους ειδικούς για να συνεχιστεί η ομαλή λειτουργία της επιχείρησης του.

2.5 Εγκατάσταση ERP

Ένα ERP σύστημα μπορεί να λειτουργεί σε δύο καταστάσεις. Αυτές είναι η τοπική ή on-premise εγκατάσταση ή η "σύννεφο" ή cloud εγκατάσταση. Οι κύρια διαφορά των δύο αυτών εγκαταστάσεων είναι ότι στην on-premise εγκατάσταση, οι πληροφορίες και το software του προγράμματος βρίσκονται σε έναν τοπικό server της εταιρείας και για να συνδεθούν οι χρήστες στο σύστημα θα πρέπει να βρίσκονται συνδεδεμένοι είτε στο ίδιο δίκτυο με τον server είτε να συνδεθούν μέσο VPN, ενώ αντίστοιχα, στην cloud εγκατάσταση οι πληροφορίες και το software του προγράμματος βρίσκονται στον server της εταιρείας που παρέχει την υπηρεσία και για να συνδεθούν οι χρήστες χρειάζονται απλά πρόσβαση στο internet. Τα πλεονεκτήματα και τα μειονεκτήματα για τις δύο αυτές εγκαταστάσεις ποικίλουν. Στην συνέχεια θα αναφερθούμε στα βασικότερα από αυτά.

2.5.1 On-premise εγκατάστασης

Το βασικότερο πλεονέκτημα στην on-premise εγκατάσταση είναι ότι τα δεδομένα της εταιρείας βρίσκονται σε τοπική εγκατάσταση το οποίο συνεπάγεται σε μεγαλύτερη ασφάλεια των δεδομένων από κακόβουλες επιθέσεις στο διαδίκτυο. Από την άλλη, ένα μειονέκτημα της on-premise εγκατάστασης είναι ότι συχνά οι ίδιες οι εταιρείες δεν λαμβάνουν τα απαραίτητα μέτρα ασφαλείας για το σύστημα και τις πληροφορίες που αυτό περιέχει. Επιπλέον λόγο της δυνατότητας που έχουν στην παραμετροποίηση του συστήματος, αν δεν διαθέτουν το κατάλληλο προσωπικό αλλά και τα κατάλληλα εργαλεία για τον έλεγχο των παραμετροποιήσεων που αναπτύσσουν στο σύστημα, είναι πιο πιθανό στο να δεχτούν κυβερνοεπίθεση.

2.5.2 Cloud εγκατάστασης

Το βασικότερο πλεονέκτημα στην cloud εγκατάσταση είναι ότι όλες οι απαιτήσεις του συστήματος διαχειρίζονται από την εταιρεία που παρέχει την εφαρμογή κι έτσι το σύστημα βρίσκεται πάντα ενημερωμένο με νέες αναβαθμίσεις. Με άλλα λόγια, σε περίπτωση επίθεσης, ή εταιρεία θα προβεί άμεσα σε έκδοση νέες έκδοσης του συστήματός προς αντιμετώπιση του προβλήματος. Παρά τα θετικά που προσφέρει η cloud εγκατάσταση, δεν μπορούμε να μην αναφέρουμε και κάποια μειονεκτήματα της. Ένα μειονέκτημα είναι ότι αυτή η μορφή όπως λέει και το όνομα της βρίσκεται στο "σύννεφο", με αποτέλεσμα να είναι πιο ευάλωτη σε κυβερνοεπιθέσεις μέσω διαδικτύου. Μπορεί να υπάρχει αμεσότερη αντιμετώπιση της επίθεσης και πιθανών οι περισσότεροι οργανισμοί που έχουν το συγκεκριμένο ERP στην εταιρεία τους να μην υποστούν σοβαρές ζημιές, αλλά αυτό δεν αναιρεί το γεγονός ότι είναι πιο ευάλωτη από την on-premise εγκατάσταση.

2.6 Πλεονεκτήματα – Μειονεκτήματα των ERP

Όπως αναφέρθηκε και προηγουμένως τα πλεονεκτήματα και τα μειονεκτήματα ενός ERP συστήματος αλλάζουν ανάλογα με τον τύπο εγκατάστασης (*on-premise ή cloud*) που θα επιλέξει ο πελάτης. Παρόλα αυτά υπάρχουν κάποια κύρια πλεονεκτήματα και μειονεκτήματα που ισχύουν γενικά για τα ERP.

Μερικά από τα βασικά πλεονεκτήματα είναι τα εξής:

- Αύξηση της παραγωγικότητας. Ο χρήστης μπορεί να πραγματοποιήσει αρκετές διαδικασίες πολύ πιο γρήγορα και εύκολα και έτσι αυξάνεται ο παραγωγικός του χρόνος.
- Μείωση του κόστους. Η επιχείρηση μπορεί να λειτουργήσει με λιγότερο προσωπικό, διότι το σύστημα επιβλέπει τις εργασίες που εκτελούνται.
- Παρακολούθηση και πρόσβαση από παντού. Ο επιχειρηματίας έχει την δυνατότητα να παρακολουθεί εξ ολοκλήρου την επιχείρησή του από όπου και να βρίσκεται.
- Βελτίωση της ροής εργασιών. Παραδείγματος χάρη, η κατάργηση εισαγωγής ίδιων δεδομένων σε πολλά διαφορετικά συστήματα.
- Επίβλεψη πολλών εργασιών από ένα μόνο σύστημα.
- Βελτιστοποίηση της εικόνας της επιχείρησης.
- Καλύτερη και αμεσότερη εξυπηρέτηση των πελατών.

Από την άλλη όμως, δεν παύουν να υπάρχουν και μερικά μειονεκτήματα σε αυτά τα συστήματα. Μερικά από αυτά τα μειονεκτήματα είναι τα εξής:

- Σε περίπτωση παραμετροποίησης του συστήματος με βάση τις ανάγκες του πελάτη, το κόστος αγοράς αυξάνεται κατά μεγάλο βαθμό και σε μικρές και μεσαίες επιχειρήσεις ίσως και να είναι αφόρητο το κόστος αγοράς.
- Στην περίπτωση της παραμετροποίησης, υπάρχει και μεγάλος χρόνος αναμονής για την εγκατάσταση του συστήματος και την έναρξη της παραγωγικής του λειτουργίας.
- Πρόβλημα ασυμβατότητας του συστήματος με άλλα ήδη υπάρχοντα συστήματα του πελάτη.
- Έλλειψη εκπαιδευμένου προσωπικού από τις εταιρείες πώλησης για παροχή συμβουλευτικών υπηρεσιών στους πελάτες.

2.7 Κριτήρια επιλογής

Τα κριτήρια για την επιλογή του κατάλληλου ERP συστήματος αλλάζουν με βάση το μέγεθος της επιχείρησης. Οι μεγάλες επιχειρήσεις έχουν διαφορετικά κριτήρια επιλογής από τις μικρομεσαίες επιχειρήσεις. Παραδείγματος χάρη, μια μεγάλη επιχείρηση, πριν φτάσει στην τελική απόφαση για το ποιο σύστημα θα αγοράσει, θα λάβει υπόψη της την οικονομική σταθερότητα και την προϊστορία που έχει ο προμηθευτής από τον οποίο θα αγοράσει το ERP, κάτι το οποίο οι μικρομεσαίες επιχειρήσεις δυστυχώς δεν δίνουν σημασία. Επιπλέον υπάρχουν κριτήρια που τα συναντάμε συχνά σε κάθε επιχείρηση

Μερικά από αυτά τα κριτήρια είναι τα εξής:

- Το κόστος αγοράς. Ο πελάτης πρέπει να έχει υπόψη του και το κόστος συντήρησης και υποστήριξης του συστήματος.
- Service και υποστήριξη. Επειδή τα προβλήματα και οι ανάγκες δεν σταματούν ποτέ να υπάρχουν, ο ενδιαφερόμενος θα πρέπει να είναι σίγουρος ότι θα έχει την υποστήριξη που χρειάζεται άμεσα και με αποτελέσματα.
- Λειτουργικότητα. Το σύστημα θα πρέπει να είναι εύκολο στην διαχείριση και να ταιριάζει στα χαρακτηριστικά και στις ανάγκες που ζητάει ο πελάτης.
- Προσαρμοστικότητα και ευελιξία του συστήματος. Ο προμηθευτής θα πρέπει να είναι σε θέση να προσφέρει σύγχρονες λύσεις και να αναβαθμίζει άμεσα το σύστημα όταν υπάρχουν νέες εκδόσεις.

- Συμβατότητα. Θα πρέπει το ERP σύστημα να είναι συμβατό με τα υπόλοιπα προγράμματα που έχει ο πελάτης στον server του.
- Χρόνος υλοποίησης και εγκατάστασης.

Επίλογος

Συνοψίζοντας, στο κεφάλαιο αυτό αναλύσαμε τις βασικές πτυχές που περιγράφουν ένα ERP σύστημα. Είδαμε την σημασία του ERP και τους λόγους για τους οποίους είναι χρήσιμο εργαλείο για τις επιχειρήσεις. Επιπλέον σχολιάσαμε τα θετικά αλλά και μερικά από τα αρνητικά που προσφέρει στις επιχειρήσεις και κλείσαμε περιγράφοντας τα βασικότερα κριτήρια που θα πρέπει να έχει ένας πελάτης στο μυαλό του πριν αποφασίσει ποιο επιχειρησιακό λογισμικό θα επιλέξει.

Κεφάλαιο 3ο : Ασφάλεια ERP συστημάτων

3.1 Ασφάλεια δεδομένων

Σύμφωνα με την δημοσίευση της TechTarget (2022), ασφάλεια δεδομένων είναι η προστασία των ψηφιακών πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, απώλεια, αποκάλυψη, τροποποίηση ή καταστροφή καθ' όλη τη διάρκεια τους κύκλου ζωής, από τη δημιουργία έως και την καταστροφή, αποτελεί τη διαδικασία της ασφάλειας των δεδομένων. Επιπλέον ο όρος της ασφάλειας των δεδομένων περιλαμβάνει και την προστασία της φυσικής ασφάλειας του υλικού (hardware) και των συσκευών αποθήκευσης, καθώς και τους ελέγχους πρόσβασης και την ασφάλεια των εφαρμογών λογισμικού (*software*). Για να εξασφαλίσει μια επιχείρηση τον πλήρη έλεγχο των σημαντικών δεδομένων της και να είναι σε θέση να γνωρίζει πάντα την τοποθεσία τους, είναι απαραίτητο να αναπτύξει εργαλεία και τεχνολογίες που μπορούν να κρυπτογραφήσουν τα δεδομένα, να επεξεργαστούν ευαίσθητα αρχεία, να αποκρύπτουν πληροφορίες και να δημιουργούν αναφορές για τους ελέγχους που διενεργούνται.

Για να μπορέσει όμως ο επιχειρηματίας να προφυλάξει τα δεδομένα του, θα πρέπει πρώτα να τα κατανοήσει. Για τον λόγο αυτό, υπάρχουν κάποιες κατηγορίες που κατατάσσονται τα δεδομένα, με σκοπό ο επιχειρηματίας να κατανοήσει καλύτερα την σημαντικότητα τους και να μπορέσει πιο εύκολα μέσο της κατηγοριοποίησης να καταλήξει σε κάποια τελικά μέτρα προστασίας. Οι κατηγορίες που χωρίζονται τα δεδομένα είναι τέσσερις και είναι τα δημόσια/ανοιχτά δεδομένα, τα απόρρητα δεδομένα, τα ευαίσθητα δεδομένα και τα προσωπικά δεδομένα. Τα δημόσια ή ανοιχτά δεδομένα είναι εκείνα τα οποία είναι προσβάσιμα σε όλους και δεν έχουν περιορισμούς για την χρήση και επαναχρησιμοποίησή τους. Για παράδειγμα, δημόσια δεδομένα θεωρούνται τα στατιστικά δεδομένα που παράγονται από τις στατιστικές υπηρεσίες, ο καιρός κλπ. Τα απόρρητα δεδομένα είναι δεδομένα που τα δίνει ης γνώσεις του κάποιος σε κάποιον άλλον, άλλα ο παραλήπτης αυτών των δεδομένων δεν έχει το δικαίωμα να τα χρησιμοποιήσει για προσωπικό του όφελος. Παραδείγματος χάρη, οι πληροφορίες (ονοματεπώνυμο, αριθμός τηλεφώνου, διεύθυνση κατοικίας κλπ.) που δίνει κάποιος σε ένα ηλεκτρονικό κατάστημα (*e-shop*) για την πραγματοποίηση μιας αγοράς ενός προϊόντος ή υπηρεσίες, δεν μπορούν να χρησιμοποιηθούν από κανένα άλλο πρόσωπο, πέραν από το αρμόδιο προσωπικό για την ορθή επικοινωνία του καταστήματος με τον πελάτη. Τα ευαίσθητα δεδομένα είναι τα δεδομένα όπως, οι θρησκευτικές πεποιθήσεις, η κατάσταση υγείας, τα ποινικά αδικήματα και πολλά άλλα. Τέλος, τα προσωπικά δεδομένα είναι πληροφορίες που μπορούν να ταυτοποιήσουν ένα άτομο και αυτά τα δεδομένα μπορεί να είναι ονοματεπώνυμο, επάγγελμα, ηλικία, τόπος κατοικίας, οικογενειακή κατάσταση και άλλα.

Σχήμα 3.1: Τύποι Δεδομένων

Με βάση τα παραπάνω, είναι εμφανές πόσο ζωτικής σημασίας είναι η προστασία των δεδομένων που διαχειρίζεται ένας οργανισμός και πόσο απαραίτητο είναι να αποτρέπονται μη εξουσιοδοτημένες προσπάθειες πρόσβασης σε αυτά.

3.2 Λόγοι που είναι απαραίτητη η ασφάλεια στα ERP συστήματα

Στόχος ενός ERP συστήματος είναι η ομαλή λειτουργία μιας επιχείρησης και για να επιτευχθεί αυτό θα πρέπει το σύστημα να διαχειρίζεται τα οικονομικά στοιχεία ενός οργανισμού, τα προσωπικά δεδομένα των πελατών, του προσωπικού αλλά και των προμηθευτών της και γενικά πολλά άλλα ευαίσθητα δεδομένα Με άλλα λόγια ένα ERP σύστημα, διαχειρίζεται προσωπικά, απόρρητα και ευαίσθητα δεδομένα. Έχοντας κατανοήσει από την προηγούμενη ενότητα το πόσο σημαντικά είναι τα δεδομένα κάθε κατηγορίας και ξέροντας τους τύπους δεδομένων που επεξεργάζονται οι επιχειρήσεις με ERP λογισμικό, μπορούμε αυτομάτως να αντιληφθούμε το πόσο σημαντική είναι η ασφάλεια σε αυτά τα συστήματα. Πέραν των χρηματικών ποσών που μπορεί μια επιχείρηση να χάσει από πιθανές επιθέσεις (παραδείγματος χάρη, ζήτηση λύτρων για την επαναφορά του προγράμματος και των δεδομένων), μπορεί να χάσει και την εμπιστοσύνη των πελατών της το οποίο είναι σημαντικό για το μέλλον της.

Όσο περνάνε τα χρόνια οι hackers ολοένα και αυξάνονται και στόχος τους πλέον δεν είναι μόνο οι μεγάλες εταιρείες αλλά οποιαδήποτε εταιρεία μπορεί να τους προσφέρει κέρδος από την επίθεσή τους.

Έρευνες της Onapsis έχουν δείξει ότι το 2018 διαφορετικές επιχειρήσεις δεχόντουσαν επίθεση κάθε 39 δευτερόλεπτα, το 2019 κάθε 14 δευτερόλεπτα ενώ το για το έτος 2021 κάθε 11 δευτερόλεπτα. Μια επιχείρηση χρειάζεται περίπου 206 μέρες για να συνειδητοποιήσει ότι δέχτηκε επίθεση ενώ οι επιθέσεις αυτές έχουν ως αποτέλεσμα να χάνονται περίπου 3,24εκατομμύρια ευρώ ανά εταιρεία και να παραμένουν κλειστές οι επιχειρήσεις για περίπου 7,3 μέρες. Επιπλέον οι επιθέσεις από το 2014 εώς και το 2019 έχουν αυξηθεί κατά 67% και το ποσό που ξοδεύουν οι επιχειρήσεις προσπαθώντας να προστατεύσουν τα δεδομένα τους αυξήθηκε κατά 72%. Επιπροσθέτως, σύμφωνα με την παραπάνω

έρευνα, αν θέλαμε να ταξινομήσουμε τα είδη των δεδομένων που είναι πιο πιθανόν να κλαπούν θα τα κατηγοριοποιούσαμε ως εξής:

- Στοιχεία πωλήσεων (50%)
- Δεδομένα προσωπικού (45%)
- Δεδομένα πελατών (41%)
- Μηχανολογικές πληροφορίες (38%)
- Πνευματικά δεδομένα (36%)
- Οικονομικά δεδομένα (34%)

Για τους λόγους αυτούς η ασφάλεια στα ERP συστήματα είναι πολύ σημαντική και δεν πρέπει να παραμελείτε από καμία επιχείρηση είτε είναι μικρή είτε μεγάλη.

3.3 Μηχανισμοί ασφαλείας στα ERP

Στην προηγούμενη ενότητα εξηγήσαμε τους λόγους για τους οποίους είναι ζωτικής σημασίας να υπάρχει ασφάλεια στα ERP συστήματα. Στην ενότητα αυτή θα αναλύσουμε την ασφάλεια που χρησιμοποιούν μέχρι και σήμερα οι πέντε κορυφαίες εταιρείες ERP λογισμικού παγκοσμίως, αλλά και γενικά τι συνηθίζεται να χρησιμοποιείται από όλες τις εταιρείες. Οι πέντε μεγαλύτερες εταιρείες ERP λογισμικού είναι η *Oracle,* η *SAP,* η *Microsoft,* η *Workday* και η *Sage*. Πριν αναφερθούμε στους μηχανισμούς ασφαλείας της κάθε εταιρείας, θα περιγράψουμε γενικότερα τις βασικές πτυχές της ασφάλειας.

Έλεγχος πρόσβασης (Access control): Αναφέρεται στον ορισμό και τη διαχείριση των εξουσιοδοτημένων χρηστών καθώς και την ανάθεση ρόλων που απαιτούνται για την πρόσβαση σε διαδικασίες και δεδομένα. Παραδείγματος χάρη, αν αναφερόμαστε σε μια βάση δεδομένων, η άδεια που παραχωρείται στους χρήστες, σχετίζεται με την εισαγωγή, την ενημέρωση, την διαγραφή αλλά και την επιλογή των δεδομένων.

Ασφάλεια επιπέδου βάσης δεδομένων (Database Level Security): Αναφέρεται σε έναν πίνακα εικονικής και ιδιωτικής βάσης δεδομένων (VPD). Ο ρόλος του VPD είναι ο περιορισμός των δεδομένων στις μεγάλες βάσεις, με σκοπό να εμφανίζεται στον χρήστη μόνο ένα υποσύνολο των δεδομένων, χωρίς όμως να γίνεται διαχωρισμός των δεδομένων σε ξεχωριστά αντικείμενα. Με άλλα λόγια, ένας πίνακας είναι προσβάσιμος από όλους τους χρήστες, αλλά ο κάθε χρήστης βλέπει διαφορετικό περιεχόμενο του πίνακα, ανάλογα με τα δικαιώματα που έχει. Το VPD λειτουργεί ως εξής: Κάθε φορά που ένα χρήστης δημιουργεί ένα SQL ερώτημα στην βάση δεδομένων, το VPD προσθέτει σε αυτό, ένα δυναμικό WHERE.

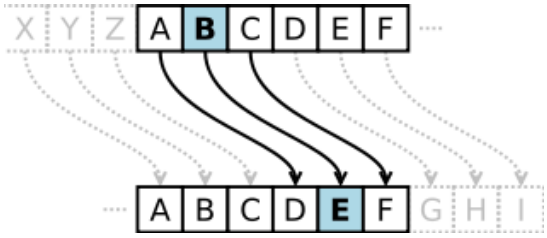
«SQL ερώτημα του χρήστη: SELECT * FROM OE.ORDERS;

VPD: SELECT * FROM OE.ORDERS

WHERE SALES_REP_ID = 159;

Ο χρήστης μπορεί να δει μόνο τις παραγγελίες από τον αντιπρόσωπο πωλήσεων με κωδικό 159» [35]

Κρυπτογράφηση δεδομένων (Data Encryption): Σκοπός της κρυπτογράφησης είναι η μετατροπή του αρχικού κειμένου σε μια διαφορετική μορφή αναπαράστασης, χρησιμοποιώντας μαθηματικούς αλγόριθμους. Για να μπορέσει ένας εξουσιοδοτημένος χρήστης να διαβάσει το αρχικό κείμενο, θα πρέπει να έχει στην κατοχή του τα σωστά κλειδιά αποκρυπτογράφησης. Η κρυπτογράφηση χρησιμοποιείται κατά την αποθήκευση των δεδομένων στην βάση δεδομένων αλλά και κατά την μεταφορά των δεδομένων μέσω δικτύου.



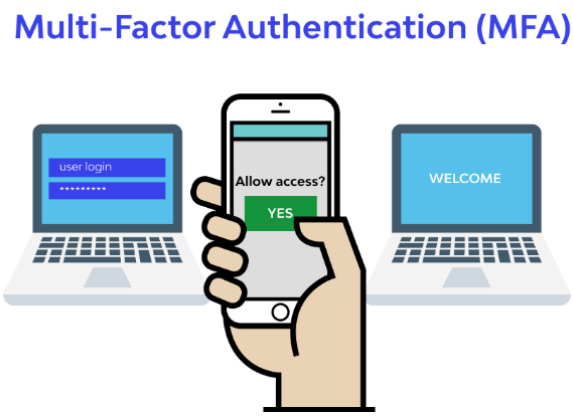
Σχήμα 3.2: Κρυπτογράφηση του Καίσαρα

Εξουσιοδότηση (Authorization): Για να μπορέσει ένας χρήστης του συστήματος να αποκτήσει πρόσβαση σε διαδικασίες και στην βάση δεδομένων, θα πρέπει να είναι εξουσιοδοτημένος από το σύστημα. Συνήθως η εξουσιοδότηση ενός χρήστη γίνεται με βάση των ομάδων που ανήκει (πχ. τμήμα πωλήσεων, τμήμα προγραμματιστών κλπ.) αλλά μπορεί να υπάρξει και μεμονωμένη εξουσιοδότηση σε κάθε χρήστη ξεχωριστά.

BAAN Security using DEM: Σε αυτό το μοντέλο ασφάλειας, χρησιμοποιείται το DEM, το οποίο βοηθάει στη μοντελοποίηση των επιχειρηματικών διαδικασιών και τον ορισμό των ρόλων. Οι τέσσερις βασικές έννοιες του μοντέλου είναι ο υπάλληλος, ο χρήστης, ο ρόλος και η διαδικασία. Ο χρήστης περιέχει όλες τις προσωπικές πληροφορίες του υπαλλήλου, ο υπάλληλος είναι ο άνθρωπος που εργάζεται στην εταιρεία, ο ρόλος καθορίζει την θέση του υπαλλήλου μέσα στην εταιρεία και η διαδικασία περιέχει τους ρόλους των εργαζομένων.

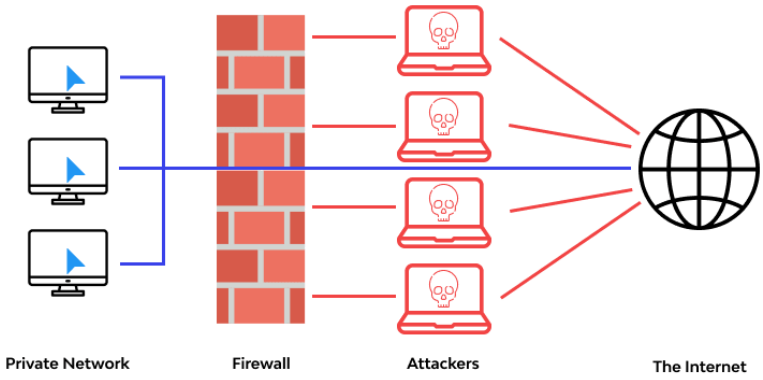
Αντίγραφα ασφαλείας δεδομένων (Data backups): Για τη διασφάλιση ότι τα δεδομένα του οργανισμού θα είναι πάντα διαθέσιμα, ακόμη και σε περίπτωση επίθεσης, μια ορθή τακτική είναι η συνεχής εξαγωγή των δεδομένων της βάσης σε μια δεύτερη backup βάση.

Πολυπαραγοντικός έλεγχος ταυτότητας (MFA): Είναι μια μέθοδος αυθεντικοποίησης κατά την οποία, για να αποκτήσει πρόσβαση ο χρήστης στην εφαρμογή θα πρέπει να ταυτοποιηθεί από δύο ή περισσότερα διαπιστευτήρια. Παραδείγματος χάρη, όταν ένας χρήστης δημιουργεί λογαριασμό σε μια εφαρμογή, εκτός από την εισαγωγή του username και του password που θα καταχωρήσει, θα του ζητηθεί να γίνει και μια περεταίρω ταυτοποίηση, είτε μέσο ηλεκτρονικού ταχυδρομείου (*email*), είτε μέσο κινητού τηλεφώνου.



Σχήμα 3.3: Πολυπαραγοντικός έλεγχος ταυτότητας

Τοίχοι προστασίας (firewalls): Ο κύριος σκοπός των firewalls είναι ο έλεγχος της κυκλοφορίας των πακέτων δεδομένων μεταξύ δύο δικτύων υπολογιστών με διαφορετικό επίπεδο εμπιστοσύνης. Τα δύο αυτά δίκτυα, είναι συνήθως το διαδίκτυο (*internet*) και το τοπικό δίκτυο που χρησιμοποιεί η εταιρεία. Το firewall έχει την δυνατότητα να επιτρέψει ή να απορρίψει την μεταφορά των πακέτων από το ένα δίκτυο στο άλλο.



Σχήμα 3.1: Λειτουργία ενός τοίχου προστασίας

Διαγραφή δεδομένων (Data Erasure): Οι περισσότερες εταιρείες που διατηρούν backup αρχεία, συνήθως έχουν αποθηκευμένα και παλιά αρχεία που πλέον τους είναι άχρηστα (πχ προσωπικά στοιχεία εργαζομένων). Γι΄αυτόν τον λόγο, οι εταιρείες πρέπει να ακολουθούν ορισμένες πολιτικές και διαδικασίες για την διαγραφή αυτών των δεδομένων.

Φυσική ασφάλεια (Physical Security): Αναφέρεται στην φυσική προστασία του συστήματος από μη εξουσιοδοτημένη πρόσβαση στο χώρο του server και από τυχόν ζημία στο hardware του server. Τα μέτρα ασφαλείας που χρησιμοποιούνται είναι ο πολλαπλός έλεγχος της ταυτότητας του ατόμου που επιθυμεί να έχει πρόσβαση στην περιοχή του server, ύπαρξη συστήματος παρακολούθησης του χώρου όλο το 24ώρο και ύπαρξη προσωπικού ασφαλείας στον χώρο.

Εκπαίδευση προσωπικού (Employee Training): Είναι ένας από τους σημαντικότερους μηχανισμούς ασφάλειας. Στόχος της εκπαίδευσης, είναι να ενημερωθεί όλο το προσωπικό της επιχείρησης σχετικά

με τον σωστό τρόπο λειτουργίας του ERP συστήματος που χρησιμοποιεί, τις πολιτικές ασφαλείας που χρησιμοποιεί το σύστημα, μια ανάλυση του κινδύνου ασφαλείας καθώς και τα μέτρα για την αντιμετώπιση τυχόν επίθεσης που μπορεί να δεχτεί το σύστημα.

Συχνές αναβαθμίσεις του συστήματος (Install Updates): Στόχος των συνεχών και σύντομων σε χρονικά διαστήματα αναβαθμίσεων του συστήματος, είναι η αντιμετώπιση τυχόν ευπαθειών που έχουν εντοπιστεί στο ERP, με σκοπό την αποτροπή μελλοντικών επιθέσεων.

Συμμόρφωση με τα Πρότυπα ασφαλείας (Data compliance): Είναι η συμμόρφωση με τις διαδικασίες και τους κανονισμούς που έχουν οριστεί στα πρότυπα ασφαλείας με στόχο την προστασία των προσωπικών δεδομένων. Ένα βασικό πρότυπο ασφαλείας είναι το ISO 27001 το οποίο συμπεριλαμβάνει και το πρότυπο του GDPR.

Στον παρακάτω πίνακα αναγράφονται οι διαδικασίες ασφαλείας που χρησιμοποιούνται από τις πέντε πιο γνωστές εταιρείες ERP λογισμικού στον κόσμο.

Πίνακας 3.1: Διαδικασίες ασφαλείας στα TOP 5 ERP

συστημάτων

	Access Control	Database Level Security	Data Encryption	Authorization	BAAN	Data Backups	MFA	Firewall	Physical Security	Employee Training	Updates	Data compliance
Oracle	✓	✓	✓	✓	✓			✓				
SAP	✓		✓	✓	✓							✓
Microsoft	✓	✓	✓		✓		✓					
Workday			✓	✓		✓	✓		✓			✓
Sage	✓		✓	✓		✓	✓	✓		✓	✓	✓

3.4 Αδυναμίες των ERP

Παρά τη μεγάλη προσπάθεια που καταβάλλουν οι εταιρείες για να παρέχουν αυξημένη ασφάλεια στο ERP λογισμικό, εξακολουθούν να υπάρχουν ελαττώματα τα οποία αποτελούν τις κύριες αιτίες των περισσότερων επιθέσεων στα συγκεκριμένα λογισμικά. Τα ελαττώματα δεν είναι αποκλειστικά προβλήματα του λογισμικού, αλλά μπορεί να οφείλονται και σε ανθρώπινα λάθη. Παρακάτω θα αναλυθούν περεταίρω τα μεγαλύτερα προβλήματα ασφαλείας των ERP συστημάτων.

Εκπρόθεσμο λογισμικό: Εξαιτίας της ραγδαίας αύξησης των hackers και των συνεχών επιθέσεων που πραγματοποιούνται στα επιχειρησιακά λογισμικά, οι πάροχοι αναβαθμίζουν σε πολύ σύντομα χρονικά διαστήματα τα συστήματά τους με σκοπό την αποτροπή των επιθέσεων. Παρόλα αυτά, το μεγαλύτερο ποσοστό των επιχειρήσεων παραμελεί να ενημερώσει το λογισμικό του με τις νέες εκδόσεις και αυτό το καθιστά ευάλωτο σε πιθανές επιθέσεις.

Πλήρη δικαιώματα πρόσβασης: Η σωστή παραχώρηση δικαιωμάτων στους χρήστες και η δημιουργία ρόλων, παίζουν σημαντικό ρόλο στην προστασία του συστήματος. Δίνοντας πλήρη δικαιώματα στους χρήστης, μπορεί ο καθένας να έχει πρόσβαση σε δεδομένα και διαδικασίες που κανονικά θα απαγορευόταν. Για παράδειγμα, ένας χρήστης με ρόλο υποστήριξης που έχει πλήρη δικαιώματα μπορεί να αποκτήσει πρόσβαση σε λογιστικά δεδομένα και να τα επεξεργαστεί, πράγμα που είναι απαγορευτικό. Επιπλέον, οι χρήστες με περιττά δικαιώματα κάνουν την παρακολούθηση των ενεργειών τους πιο δύσκολη και υπάρχει κίνδυνος αργής ανίχνευσης προβλημάτων που μπορεί να δημιουργηθούν.

Έλλειψη εκπαίδευσης: Έχοντας στο δυναμικό της εταιρείας άτομα που δεν γνωρίζουν από πρωτόκολλα ασφαλείας και από απλές τακτικές προστασίας των δεδομένων, είναι πολύ εύκολο να γίνει κάποιο λάθος το οποίο θα έχει ως συνέπεια μελλοντικές επιθέσεις στο σύστημα. Επιπλέον, η έλλειψη εκπαίδευσης μπορεί να αναφέρεται και στη χρήση του λογισμικού συστήματος και όχι μόνο στους κανόνες ασφαλείας.

Αποτυχία συμμόρφωσης με τα πρότυπα ασφαλείας: Κάθε ERP σύστημα που διαχειρίζεται ευαίσθητα δεδομένα, θα πρέπει να τηρεί και τα πρότυπα ασφαλείας που τίθενται από τις αρμόδιες αρχές. Η μη συμμόρφωση, έκτος από το ότι θέτει το σύστημα ευάλωτο και εύκολο στόχο σε επιθέσεις, μπορεί να οδηγήσει σε κυρώσεις και νομικές επιπτώσεις.

Έλεγχος ταυτότητας ενός παράγοντα: Ακόμη και σήμερα, η πλειοψηφία των επιχειρήσεων χρησιμοποιεί one-factor authentication. Το χακάρισμα ενός απλού κωδικού πρόσβασης είναι πολύ εύκολο για τους χάκερς. Γι΄αυτόν τον λόγο, το να προστατεύει κανείς τα κρίσιμα δεδομένα τις επιχειρήσεις του με την χρήση ενός μόνο κωδικού είναι σαν να μην χρησιμοποιεί καμία μέθοδο ασφαλείας.

Προσαρμογή του συστήματος: Για να προσαρμοστεί πλήρως ένα ERP στις ανάγκες του πελάτη, πολλές φορές απαιτούνται αλλαγές στις υπάρχουσες λειτουργίες ή προσθήκη νέων λειτουργιών. Ωστόσο, αυτή η παραμετροποίηση μπορεί να προκαλέσει νέες ευαισθησίες στο σύστημα. Αυτές οι ευαισθησίες προκύπτουν κυρίως από λανθασμένο προγραμματισμό των λειτουργιών ή από ελαττώματα στη γλώσσα προγραμματισμού που χρησιμοποιεί ο προγραμματιστής για την ανάπτυξη των νέων λειτουργιών.

Αυτές ήταν μερικές από τις μεγαλύτερες και πιο συχνά εμφανιζόμενες ευαισθησίες που εντοπίζονται στα ERP συστήματα και καθιστούν το σύστημα εύκολο στόχο για τους χάκερς.

3.5 Επιθέσεις στα ERP συστήματα

Σε αυτήν την ενότητα, θα επικεντρωθούμε περισσότερο στις επιθέσεις που έχουν δημοσιευτεί γενικά για τα ERP και όχι αποκλειστικά για τα πέντε κορυφαία συστήματα. Οι πληροφορίες των παρακάτω επιθέσεις πάρθηκαν από το CVE καθώς και το EXPLOIT DATABASE. Συγκεκριμένα, θα δούμε το ERP λογισμικό που δέχτηκε την επίθεση, την ευαισθησία του συστήματος που οδήγησε στην επίθεση, μια ενδεικτική ημερομηνία για το πότε έλαβε χώρα το γεγονός, καθώς και μια σύντομη περιγραφή της.

Συνήθως η ημερομηνία που αναφέρεται δεν αντιστοιχεί στην ημερομηνία της επίθεσης αλλά μάλλον στην ημερομηνία κατά την οποία αποκαλύφθηκε ή δημοσιεύτηκε η επίθεση. Επιπλέον οι παρακάτω επιθέσεις είναι ταξινομημένες με βάση την ημερομηνία τους, από την παλαιότερη στην πιο πρόσφατη.

Πίνακας 3.2: Καταγεγραμμένες επιθέσεις σε ERP συστήματα

ERP	**Ευαισθησία συστήματος**	**Ημερομηνία**	**Περιγραφή**
Dolibarr ERP/CRM	Εκμετάλλευση αδύναμου αλγορίθμου κρυπτογράφησης	16/4/2017	Αποθήκευε τους κωδικούς πρόσβασης με τον αλγόριθμο MD5. Εύκολος στο να χακαριστεί από επιθέσεις εξαντλητικής αναζήτησης (brute force)
Dolibarr ERP/CRM	Εκμετάλλευση one-factor authentication	10/05/2017	Επέτρεπε την αλλαγή του κωδικού πρόσβασης χωρίς να ζητάει την καταχώρηση του τρέχοντος κωδικού.
SAP Fiori	Εκμετάλλευση ανεπαρκής προστασία CSRF	15/12/2017	Επέτρεπε στον επιτιθέμενο να ξεγελάσει έναν εξουσιοδοτημένο χρήστη για να στείλει ακούσιο αίτημα στον διακομιστή ιστού.

SAP ERP HCM	Εκμετάλλευση της έλλειψης ελέγχων εξουσιοδότησης	26/11/2018	Επέτρεπε σε έναν χρήστη του συστήματος που κάποτε είχε πρόσβαση σε δεδομένα μισθοδοσίας των εργαζομένων και πλέον του ανακλήθηκε η πρόσβαση, να συνεχίζει να βλέπει τα δεδομένα.
Dolibarr ERP/CRM	Εκμετάλλευση της βάσης δεδομένων	11/04/2019	Είχε μια λειτουργία κατά την οποία δημιουργόντουσαν αντίγραφα ασφάλειας. Η ευπάθεια βρέθηκε στην έλλειψη των απαραίτητων ελέγχων στις παραμέτρους εξαγωγής στο mysqldump. Αυτό οδηγούσε σε εκτέλεση αυθαίρετων δυαδικών αρχείων στον server.
SAP ERP και SAP_FIN και SAP S/4 HANA	Εκμετάλλευση της έλλειψης ελέγχων εξουσιοδότησης (Authorization check)	08/01/2020	Η ευπάθεια βρέθηκε στην έλλειψη των απαραίτητων ελέγχων εξουσιοδότησης χάρη στην οποία ο επιτιθέμενος που δεν είχε εξουσιοδοτημένη πρόσβαση, μπορούσε να αποκτήσει οποιοδήποτε εταιρικό πιστοποιητικό ήθελε.
SAP ERP	Εκμετάλλευση της έλλειψης ελέγχων εξουσιοδότησης (Authorization check)	08/01/2020	Η ευπάθεια βρέθηκε στην έλλειψη των απαραίτητων ελέγχων εξουσιοδότησης για επαληθευμένους χρήστες, επιτρέποντας έτσι σε έναν επιτιθέμενο να διαβάζει και να παραμετροποιεί περιορισμένα δεδομένα

SAP ERP και SAP S/4 HANA	Εκμετάλλευση της έλλειψης ελέγχων εξουσιοδότησης (Authorization check)	08/01/2020	Επέτρεπε σε έναν εξουσιοδοτημένο χρήστη να βλέπει εγγραφές κόστους για τις οποίες δεν είχε κανονικά εξουσιοδότηση για να τις δει.
SAP ERP	Εκμετάλλευση της έλλειψης ελέγχων εξουσιοδότησης (Authorization check)	08/01/2020	Σε εταιρεία διαχείρισης ταξιδιών, επέτρεπε σε έναν επαληθευμένο αλλά μη εξουσιοδοτημένο χρήστη να επεξεργάζεται ταξίδια. Ως αποτέλεσμα είχε την κλιμάκωση των προνομίων
SAP ERP	Εκμετάλλευση λάθος δικαιωμάτων πρόσβασης	07/10/2020	Επέτρεπε στον οποιονδήποτε να έχει πρόσβαση στα αρχεία του φακέλου και επομένως την τροποποίηση των αρχείων αυτών από μη εξουσιοδοτημένους χρήστες.
In4Suite ERP	Εκμετάλλευση της βάσης δεδομένων	01/03/2021	Επέτρεπε στους επιτιθέμενους να χρησιμοποιούν κακόβουλα ερωτήματα SQL που τους έδιναν την δυνατότητα τροποποίησης και διαγραφής των δεδομένων, με αποτέλεσμα την αλλαγή της συμπεριφοράς της εφαρμογής.

Dolibarr ERP/CRM	Εκμετάλλευση του ελέγχου πρόσβασης (Access control)	26/07/2021	Επειδή η εφαρμογή επέτρεπε ως username την εκχώρηση των email, σε περίπτωση που κάποιος χρήστης πατούσε το κουμπί “forgot-password”, ο επιτιθέμενος μπορούσε να αποκτήσει τα στοιχεία πρόσβασης και να προκαλέσει επίθεση άρνησης εξυπηρέτησης
SAP ERP	Εκμετάλλευση δικτύου	07/08/2021	Επέτρεπε σε έναν εγγεγραμμένο επιτιθέμενο να πραγματοποιεί λειτουργίες που διαφορετικά θα απαγορευόταν σε συγκεκριμένους χρήστες. Οι λειτουργίες αυτές του επέτρεπαν να τροποποιεί οικονομικά, λογιστικά δεδομένα.
SAP ERP	Εκμετάλλευση του ελέγχου εξουσιοδότησης (Authorization check)	07/10/2021	Η ευπάθεια βρέθηκε στην έλλειψη των απαραίτητων ελέγχων εξουσιοδότησης σε αρχεία μισθοδοσίας των εργαζομένων. Υπήρχε η δυνατότητα μόνο διαβάσματος του αρχείου και όχι παραμετροποίησης του
Dalmark Systems	Εκμετάλλευση του ελέγχου πρόσβασης (Access control)	13/12/2021	Η ευπάθεια βρέθηκε κατά την χρήση ενός προσωρινού token σε μια api κλήση. Η ευπάθεια επέτρεπε στον επιτιθέμενο να χρησιμοποιεί ένα endpoint api, για να δημιουργήσει ένα διακριτό JWT. Η εκμετάλλευση αυτής της ευπάθειες οδηγεί σε έκθεση των ευαίσθητων πληροφοριών.

Sage 300 ERP	Εκμετάλλευση λάθος δικαιωμάτων πρόσβασης	25/12/2021	Κατά την εγκατάσταση του προγράμματος δημιουργείται ένας κατάλογος. Αυτός ο κατάλογος μπορεί να εγγραφεί και από μη εξουσιοδοτημένους χρήστες, εξαιτίας των λάθος δικαιωμάτων που ορίζει το πρόγραμμα εγκατάστασης του Sage.
SAP ERP	Εκμετάλλευση της έλλειψης ελέγχων εξουσιοδότησης (Authorization check)	04/01/2022	Επιτρέπει την ανάγνωση αναφορών που περιέχουν στοιχεία μισθοδοσίας των εργαζομένων. Επιτρέπει μόνο την ανάγνωση και όχι την τροποποίηση του περιεχομένου ή την πρόκληση επιπτώσεων στην διαθεσιμότητα του συστήματος.
SalonERP	Εκμετάλλευση της βάσης δεδομένων	11/01/2022	Επιτρέπει σε έναν επιτιθέμενο, χρησιμοποιώντας μια SQL παράμετρο στο SQL ερώτημα κατά την δημιουργία της αναφοράς, να διαβάσει τον κατακερματισμένο κωδικό πρόσβασης του διαχειριστή, αποκρυπτογραφώντας τον.
Abacus ERP	Εκμετάλλευση του Multifactor Authentication	24/03/2022	Επέτρεπε στον επιτιθέμενο να παρακάμψει τον δεύτερο έλεγχο ταυτότητας (Multifactor Authentication)

SAP Fiori	Εκμετάλλευση δικτύου	25/01/2023	Επέτρεπε την εκμετάλλευση ενός τελικού σημείου (endpoint) της εφαρμογής που είχε λανθασμένες παραμέτρους, με αποτέλεσμα την προβολή ευαίσθητων δεδομένων. Συγκεκριμένα υπήρχε έκθεση ταξιδιωτικών εγγράφων.

Παρατηρώντας όλες τις παραπάνω επιθέσεις που αναφέραμε, μπορούμε εύκολα να διαπιστώσουμε ότι το μεγαλύτερο ποσοστό των επιθέσεων έχει γίνει σε γνωστά ERP συστήματα και συγκεκριμένα στο λογισμικό της εταιρείας SAP. Επιπλέον, παρατηρούμε ότι υπάρχουν πολλών ειδών επιθέσεις, είτε αυτές είναι εκμετάλλευση της βάσης δεδομένων, είτε εκμετάλλευση στην έλλειψη ελέγχων εξουσιοδότησης είτε ακόμη και εκμετάλλευση σε αδύναμους αλγορίθμους κρυπτογράφησης και ανεπαρκής προστασία CSRF. Οι παραπάνω επιθέσεις είναι μόλις το 3,55% των συνολικών επιθέσεων που έχουν δημοσιευτεί από το έτος 2001 έως και σήμερα.

3.5.1 Στάδια μια επίθεσης

Το μεγαλύτερο ποσοστό των χάκερς και κυρίως των έμπειρων χάκερς, ακολουθούν ένα συγκεκριμένο σετ βημάτων για να πραγματοποιήσουν μια επιθετική ενέργεια με επιτυχία. Αυτά τα βήμα είναι επτά και η ανάλυσή τους είναι σημαντική για την πρόληψη επιθέσεων στα συστήματα ERP. Εάν μια επιχείρηση γνωρίζει αυτά τα βήματα, μπορεί να ενισχύσει την ασφάλεια του συστήματός της και να αποτρέψει τυχόν επιθέσεις.

Τα επτά στάδια μιας επίθεσης (seven stages of a cyber-attack).

Στάδιο 1: Αναγνώριση στόχου

Στο στάδιο της αναγνώρισης ο επιτιθέμενος αναζητεί έναν ευάλωτο στόχο και αφού τον εντοπίσει, ψάχνει να βρει τον καλύτερο δυνατό τρόπο για τον επιτεθεί. Η πιο γνωστή επίθεση σε αυτό το στάδιο είναι αυτή του ηλεκτρονικού ψαρέματος (*phishing*). Ο τελικός στόχος της πρώτης φάσης είναι η διεξοδική έρευνα του στόχου με σκοπό να γνωρίσουν κάθε πτυχή αυτού. Για να το επιτύχουν αυτό, οι χάκερς συνήθως μαζεύουν τις πληροφορίες μέσω του ίντερνετ και από τα μέσα κοινωνικής δικτύωσης (social media) της εταιρείας/στόχο.

Στάδιο 2: Οπλοφορία (Weaponizing)

Έχοντας συγκεντρώσει όλες τις απαραίτητες πληροφορίες που χρειάζονται οι επιτιθέμενοι, σειρά έχει η εύρεση τρόπων για τη διείσδυσης τους στην εταιρεία/στόχο. Μερικοί από αυτούς τους τρόπους θα μπορούσε να είναι είτε η δημιουργία ενός κακόβουλου λογισμικού (*malware*) , είτε η δημιουργία μηνυμάτων ηλεκτρονικού ψαρέματος που να μοιάζουν με μηνύματα που θα μπορούσε να λάβει ο χρήστης από κάποια γνωστή επαφή. Ένας διαφορετικός τρόπος διείσδυσης είναι η δημιουργία

ψεύτικων ιστοσελίδων, φτιαγμένες με τέτοιον τρόπο που να μοιάζουν με κάποια σελίδα ενός προμηθευτή ή με σελίδα τράπεζας που επισκέπτεται συχνά ο στόχος. Αυτό έχει ως σκοπό να καταγράψει κωδικούς πρόσβασης του χρήστη ή ακόμη και να κατεβάσει στον υπολογιστή του στόχου έγγραφα που έχουν μολυνθεί από κακόβουλο λογισμικό. Τέλος, ο επιτιθέμενος, συλλέγει εργαλεία που θα τον βοηθήσουν όταν καταφέρει να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε μία συσκευή του στόχου.

Στάδιο 3: Παραδίδοντας την επίθεση

Σε αυτό το στάδιο ο επιτιθέμενος στέλνει τα όπλα που δημιούργησε στην φάση δυο και περιμένει μέχρι το θύμα να πέσει σε κάποιο από αυτά. Δηλαδή, δημοσιεύει τις ψεύτικες ιστοσελίδες στο διαδίκτυο και στέλνει τα ηλεκτρονικά μηνύματα ψαρέματος που δημιούργησε στους παραλήπτες. Επιπλέον, μια ακόμη μέθοδος για την παράδοση του όπλου είναι μέσο USB συσκευής. Αυτό προϋποθέτει να έχει ο επιτιθέμενος πρόσβαση μέσα στον οργανισμό ή να το δώσει σε κάποιον εργαζόμενο παραπλανώντας τον για το περιερχόμενο που περιέχει το στικάκι.

Στάδιο 4: Εκμετάλλευση

Ο χάκερ αρχίζει πλέον να εκμεταλλεύεται τα δεδομένα που κατάφερε να συλλέξει από το στάδιο τρία. Με άλλα λόγια, εκμεταλλεύεται τα τρωτά σημεία που εντόπισε στο σύστημα ή στο δίκτυο του στόχου.

Στάδιο 5: Εγκατάσταση μόνιμης σύνδεσης

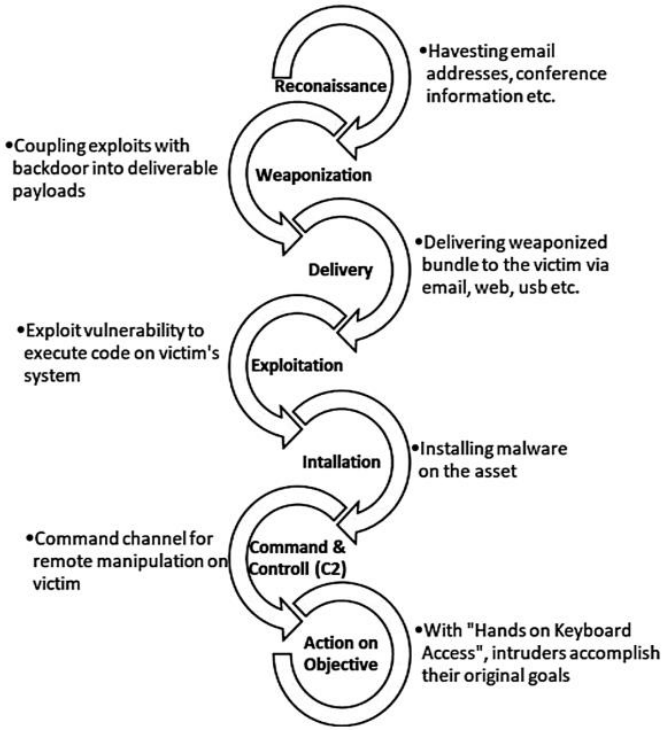
Σε αυτήν την φάση ο χάκερ προσπαθεί να διασφαλίσει την συνεχόμενη σύνδεσή του στο επιτιθέμενο σύστημα για όσο αυτός την χρειάζεται. Για να το επιτύχει αυτό, συνήθως εγκαθιστά μια μόνιμη κερκόπορτα (*backdoor*) ή δημιουργεί λογαριασμό διαχειριστή στο δίκτυο με σκοπό να ρίξει το τείχος προστασίας (*firewall*). Επιπλέον, ένας ακόμη τρόπος για την διασφάλιση της σύνδεσης, είναι η ενεργοποίηση της απομακρυσμένης πρόσβασης στην επιφάνεια εργασίας (*remote desktop*) του διακομιστή.

Στάδιο 6: Άσκηση διοίκησης και ελέγχου

Έχοντας καταφέρει να αποκτήσει απεριόριστη πρόσβαση στο δίκτυο και στους λογαριασμούς των χρηστών, ο εισβολέας δημιουργεί ένα κανάλι επικοινωνίας μεταξύ του δικού του server και του στόχου. Συγκεκριμένα, αυτό γίνεται χρησιμοποιώντας μεγάλο τμήμα της κερκόπορτας. Έχοντας εγκαταστήσει το κανάλι επικοινωνίας, ο χάκερ είναι πλέον σε θέση να πραγματοποιήσει οποιαδήποτε αλλαγή στο σύστημα θέλει προσποιούμενος ότι είναι ένας εξουσιοδοτημένος χρήστης.

Στάδιο 7: Επίτευξη του στόχου

Στο έβδομο και τελικό στάδιο, σειρά έχει η δράση του εισβολέα. Με άλλα λόγια, μπορεί πλέον να υποκλέψει πληροφορίες από το σύστημα είτε αυτές είναι προσωπικά δεδομένα υπαλλήλων, είτε οικονομικά στοιχεία της εταιρείας, να διακόψει τη λειτουργία του συστήματος προκαλώντας την γνωστή επίθεση άρνησης εξυπηρέτησης (DoS), να προκαλέσει αναστάτωση στην εταιρεία, ή απλά να μείωση την αξιοπιστία της.



Σχήμα 3.2: Τα 7 στάδια μια επίθεσης

3.5.2 Τύποι επιθέσεων

Καθώς αυξάνεται ο αριθμός των χάκερς αυξάνονται και οι τύποι των επιθέσεων που ένας χάκερ μπορεί να πραγματοποιήσει. Όλοι αυτοί οι τύποι όμως, χωρίζονται σε δύο μεγάλες κατηγορίες, τις επιθέσεις από έξω προς τα μέσα (*outsiders*) και τις επιθέσεις από μέσα προς τα έξω (*insiders*).

Επίθεση από έξω προς τα μέσα (outsiders)

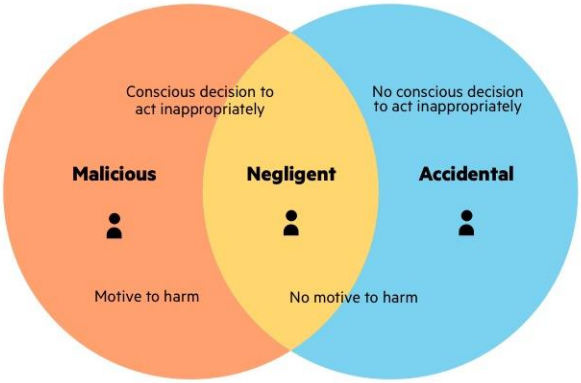
Οι εξωτερικές απειλές (*outsiders*) προέρχονται κυρίως από χάκερς, κυβερνοεγκληματίες, κυβερνοκατάσκοπους ή ανταγωνιστές. Από άτομα δηλαδή που δεν έχουν καμία σχέση με τον στόχο που σκοπεύουν να χτυπήσουν. Σύμφωνα με μια πρόσφατη έρευνα της *U.S. Secret Service/CERT/Microsoft E-Crime,* από τις καταγεγραμμένες επιθέσεις που έχουν συμβεί, οι outsiders ανήκουν στο 37% των επιθέσεων. Επιπλέον, θεωρούνται από τις πιο δύσκολες επιθέσεις προς αντιμετώπιση και αυτό συμβαίνει γιατί δεν είναι δυνατόν να προβλέψουμε ποτέ πλήρως τι συμβαίνει έξω από την εταιρεία μας.

Επιθέσεις από μέσα προς τα έξω (insiders)

Από την άλλη, οι εσωτερικές απειλές (*insiders*), προέρχονται από άτομα που βρίσκονται ή βρισκόντουσαν στον οργανισμό και έχουν/είχαν εξουσιοδοτημένη πρόσβαση στα συστήματα και στο δίκτυο του. Η συγκεκριμένη κατηγορία επιθέσεων ανήκει στο 34% βάση της έρευνα της *U.S. Secret Service/CERT/Microsoft E-Crime* ενώ το υπόλοιπο 29% ανήκει σε επιθέσεις που δεν έχουν επιβεβαιωθεί. Οι insiders κατηγοριοποιούνται σε τρεις κατηγορίες επιθέσεων, τις κακόβουλες επιθέσεις (*malicious attacks*), τις επιθέσεις από αμέλεια (*negligent attack*) και τις τυχαίες επιθέσεις (*accidental attacks*). Αναλυτικότερα,

- **Κακόβουλες επιθέσεις (malicious attacks),** είναι όταν ένα άτομο της εταιρείας έχει εξουσιοδοτημένη πρόσβαση στα συστήματα και στο δίκτυο της και εσκεμμένα καταχράζεται αυτήν την πρόσβαση προκαλώντας αρνητικές επιπτώσεις στην εταιρεία. Οι συνέπειες που μπορεί να προκύψουν ενδέχεται να περιλαμβάνουν τη μείωση της εμπιστοσύνης, της ακεραιότητας και της διαθεσιμότητας της εταιρείας.
- **Επιθέσεις από αμέλεια (negligent attacks),** συμβαίνουν όταν ένα εξουσιοδοτημένο άτομο της εταιρείας πραγματοποιεί απρόσεκτες κινήσεις στο σύστημα ή στο δίκτυο της εταιρείας ή αγνοεί επίτηδες τα πρωτόκολλα ασφαλείας που υπάρχουν. Το πανεπιστήμιο του *Ponemon* 2016 πραγματοποίησε μια μελέτη συγκριτικής αξιολόγησης (*benchmarking*) η οποία έδειξε ότι οι επιθέσεις από αμέλεια καταλαμβάνουν το 68% των insiders επιθέσεων.
- **Τυχαίες επιθέσεις (accidental attacks),** είναι παρόμοιες με τις επιθέσεις από αμέλεια. Συγκεκριμένα, είναι όταν ένα εξουσιοδοτημένο άτομο της εταιρείας που δεν έχει καμία πρόθεση να βλάψει την εταιρεία, αλλά ακούσια πραγματοποιεί κινήσεις στο σύστημα και στο δίκτυο της εταιρείας αυξάνοντας τις πιθανότητες μελλοντικής επιθέσεις. Οι επιπτώσεις αυτής την περίπτωσης είναι μείωση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας της εταιρείας.

Οι επιθέσεις αυτές έχουν κυρίως οικονομικά κίνητρα, καθώς ο επιτιθέμενος επιδιώκει να αποκτήσει χρήματα είτε μέσω εκβιασμού εναντίον του στόχου του για την επιστροφή πληροφοριών ή της λειτουργίας του συστήματος, είτε με την πώληση των κλοπιμαίων σε τρίτους. Επιπλέον, ο χάκερ μπορεί να επιδιώκει να βλάψει την εταιρεία επειδή είναι ανταγωνιστής ή για άλλους προσωπικούς λόγους.



Σχήμα 3.3: Τύποι Insiders

Αφού εξηγήσαμε τις κατηγορίες στις οποίες κατατάσσονται οι επιθέσεις, σειρά έχει η καταγραφή των σημαντικότερων και των πιο γνωστών επιθέσεων που λαμβάνουν χώρα στις σημερινές επιθέσεις κατά των επιχειρήσεων.

- **Κακόβουλο λογισμικό (malware):** Ο χάκερ δημιουργεί ένα κομμάτι κώδικα με τέτοιον τρόπο ώστε να μπορεί να αποκτήσει πρόσβαση σε συσκευές που δεν έχει εξουσιοδοτημένη πρόσβαση. Η επίθεση αυτή χωρίζεται σε πέντε επιμέρους κατηγορίες. Την spyware η οποία είναι και η πιο συνηθισμένη επίθεση κακόβουλου λογισμικού και

είναι γνωστή για την ικανότητας της να υποκλέβει ευαίσθητα δεδομένα χωρίς να γίνεται αντιληπτή από τον χρήστη. Η επόμενη κατηγορία είναι η Viruses. Σκοπός της είναι να εισβάλει στον σύστημα του χρήστη και να προκαλεί σύγχυση στο σύστημα καθώς και να καταστρέφει τα δεδομένα του. Επιπλέον ένα χαρακτηριστικό του Viruses είναι η δυνατότητα που έχει να αναπαράγει και να εξαπλώνει το κακόβουλο κώδικα που περιέχει. Μία ακόμη κατηγορία είναι τα Worms. Αυτό που τα χαρακτηρίζει και τα κάνει να ξεχωρίζουν από τους απλούς ιούς, είναι η ικανότητα που έχουν να υπάρχουν και να ενεργούν από μόνα τους. Η τέταρτη κατηγορία είναι ο δούρειος Ίππος (*Trojan Horse*), ο οποίος προσποιείται ότι είναι ένα χρήσιμο πρόγραμμα αλλά στην ουσία περιέχει κακόβουλο λογισμικό. Ο δούρειος ίππος είναι και αυτός αυτόνομο πρόγραμμα και το μόνο που χρειάζεται για να ενεργοποιηθεί είναι η εκτέλεσή του από τον χρήστη. Η τελευταία κατηγορία είναι τα ζόμπι (*Zombies*) τα οποία αναπαράγονται συνεχώς μέχρι να καταλάβουν όλους τους πόρους του συστήματος. Αυτή η κατηγορία χρησιμοποιείται κυρίως σε επιθέσεις άρνησης εξυπηρέτησης

- **SQL injection:** Με αυτόν τον τρόπο ο χάκερ επιτίθεται απευθείας στη βάση δεδομένων του οργανισμού χρησιμοποιώντας SQL queries, με σκοπό να τροποποιήσει ή να διαγράψει δεδομένα, προκαλώντας σημαντικές αλλαγές στη λειτουργία της εφαρμογής. Και όπως έχουμε αναφέρει η βάση δεδομένων των ERP συστημάτων περιέχουν ποικίλες και ταυτόχρονα ευαίσθητες πληροφορίες για τον οργανισμό.
- **Ηλεκτρονικό "Ψάρεμα" (Phishing):** Είναι μια μορφή επιθέσεων στην οποία ο χάκερ προσποιείται μια νόμιμη πηγή (πχ τράπεζα, ή προμηθευτή) ζητώντας από τον χρήστη να καταχωρήσει πληροφορίες όπως οι κωδικοί πρόσβασης και στοιχεία λογαριασμού. Το phishing χωρίζεται σε τρείς κατηγορίες. Στην spear, κατά την οποίο ο χάκερ αφήνει τον χρήστη να συμπληρώσει μόνος του τα στοιχεία πρόσβασης του λογαριασμού του, στην clone, κατά την οποία ο χάκερ δημιουργεί μια ψεύτικη ιστοσελίδα που να είναι κλώνος μιας αυθεντικής με σκοπό να παρασύρει τον χρήστη σε αυτήν και τέλος στην whaling κατά την οποία ο χάκερ εκμεταλλεύεται τις ευαισθησίες που υπάρχουν στα ανώτερα επίπεδα ασφαλείας για να αποκτήσει πρόσβαση στο σύστημα του χρήστη.
- **Άρνηση εξυπηρέτησης (Dos Attacks):** Στόχος της είναι η παρεμπόδιση της ομαλής λειτουργίας του συστήματος, του δικτύου ή των εφαρμογών από εξουσιοδοτημένους χρήστες, εξαντλώντας πόρους όπως είναι οι κεντρικές μονάδες επεξεργασίας (CPU), η μνήμη, το εύρος ζώνης και ο αποθηκευτικό χώρο του δίσκου.
- **Δημόσιο μη ασφαλής δίκτυο (Public Unsecured Wi-Fi Network Attack):** Δημόσια δίκτυα θεωρούνται τα δίκτυα που βρίσκουμε σε μαγαζιά, αεροδρόμια και σε πολλά άλλα μέρη, τα οποία δεν διαθέτουν κάποιον κωδικό πρόσβασης ή αν έχουν είναι εύκολος για κάποιον χάκερ να τον διαπεράσει. Οι χάκερ γνωρίζοντας αυτήν την κατάσταση επιτίθενται συχνά σε τέτοια δίκτυα για να υποκλέψουν ευαίσθητες πληροφορίες. Συνεπώς σκεφτείτε έναν B2B υπάλληλο ο οποίος διαθέτει την εφαρμογή του ERP σε μια φορητή συσκευή και συνδέεται σε ένα δημόσιο δίκτυο για να συγχρονίσει τα δεδομένα του με την βάση του ERP, πόσο εύκολο είναι να δεχτεί επίθεση!
- **Man-In-The-Middle Attack:** Σύμφωνα με τους Conti, Dragoni και Lesyk (2016), ο χάκερ "παίρνει τον έλεγχο των καναλιών επικοινωνίας μεταξύ δύο ή περισσότερων τελικών σημείων". Με άλλα λόγια, μπορεί να διακόψει και να τροποποιήσει τα πακέτα επικοινωνίας που στέλνονται στο συγκεκριμένο κανάλι. Παραδείγματος χάρη, μπορεί να

διακόψει τα πακέτα παραγγελιών που εισέρχονται στην εταιρεία με σκοπό να μειώσει την αξιοπιστία και τον τζίρο της.

- **Φυσικές απειλές (Physical Attacks):** Είναι οι επιθέσεις στο υλικό (*hardware*) του συστήματος με σκοπό την καταστροφή ή την κλοπή του εξοπλισμού.
- **Επιθέσεις για εύρεση συνθηματικών (Password Attacks):** Αυτή η επίθεση ονομάζεται και απευθείας επίθεση (*brute force*). Ο χάκερ συνδυάζει όλους τους πιθανούς συνδυασμούς με σκοπό να "σπάσει" τον κρυπτογραφημένο κωδικό πρόσβασης του χρήστη. Η brute-force είναι μία χρονοβόρα διαδικασία και για τον λόγο αυτό υπάρχουν ειδικά λογισμικά που επιταχύνουν την διαδικασία χακαρίσματος του κωδικού.

3.6 Επιπτώσεις των επιθέσεων

Γνωρίζοντας πλέον το πόσο σημαντικό είναι μια εταιρεία να προστατεύει τα δεδομένα της αλλά και τους τρόπους που μπορεί να δεχτεί επίθεση, σειρά έχει να αναφέρουμε τις επιπτώσεις που θα έχει μια εταιρεία στην περίπτωση που πέσει θύμα επιθέσεις.

Οικονομικές επιπτώσεις

Η πρώτη και ίσως και η πιο σοβαρή είναι η οικονομική επίπτωση που θα προκαλέσει η επίθεση στην εταιρεία. Τα χρηματικά ποσά που μπορεί να χάσει μια εταιρεία, ανέρχονται μέχρι και σε πολλά εκατομμύρια είτε αυτά είναι άμεσα είτε έμμεσα. Ο όρος άμεσα αναφέρεται στα χρηματικά ποσά που θα καταθέσει η εταιρεία για την επιδιόρθωση των ζημιών που προκλήθηκαν από την επίθεση (επισκευή hardware, επισκευή δικτύου κλπ.), στα χρήματα που έχασε η εταιρεία λόγω αδυναμίας παραγωγής και αδυναμία εξυπηρέτησης πελατών (*Dos Attack*) και στα χρήματα για την πρόσληψη νέου προσωπικού ικανό να αντιμετωπίσει τέτοιου είδους απειλές. Επιπλέον αναφέρεται και στα χρηματικά πόσα που θα χάσει μελλοντικά η εταιρεία από την έλλειψη πελατών και προμηθευτών, λόγω μείωσης της εμπιστευτικότητας που απέκτησε από την επίθεση. Ο λόγος για αυτήν την έλλειψη είναι γιατί ο κάθε πελάτης και ο κάθε προμηθευτής, για να παραχωρήσει προσωπικά δεδομένα σε μια εταιρεία θα πρέπει να είναι σίγουρος ότι αυτή δεν θα τα δημοσιεύσει με κανέναν τρόπο σε τρίτους χωρίς την συγκατάθεση του. Συνεπώς, όταν μια εταιρεία δέχεται επίθεση καθιστάτε ευάλωτη και ανίκανη στο να τηρήσει τον λόγο της στην προστασία αυτών των δεδομένων. Επιπροσθέτως, ο όρος άμεσα συμπεριλαμβάνει και τα χρηματικά ποσά που θα χάσει από πιθανές καταγγελίες που θα δεχτεί από τους πελάτες ή τους προμηθευτές ή από άλλους συναλλασσόμενους της εταιρείας, για την δημοσίευση των προσωπικών τους δεδομένων σε μη εξουσιοδοτημένα άτομα. Τέλος, ο όρος άμεσα περιέχει και τα χρήματα που θα δώσει σε εξωτερικούς συνεργάτες για την προστασία του συστήματος (υλικού και λογισμικού) από μελλοντικές επιθέσεις. Από την άλλη, ο όρος έμμεσα αναφέρεται αρχικά στα χρηματικά ποσά που θα διαθέσει η εταιρεία για την αγορά αδειών χρήσης ειδικού λογισμικού (*antivirus*) για την προστασία των συστημάτων της. Επίσης, περιλαμβάνει τα χρηματικά ποσά που θα καταθέσουν για την μελλοντική συμμόρφωση του οργανισμού με τους κανονισμούς που ορίζουν οι αρμόδιες αρχές για την καλύτερη προστασία της επιχείρηση τους. Τέλος ο όρος έμμεσα συμπεριλαμβάνει και τα πρόστιμα που μπορεί να δεχτεί η εταιρεία από το κράτος για την μη συμμόρφωση της με τις απαραίτητες διατάξεις για την προστασία των προσωπικών δεδομένων.

Πρόσφατες έρευνες της *International Journal of Engineering Research and Applications* έδειξαν ότι το 80% των επιχειρήσεων έχουν δεχτεί επίθεση που τους οδήγησε σε οικονομικές καταστροφές. Το συνολικό κόστος των οικονομικών ζημιών, των επηρεαζόμενων επιχειρήσεων ανέρχεται στο περίπου στα 450 εκατομμύρια δολάρια. Επιπλέον, μια άλλη έρευνα έδειξε ότι το μεγαλύτερο ποσοστό των

επιθέσεων με οικονομικό κίνητρο λαμβάνουν χώρα, σε χώρες με ισχυρή οικονομία. Εύκολα καταλαβαίνουμε την σοβαρότητα των επιθέσεων στις επιχειρήσεις και των τεράστιων οικονομικών επιπτώσεων που αποφέρουν παγκοσμίως.

Επιπτώσεις στην εμπιστοσύνη

Πέραν των οικονομικών επιπτώσεων, όταν μια εταιρεία πέφτει θύμα κυβερνοεπίθεσης δυσφημίζεται. Αυτό έχει ως συνέπεια να χαθεί και η εμπιστοσύνη από τους προμηθευτές και τους πελάτες της. Όπως αναφέρθηκε και προηγουμένως, όταν συζητήσαμε τις οικονομικές επιπτώσεις μιας επίθεσης, οι πελάτες, οι προμηθευτές αλλά και σε γενικότερο πλαίσιο όσοι συναναστρέφονται με την εταιρεία, εμπιστεύονται σε αυτήν ευαίσθητες προσωπικές τους πληροφορίες. Έχοντας όμως δεχτεί επίθεση, εκθέτει τις ευαίσθητες αυτές πληροφορίες σε ξένους χωρίς την συγκατάθεση τους. Επομένως, ακόμη και αν η εταιρεία καταφέρει να ανακάμψει από την επίθεση, οι πελάτες και οι προμηθευτές της, το πιο πιθανόν είναι να αποσυρθούν από την εταιρεία, φοβούμενοι τις ευαισθησίες της και την πιθανότητα να ξανά δεχτεί επίθεση. Πέραν όμως από τους τωρινούς πελάτες και προμηθευτές που χάνουν την εμπιστοσύνη τους στην εταιρεία, οι μελλοντικοί της πελάτες και προμηθευτές, αξιολογώντας την κακή της πλέον φήμη, είναι πιθανών να μην συνεργαστούν μαζί της. Όλα τα παραπάνω οδηγούν σε έναν και μόνο δρόμο. Το οικονομικό πλήγμα που θα δεχτεί η εταιρεία και το πιθανό κλείσιμο αυτής λόγο πτώχευσης.

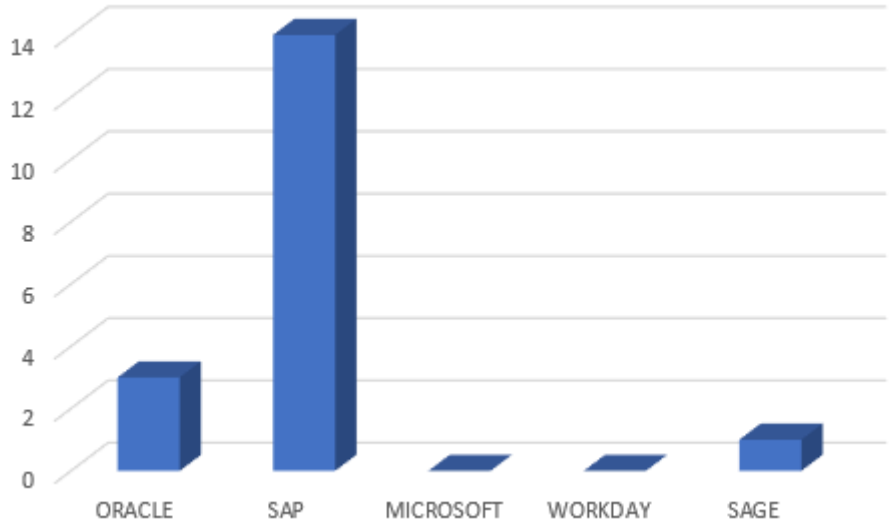
Σύμφωνα με τον Μπασδάρα (2017), το 33% των πελατών μιας εταιρείας δεν είναι απολύτως σίγουροι για το πόσο ασφαλής νιώθουν εκθέτοντας τα προσωπικά τους στοιχεία σε μια εταιρεία. Επιπροσθέτως, όταν μια εταιρεία δέχεται επίθεση το 19% των πελατών της τείνουν να αποχωρούν από την συνεργασία που είχαν.

Επίλογος

Στο τρίτο κεφάλαιο αναφερθήκαμε πιο συγκεκριμένα στον όρο ασφάλεια των δεδομένων και τους λόγους για τους οποίους είναι ένα πολύ σημαντικό και αναπόσπαστο κομμάτι των ERP συστημάτων. Επίσης, αφού πρώτα περιγράψαμε τις μεθόδους ασφάλειας που χρησιμοποιούν μέχρι και σήμερα οι πιο γνωστές εταιρείες επιχειρησιακού λογισμικού, αναλύσαμε και τα ελαττώματα αυτών των συστημάτων που οδήγησαν σε επιθέσεις. Επιπλέον αναφερθήκαμε σε μερικές από αυτές τις επιθέσεις καθώς και τα στάδια που χρησιμοποιήθηκαν για την πραγματοποίησή τους αλλά και στους σημαντικότερους τύπους των επιθέσεων των ERP. Τελειώνοντας, περιγράψαμε τις επιπτώσεις που επιφέρουν στις επιχειρήσεις αυτές οι επιθέσεις.

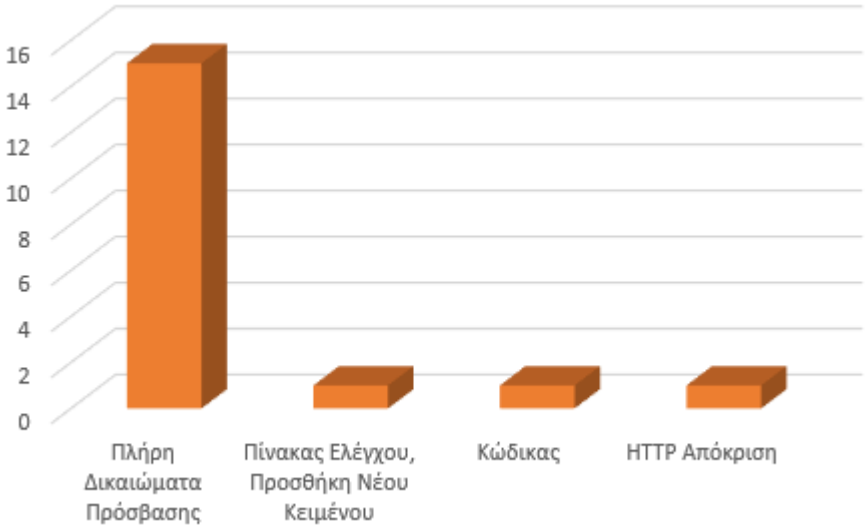
Κεφάλαιο 4ο : Αξιολόγηση επιθέσεων και ευπαθειών

Στο κεφάλαιο αυτό θα αναλύσουμε μέσα από γραφήματα μερικές παρατηρήσεις που προκύπτουν βάση των καταγεγραμμένων επιθέσεων που έχουν πραγματοποιηθεί στις εταιρείες ORACLE, SAP, MICROSOFT, WORKDAY και SAGE. Τα δεδομένα των παρακάτω γραφημάτων προέκυψαν από τις επιθέσεις που είναι καταγεγραμμένες στο CVE καθώς και το EXPLOIT DATABASE.



Σχήμα 4.1: Επιθέσεις για το χρονικό διάστημα 2017-2022

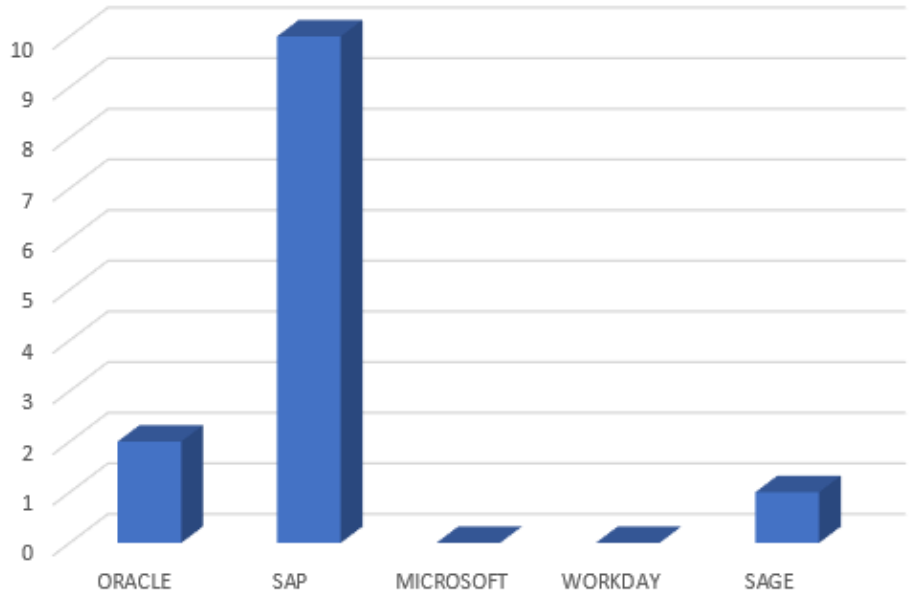
Αρχικά, αυτό που παρατηρούμε από το παραπάνω γράφημα είναι το μέγεθος των επιθέσεων (14 επιθέσεις) που έχουν πραγματοποιηθεί στην εταιρεία SAP μέσα σε μια πενταετία. Επιπλέον, η SAP θεωρείται πρωτοπόρος εταιρεία ERP λογισμικού και αυτό μας προβληματίζει σχετικά με το αυξημένο πλήθος των επιθέσεων της. Από την άλλη βλέπουμε ότι οι υπόλοιπες εταιρείες έχουν από καμία έως και τρείς καταγεγραμμένες επιθέσεις μέσα σε αυτήν την χρονική περίοδο. Συγκεκριμένα η Oracle έχει τρείς επιθέσεις, η Sage έχει μία, ενώ η Microsoft και η Workday δεν έχουν καμία καταγεγραμμένη επίθεση.



Σχήμα 4.2: Τύποι των επιθέσεων

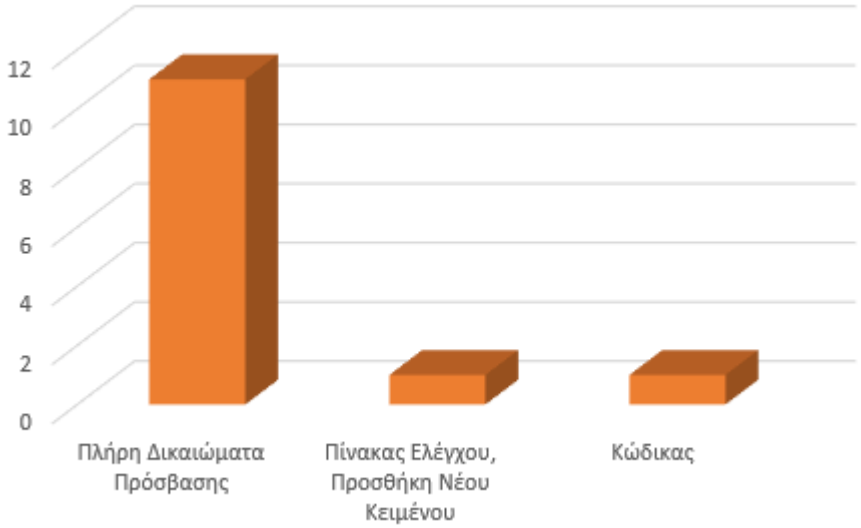
Στο γράφημα 2 βλέπουμε τα είδη των επιθέσεων που καταγράψαμε στο γράφημα 1. Εύκολα μπορούμε να παρατηρήσουμε ότι οι περισσότερες επιθέσεις πραγματοποιήθηκαν από καταχώρηση λάθος δικαιωμάτων στους χρήστες του οργανισμού και έλλειψη επίβλεψης αυτών. Συγκεκριμένα όλες οι επιθέσεις της SAP ανήκουν στην κατηγορία "Πλήρη Δικαιώματα Πρόσβασης" καθώς και η μία καταγεγραμμένη επίθεση της Sage. Από την άλλη, οι τρείς επιθέσεις της Oracle ανήκουν σε ξεχωριστές κατηγορίες. Η μία επίθεση ανήκει στην κατηγορία "Πίνακας Ελέγχου, Προσθήκη Νέου Κειμένου", η άλλη ανήκει στην κατηγορία λάθος από "Κώδικα" και η τρίτη ανήκει στην κατηγορία "HTTP Απόκριση".

Τα παρακάτω γραφήματα είναι εστιασμένα στην περίοδο του Covid-19 και συγκεκριμένα από την περίοδο Μάρτιος 2020 έως και το Δεκέμβριο 2022.



Σχήμα 4.3: Επιθέσεις κατά την διάρκεια της πανδημίας

Στο γράφημα 3 παρατηρούμε ότι από το γενικό σύνολο των καταγεγραμμένων επιθέσεων (18 επιθέσεις) για το διάστημα 2018-2022, το 72,22% αυτών των επιθέσεων (14 επιθέσεις), έλαβαν χώρα κατά τη διάρκεια της πανδημίας. Ειδικότερα από τις 14 επιθέσεις της εταιρείας SAP, οι 10 πραγματοποιήθηκαν κατά την διάρκεια του covid-19, από τις 3 επιθέσεις της εταιρείας Oracle, οι 2 πραγματοποιήθηκαν κατά την ίδια χρονική περίοδο και η μια καταγεγραμμένη επίθεση της εταιρείας Sage πραγματοποιήθηκε και αυτή στο ίδιο χρονικό διάστημα.



Σχήμα 4.4: Τύποι επιθέσεων κατά την διάρκεια της πανδημίας

Στο γράφημα 4 παρατηρούμε ότι από το συνολικό πλήθος των επιθέσεων (14 επιθέσεις) που ανήκουν την κατηγορία “Πλήρη δικαιώματα Πρόσβασης”, μόλις οι 11 πραγματοποιήθηκαν κατά την διάρκεια του covid-19 και συγκεκριμένα οι 10 ανήκουν στην εταιρεία της SAP, ενώ η μια στην εταιρεία της Sage. Από την άλλη, οι άλλες δύο κατηγορίες, “Πίνακας Ελέγχου, Προσθήκη Νέου Κειμένου” και “Κώδικας” ανήκουν στις επιθέσεις της εταιρείας Oracle. Το πλήθος αυτών των δύο τύπων επιθέσεων είναι ένα και για τις δύο ξεχωριστά και όπως παρατηρούμε, αυτές έλαβαν χώρα στην διάρκεια της πανδημίας.

Επίλογος

Το τελικός μας συμπέρασμα στο κεφάλαιο αυτό είναι ότι οι μεγάλες εταιρείες ERP λογισμικού είναι και αυτές εξίσου ευάλωτες και πιθανόν να δεχτούνε επίθεση, παρά την αυξημένη προσπάθεια που καταβάλλουν για την ασφάλεια των συστημάτων τους. Επιπλέον, αυτό που μπορούμε να κρατήσουμε από αυτό το κεφάλαιο και από τα γραφήματα που αναλύσαμε είναι ότι το μεγαλύτερο ποσοστό των επιθέσεων έλαβαν χώρα κατά την διάρκεια της πανδημίας, πράγμα που θεωρείται λογικό, λόγο της αύξησης της τηλεργασίας η οποία συνεπάγεται σε μείωση της επίβλεψης του προσωπικού από τους αρμόδιους καθώς και την αύξηση των εργαλείων τηλεδιάσκεψης και τηλεργασίας (παραδείγματος χάρη Anydesk, TeamViewer και VPN).

Κεφάλαιο 5ο : Υφιστάμενες τεχνολογικές λύσεις

Στόχος του πέμπτου κεφαλαίου είναι η καταγραφή των υφιστάμενων τεχνολογικών λύσεων που πρέπει να εντάξουν οι επιχειρήσεις για την πρόληψη, τον εντοπισμό και την αντιμετώπιση μίας κυβερνοεπίθεσης στο ERP σύστημά τους. Στην αρχή θα καταγράψουμε έναν πλήρη οδηγό για μια ασφαλή χρήση του συστήματος και τέλος θα αναφερθούμε σε frameworks για τον εντοπισμό των ευπαθειών που καθιστούν ευάλωτο τον οργανισμό.

5.1 Ένας πλήρες οδηγός για ασφαλή χρήση του συστήματος

Στην ενότητα αυτή θα καταγράψουμε αναλυτικά 14 μέτρα που πρέπει να πάρει κάθε εταιρεία που θέλει να κρατήσει ασφαλές από επιθέσεις, το ERP σύστημά της. Τα παρακάτω μέτρα δεν είναι ειδικά για το ERP σύστημα αλλά είναι γενικότερα μέτρα πρόληψης της εταιρείας ώστε να μην καταφέρει ο επιτιθέμενος να φτάσει στο ERP σύστημα. Για κάθε ένα από τα παρακάτω 14 μέτρα που θα αναφέρουμε, τα «Μέτρα προστασίας» τους, βασίζονται κατά βάση στο εγχειρίδιο κυβερνοασφάλειας που έχει εκδοθεί από την Εθνική Αρχή Κυβερνοασφάλειας της Ελληνικής Δημοκρατίας.

1. **Έλεγχος Πρόσβασης (Access Control)**

Είναι ο περιορισμός πρόσβασης στους εξουσιοδοτημένους χρήστες, σε λειτουργίες και υπηρεσίες του συστήματος. Είναι πολύ σημαντικό οι χρήστες του οργανισμού να έχουν τα σωστά προνόμια ο καθένας, με βάση τον ρόλο του στην εταιρεία και όχι παραπάνω από αυτά που απαιτούνται για να πραγματοποιηθούν με επιτυχία τα εργασιακά τους καθήκοντα. Δίνοντας επιπλέον δικαιώματα σε έναν χρήστη, αυτομάτως δίνει και περισσότερες δυνατότητες στον επιτιθέμενο να εξαπλώσει την επίθεση του σε όλο το δίκτυο της εταιρείας. Παραδείγματος χάρη, ο ρόλος ενός εξουσιοδοτημένου χρήστη στην εταιρεία είναι η τεχνική υποστήριξη και του παραχωρούμε δικαιώματα να βλέπει και να επεξεργάζεται και τα λογιστικά στοιχεία της εταιρείας. Ως αποτέλεσμα, σε περίπτωση επίθεσης στο σύστημα του συγκεκριμένου χρήστη, ο επιτιθέμενος θα αποκτήσει αυτομάτως και αυτός πρόσβαση στα λογιστικά στοιχεία της εταιρείας. Ένα ακόμη παράδειγμα λάθους καταχώρησης δικαιωμάτων είναι το εξής: χρήστης που τα εργασιακά του καθήκοντα είναι απλές εργασίες τύπου χρήση word, excel, ανάγνωση email και λοιπά και έχει δικαιώματα administrator, σε περίπτωση επίθεσης στο σύστημα του, ο επιτιθέμενος μεταξύ άλλον μπορεί να δημιουργήσει νέους administrator λογαριασμούς με στόχο την εξάπλωση του σε όλο το δίκτυο του οργανισμού για την υποκλοπή ευαίσθητων δεδομένων.

Σε συστήματα Ελέγχου Πρόσβασης, υπάρχουν οι μηχανισμοί οι οποίοι είναι λογισμικά χαμηλού επιπέδου, σε λογισμικό και σε υλικό και έχουν αναπτυχθεί από προγραμματιστές με σκοπό την ενσωμάτωση πολιτικών ασφαλείας σε αυτά, και οι πολιτικές οι οποίες είναι οδηγοί χρήσης υψηλού επιπέδου, οι οποίες καθορίζουν τις συνθήκες με τις οποίες ένας χρήστης έχει άδεια πρόσβασης σε μία λειτουργία ή ένα σύστημα. Η κάθε εταιρεία έχει τις δικές τις λειτουργίες και ανάγκες για ασφάλεια και γι΄αυτόν τον λόγο οι πολιτικές πρέπει να είναι ποικίλες για να προσαρμόζονται με αυτές. Σύμφωνα με τους Sandhu και Samarati, «Δεν υπάρχουν πολιτικές οι οποίες είναι καλύτερες από κάποιες άλλες, αλλά υπάρχουν πολιτικές που διασφαλίζουν μεγαλύτερη ασφάλεια από κάποιες άλλες»[91]

Σύμφωνα με τους Samarati και Vimercati (2000) οι πολιτικές Ελέγχου Πρόσβασης κατατάσσονται σε τρείς βασικές κατηγορίες: την Διακριτική ή Discretionary (DAC) η οποία βασίζεται στην ταυτότητα του αιτούντος καθώς και στους κανόνες πρόσβασης που δηλώνουν τι επιτρέπεται (ή όχι) να κάνουν οι αιτούντες, την Επιτακτική ή Mandatory (MAC) η οποία βασίζεται σε εντεταλμένους κανονισμούς που έχουν καθοριστεί από μια κεντρική αρχή και την Βασισμένη σε ρόλους ή Role-Based (RBAC) η οποία βασίζεται στους ρόλους που έχουν οι χρήστες εντός του συστήματος και τους κανόνες που δηλώνουν ποιες προσβάσεις επιτρέπονται στους χρήστες, σε συγκεκριμένους ρόλους. Οι δύο πρώτες κατηγορίες δεν χρησιμοποιούνται συχνά όσο η τρίτη κατηγορία.

Έχοντας κατανοήσει τη χρησιμότητα του Ελέγχου Πρόσβασης και τις κατηγορίες που υπάρχουν, σειρά έχει η καταγραφή μερικών βασικών μέτρων, που πρέπει να ακολουθούν οι εταιρείες, ώστε να αποφύγουν τυχόν επιθέσεις αυτής της περίπτωσης.

Μέτρα προστασίας:

1.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές ελέγχου πρόσβασης, οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφέρουν τους τρόπους υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζει.

1.2 Για τη διασφάλιση της λογοδοσίας, είναι απαραίτητο να εξασφαλίσουν ότι το προσωπικό και οι εξωτερικοί συνεργάτες που διαθέτουν λογαριασμούς χρηστών αναγνωρίζονται με μοναδικό και αξιόπιστο τρόπο.

1.3 Να συντάξουν έναν κατάλογο που θα περιλαμβάνει όλους τους λογαριασμούς χρηστών, συμπεριλαμβανομένων του ονόματος και του επωνύμου του κάθε χρήστη, της ημερομηνίας έναρξης και λήξης του λογαριασμού, των δικαιωμάτων πρόσβασης και την υπηρεσία εργασία που ανήκει ο κάθε χρήστης.

1.4 Οι χρήστες που ασχολούνται αποκλειστικά με μη διαχειριστικές καθημερινές εργασίες, όπως η χρήση εφαρμογών word, excel, ανάγνωση και αποστολή email, περιήγηση στο Internet και άλλες παρόμοιες εργασίες, θα διαθέτουν μόνο έναν απλό λογαριασμό χρήστη (*non-privileged*) και όχι με διαχειριστικά δικαιώματα.

1.5 Για τους χρήστες που έχουν λογαριασμό αυξημένων προνομίων (*privileged account*) λόγω εργασιακών καθηκόντων, απαιτείται η χορήγηση ενός δεύτερου standard λογαριασμού απλού χρήστη (*non-privileged*). Ο δεύτερος αυτός λογαριασμός θα χρησιμοποιείται για την εκτέλεση μη διαχειριστικών εργασιών καθημερινής ρουτίνας, όπως η χρήση προγραμμάτων word, excel, ανάγνωση και αποστολή email, περιήγηση στο Internet άλλες παρόμοιες εργασίες.

1.6 Με σκοπό να διασφαλιστεί ότι οι χρήστες έχουν πρόσβαση στην απαραίτητη πληροφορία για την εκτέλεση των καθηκόντων τους, πρέπει να γίνει εκχώρηση δικαιωμάτων πρόσβασης με βάση διακριτούς ρόλους. Κάθε ρόλος θα πρέπει να λαμβάνει τα ελάχιστα προνόμια που απαιτούνται για την εκτέλεση των συγκεκριμένων εργασιακών καθηκόντων του.

1.7 Να αναπτύξουν μια υπηρεσία καταλόγου για την κεντρική διαχείριση λογαριασμών.

1.8 Για την εκτέλεση ιδιαίτερα κρίσιμων και ευαίσθητων εντολών ή λειτουργιών, απαιτείται η εφαρμογή της τεχνικής της διπλής εξουσιοδότησης, η οποία προβλέπει την έγκριση από δύο εξουσιοδοτημένους χρήστες πριν από την πραγματοποίηση των εν λόγω εντολών ή λειτουργιών.

2. Αυθεντικοποίηση Χρηστών

Η αυθεντικοποίηση είναι η διαδικασία επαλήθευσης της ταυτότητας ενός χρήστη στο σύστημα ή στο δίκτυο και βοηθάει στον περιορισμό των μη εξουσιοδοτημένων χρηστών που προσπαθούν να αποκτήσουν πρόσβαση σε αυτό. Το δεύτερο βήμα της αυθεντικοποίησης είναι η εξουσιοδότηση του χρήστη κατά το οποίο, τα διαπιστευτήρια του επαληθεύονται από το υπολογιστικό σύστημα προτού του επιτραπεί η πρόσβαση σε αυτό και για προκαθορισμένο χρονικό διάστημα, σύμφωνα με την πολιτική ασφαλείας των χρηστών.

Η αυθεντικοποίησης χωρίζεται σε τρεις τύπους:

- Τι ξέρεις (What you know)
- Τι έχεις (What you have)
- Και ποιος είσαι (Who you are)

Παραδείγματος χάρη, το τι ξέρεις μπορεί να είναι ο κωδικός πρόσβασης, το τι έχεις μπορεί να είναι το διακριτικό σου (*token*) και το ποιος είσαι είναι τα βιομετρικά χαρακτηριστικά σου (π.χ. δακτυλικό αποτύπωμα).

Σε περίπτωση κλοπής της ταυτότητας του χρήστη, ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε σημαντικές πληροφορίες της εταιρείας. Για τον λόγο αυτόν η σωστή επιβεβαίωση της ταυτότητας των χρηστών που επιθυμούν να αποκτήσουν πρόσβαση στο σύστημα, είναι ζωτικής σημασίας για τον οργανισμό.

Παρακάτω, καταγράφονται τα βασικά μέτρα για την σωστή αυθεντικοποίηση των χρηστών με σκοπό την αποτροπή υποκλοπής της ταυτότητάς τους.

Μέτρα Προστασίας:

2.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές αυθεντικοποίησης των χρηστών, οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφέρουν τους τρόπους υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζει.

2.2 Για να εξασφαλίσουν την ασφάλεια του λογαριασμού τους, οι χρήστες πρέπει να χρησιμοποιούν κωδικούς πρόσβασης που πληρούν τις παρακάτω προδιαγραφές:

- Οι κωδικοί πρόσβασης πρέπει να είναι αρκετά ισχυροί και πολύπλοκοι. Αυτό σημαίνει ότι οι κωδικοί πρέπει να έχουν μήκος τουλάχιστον δώδεκα χαρακτήρων και να περιλαμβάνουν τουλάχιστον ένα κεφαλαίο γράμμα, ένα μικρό γράμμα, έναν αριθμό και έναν ειδικό χαρακτήρα.
- Οι κωδικοί πρόσβασης δεν πρέπει να περιλαμβάνουν ονόματα ή κοινές λέξεις που μπορούν να βρεθούν σε λεξικά. Αυτό μειώνει τον κίνδυνο εύρεσης του κωδικού από κακόβουλα προγράμματα ή επιτιθέμενους.
- Είναι απαραίτητο να αλλάζουν τους κωδικούς τους τουλάχιστον κάθε έξι μήνες. Αυτή η πρακτική συμβάλλει στην διατήρηση της ασφάλειας του λογαριασμού τους. Αν για κάποιο λόγο κάποιος καταφέρει να εντοπίσει τον κωδικό πρόσβασης, δεν θα μπορεί να έχει πρόσβαση στον λογαριασμό τους για μεγάλο χρονικό διάστημα

2.3 Θα πρέπει να οριστεί ένα μέγιστο όριο από πέντε ανεπιτυχείς συνεχόμενες προσπάθειες για είσοδο σε ένα λογαριασμό. Μετά από αυτό το όριο, ο λογαριασμός θα κλειδώνετε για ένα προκαθορισμένο χρονικό διάστημα.

2.4 Οι κωδικοί πρόσβασης, πρέπει να αποθηκεύονται σε μια μορφή που δεν μπορεί να αποκρυπτογραφηθεί εύκολα. Για αυτό το λόγο, χρησιμοποιούνται one-way hash αλγόριθμοι για την κρυπτογράφησή τους. Αυτοί οι αλγόριθμοι δημιουργούν ένα μοναδικό αλφαριθμητικό κωδικό από τον αρχικό κωδικό, αλλά δεν επιτρέπουν την επαναφορά του αρχικού κωδικού. Επιπλέον, προστίθεται μια ακολουθία τυχαίων δεδομένων (*salt*) στη διαδικασία κρυπτογράφησης για να αυξηθεί η πολυπλοκότητα της αποκρυπτογράφησης και να δυσκολέψει έναν επιθετικό εξωτερικό παράγοντα από το να βρει τον αρχικό κωδικό.

2.5 Πρέπει να χρησιμοποιούν κρυπτογράφηση για τη μεταφορά κωδικών πρόσβασης μέσω δικτύου.

2.6 Είναι απαραίτητη η χρήση ενός διπλού μηχανισμού ασφαλείας (*2-factor authentication*) για την εξουσιοδότηση της πρόσβασης σε λογαριασμούς χρηστών με επιπλέον δικαιώματα. Αυτό σημαίνει ότι, εκτός από την καταχώρηση ενός κωδικού πρόσβασης, οι χρήστες θα πρέπει να παρέχουν μια δεύτερη μορφή αυθεντικοποίησης, όπως για παράδειγμα έναν κωδικό που αποστέλλεται στο κινητό τους τηλέφωνο.

2.7 Είναι επιπλέον απαραίτητη η χρήση ενός διπλού μηχανισμού ασφαλείας (*2-factor authentication*) για την επιβεβαίωση της ταυτότητας των χρηστών προκειμένου να αποκτήσουν απομακρυσμένη πρόσβαση στο εσωτερικό δίκτυο του Οργανισμού.

2.8 Απαραίτητη είναι και η χρήση ενός διπλού μηχανισμού ασφαλείας (*2-factor authentication*) για την επιβεβαίωση της ταυτότητας των χρηστών που επιθυμούν να αποκτήσουν πρόσβαση σε κρίσιμα ή ευαίσθητα δεδομένα.

2.9 Πρέπει να ρυθμίσουν τους υπολογιστές στον χώρο εργασίας, έτσι ώστε να κλειδώνουν αυτόματα την οθόνη μετά από 15 λεπτά αδράνειας του χρήστη, προκειμένου να αποτραπεί η πρόσβαση από άτομα που δεν έχουν την ανάλογη εξουσιοδότηση. Για να ξεκλειδωθεί η οθόνη, ο χρήστης θα πρέπει να επαληθεύσει την ταυτότητά του εκ νέου.

2.10 Τέλος απαιτείται η χρήση ενός συστήματος ασφαλείας που βασίζεται στο δημόσιο κλειδί για να επιβεβαιώσει την ταυτότητα των χρηστών με τη χρήση ενός ψηφιακού πιστοποιητικού.

3. Ασφάλεια Δικτύων

Η έλλειψη ασφάλειας στο εταιρικό δίκτυο μπορεί να οδηγήσει σε πολλών ειδών επιθέσεις καθώς και σε επίθεση άρνησης παροχής υπηρεσιών. Για τον λόγο αυτό τα παρακάτω μέτρα προστασίας που θα αναλυθούν είναι πολύ σημαντικό να λαμβάνονται υπόψιν από όλες τις εταιρείες που διαχειρίζονται και κατέχουν κρίσιμες πληροφορίες. Εκτός από τα γενικά μέτρα προστασίας που θα καταγράψουμε, θα αναφερθούμε και πιο συγκεκριμένα σε μερικά μέτρα προστασίας σε περίπτωση επίθεσης άρνησης παροχής υπηρεσιών.

Μέτρα Προστασίας:

3.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές ασφάλειας δικτύων, οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφέρουν τους τρόπους υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζουν.

3.2 Πρέπει να δημιουργήσουν λεπτομερή διαγράμματα του δικτύου που θα περιλαμβάνουν όλες τις συσκευές και τις δικτυακές συνδέσεις τους, καθώς και τα βασικά τους χαρακτηριστικά και τις κρίσιμες υπηρεσίες και συστήματα. Αυτά τα διαγράμματα θα πρέπει να φυλάσσονται σε ασφαλές μέρος.

3.3 Πρέπει να αποθηκεύσουν όλους τους κανόνες που χρησιμοποιούν για να καθορίσουν τη διαδρομή δεδομένων στο δίκτυο, καθώς και τους κανόνες που ρυθμίζουν ποιοι χρήστες έχουν πρόσβαση στο δίκτυο μέσω του firewall. Αυτό το αρχείο πρέπει να προστατεύεται επαρκώς για να αποτρέπεται η παραβίαση των κανόνων από μη εξουσιοδοτημένα άτομα.

3.4 Πρέπει να βεβαιωθούν ότι οι διακομιστές του Οργανισμού που διαθέτουν δημόσια IP διεύθυνση (π.χ. web servers, mail servers, VPN servers κ.λπ.) βρίσκονται σε μια διακριτή δικτυακή ζώνη (υποδίκτυο), η οποία έχει χωριστεί με φυσικό ή λογικό τρόπο από το εσωτερικό δίκτυο του Οργανισμού.

3.5 Πρέπει να εγκαταστήσουν ένα τείχος προστασίας (*firewall*) στην εξωτερική περίμετρο του δικτύου τους. Αυτό το τείχος θα πρέπει να επιτρέπει μόνο την εισερχόμενη και εξερχόμενη ροή της πληροφορίας που απαιτείται για την κανονική λειτουργία των επιχειρησιακών τους δραστηριοτήτων.

3.6 Αναλύοντας το εσωτερικό δίκτυο του Οργανισμού, πρέπει να διαχωρίσουν τις διαφορετικές περιοχές του βάση του επιπέδου κρισιμότητας και ευαισθησίας των επιχειρησιακών τομέων. Συγκεκριμένα, πρέπει να καθοριστούν διακριτά υποδίκτυα για τις διάφορες περιοχές του δικτύου, που θα έχουν διαφορετικά επίπεδα πρόσβασης και ασφάλειας, ανάλογα με τον κίνδυνο που αντιμετωπίζουν.

3.7 Πρέπει επίσης να εφαρμόσουν φιλτράρισμα δικτυακής κίνησης μεταξύ των υποδικτύων προκειμένου να περιοριστεί η ροή της πληροφορίας στο ελάχιστο απαραίτητο επίπεδο για τις επιχειρησιακές ανάγκες του Οργανισμού.

3.8 Για να διασφαλιστεί η ασφαλή πρόσβαση των χρηστών στο εσωτερικό δίκτυο του Οργανισμού, πρέπει να χρησιμοποιηθεί ένα VPN και να επιβεβαιώνεται η ταυτότητα με διπλή πιστοποίηση (*2-factor authentication*). Επιπλέον, θα πρέπει να χρησιμοποιούνται οι πιο πρόσφατοι αλγόριθμους κρυπτογράφησης για να διασφαλιστεί ότι οι επικοινωνίες είναι ασφαλείς και προστατευμένες από εξωτερικές απειλές.

3.9 Απαραίτητη είναι η διασφάλιση του ελέγχου της συνολικής δικτυακής κίνησης που περνάει ανάμεσα στο δίκτυό τους και το Διαδίκτυο μέσω ενός αυθεντικοποιημένου διακομιστή πρόσβασης επιπέδου εφαρμογής (*application layer (web) proxy server*), που έχει ρυθμιστεί έτσι ώστε να αποκλείει μη εξουσιοδοτημένες συνδέσεις.

3.10 Πρέπει να εφαρμόσουν επίσης δικτυακά συστήματα ανίχνευσης και πρόληψης εισβολών σε κάθε υποδίκτυο του Οργανισμού, με σκοπό την αναγνώριση και την αποτροπή πιθανών επιθέσεων.

3.11 Η κατασκευή μιας συσκευής σε μορφή hardware, η οποία θα λειτουργεί ως δίοδος δεδομένων (*data diode*) και θα διασφαλίζει ότι η ροή των δεδομένων θα πραγματοποιείται μόνο προς μία κατεύθυνση είναι απαραίτητη. Σκοπός της διόδου, είναι η προστασία κρίσιμης πληροφορίας σε υποδίκτυα υψηλών απαιτήσεων ασφάλειας.

3.12 Εάν ο Οργανισμός παρέχει ασύρματα δίκτυα για δημόσια πρόσβαση, αυτά θα πρέπει υποχρεωτικά να είναι διαχωρισμένα από το υπόλοιπο δίκτυο του Οργανισμού.

3.13 Σημαντική είναι επίσης η απενεργοποίηση της ασύρματης πρόσβασης στο διαχειριστικό περιβάλλον του wireless access point.

3.14 Η εφαρμογή του πρωτόκολλου 802.1x (network access control) θα βοηθήσει στον έλεγχο των συσκευών που μπορούν να αυθεντικοποιηθούν στο δίκτυο.

3.15 Όταν η ασύρματη δικτυακή κυκλοφορία κρυπτογραφείται με τον αλγόριθμο AES με χρήση κλειδιού μήκους 256 bits αυξάνεται η ασφάλεια του δικτύου.

3.16 Απαραίτητη θεωρείται επίσης η εγκατάσταση ενός ασύρματου συστήματος ανίχνευσης εισβολών (WIDS) για την ανίχνευση μη εξουσιοδοτημένων ασύρματων σημείων πρόσβασης (ασύρματα access points) που είναι συνδεδεμένα στο δίκτυο του Οργανισμού.

Τα επόμενα μέτρα προστασίας αναφέρονται συγκεκριμένα σε περιπτώσεις επίθεσης άρνησης παροχής υπηρεσιών (DDoS)

3.17 Η κατανόηση των τρόπων με τους οποίους η υπηρεσία που παρέχετε μπορεί να υπερφορτωθεί, καθώς και τα όρια (σε bandwidth, επεξεργαστική ισχύ και αποθηκευτικό χώρο) πέρα από τα οποία η διαθεσιμότητα της υπηρεσίας κινδυνεύει με διακοπή.

3.18 Η χρήση του domain registrar locking για να αποτραπεί η άρνηση παροχής υπηρεσιών λόγω μη εξουσιοδοτημένης διαγραφής, μεταφοράς ή τροποποίησης της εγγραφής του domain.

3.19 Η υποδομή πρέπει να διαθέτει επαρκείς πόρους, όπως hardware, έτσι ώστε να είναι σε θέση να αντιμετωπίσει μια επίθεση άρνησης υπηρεσίας.

3.20 Η απομόνωση των κρίσιμων δικτυακών υπηρεσιών από άλλες υπηρεσίες που είναι ευάλωτες σε επιθέσεις, όπως οι διαδικτυακές.

3.21 Η ανάπτυξη συστημάτων παρακολούθησης της διαθεσιμότητας των κρίσιμων υπηρεσιών, τα οποία θα ανιχνεύουν επιθέσεις άρνησης παροχής υπηρεσιών (DDoS) και θα αποστέλλουν ειδοποιήσεις σε πραγματικό χρόνο είναι απαραίτητη.

3.22 Η ανάθεση της φιλοξενίας των δημόσιας πρόσβασης εφαρμογών σε έναν πάροχο cloud υπηρεσιών, αφού πρώτα πραγματοποιηθεί μια λεπτομερή αξιολόγηση και αναζήτηση των χαρακτηριστικών του παρόχου, σχετικά με την ικανότητά του να ανταπεξέλθει σε επιθέσεις άρνησης υπηρεσίας, είναι σημαντική. Επιπλέον, συνιστάτε να ληφθεί υπόψη η παράμετρος της εμπιστευτικότητας κατά την επιλογή του παρόχου.

3.23 Η ανάθεση σε έναν εξειδικευμένο πάροχο cloud υπηρεσιών ασφάλειας (*security as a service*) που θα παρέχει υπηρεσίες προστασίας για των δημόσιας πρόσβασης εφαρμογών σας από κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών, είναι επίσης απαραίτητη.

4. Περιορισμός χρήσης και εκτέλεσης προγραμμάτων και Υπηρεσιών

Είναι σημαντικό να περιορίσουμε τη χρήση των μη σημαντικών προγραμμάτων σε ένα σύστημα κατά το ελάχιστο δυνατό. Χρησιμοποιώντας μόνο προγράμματα που είναι απαραίτητα για την ομαλή λειτουργία του συστήματος, μειώνουμε σημαντικά και την επιφάνεια επίθεσης στο σύστημά μας. Σύμφωνα με τον Μπαμπούρη (2022), με τον όρο επιφάνεια επίθεσης εννοούμε το σύνολο των σημείων εισόδου που είναι δυνητικά εκτεθειμένα σε έναν επιτιθέμενο, και που μπορούν να χρησιμοποιηθούν για να αποκτηθεί πρόσβαση στο σύστημα και στα δεδομένα της εφαρμογής. Επιπλέον, ο όρος αυτός, αναφέρεται στα δεδομένα που χρησιμοποιούνται από τις εφαρμογές και υπάρχει η δυνατότητα εξαγωγής τους από το σύστημα. Τέτοια δεδομένα μπορεί να είναι οι κωδικοί, τα προσωπικά δεδομένα, τα εταιρικά δεδομένα και πολλά ακόμη.

Ο καλύτερος τρόπος για να εφαρμοστεί αυτό το μέτρο, είναι να εντάξουν οι εταιρείας την «αρχή της ελάχιστης λειτουργικότητας». Αυτή η αρχή, δεν αναφέρεται μόνο στον περιορισμό της χρήσης των προγραμμάτων αλλά και στις λειτουργίες που μπορούν να εκτελέσουν τα προγράμματα. Τα παρακάτω μέτρα υπάρχουν για την μείωση της επιφάνειας επίθεσης.

Μέτρα Προστασίας:

4.1 Η ανάπτυξη και η καταγραφή πολιτικών εγκατάστασης, χρήσης και εκτέλεσης των λογισμικών οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

4.2 Απαραίτητος είναι ο έλεγχος στους servers και στους υπολογιστές των εργαζομένων, έτσι ώστε να είναι σε λειτουργία μόνο οι θύρες, τα πρωτόκολλα και οι δικτυακές υπηρεσίες που απαιτούνται για την διεκπεραίωση των επιχειρησιακών λειτουργιών του οργανισμού.

4.3 Πρέπει να ζητείται να πραγματοποιηθεί αυτοματοποιημένος έλεγχος θυρών και υπηρεσιών στα συστήματα του οργανισμού, με στόχο τον εντοπισμό μη εξουσιοδοτημένων ανοικτών δικτυακών θυρών και υπηρεσιών, ανά τακτά χρονικά διαστήματα.

4.4 Η εξασφάλιση ότι οι χρήστες με μη προνομιούχα δικαιώματα δεν έχουν τη δυνατότητα να απενεργοποιήσουν ή να τροποποιήσουν τις ρυθμίσεις ασφαλείας στο λειτουργικό τους σύστημα είναι άκρως απαραίτητη.

4.5 Για να διασφαλιστεί ότι οι χρήστες με standard δικαιώματα δεν εγκαθιστούν μη εγκεκριμένο λογισμικό σε περίπτωση επιχειρησιακής ανάγκης, απαιτείται η χρήση εγκεκριμένων εφαρμογών που αποθηκεύονται σε αποθετήρια λογισμικού τα οποία ελέγχονται από την εταιρεία.

4.6 Η δημιουργία ενός καταλόγου με μη εξουσιοδοτημένες εφαρμογές και κατηγορίες εκτελέσιμων αρχείων και η εξασφάλιση ότι η εκτέλεσή τους δεν θα επιτρέπεται στους servers και στους σταθμούς εργασίας του οργανισμού πρέπει να υλοποιηθεί.

4.7 Απαραίτητη είναι η προσοχή στη ρύθμιση της χρήσης του πρωτοκόλλου SMB (Server Message Block). Το πρωτόκολλο αυτό περιλαμβάνει τα εξής βήματα: 1) Στο firewall της εξωτερικής περιμέτρου του δικτύου, πρέπει να τίθενται αποκλειστικοί κανόνες που θα φράζουν την εισερχόμενη και εξερχόμενη επικοινωνία προς το Internet σε ορισμένες θύρες. Πιο συγκεκριμένα, θα πρέπει να αποκλείονται η είσοδος και έξοδος στις θύρες TCP 445 (SMB), UDP 137 (NetBIOS Name Resolution), UDP 138 (NetBIOS Datagram Service) και TCP 139 (NetBIOS Session Service). 2) Ο αποκλεισμός των εισερχόμενων συνδέσεων SMB στη θύρα TCP 445 σε οποιοδήποτε υπολογιστή ή διακομιστή που δεν φιλοξενεί κοινόχρηστα αρχεία. 3) Η απενεργοποίηση των εκδόσεων του πρωτοκόλλου SMBv1 και SMBv2 στο εσωτερικό δίκτυο και η αναβάθμιση σε μια νεότερη έκδοση όπως η SMBv3 ή η πιο πρόσφατη διαθέσιμη έκδοση.

4.8 Απαιτείται η επιβολή μιας πολιτικής εκτέλεσης λογισμικού στο λειτουργικό σύστημα, η οποία θα εξασφαλίζει την εκτέλεση αποκλειστικά ψηφιακά υπογεγραμμένων scripts, εκτελέσιμων αρχείων, οδηγών συσκευών και υλικολογισμικού. Επιπλέον, πρέπει να διατηρείται ένας κατάλογος αξιόπιστων πιστοποιητικών, προκειμένου να ανιχνεύονται και να αποτρέπεται η εκτέλεση κακόβουλου κώδικα.

4.9 Σε ένα περιβάλλον Microsoft Windows καθώς και σε λογαριασμούς χρηστών με μη προνομιούχα δικαιώματα, οι παρακάτω μηχανές εκτέλεσης script κώδικα πρέπει να απενεργοποιηθούν: PowerShell, Command Prompt, Windows Script Host, Windows Management Instrumentation και Microsoft HTML Application Host.

4.10 Η δημιουργία ενός καταλόγου που θα περιλαμβάνει μόνο τις εξουσιοδοτημένες εφαρμογές και τα συστατικά τους, όπως είναι οι βιβλιοθήκες είναι απαραίτητη. Στόχος είναι να

διασφαλιστεί ότι μόνο αυτές οι εφαρμογές θα μπορούν να εκτελούνται στους servers και στους σταθμούς εργασίας του οργανισμού (*application whitelisting*).

5. Απομακρυσμένη εργασία

Τα τελευταία χρόνια, χάρη στην ύπαρξη της πανδημίας η απομακρυσμένη εργασία αυξήθηκε ολοένα και περισσότερο σε όλους τους εργασιακούς τομείς. Αυτό το μοντέλο όμως επιφέρει μερικούς σοβαρούς κινδύνους που μπορούν να οδηγήσουν σε επιθέσεις του οργανισμού. Μερικά παραδείγματα κινδύνων είναι τα εξής:

Ας υποθέσουμε ότι μια εταιρεία παραχωρεί στους εργαζομένους της για την διευκόλυνση της εργασίας τους από το σπίτι, φορητούς υπολογιστές που έχουν εγκατεστημένα τα λογισμικά που χρειάζονται για την διεκπεραίωση των εργασιών τους και μαζί με αυτών και το ERP λογισμικό. Σε περίπτωση κλοπής, αυτού του φορητού υπολογιστή, τα δεδομένα της εταιρείας φανερώνονται σε λάθος άτομα. Επιπλέον αν ο εργαζόμενος που δουλεύει από το σπίτι του συνδεδεμένος στο εταιρικό δίκτυο μέσω λογισμικού απομακρυσμένης επιφάνειας εργασίας (π.χ. Anydesk, TeamViewer), πέσει θύμα επίθεσης στο οικιακό του δίκτυο, ο επιτιθέμενος μπορεί να παραβιάσει εκτός από τα προσωπικά δεδομένα του χρήστη και τα εταιρικά δεδομένα.

Επειδή ακόμη και σήμερα οι εταιρείες χρησιμοποιούν αρκετά αυτό το μοντέλο εργασίας, θα πρέπει τόσο οι ίδιες όσο και οι εργαζόμενοι τους να τηρούν μέτρα προστασίας προς την αποφυγή επίθεσης. Τα παρακάτω μέτρα προστασίας αναφέρονται και στις δύο πλευρές.

Μέτρα Προστασίας:

5.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές απομακρυσμένης εργασίας οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

5.2 Απαραίτητη είναι η αναβάθμιση του VPN και του δικτυακού εξοπλισμού με τις τελευταίες εκδόσεις λογισμικού και ρυθμίσεις ασφάλειας, προκειμένου να διασφαλιστεί η ασφάλεια του οργανισμού.

5.3 Επιπλέον απαραίτητη είναι η εφαρμογή ελέγχου ταυτότητας δύο παραγόντων καθώς και η χρήση ισχυρών κωδικών πρόσβασης για όλες τις συνδέσεις VPN που αποσκοπούν στην πρόσβαση του δικτύου του οργανισμού.

5.4 Ο εργαζόμενος θα πρέπει να ακολουθεί πιστά τις οδηγίες για ασφαλή διαμόρφωση του οικιακού του υπολογιστή και δικτυακού του εξοπλισμού που ορίζει ο φορέας του.

5.5 Ο εργαζόμενος θα πρέπει στο router του να χρησιμοποιεί κάποια πρότυπα για την κρυπτογράφηση της επικοινωνίας. Συγκεκριμένα, τα πρότυπα που πρέπει να χρησιμοποιεί είναι τα WPA2 και WPA3. Επιπλέον θα πρέπει να χρησιμοποιεί ισχυρούς κωδικούς για την πρόσβαση στο δίκτυο καθώς και στο διαχειριστικό περιβάλλον του router.

5.6 Ο εργαζόμενος θα πρέπει πάντα να χρησιμοποιεί ισχυρούς κωδικούς πρόσβασης. Συγκεκριμένα οι κωδικοί θα πρέπει να έχουν το ελάχιστον 12 χαρακτήρες εκ των οποίων, ο ένας να είναι κεφαλαίο γράμμα, ο ένας μικρό γράμμα, ο ένας να είναι αριθμός και ο ένας να είναι ειδικός χαρακτήρας. Απαγορεύεται ο κωδικός να περιέχει ονόματα και γνωστές λέξεις που μπορούν να εντοπιστούν στα λεξικά. Επιπλέον, θα πρέπει οι κωδικοί που χρησιμοποιεί

για την είσοδό του σε κάθε υπηρεσιακό ή προσωπικό λογαριασμό να είναι διαφορετικοί και να αλλάζονται σε σύντομα χρονικά διαστήματα. Θα ήταν συνετό να χρησιμοποιείται 2FA αυθεντικοποίηση όπου είναι δυνατόν. Στην περίπτωση χρήσης 2FA προτιμήστε να χρησιμοποιήσετε μια mobile εφαρμογή που δημιουργεί κωδικούς μιας χρήσης απευθείας στην συσκευή του χρήστη, από την αποστολή SMS.

5.7 Ο εργαζόμενος, όταν πραγματοποιεί τηλεδιάσκεψη, να χρησιμοποιεί την πιο πρόσφατη εγκεκριμένη έκδοση μιας εφαρμογής τηλεδιάσκεψης και να ορίζεται ρύθμιση αυτόματων ενημερώσεων της εγκατάστασης. Είναι σημαντικό να μην ορίζονται οι τηλεδιασκέψεις ως δημόσιες, εκτός αν υπάρχει σαφής λόγος για αυτό. Επιπλέον, χρησιμοποιείστε μιας χρήσης και ισχυρούς κωδικούς πρόσβασης για κάθε τηλεδιάσκεψη. Οι σύνδεσμοι των τηλεδιασκέψεων και οι κωδικοί πρόσβασης θα πρέπει να αποστέλλονται κατευθείαν στους αποδέκτες και να μην αναρτώνται σε δημόσιους ιστοτόπους.

5.8 Ο εργαζόμενος θα πρέπει να χρησιμοποιεί διαφορετικό λογαριασμό χρήστη με ελάχιστα προνόμια όταν εργάζεται από τον οικιακό του υπολογιστή. Είναι συνετό να χρησιμοποιεί administrator λογαριασμό μόνο όταν απαιτείται η συντήρηση του προσωπικού υπολογιστή ή η εγκατάσταση προγραμμάτων και ενημερώσεων.

5.9 Ο εργαζόμενος θα πρέπει να έχει πάντα ενημερωμένο λειτουργικό σύστημα και εφαρμογές στον οικιακό του υπολογιστή και να έχει ενεργοποιημένη την αυτόματη εγκατάσταση νέων ενημερώσεων.

5.10 Ο εργαζόμενος θα πρέπει να εγκαταστήσει στον οικιακό του υπολογιστή ένα λογισμικό antivirus το οποίο θα είναι πάντα ενημερωμένο στις τελευταίες εκδόσεις και με ενεργοποιημένη την αυτόματη εγκατάσταση νέων ενημερώσεων. Επιπροσθέτως, το λογισμικό πέραν τον standard υπηρεσιών που προσφέρει, θα πρέπει να παρέχει επιπλέον υπηρεσίες anti-phishing, anti-malware, ασφαλή πλοήγηση και δυνατότητες firewall.

5.11 Ο εργαζόμενος θα πρέπει να κρατά σε τακτά χρονικά διαστήματα λήψη αντιγράφων ασφαλείας σε ένα εξωτερικό μέσο αποθήκευσης για την αποφυγή μόλυνσης από ransomware. Το μέσο στο οποίο θα αποθηκεύονται τα αρχεία backup θα πρέπει να βρίσκεται αποσυνδεδεμένο από τον υπολογιστή όταν δεν χρησιμοποιείται.

5.12 Ο εργαζόμενος κατά την πλοήγησή του στο διαδίκτυο θα πρέπει να χρησιμοποιεί την τελευταία έκδοση web browser και να έχει ενεργοποιημένη την αυτόματη εγκατάσταση νέων ενημερώσεων. Επιπλέον, θα πρέπει να βρίσκονται απενεργοποιημένα browser plugins και extensions που δεν χρησιμοποιούνται. Πολύ σημαντικό επίσης είναι η μη αποθήκευση των κωδικών πρόσβασης στον browser. Ο εργαζόμενος θα πρέπει πάντα να ελέγχει τις ιστοσελίδες που επισκέπτεται και να αποφεύγει όσο τον δυνατόν περισσότερο τις ιστοσελίδες που είναι περισσότερο πιθανό να είναι μολυσμένες. Τέτοιες σελίδες μπορεί να είναι, ιστοσελίδες παράνομου κατεβάσματος μουσικής. Ιδιαίτερη προσοχή, όλες οι ιστοσελίδες με τις οποίες ο εργαζόμενες διαμοιράζεται ευαίσθητες πληροφορίες (π.χ. κωδικούς πρόσβασης) να χρησιμοποιούν το πρωτόκολλο https.

5.13 Σε περίπτωση που ο εργαζόμενος λάβει κάποιο ύποπτο email, απαγορεύεται το άνοιγμα του συνημμένου αρχείου καθώς και η επίσκεψη στον σύνδεσμο που μπορεί να περιέχει. Για την επιβεβαίωση της ταυτότητας του αποστολέα να επικοινωνεί μέσω τηλεφώνου μαζί του και σε περίπτωση που το email δεν έχει αποσταλεί από αυτόν να το διαγράφει άμεσα.

5.14 Ο εργαζόμενος καλό είναι να αποφεύγει την χρήση public Wi-Fi hot spots και κυρίως αν επιθυμεί να πραγματοποιήσει είσοδο σε ευαίσθητους λογαριασμούς. Να προτιμά τη δημιουργία δικού του hot spot μέσω του δικτύου κινητής τηλεφωνίας της συσκευής του και

χρησιμοποιώντας πάντα ισχυρούς κωδικούς. Αν όμως είναι αναπόφευκτη η χρήση κάποιου public Wi-Fi hot spot, να γίνεται χρήση υπηρεσίας VPN του φορέα.

6. Χρήση κρυπτογραφίας

Με την χρήση αλγορίθμων κρυπτογραφίας εξασφαλίζουμε ότι η πληροφορία που θα αποθηκεύσουμε ή θα μεταδώσουμε θα είναι πάντα η ίδια. Για να είναι ένας αλγόριθμος κρυπτογραφίας αποτελεσματικός θα πρέπει να διασφαλίζει τέσσερις βασικές αρχές:

1. Την εμπιστευτικότητα, την εξασφάλιση δηλαδή ότι τα δεδομένα μπορούν να αναγνωστούν μόνο από εξουσιοδοτημένα άτομα που έχουν στην κατοχή τους το κλειδί κρυπτογράφησης,
2. Την ακεραιότητα, την ικανότητα δηλαδή να εξασφαλίζουμε ότι το μήνυμα που παραλήφθηκε είναι ίδιο με το μήνυμα που στάλθηκε. Αυτό γίνεται με την χρήση hash αλγορίθμων
3. Την μη αποκήρυξη, την ικανότητα δηλαδή να διασφαλίσουμε ότι ο αποστολέας δεν μπορεί σε μεταγενέστερο χρόνο να ισχυριστεί ότι δεν ήταν αυτός ο ίδιος που έστειλε το μήνυμα. Παραδείγματος χάρη, ένας προϊστάμενος στον εργασιακό χώρο δίνει μια εντολή προς εκτέλεση σε κάποιον άλλον. Αργότερα, ο προϊστάμενος δεν μπορεί να αρνηθεί ότι έστειλε αυτή την εντολή. Και τέλος,
4. Την αυθεντικοποίηση, την δυνατότητα δηλαδή, ο χρήστης ή το σύστημα να αποδείξουν την ταυτότητά τους κάνοντας χρήση το ψηφιακό πιστοποιητικό.

Όταν μια εταιρεία επεξεργάζεται ευαίσθητα δεδομένα είναι ζωτικής σημασίας να χρησιμοποιεί αλγορίθμους κρυπτογράφησης για την προστασία των δεδομένων της. Για να διασφαλιστεί λοιπόν η τήρηση των παραπάνω αρχών, θα πρέπει να εφαρμοστούν κάποια μέτρα προστασίας. Αυτά τα μέτρα αναγράφονται στην συνέχεια.

Μέτρα Προστασίας:

6.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές για την χρήση της κρυπτογραφίας οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

6.2 Κάθε πληροφορία που έχει κατηγοριοποιηθεί ως ευαίσθητη, πρέπει να υπόκειται σε κρυπτογράφηση κατά την αποθήκευσή της και τη μεταφορά της.

6.3 Για την εξασφάλιση της ασφαλής κρυπτογράφησης, πρέπει να γίνεται χρήση μόνο των πιο πρόσφατων εκδόσεων των εγκεκριμένων κρυπτογραφικών πρωτοκόλλων και λογισμικού, ενώ παράλληλα θα πρέπει να γίνεται η επιλογή του κατάλληλου μήκους κλειδιού.

6.4 Στις περιπτώσεις που εφαρμόζεται ο αλγόριθμος RSA, τα κλειδιά πρέπει να έχουν ένα μήκος το λιγότερο 2048 bits.

6.5 Σε περίπτωση που είναι απαραίτητη η ασφάλεια των δεδομένων με συμμετρική κρυπτογράφηση, πρέπει να γίνεται με την χρήση του αλγόριθμο AES με ένα κλειδί μήκους 256 bit.

6.6 Για τη περίπτωση χρήσης κρυπτογραφικών hash αλγορίθμων, όπως στην ψηφιακή υπογραφή, συνιστάται η χρήση του Secure Hash Algorithm 2. Οι αλγόριθμοι SHA-1 και MD5 έχουν αποδειχθεί μη ασφαλείς, και επομένως τονίζεται η αποφυγή της χρήσης του.

6.7 Απαραίτητη είναι η υλοποίηση ενός ολοκληρωμένου συστήματος διαχείρισης για συμμετρικά και ασύμμετρα κλειδιά κρυπτογράφησης. Το σύστημα θα πρέπει να ακολουθεί διεθνή πρότυπα και διαδικασίες για τη δημιουργία, την αποθήκευση, τον έλεγχο και την διανομή κλειδιών κρυπτογράφησης. Επιπλέον, θα πρέπει να εφαρμόζονται αυστηροί κανόνες πρόσβασης στην πλατφόρμα διαχείρισης για τη διασφάλιση της ασφάλειας του συστήματος.

6.8 Για την εξασφάλιση της ασφάλειας στις συνδέσεις SSH, προτείνεται η χρήση αυθεντικοποίησης με βάση το δημόσιο κλειδί.

7. Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας

Η εκπαίδευση και η ευαισθητοποίηση των εργαζομένων στα θέματα κυβερνοασφάλειας είναι ένας πολύ σημαντικός παράγοντας για την αποτροπή μιας κυβερνοεπίθεσης. Όσο πιο εκπαιδευμένο είναι το προσωπικό, τόσο μικρότερες οι πιθανότητες να δεχτεί επίθεση η εταιρεία εκ των έσω καθώς αυξάνονται και οι πιθανότητες για μια πιο γρήγορη αντιμετώπιση του προβλήματος.

Εξαιτίας της πανδημία του covid-19 και της αύξηση της τηλεργασίας, αυξάνονται παράλληλα και οι πιθανότητες να δεχτεί μια εταιρεία επίθεση λόγο του περιορισμένου ελέγχου των εργαζομένων και των κινήσεων που πραγματοποιούν από το δίκτυο και το σύστημα τους. Σήμερα, είναι ακόμη πιο σημαντικό από ποτέ να εκπαιδεύονται οι εργαζόμενοι σχετικά με την ψηφιακή ασφάλεια, ώστε να είναι σε θέση να αναγνωρίζουν τους κινδύνους και να αντιμετωπίζουν αποτελεσματικά τις κυβερνοαπειλές. Επιπλέον, εκτός από τις επαναληπτικές εκπαιδεύσεις που πρέπει να οργανώνονται για όλο το προσωπικό, μεγαλύτερη βαρύτητα θα πρέπει να δίνουν οι αρμόδιοι στα νέα μέλη της εταιρείας και να αφιερώνουν μεγάλο μέρος από τις προκαθορισμένες ώρες εκπαίδευσης συγκεκριμένα σε αυτούς. Τα παρακάτω είναι μερικά από το βήματα που πρέπει να ακολουθούν οι εταιρείες για την σωστή εκπαίδευση του προσωπικού.

Μέτρα Προστασίας:

7.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές για την εκπαίδευση των χρηστών στα θέματα της κυβερνοασφάλειας οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

7.2 Απαραίτητος είναι ο σχεδιασμός ενός εκπαιδευτικού προγράμματος για την ευαισθητοποίηση και την επίγνωση του προσωπικού σχετικά με θέματα κυβερνοασφάλειας, το οποίο θα περιλαμβάνει όλους τους εργαζομένους και θα διενεργείται το λιγότερο δύο φορές το χρόνο. Το πρόγραμμα θα πρέπει να καλύπτει τα εξής θέματα:

- Τον ασφαλή τρόπο για την αλληλεπίδραση του χρήστη με τις συσκευές και το δίκτυο,
- Την αναγκαιότητα για την δημιουργία ισχυρών κωδικών πρόσβασης και 2FA αυθεντικοποίηση,
- Τον τρόπο με τον οποίο θα γίνεται η ανίχνευση των διαφόρων μορφών επιθέσεων, όπως είναι για παράδειγμα το phishing και οι τηλεφωνικές κλήσεις πλαστοπροσωπίας, και τέλος
- Τον τρόπο για την σωστή και άμεση αναγνώριση των ενδείξεων παραβίασης των συστημάτων καθώς και των περιστατικών εκ των έσω απειλών.

7.3 Επιπλέον απαραίτητος είναι η διοργάνωση, σε σύντομα χρονικά διαστήματα, ξεχωριστά εκπαιδευτικά σεμινάρια ευαισθητοποίησης των εργαζομένων με βάση τους ρόλους τους στην εταιρεία και ειδικότερα με βάση το επίπεδο τεχνικής εξειδίκευσης που κατέχουν.

7.4 Συνιστάται ο προγραμματισμός μιας αξιολόγησης των γνωστικών κενών του προσωπικού, με στόχο τη δημιουργία ενός σχεδίου που θα περιλαμβάνει μια σειρά συνεχόμενων εκπαιδευτικών δραστηριοτήτων.

7.5 Τέλος απαραίτητη είναι η πραγματοποίηση πρακτικών ασκήσεων προσομοίωσης για περιστατικά κυβερνοασφάλειας, με στόχο την ανάλυση των επιπτώσεων που μπορεί να έχουν τέτοιες επιθέσεις. Για παράδειγμα, η δοκιμή ανοίγματος ενός κακόβουλου αρχείου που είναι συνημμένο σε ένα email ή επίσκεψη μιας κακόβουλης ιστοσελίδα.

8. Φυσική Προστασία

Όταν αναφερόμαστε στον όρο φυσική προστασία, αναφερόμαστε στην φυσική πρόσβαση, τις παρεμβολές και την καταστροφή των εγκαταστάσεων του πληροφοριακού συστήματος από μη εξουσιοδοτημένα άτομα. Επιπλέον, αναφερόμαστε και σε καταστροφές που μπορεί να δεχτούν οι εγκαταστάσεις από περιβαλλοντικές συνθήκες (π.χ. λόγο σεισμού).

Η ανεπιθύμητη πρόσβαση από μη εξουσιοδοτημένα άτομα πρέπει να αντιμετωπίζεται με σοβαρότητα, καθώς μπορεί να οδηγήσει σε κλοπή συσκευών με πολύτιμα δεδομένα, σε μόλυνση συστημάτων με ειδικά διαμορφωμένα USB ή ακόμη και φυσικό βανδαλισμό του εξοπλισμού. Επιπροσθέτως, περιβαλλοντικά συμβάντα, όπως φωτιά, σεισμός, πλημμύρα κ.λπ., μπορούν να προκαλέσουν σοβαρές ζημιές στον Οργανισμό. Για όλους τους παραπάνω λόγους, η προστασία των εγκαταστάσεων του οργανισμού πρέπει να λαμβάνονται ιδιαιτέρως υπόψη. Τα παρακάτω βοηθούν να διασφαλιστεί η ασφάλεια των εγκαταστάσεων.

Μέτρα Προστασίας:

8.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές για την φυσική και την περιβαλλοντική ασφάλεια οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

8.2 Απαραίτητη είναι η ύπαρξη μηχανισμών ελέγχου στην εξωτερική περίμετρο των κτηριακών εγκαταστάσεων που φιλοξενούν τους διακομιστές του οργανισμού προκειμένου να αποτραπεί η μη εξουσιοδοτημένη φυσική πρόσβαση. Αυτοί οι μηχανισμοί μπορεί να περιλαμβάνουν μπάρες, κλειδαριές ή συστήματα συναγερμού.

8.3 Απαιτείται να διασφαλιστεί η παρουσία ενός κατάλληλα εκπαιδευμένου προσωπικού στον χώρο υποδοχής των κτηριακών εγκαταστάσεων που φιλοξενούν τους διακομιστές του οργανισμού, ο οποίος θα έχει την ευθύνη να καταγράφει τα στοιχεία των επισκεπτών κατά την είσοδό τους στο κτήριο.

8.4 Απαιτείται η δημιουργία ενός αρχείου με τα εξουσιοδοτημένα άτομα που έχουν πρόσβαση στο χώρο του server, με βάση τη θέση ή τον ρόλο τους. Η είσοδος στον χώρο που υπάρχει ο server θα επιτρέπεται μόνο στα άτομα που έχουν εξουσιοδότηση και διαθέτουν έξυπνη κάρτα.

8.5 Για την εξασφάλιση της ασφάλεια και της αδιάλειπτη λειτουργία του χώρου που φιλοξενεί τον server, θα πρέπει να τοποθετηθούν τουλάχιστον οι εξής παρακάτω μηχανισμοί:

- Σύστημα συναγερμού,
- Παραπάνω συστήματα και κυκλώματα δικτύωσης από αυτά που χρειάζονται για την ομαλή λειτουργία του συστήματος,
- Χρήση UPS για την αδιάλειπτη παροχή του ρεύματος και για τον ελεγχόμενο κλείσιμο των μηχανημάτων και των συσκευών,
- Συστήματα πυρανίχνευσης και πυρόσβεσης
- Αυτοματοποιημένους ελεγκτές για τον έλεγχο της θερμοκρασίας, της υγρασίας και της πίεσης και
- Συστήματα προστασίας από τυχόν διαρροή νερού.

8.6 Για την σωστή και συνεχόμενη παρακολούθηση του εξωτερικού και του εσωτερικού δωματίου του server, απαιτείται η εγκατάσταση ενός κλειστού κύκλωμα τηλεόρασης (CCTV).

9. Λήψη αντιγράφων ασφαλείας

Σύμφωνα με τους Politou, Michota, Alepis, Pocs (2018), Η λήψη αντιγράφων ασφαλείας είναι η διαδικασία αντιγραφής των πληροφοριών που υπάρχουν σε ένα υπολογιστικό σύστημα και αποθηκεύονται ξεχωριστά από τον ίδιο τον υπολογιστή

Η λήψη αντιγράφων ασφαλείας, ίσως και να ανήκει στα τελευταία βήματα αντιμετώπισης έναντι των κυβερνοεπιθέσεων, αλλά είναι πολύ σημαντικό για την διασφάλιση της συνέχειας της ομαλής λειτουργίας του οργανισμού. Ο στόχος της ύπαρξης των αντιγράφων ασφαλείας δεν είναι απλά για την διατήρηση των δεδομένων, αλλά είναι το μέσω για την άμεση ανάρρωση του οργανισμού σε περίπτωση επίθεσης ή καταστροφής των δεδομένων. Ανάλογα της σπουδαιότητας των δεδομένων που διαχειρίζεται η εταιρείας, πρέπει να υπάρχουν και αντίστοιχα μέτρα για τη συχνότητα λήψης των backups.

Η πιο γνωστή μέθοδος διατήρησης των backups είναι η λεγόμενη “3-2-1”. Ο κανόνας αυτός αναφέρει τα εξής:

- Το 3 συμβολίζει το ότι πρέπει να διατηρούμε 3 αντίγραφα όλων των σημαντικών αρχείων από τα οποία το 1 θα είναι το βασικό αρχείο ενώ τα άλλα δύο θα είναι αντίγραφα.
- Το 2 συμβολίζει το ότι πρέπει να διατηρούμε τα βασικά αρχεία και τα αντίγραφα αρχεία σε 2 διαφορετικές συσκευές αποθήκευσης και
- Το 1 συμβολίζει ότι πρέπει τουλάχιστον 1 αντίγραφο ασφαλείας να αποθηκεύεται σε έναν χώρο ξεχωριστό από το δίκτυο και τον χώρο του οργανισμού.

Σημαντική σημείωση είναι ότι σε περίπτωση που η εταιρεία χάσει τα κρίσιμα δεδομένα της ή στην περίπτωση που αυτά αλλοιωθούν, θα υπάρξουν επιπτώσεις στην επιχειρησιακή συνέχεια της εταιρείας. Για τον λόγο αυτό είναι ζωτικής σημασίας η εφαρμογή των παρακάτω μέτρων.

Μέτρα προστασίας:

9.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές αντιγράφων ασφαλείας οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και

τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

9.2 Απαιτείται η τακτική δημιουργία αντιγράφων ασφαλείας από όλα τα σημαντικά συστήματα πληροφορικής του Οργανισμού, σε καθημερινή βάση και με χρήση των κατάλληλων τεχνολογιών.

9.3 Για την διασφάλιση την προστασία των αντιγράφων ασφαλείας, απαιτείται η εφαρμογή κρυπτογράφησης κατά την αποθήκευση και την μεταφορά τους. Αυτό ισχύει τόσο για τα τοπικά όσο και για τα απομακρυσμένα αντίγραφα ασφαλείας, καθώς και για τις αντίστοιχες υπηρεσίες cloud.

9.4 Απαραίτητος είναι ο έλεγχος ότι όλα τα αντίγραφα ασφαλείας αποθηκεύονται το λιγότερο σε έναν μη συνδεδεμένο σε δίκτυο προορισμό.

9.5 Επιπλέον απαραίτητη είναι ο έλεγχος ανά τακτά χρονικά διαστήματα για την επαλήθευση της ακεραιότητας των αντιγράφων ασφαλείας.

9.6 Σημαντική είναι η πραγματοποίηση μιας δοκιμής επαναφοράς των δεδομένων τουλάχιστον μια φορά τον χρόνο, προκειμένου να διασφαλιστεί ότι η διαδικασία λήψης αντιγράφων λειτουργεί ορθά.

9.7 Τέλος απαιτείται η αποθήκευση των αντιγράφων ασφαλείας σε διαφορετικές γεωγραφικές τοποθεσίες.

10. Προστασία από κακόβουλο λογισμικό

Όπως έχουμε ήδη αναφέρει σε προηγούμενο κεφάλαιο κακόβουλο λογισμικό είναι ένα λογισμικό με το οποίο ο επιτιθέμενος προσπαθεί να εκτελέσει κακόβουλες ενέργειες σε ένα λογισμικό σύστημα φερόμενος ως ένας εξουσιοδοτημένος χρήστης. Τέτοιες ενέργειες μπορεί να είναι η κλοπή ευαίσθητων δεδομένων ή και η αλλοίωση αυτών των δεδομένων. Για τον λόγο αυτό όλες οι εταιρείες διαχείρισης ERP συστημάτων, από την στιγμή που έχουν την κατοχή τους ευαίσθητες πληροφορίες των πελατών τους, των προμηθευτών τους, δικές τους αλλά και γενικά όλων των ανθρώπων που συναναστρέφονται με την εταιρεία, είναι υποχρεωμένοι να τηρούν μερικά μέτρα προστασίας για την αποφυγή μόλυνσης του συστήματος τους από κακόβουλα λογισμικά.

Ένα κακόβουλο λογισμικό όπως έχουμε ήδη προαναφέρει, μπορεί να εισχωρήσει στο σύστημα που στοχεύει να μολύνει με πολλούς τρόπους. Μερικοί από αυτούς είναι οι εξής:

- Μέσω email, επισυνάπτοντας μολυσμένα αρχεία ή παρακινώντας τον χρήση να επισκεφθεί κάποια μολυσμένη σελίδα στο διαδίκτυο καθώς και
- Μέσω συσκευών αποθήκευσης, δηλαδή εκχωρώντας στο σύστημα κάποιο USB στικάκι ή κάποιον εξωτερικό σκληρό δίσκο τα οποία φιλοξενούν το κακόβουλο λογισμικό.

Στόχος της προστασίας του συστήματος από κακόβουλα λογισμικά είναι η διασφάλιση της ακεραιότητας του λογισμικού και των πληροφοριών. Για τους παραπάνω λόγους οι μηχανισμοί προστασίας από κακόβουλο λογισμικό, θα πρέπει να εφαρμοστούν στο σύστημα σε όλα τα σημεία εισόδου και εξόδου.

Μέτρα Προστασίας:

10.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές προστασίας από κακόβουλο λογισμικό οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

10.2 Απαιτείται η ανάπτυξη ενός λογισμικού που θα προστατεύει τους σταθμούς εργασίας και τους servers από κακόβουλα προγράμματα. Η λειτουργία του θα είναι αυτοματοποιημένη μέσω ενός κεντρικού συστήματος διαχείρισης. Το λογισμικό θα εκτελεί ανελλιπώς λειτουργίες προστασίας, ενώ η βάση δεδομένων των υπογραφών του θα ενημερώνεται σε τακτά χρονικά διαστήματα.

10.3 Σημαντική είναι η ενεργοποίηση της ρύθμιση για τη σάρωση κακόβουλου λογισμικού στα φορητά μέσα αποθήκευσης (όπως είναι το USB, οι εξωτερικούς σκληρούς δίσκους, τα CD, τα DVD) έτσι ώστε να εκτελείται αυτόματα κάθε φορά που συνδέονται σε συσκευές.

10.4 Επιπλέον είναι σημαντικός ο έλεγχος ότι οι εκδόσεις των προγραμμάτων περιήγησης στο διαδίκτυο και των email client που είναι εγκατεστημένες στα συστήματα του οργανισμού είναι οι πιο πρόσφατες, ενημερώνονται αυτόματα και λαμβάνουν πλήρη υποστήριξη.

10.5 Απαιτείται η απενεργοποίηση ή απεγκατάσταση οποιοδήποτε πρόσθετο ή πρόσθετο πρόγραμμα σε web browsers και e-mail clients που δεν έχει εγκριθεί.

10.6 Συστήνεται η χρήση της υπηρεσίας φιλτραρίσματος DNS για να αποτρέπεται η πρόσβαση σε γνωστά επικίνδυνα domain.

10.7 Για περιορισμό της πρόσβασης σε ιστοσελίδες που δεν έχουν εγκριθεί από την πολιτική ασφάλειας του Οργανισμού, επιβάλλεται η χρήση φίλτρων URL σε επίπεδο δικτύου.

10.8 Προκειμένου να γίνει ο απαραίτητος έλεγχος για τα κακόβουλα e-mails που εισέρχονται στο σύστημα, συνιστάται η εφαρμογή της διαδικασία φιλτραρίσματος περιεχομένου.

10.9 Συστήνεται η εγκατάσταση συστημάτων ανίχνευσης και πρόληψης εισβολών σε όλους τους κρίσιμους servers.

10.10 Συστήνεται η εγκατάσταση συστημάτων ανίχνευσης και πρόληψης εισβολών σε όλους τους σταθμούς εργασίας.

11. Ασφάλεια διαδικτυακών εφαρμογών

Πολλές φορές για να ταιριάζει πλήρως στις ανάγκες του πελάτη ένα ERP σύστημα χρειάζεται να δεχτεί κάποιες παραμετροποιήσεις. Μια από αυτές είναι η γεφύρωση του ERP με κάποια ιστοσελίδα e-shop που μπορεί να έχει ο πελάτης με στόχο την αποστολή των παραγγελιών που δέχεται στο e-shop απευθείας στο ERP για την έκδοση του παραστατικού ή και για την ενημέρωση του αποθέματος στην αποθήκη. Για τον λόγο αυτό είναι σημαντικό όλες οι εταιρείες οι οποίες γεφυρώνουν το ERP λογισμικό τους με κάποια διαδικτυακή εφαρμογή, να διασφαλίζουν την ύπαρξη της ασφάλεια και στις εφαρμογές αυτές. Η ασφάλεια θα πρέπει να εφαρμόζεται σε όλη τη διάρκεια του κύκλου ζωής της διαδικτυακής εφαρμογής. Με άλλα λόγια θα πρέπει να υπάρχει και κατά τον σχεδιασμό και κατά την ανάπτυξη και στις δοκιμές αλλά και κατά την παραγωγική λειτουργία και συντήρηση.

Για να διασφαλίσουμε λοιπόν ότι τηρείται η ασφάλεια σε όλα τα στάδια ανάπτυξης, λειτουργίας και συντήρησης των διαδικτυακών εφαρμογών, θα πρέπει να εφαρμοστούν τα εξής παρακάτω βήματα.

Μέτρα Προστασίας:

11.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές ασφαλείας των διαδικτυακών εφαρμογών οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

11.2 Αναλύοντας τη σημασία της εφαρμογής και των δεδομένων που επεξεργάζεται, απαραίτητη είναι παράθεση των απαιτήσεων ασφαλείας που είναι αναγκαίες για την κάλυψη του βαθμού κρισιμότητας των λειτουργιών της και της ευαισθησίας των δεδομένων που επεξεργάζεται.

11.3 Με σκοπό την ανάπτυξη εφαρμογών με ασφάλεια, θα πρέπει να χρησιμοποιούνται πλατφόρμες ανάπτυξης εφαρμογών που είναι ενημερωμένες και έχουν αποδεδειγμένη αξιοπιστία. Επίσης, συνιστάται η επιλογή των βιβλιοθηκών των λογισμικών που προέρχονται από έμπιστες πηγές και συντηρούνται συστηματικά.

11.4 Για την εξασφάλιση ότι τα δεδομένα εισόδου επικυρώνονται συντακτικά και σημασιολογικά συνιστάται η χρήση του «λευκού καταλόγου» στην πλευρά του server. Αυτό σημαίνει ότι θα πρέπει να δημιουργηθεί μια λίστα με τα επιτρεπόμενα δεδομένα εισόδου για κάθε πεδίο εισόδου και να επιτρέπετε η είσοδο μόνο στα δεδομένα που ανήκουν στη λίστα αυτή.

11.5 Επίσης για την εξασφάλιση ότι τα δεδομένα εισόδου στο διερμηνευτή της εφαρμογής είναι ασφαλή, πρέπει να γίνει εφαρμογή τεχνικών κωδικοποίησης των χαρακτήρων, ακριβώς πριν από την εισαγωγή των δεδομένων στον διερμηνευτή της εφαρμογής.

11.6 Απαιτείται η χρήση τεχνικών παραμετροποίησης ερωτημάτων σε κάθε στοιχείο που εισέρχεται στο σύστημα διαχείρισης βάσεων δεδομένων της εφαρμογής, προκειμένου να διασφαλιστεί η ασφαλής και αποτελεσματική λειτουργία του.

11.7 Απαραίτητη είναι η διαμόρφωση των κεφαλίδων απάντησης του HTTP πρωτοκόλλου έτσι ώστε να εφαρμόζονται τα παρακάτω μέτρα ασφαλείας: Content-Security-Policy, HSTS και X-Frame-Options.

11.8 Για την διασφάλιση της ασφάλεια της διαδικτυακής εφαρμογής, θα πρέπει να ληφθούν υπόψη οι παρακάτω τεχνικές για την αυθεντικοποίηση και την διαχείριση συνόδου των χρηστών:

- Απαραίτητη είναι η δημιουργία ισχυρών κωδικών πρόσβασης,
- Η εφαρμογή της αυθεντικοποίησης δύο παραγόντων, σύμφωνα με τις απαιτήσεις ασφαλείας της εφαρμογής,
- Επιπλέον απαραίτητη είναι αποθήκευση των κωδικών πρόσβασης σε κρυπτογραφημένη μορφή, χρησιμοποιώντας μία εγκεκριμένη one-way hash function και προσθέτοντας μια ακολουθία τυχαίων δεδομένων με μήκος το λιγότερο 32 bits,
- Η δημιουργία ενός νέου token συνόδου με τη χρήση εγκεκριμένων κρυπτογραφικών αλγορίθμων κατά την αυθεντικοποίηση του χρήστη,
- Η ακύρωση του token συνόδου κατά την αποσύνδεση του χρήστη ή τη λήξη της συνεδρίας.
- Τέλος απαραίτητη είναι η χρήση των ιδιοτήτων "Secure", "HttpOnly" και "SameSite" για τα tokens συνόδου που βασίζονται σε cookies.

11.9 Απαιτείται η υλοποίηση ενός συστήματος ελέγχου πρόσβασης για τις λειτουργίες, τα αρχεία δεδομένων, τους συνδέσμους URL, τις υπηρεσίες και άλλους πόρους, λαμβάνοντας υπόψη την αρχή των ελάχιστων προνομίων. Αυτό θα επιτρέψει στους χρήστες και τις διεργασίες να έχουν πρόσβαση μόνο στους πόρους που χρειάζονται για την εκτέλεση των εργασιών τους,

περιορίζοντας έτσι την πιθανότητα καταχρηστικής χρήσης ή παραβίασης των δικαιωμάτων πρόσβασης.

11.10 Για την εξασφάλιση της ασφάλειας του web server, απαιτείται ο έλεγχος ότι κάθε επικοινωνία που πραγματοποιείται μέσω αυτού, όπως κλήσεις προς άλλες web υπηρεσίες, αναζητήσεις στη βάση δεδομένων, αποθήκευση δεδομένων στο cloud κ.λπ. πραγματοποιείται με κρυπτογράφηση της σύνδεσης χρησιμοποιώντας την πιο πρόσφατη έκδοση του πρωτοκόλλου TLS.

11.11 Απαιτείται η υλοποίηση τεχνικών καταγραφής συμβάντων (*event logs*) στην διαδικτυακή εφαρμογή, οι οποίες θα παρέχουν στοιχεία για μελλοντική αναφορά και λεπτομερή έρευνα σε περίπτωση επιθέσεων κυβερνοασφάλειας ή άλλων παρόμοιων περιστατικών.

11.12 Επιπλέον σημαντική είναι η διασφάλιση ότι εφαρμόζονται τεχνικές για τη διαχείριση σφαλμάτων και εξαιρέσεων σε περίπτωση που συμβεί κάποιο απρόσμενο γεγονός ή κάποιο συμβάν ασφαλείας.

11.13 Ο έλεγχος ευπαθειών για κάθε νέα λειτουργία που προστίθεται στην εφαρμογή κατά τα στάδια της ανάπτυξη της είναι απαραίτητος.

11.14 Πριν η εφαρμογή τεθεί σε παραγωγική λειτουργία, πρέπει να πραγματοποιηθεί μια δοκιμή παρείσδυσης ή αλλιώς penetration test για να ελεγχθεί η ασφάλεια της.

11.15 Συνιστάται η υλοποίηση ενός firewall σε επίπεδο εφαρμογής, γνωστό και ως web application firewall, είτε στην υποδομή είτε ως υπηρεσία ασφαλείας στο cloud, γνωστή και ως security as a service. Αυτό το firewall θα ελέγχει την HTTP κίνηση που κατευθύνεται προς τη web εφαρμογή, ανιχνεύοντας και αποκλείοντας γνωστούς τύπους επιθέσεων.

11.16 Τέλος είναι σημαντικό τα ευαίσθητα δεδομένα που αποθηκεύονται στην εφαρμογή να έχουν κρυπτογραφηθεί κατάλληλα κατά την αποθήκευσή τους.

12. Ασφαλής διαμόρφωσης του εξοπλισμού και των εφαρμογών

Το μεγαλύτερο ποσοστό των υλικών και των λογισμικών αγοράζονται έχοντας εγκατεστημένα και ρυθμισμένα τις προκαθορισμένες ρυθμίσεις οι οποίες δεν θα μπορούσε κανείς να πει ότι είναι ασφαλής από κυβερνοεπιθέσεις. Για παράδειγμα ένα πολύ συνηθισμένο φαινόμενο μη ασφαλών ρυθμίσεων είναι όταν τα στοιχεία πρόσβασης σε νέα λογισμικά είναι το admin / admin. Οι επιτιθέμενοι γνωρίζουν πολύ καλά αυτό το ελάττωμα που έχουν τα νέα υλικά και λογισμικά όταν παραδίδονται στον αγοραστή και γι΄αυτόν τον λόγο αυτή η περίπτωση είναι μια αρκετά συχνή αιτία κυβερνοεπίθεσης.

Για την αποφυγή να δεχτεί το σύστημα κυβερνοεπίθεση από τον παραπάνω λόγο, είναι σημαντικό οι εταιρείες κατά την αγορά και εγκατάσταση νέων εφαρμογών και λογισμικών να αλλάζουν αυτές τις ρυθμίσεις πριν την έναρξη της λειτουργίας τους. Παρακάτω αναφέρονται κάποια βασικά βήματα για την διασφάλιση της σωστής διαμόρφωσης του εξοπλισμού και των εφαρμογών της εταιρείας.

Μέτρα Προστασίας:

12.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές ασφαλείας για την ασφαλή διαμόρφωση του εξοπλισμού πληροφορικής και των εφαρμογών οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

12.2 Απαγορευτική είναι η χρήση εξοπλισμού, λειτουργικών συστημάτων και εφαρμογών για τα οποία ο κατασκευαστής ή ο πάροχος έχει σταματήσει να παρέχει υποστήριξη.

12.3 Απαραίτητος είναι ο έλεγχος ότι πραγματοποιήθηκε αλλαγή των προκαθορισμένων κωδικών πρόσβασης σε κάθε νέο προϊόν κατά την πρώτη φορά που εγκαθιστάτε, προκειμένου να εξασφαλισθεί η ασφάλεια του προϊόντος.

12.4 Είναι απαραίτητη η εφαρμογή των βασικών ρυθμίσεων ασφάλειας που συμμορφώνονται με τα διεθνή πρότυπα και τις οδηγίες για τα λειτουργικά συστήματα των υπολογιστών, τους server και τις δικτυακές συσκευές, λαμβάνοντας υπόψη την πολιτική ασφάλειας του οργανισμού. Επιπλέον, θα πρέπει να πραγματοποιηθεί αποθήκευση αυτών των ρυθμίσεων σε ένα αρχείο για μελλοντική αναφορά και αξιολόγηση.

12.5 Η χρήση μόνο υποστηριζόμενων εκδόσεων των λειτουργικών συστημάτων στους υπολογιστές εργασίας, στους διακομιστές και στις δικτυακές συσκευές είναι απαραίτητη. Να σημειωθεί, ότι σημαντικό είναι να πραγματοποιηθούν οι απαραίτητες ρυθμίσεις των τριών παραπάνω, με στόχο να λαμβάνουν αυτόματα ενημερώσεις.

12.6 Συνιστάται η χρήση μόνο των πιο πρόσφατων και ενημερωμένων εκδόσεων για σημαντικές επιχειρησιακές εφαρμογές, όπως κάποιο λογισμικό γραφείου, οι αναγνώστες pdf, οι περιηγητές ιστού και τα πρόσθετα του περιηγητή, καθώς επίσης και για email client.

12.7 Συνιστάται η χρήση μόνο των πιο πρόσφατων και ενημερωμένων εκδόσεων για κάθε εφαρμογή διακομιστή της εταιρείας που είναι προσβάσιμη από το Διαδίκτυο.

12.8 Συνιστάται η χρήση εργαλείων που μπορούν να αυτοματοποιήσουν την εγκατάσταση των ενημερώσεων και των επιδιορθώσεων στα λειτουργικά συστήματα και στις εφαρμογές που χρησιμοποιεί ο Οργανισμός.

12.9 Απαιτείται η δημιουργία ενός firewall σε κάθε υπολογιστή εργασίας και στον server, ο οποίος θα λειτουργεί σε επίπεδο οικοδεσπότη και θα περιορίζει τις δικτυακές συνδέσεις που εισέρχονται και εξέρχονται από τη συσκευή, εκτός από τις θύρες και υπηρεσίες που απαιτούνται για την κάλυψη των επιχειρησιακών αναγκών, όπως αυτές ορίζονται.

12.10 Για αυξημένη ασφάλεια των δικτυακών συσκευών, συνιστάται η εκτέλεση των εξής ρυθμίσεων: Απενεργοποίηση όλων των περιττών υπηρεσιών στις δικτυακές συσκευές και ενεργοποίηση της λειτουργία "port security" στα switches. Επιπλέον, απαιτείται η απενεργοποίηση των αχρησιμοποίητων interfaces και πρωτόκολλα δρομολόγησης στους routers και τις θύρες στους switches. Τέλος, για την εξασφάλιση της πρόσβασης στο διαχειριστικό περιβάλλον όλων των κρίσιμων δικτυακών συσκευών, συνιστάται η χρήση της αυθεντικοποίηση δύο παραγόντων.

12.11 Προτείνεται η απενεργοποίηση των λογαριασμών που δεν έχουν καμία σχέση πλέον με κάποιον χρήστη ή δεν υπάρχει πλέον η ανάγκη τους για την ομαλή λειτουργία των υπηρεσιακών αναγκών.

12.12 Απαιτείται η χρήση εργαλείων που αυτοματοποιούν την εγκατάσταση και ενημέρωση των ρυθμίσεων ασφαλείας σε συγκεκριμένα χρονικά διαστήματα.

12.13 Επιπλέον απαιτείται η απαγόρευση της σύνδεσης φορητών μέσων αποθήκευσης (όπως USB) στα κρίσιμα συστήματα, εκτός αν υπάρχει σαφής επιχειρησιακή ανάγκη.

12.14 Για την διασφάλιση της ασφάλειας των λογαριασμών υπηρεσιών, προτείνεται η χρήση αυτοματοποιημένων μεθόδων διαχείρισης. Αυτό μπορεί να επιτευχθεί με τις ακόλουθες πρακτικές:

- Εκχώρηση μόνο των απαραίτητων δικαιωμάτων πρόσβασης στους λογαριασμούς υπηρεσιών.
- Αλλαγή των κωδικών σε τακτά χρονικά διαστήματα.
- Απενεργοποίηση των λογαριασμών υπηρεσιών που δεν υπάρχει πλέον η ανάγκη τους για την ομαλή λειτουργία των υπηρεσιακών αναγκών.

12.15 Προτείνεται η δημιουργία πλήρη αντιγράφων ασφαλείας για τα λειτουργικά συστήματα της εταιρείας σε μορφή που έχει κρυπτογραφηθεί, περιορίζοντας την πρόσβαση και διασφαλίζοντας την ακεραιότητα των αρχείων.

13. Τήρηση και ανάλυση αρχείων καταγραφής συμβάντων

Η τήρηση και η ανάλυση των αρχείων καταγραφής συμβάντων είναι ένας τρόπος για τον άμεσο εντοπισμό και αντιμετώπιση τυχόν κακόβουλης ενέργειας του συστήματος. Τα αρχεία καταγραφής θεωρούνται η πιο έμπιστη πηγή πληροφοριών, στόχος της οποίας είναι η περιγραφή της ροής των διαδικασιών που πραγματοποιήθηκαν σε μια εταιρεία.

Η διατήρηση αρχείων καταγραφής αποτελεί αναγκαία πρακτική για κάθε εταιρεία που χρησιμοποιεί ERP λογισμικό. Ωστόσο, η σωστή διαχείριση και ανάγνωση αυτών των αρχείων είναι ακόμη πιο σημαντική από την απλή διατήρησή τους. Η μη σωστή εξαγωγή των αρχείων καταγραφής μπορεί να οδηγήσει σε αργό εντοπισμό ύποπτων συμβάντων, τα οποία μπορούν να αποτελέσουν απειλή στην ασφάλεια της εταιρείας. Για τον λόγο αυτό, είναι απαραίτητο να ληφθούν τα κατάλληλα μέτρα προστασίας προκειμένου να διασφαλιστεί η σωστή διεξαγωγή των αρχείων καταγραφής. Τα μέτρα αυτά αναγράφονται παρακάτω.

Μέτρα Προστασίας

13.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές καταγραφής και παρακολούθησης συμβάντων οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

13.2 Απαραίτητος είναι ο έλεγχος ότι η καταγραφή συμβάντων είναι ενεργοποιημένη σε όλους τους υπολογιστές εργασίας, τους διακομιστές και τις δικτυακές συσκευές.

13.3 Απαιτείται η εξασφάλιση του συγχρονισμού μεταξύ των ρολογιών όλων των συσκευών, προκειμένου να επιτευχθεί ακρίβεια στο ταίριασμα των συμβάντων μεταξύ διαφορετικών συστημάτων.

13.4 Για την εξασφάλιση ότι καταγράφονται τα σημαντικότερα συμβάντα, θα πρέπει να γίνει εφαρμογή των παρακάτω πρακτικών ασφαλείας:

- Καταγραφή των εισόδων και εξόδων για όλα τα συστήματα που απαιτούν αυθεντικοποίηση, συμπεριλαμβανομένων των επιτυχημένων και ανεπιτυχών προσπαθειών.

- Καταγραφή της πρόσβασης σε αρχεία και διεργασίες διακομιστών (*servers*) για την παρακολούθηση της χρήσης τους και τον εντοπισμό τυχόν κακόβουλων δραστηριοτήτων.
- Καταγραφή των αποτυχημένων προσπαθειών εκτέλεσης αρχείων για να προλαμβάνονται επιθέσεις μέσω κακόβουλου κώδικα.
- Καταγραφή της χρήσης και απόπειρας χρήσης ειδικών προνομίων για να εντοπίζονται απόπειρες εξουσιοδότησης ή παράνομης πρόσβασης.
- Καταγραφή της χρήσης των εφαρμογών συστήματος για να παρακολουθείτε η χρήση τους και να εντοπίζονται απόπειρες παράνομης πρόσβασης ή χρήσης.
- Καταγραφή όλων των αλλαγών που πραγματοποιούνται σε λογαριασμούς ή στις πολιτικές ασφαλείας.
- Καταγραφή όλων των αιτημάτων HTTP ή DNS που γίνονται.
- Καταγραφή όλων των μεταφορών δεδομένων που γίνονται από ή προς τα φορητά μέσα αποθήκευσης.

13.5 Απαραίτητη είναι η ρύθμιση των αρχείων καταγραφής έτσι ώστε να περιλαμβάνουν λεπτομερείς πληροφορίες για τα metadata όπως είναι οι παρακάτω,

- Ημερομηνία
- Χρήστης
- Χρονοσήμανση
- IP διεύθυνση της πηγής
- IP διεύθυνση του προορισμού

13.6 Απαραίτητος είναι ο έλεγχος ότι οι καταγραφές συμβάντων διατηρούνται για τουλάχιστον ένα έτος.

13.7 Επιπλέον απαραίτητος είναι ο έλεγχος ότι οι καταγραφές συμβάντων ασφαλίζονται επαρκώς από μη εξουσιοδοτημένη πρόσβαση, μεταβολή και διαγραφή.

13.8 Επίσης απαραίτητος είναι ο έλεγχος ότι η ευθύνη της διαχείρισης της λειτουργίας των αρχείων καταγραφής συμβάντων έχει ανατεθεί σε μια ομάδα χρηστών που κατέχουν ειδικούς λογαριασμούς με αυξημένα δικαιώματα.

13.9 Απαιτείται έλεγχος ότι τα κρίσιμα αρχεία καταγραφής συμβάντων, συλλέγονται και αποθηκεύονται σε έναν κεντρικό server καταγραφής, προκειμένου να είναι διαθέσιμα για ανάλυση και έλεγχο.

13.10 Προτείνεται η εγκατάσταση ενός εργαλείου ασφάλειας πληροφοριών και διαχείρισης συμβάντων (SIEM), το οποίο θα βοηθήσει στον συσχετισμό των συμβάντων και στον εντοπισμό ενδεχόμενων ύποπτων δραστηριοτήτων.

14. Διασφάλιση επιχειρησιακής συνέχεια και ανάκαμψης από καταστροφές

Παρά τα μέτρα ασφαλείας που μπορεί να έχει εφαρμόσει μια επιχείρηση για την αποφυγή κυβερνοεπίθεσης, αυτό δεν παύει να σημαίνει ότι είναι πλέον αδιαπέραστο το σύστημά της και ότι δεν θα πέσει ποτέ θύμα κυβερνοεπίθεσης. Για τον λόγο αυτόν, πέρα από τα βασικά μέτρα ασφαλείας που αναφέρθηκαν στα προηγούμενα 13 βήματα, είναι σημαντικό να αναφέρουμε και κάποια βασικά βήματα για να διασφαλίσουμε ότι η επιχείρηση θα συνεχίσει να λειτουργεί κανονικά ακόμη και αν δεχτεί επίθεση.

Μέτρα Προστασίας:

14.1 Να αναπτύξουν και να καταγράψουν δικές τους πολιτικές επιχειρησιακής συνέχειας και ανάκαμψης οι οποίες θα αναφέρουν τον σκοπό αυτής της πολιτικής, το πεδίο στο οποίο θα εφαρμόζετε καθώς και τους ρόλους και τις ευθύνες που υπάρχουν στην εταιρεία. Επιπλέον θα πρέπει να αναφερθούν οι τρόποι υλοποίησης της πολιτικής αλλά και των σχετικών μέτρων προστασίας που θα εφαρμόζονται.

14.2 Απαραίτητη είναι η αξιολόγηση των επιπτώσεων που προκύπτουν από ανεπιθύμητα συμβάντα, όπως κυβερνοεπιθέσεις ή φυσικές καταστροφές, στον Οργανισμό. Αυτό έχει ως στόχο να μπορούν να ανιχνευτούν τα κρίσιμα συστήματα που υπάρχουν καθώς και τους πόρους με τις μεγαλύτερες απαιτήσεις σε διαθεσιμότητα και αποκατάσταση, με σκοπό να δοθεί υψηλότερη προτεραιότητα στην υλοποίηση μέτρων ανάκαμψης για αυτά.

14.3 Απαραίτητη είναι η χρήση πλεοναζόντων πόρων στην αρχιτεκτονική που έχουν τα συστήματα της εταιρείας, έτσι ώστε να εξασφαλιστεί η απαιτούμενη διαθεσιμότητα.

14.4 Συνιστάται η πραγματοποίηση σε τακτικά χρονικά διαστήματα εκπαίδευσης μιας συγκεκριμένης ομάδας από το προσωπικό, προκειμένου να διαθέτουν πλήρη κατανόηση για τα σχέδια της επιχειρησιακής συνέχειας και να είναι σε θέση να υλοποιούν τις απαραίτητες ενέργειες για την αποκατάσταση των επιχειρησιακών λειτουργιών της εταιρείας.

14.5 Επιπλέον συνιστάται η πραγματοποίηση σε σύντομα χρονικά διαστήματα μεταξύ τους ασκήσεις δοκιμής για τα μέτρα που διασφαλίζουν την επιχειρησιακή συνέχεια και αποκατάσταση μετά από καταστροφές, ειδικά όταν παρατηρούνται σημαντικές τεχνικές και διαδικαστικές αλλαγές στη λειτουργία της επιχείρησης.

14.6 Απαιτείται η δημιουργία ενός διαφορετικού χώρου αποθήκευσης των δεδομένων ο οποίος θα βρίσκεται σε ασφαλή απόσταση από τον πρωταρχικό χώρο αποθήκευσης, έτσι ώστε να αποφευχθεί η πιθανότητα να δεχτεί η εταιρεία ίδιες κατηγορίες απειλών.

14.7 Συνιστάται η ανάθεση της αποκατάστασης μετά από μια καταστροφή σε έναν εξειδικευμένο πάροχο υπηρεσιών cloud, ο οποίος θα αναλάβει την άμεση μεταφορά των λειτουργιών της εταιρείας σε ένα άλλο περιβάλλον, χρησιμοποιώντας τεχνολογίες εικονικοποίησης.

14.8 Τέλος απαραίτητη είναι η δημιουργία ενός διαφορετικού χώρου επεξεργασίας των δεδομένων ο οποίος θα βρίσκεται σε ασφαλή απόσταση από τον πρωταρχικό χώρο αποθήκευσης, έτσι ώστε να αποφευχθεί η πιθανότητα να δεχτεί η εταιρεία ίδιες κατηγορίες απειλών.

Τα παραπάνω αποτελούν μερικά από τα βασικότερα μέτρα ασφαλείας που πρέπει να ακολουθεί κάθε επιχείρηση που επιθυμεί να διασφαλίσει τη μέγιστη δυνατή προστασία από πιθανές κυβερνοεπιθέσεις.

5.2 Frameworks

Στόχος αυτής της ενότητας είναι να καταγράψουμε ένα πλαίσιο το οποίο θα βοηθήσει τις εταιρείες να χαρτογραφήσουν τα συστήματα και τα υλικά τους με σκοπό τον εντοπισμό των ευπαθειών που κατά πάσα πιθανότητα θα έχουν. Επιπλέον, η αξιολόγηση του κινδύνου θεωρείται αναπόσπαστο κομμάτι ενός πλαισίου διαχείρισης κινδύνου και γιαύτον τον λόγο στην ενότητα αυτή θα περιγράψουμε αναλυτικότερα τα βασικά βήματα για την επιτυχής ολοκλήρωση αυτού.

Για να καταλάβουμε καλύτερα την έννοια του πλαισίου θα δώσουμε τον εξής ορισμό:

Σύμφωνα με το NIST (2018), πλαίσιο είναι μια κοινή γλώσσα που αποτελείται από πρότυπα, κατευθυντήριες γραμμές και βέλτιστες πρακτικές για την κατανόηση και την διαχείριση του κινδύνου

της κυβερνοασφάλειας. Στόχος του πλαισίου είναι να βοηθήσει στον εντοπισμό και την κατηγοριοποίηση των ενεργειών με σκοπό την μείωση των κυβερνοεπιθέσεων. Το πλαίσιο δεν είναι ίδιο για όλους τους οργανισμούς, αλλά κάθε οργανισμός το αναπροσαρμόζει με βάση τις ανάγκες του.

Λόγο του ότι οι ανάγκες ποικίλουν από εταιρεία σε εταιρεία και από οργανισμό σε οργανισμό, έχουν αναπτυχθεί πάρα πολλά πλαίσια για να καλυφθούν αυτές οι ανάγκες για προστασία από κυβερνοεπιθέσεις. Στην παρούσα διπλωματική θα αναλυθεί το πλαίσιο NIST.

5.2.1 Πλαίσιο NIST

Το πλαίσιο NIST (National Institute of Standards and Technology), πρωτο-δημοσιεύτηκε το 2014 από την National Institute of Standards and Technology και περιέχει όλα όσα αναφέρονται στον ορισμό του πλαισίου. Όπως σε όλα τα πλαίσια, έτσι και στο NIST στόχος του είναι η διαχείριση του κινδύνου από κυβερνοεπιθέσεις. Μεγαλοεταιρείες όπως είναι η MICROSOFT, η INTEL και η BANK OF ENGLAND έχουν εντάξει το πλαίσιο NIST στις αρχές του οργανισμού τους.

Τα πλεονεκτήματα που προσφέρει αυτό το πλαίσιο είναι τα παρακάτω πέντε

- Κάνει χρήση κοινής ορολογίας και γλώσσας για την περιγραφή και ανάλυση των κίνδυνων της κυβερνοασφάλειας.
- Κάνει χρήση ήδη υπαρκτών και βέλτιστων πρακτικών και προτύπων όπως είναι το COBIT και το ISO.
- Αναπτύχθηκε με στόχο την ενσωμάτωση του και στον ιδιωτικό και στον δημόσιο τομέα σε όλο το εύρος του κόσμου.
- Κάνει χρήση επιχειρηματικούς οδηγούς, οι οποίοι περιλαμβάνουν διαδικασίες διαχείρισης κινδύνου και
- Παρέχει την δυνατότητα διαχείρισης των κινδύνων της κυβερνοασφάλειας με πολύ μικρό κόστος, καταφέρνοντας παράλληλα να προστατέψει το απόρρητο και τις πολιτικές ελευθερίες.

Το πλαίσιο NIST αποτελείται από πέντε βασικές λειτουργίες.

- Αναγνώριση (Identify)
- Προστασία (Protect)
- Ανίχνευση (Detect)
- Ανταπόκριση (Respond)
- Ανάκαμψη (Recover)

Οι πέντε αυτές λειτουργίες περιέχουν συνολικά 23 επιμέρους κατηγορίες και 108 υποκατηγορίες. Ο παρακάτω πίνακας είναι μια αναπαράσταση των 5 λειτουργιών και των επιμέρους κατηγοριών του πλαισίου. Επιπλέον, τα χρώματα που απεικονίζονται στις κατηγορίες έχουν επιλεχθεί με βάση τα πρωτότυπα χρώματα που χρησιμοποιούνται στο πλαίσιο NIST.

Πίνακας 5.1: Λειτουργίες και κατηγορίες NIST πλαισίου

Αναγνώριση	**Προστασία**	**Ανίχνευση**	**Ανταπόκριση**	**Ανάκαμψη**
Διαχείριση περιουσιακών στοιχείων	Διαχείριση Ταυτότητας και Έλεγχος Πρόσβασης	Ανωμαλίες και γεγονότα	Σχεδιασμός απόκρισης	Σχεδιασμός ανάκαμψης
Επιχειρηματικά Περιβάλλοντα	Ευαισθητοποίηση και Εκπαίδευση	Ασφάλεια Συνεχής Παρακολούθηση	Διαβιβάσεις	Βελτιώσεις
Διακυβέρνηση	Ασφάλεια δεδομένων	Διαδικασίες ανίχνευσης	Ανάλυση	Διαβιβάσεις
Εκτίμηση Κινδύνου	Διαδικασίες και Διαδικασίες Προστασίας Πληροφοριών		Μετρίαση	
Στρατηγική Διαχείρισης Κινδύνων	Συντήρηση		Βελτιώσεις	
Διαχείριση Κινδύνων Εφοδιαστικής Αλυσίδας	Προστατευτική Τεχνολογία			

Παρατηρούμε, ότι η αξιολόγηση κινδύνου που αναφέραμε στην αρχή της ενότητας, ανήκει στην πρώτη κατηγορία (Αναγνώριση) του NIST και είναι ένα αναπόσπαστο κομμάτι του πλαισίου.

Ένα ακόμη από τα θετικά που παρέχει το πλαίσιο NIST είναι οι βαθμίδες υλοποίησης (*Tiers*). Οι βαθμίδες αυτές αντικατοπτρίζουν τον τρόπο που μια εταιρεία παρακολουθεί τον κίνδυνο της κυβερνοασφάλειας καθώς και τις διαδικασίες που εφαρμόζει για την διαχείριση αυτού του κινδύνου. Οι βαθμίδες αυτές ταξινομούνται από το 1 έως το 4 όπου η κάθε βαθμίδα περιγράφει τον βαθμό αυστηρότητας και πολυπλοκότητας των διαδικασιών που χρησιμοποιεί μια επιχείρηση για την διαχείριση του κίνδυνου στον κυβερνοχώρο. Οι βαθμίδες δεν είναι κάποιος μηχανισμός υλοποίησης αλλά υπάρχουν για την υποστήριξη των οργανωτικών λήψεων αποφάσεων σχετικά με τον τρόπο που διαχειρίζεται μια εταιρεία τον κίνδυνο της κυβερνοασφάλειας.

Για μπορέσει όμως η εταιρεία να διαλέξει την σωστή βαθμίδα στην οποία ανήκει θα πρέπει να γνωρίζει και τους ορισμούς που κατέχει η κάθε μια βαθμίδα. Για τον λόγο αυτό, παρακάτω αναγράφονται αναλυτικά οι ορισμοί και το τι αντιπροσωπεύει η κάθε μια από τις 4 βαθμίδες.

1. **Βαθμίδα 1: Μερικός (Partial)**

Διαδικασία διαχείρισης κινδύνου: Στην πρώτη βαθμίδα οι διαδικασίες για την διαχείριση του κινδύνου δεν είναι επίσημες και ένα πάρα πολύ συχνό φαινόμενο αυτής της περίπτωσης είναι η αυθόρμητες και αντιδραστικές κινήσεις για την διαχείριση του κινδύνου. Επιπλέον, σε πολλές περιπτώσεις η ιεραρχία των δραστηριοτήτων στον κυβερνοχώρο, είναι πολύ πιθανό να μην είναι άμεσα ενημερωμένες από την εταιρεία.

Πρόγραμμα ολοκληρωμένης διαχείρισης κινδύνου: Δεν υπάρχει επαρκής ενημέρωση σχετικά με τους κινδύνους στον κυβερνοχώρο. Για τον λόγο αυτό, οι εταιρείες εφαρμόζουν πρακτικές διαχείρισης των κινδύνων με βάση την εμπειρία τους ή από πληροφορίες που έχουν ακούσει από τρίτους.

Εξωτερική συμμετοχή: Σε αυτήν την περίπτωση, η εταιρεία δεν έχει επίγνωση των κινδύνων που προέρχονται από την εφοδιαστική αλυσίδα στον κυβερνοχώρο καθώς και των προϊόντων και των υπηρεσιών που συμπεριλαμβάνονται και χρησιμοποιούνται σε αυτήν την αλυσίδα.

2. **Βαθμίδα 2: Ενημέρωση κινδύνου (Risk Informed)**

Διαδικασία διαχείρισης κινδύνου: Στην δεύτερη βαθμίδα, οι διαδικασίες για την διαχείριση του κινδύνου που χρησιμοποιεί η εταιρεία είναι εγκεκριμένες από την διοίκηση αλλά μπορεί να μην είναι οι καθιερωμένες ως πολιτικές της εταιρείας.

Πρόγραμμα ολοκληρωμένης διαχείρισης κινδύνου: Στην δεύτερη βαθμίδα, σε αντίθεση με την πρώτη, υπάρχει η επίγνωση του κινδύνου στον κυβερνοχώρο από όλη την εταιρεία αλλά παρόλα αυτά ακόμη δεν υπάρχει κάποια καθιερωμένη αντιμετώπιση του κινδύνου. Επιπλέον, μέτρα ασφάλεια από κυβερνοεπιθέσεις δεν λαμβάνονται υπόψη σε όλο το εύρος της εταιρείας αλλά μόνο σε κάποια επιλεγμένα επίπεδα.

Εξωτερική συμμετοχή: Η εταιρεία έχει επίγνωση των κινδύνων που προέρχονται από την εφοδιαστική αλυσίδα στον κυβερνοχώρο καθώς και των προϊόντων και των υπηρεσιών που συμπεριλαμβάνονται και χρησιμοποιούνται σε αυτήν, αλλά τις περισσότερες φορές δεν ενεργεί με συνέπεια σε αυτούς τους κινδύνους.

3. **Βαθμίδα 3: Επαναληπτός (Repeatable)**

Διαδικασία διαχείρισης κινδύνου: Στην τρίτη βαθμίδα, οι διαδικασίες για την διαχείριση του κινδύνου που χρησιμοποιεί η εταιρεία είναι εγκεκριμένες και είναι καθιερωμένες ως πολιτικές τις εταιρείας. Επιπροσθέτως, οι διαδικασίες αυτές ενημερώνονται σε τακτά χρονικά διαστήματα για να είναι πάντα ενημερωμένες με τις ανάγκες της εταιρείας, τις νέες απειλές στον κυβερνοχώρο αλλά και τις νέες τεχνολογίες που υπάρχουν.

Πρόγραμμα ολοκληρωμένης διαχείρισης κινδύνου: Σε αυτήν την περίπτωση υπάρχει μια καθιερωμένη αντιμετώπιση του κινδύνου από όλα τα μέλη της εταιρείας και υπάρχουν πάντα έτοιμοι μέθοδοι για την άμεση και αποτελεσματική ανταπόκριση στις αλλαγές του κινδύνου που

μπορεί να προκύψουν. Επιπλέον, η εταιρεία παρακολουθεί στενά και σε τακτά χρονικά διαστήματα τις απειλές στην κυβερνοασφάλεια που εμφανίζονται στα υλικά και λογισμικά της.

Εξωτερική συμμετοχή: Η εταιρεία έχει επίγνωση των κινδύνων που προέρχονται από την εφοδιαστική αλυσίδα στον κυβερνοχώρο καθώς και των προϊόντων και των υπηρεσιών που συμπεριλαμβάνονται και χρησιμοποιούνται σε αυτήν. Ως αποτέλεσμα, το μεγαλύτερο ποσοστό των εταιρειών που ανήκουν σε αυτήν την βαθμίδα, ενεργούν με συνέπεια σε αυτούς τους κινδύνους. Σε αυτές τις ενέργειες συμπεριλαμβάνονται γραπτές συμφωνίες οι οποίες περιλαμβάνουν τις βασικές απαιτήσεις για την διαχείριση του κινδύνου και πολιτικές για την σωστή εφαρμογή και παρακολούθηση των κινδύνων.

4. Βαθμίδα 4: Προσαρμοστικός (Adaptive)

Διαδικασία διαχείρισης κινδύνου: Στην τέταρτη και υψηλότερη βαθμίδα, η εταιρεία αναδιαμορφώνει τις διαδικασίες ασφαλείας της στον κυβερνοχώρο, βασιζόμενη σε προηγούμενες ή και τρέχουσες πρακτικές κυβερνοασφάλειας. Σε αυτές τις πρακτικές συμπεριλαμβάνονται και τα σεμινάρια αλλά και οι προγνωστικοί δείκτες. Αυτή η αναδιαμόρφωση την βοηθάει να ανταποκρίνεται άμεσα και αποτελεσματικά σε τυχόν νέες απειλές που μπορεί να προκύψουν.

Πρόγραμμα ολοκληρωμένης διαχείρισης κινδύνου: Σε αυτήν την περίπτωση η διαχείριση των κινδύνων αποτελεί αναπόσπαστο κομμάτι της εταιρείας και συνεχώς εξελίσσεται. Η εξέλιξη αυτή προκύπτει βάση των προηγούμενων ενεργειών που έχουν πραγματοποιηθεί αλλά και με συνεχής επίβλεψη των τωρινών ενεργειών στα συστήματα και στα δίκτυα της εταιρείας. Το αποτέλεσμα της συνεχής επίβλεψης είναι η άμεση και αποτελεσματική ανταπόκριση της εταιρείας σε πιθανές αλλαγές στους στόχους της σχετικά με τον τρόπο προσέγγισης αλλά και την διαχείριση των κινδύνων.

Εξωτερική συμμέτοχή: Η εταιρεία, για να κατανοήσει πλήρως και να φερθεί με συνέπεια στους κινδύνους της εφοδιαστικής αλυσίδας καθώς και των προϊόντων και των υπηρεσιών που συμπεριλαμβάνονται και χρησιμοποιούνται σε αυτήν, χρησιμοποιεί πληροφορίες πραγματικού χρόνου.

5.2.2 Αξιολόγηση του κινδύνου

Η αξιολόγηση του κινδύνου όπως είδαμε και στην προηγούμενη ενότητα ανήκει στο πρώτο βήμα του NIST πλαισίου και είναι ένα από τα βασικότερα μέρη της ασφάλειας. Στόχος της αξιολόγησης είναι ο εντοπισμός και η ταξινόμηση όλων των ευαίσθητων σημείων της εταιρείας, τους κινδύνους και τις απειλές στις οποίες είναι εκτεθειμένη καθώς και στις επιπτώσεις που θα έχει στην λειτουργία της.

Το πρώτο βήμα της αξιολόγησης του κίνδυνου είναι ο εντοπισμός των πηγών από τις οποίες είναι πιθανό να προέλθουν απειλές προς την εταιρεία και το σύστημα της. Μερικές από αυτές τις πηγές μπορεί να είναι είτε μια φυσική απειλή, είτε κάποιο ανθρώπινο λάθος, είτε μια κακόβουλη ομάδα ανθρώπων, είτε ακόμη και κάποιος ανταγωνιστής της εταιρείας.

Το δεύτερο βήμα είναι η αναγνώριση του χαρακτήρα των ενεργειών που μπορούν να προκύψουν από τις παραπάνω πηγές κινδύνου. Ο χαρακτήρας των ενεργειών μπορεί να είναι είτε μια κυβερνοεπίθεση, είτε καταστροφή από φυσικά αίτια, είτε ακόμη και μια βλάβη κάποιου υλικού.

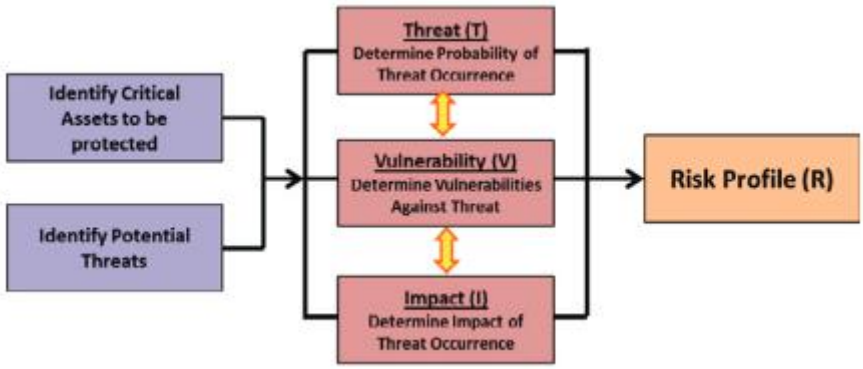
Σειρά έχει ο εντοπισμός των ευπαθειών που υπάρχουν στην εταιρεία και τις οποίες θα μπορούσε εύκολα μια πηγή κινδύνου να τις εκμεταλλευτεί εκτελώντας κάποιες συγκεκριμένες ενέργειες.

Σαν τέταρτο βήμα κατατάσσουμε την διαδικασία υπολογισμού της πιθανότητας ότι οι πηγές κινδύνου που αναφέραμε στο βήμα πρώτο θα ξεκινήσουν μια κακόβουλη ενέργεια καθώς και την πιθανότητα αυτή η κακόβουλη ενέργεια να ολοκληρωθεί με επιτυχία

Έπειτα στο προτελευταίο βήμα, γίνεται η καταγραφή των επιπτώσεων που θα δεχτεί η εταιρεία στην πιθανότητα επιτυχούς πραγματοποίησης της κακόβουλης ενέργειας. Επιπλέον, να σημειωθεί ότι οι επιπτώσεις δεν αφορούν και δεν επηρεάζουν μόνο την λειτουργία και τα συστήματα της εταιρεία αλλά είναι πιθανών να επηρεάσουν και άλλα πρόσωπα που συναναστρέφονται με αυτήν.

Στο τελευταίο βήμα, γίνεται ο ολοκληρωτικός καθορισμός του κινδύνου για την ασφάλεια της εταιρείας, ο οποίος προκύπτει από τον συνδυασμό του βήματος τέσσερα και πέντε, δηλαδή από την πιθανότητα επιτυχούς ολοκλήρωσης των κακόβουλών ενεργειών και των επιπτώσεων που θα δεχτεί η εταιρεία στην περίπτωση επιτυχούς ολοκλήρωσης των κακόβουλών ενεργειών.

Το παρακάτω σχήμα είναι μια αναπαράσταση των παραπάνω έξι βημάτων.



Σχήμα 5.8: Αναπαράσταση των βημάτων για την αξιολόγηση των κινδύνων

Στην διαδικασία της χαρτογράφησης της εταιρείας, για να μπορέσουμε να κατατάξουμε τα υλικά και λογισμικά σε μία κλίμακα από το πιο ευάλωτο στο λιγότερο ευάλωτο χρησιμοποιούμε μια μέθοδο οι οποία συμπεριλαμβάνει τα εξής 3 κριτήρια για την διεξαγωγή του αποτελέσματος:

- Αξιολόγηση της απειλής που μπορεί να δεχτεί (T) ή Threat Rating
- Τις ευαισθησίες που έχει και (V) ή Vulnerability Rating
- Τις επιπτώσεις που θα υπάρξουν (I) ή Impact Rating

Ο βαθμός που ορίζεται για κάθε ένα από τα παραπάνω 3 κριτήρια είναι τις κλίμακας από το 1 έως το 5 όπου το προφίλ του κάθε ένα είναι:

- Το 1 αντιπροσωπεύει το πολύ χαμηλού κινδύνου
- Το 2 αντιπροσωπεύει το χαμηλού κινδύνου
- Το 3 αντιπροσωπεύει το μέτριου κινδύνου
- Το 4 αντιπροσωπεύει το υψηλού κινδύνου και
- Το 5 αντιπροσωπεύει το πολύ υψηλού κινδύνου

Για τον υπολογισμό όμως του τελικού αποτελέσματος των προηγούμενων τριών κριτηρίων εκτελούμε την παρακάτω μαθηματική πράξη:

Κίνδυνος = T x V x I

Εξίσωση 5.1: *Εξίσωση υπολογισμού βαθμού κινδύνου*

Εκτελώντας αυτήν την πράξη για κάθε υλικό και λογισμικό που έχει χαρτογραφηθεί στην εταιρεία και με βάση το τελικό αποτέλεσμα της πράξης, θα προκύψει και η τελική κατάταξη κινδύνου.

Για τα το εύρος από το 1 έως το 5, υπάρχει και το αντίστοιχο εύρος ποσοτικού κινδύνου που προκύπτει από το αποτέλεσμα της παραπάνω πράξης Κινδύνου.

Πίνακας 5.2: Κατάταξη κινδύνου

Κατάταξης	**Επίπεδο κινδύνου**	**Εύρος ποσοτικού κινδύνου**
1	Πολύ χαμηλό	1 έως 2
2	Χαμηλό	3 έως 15
3	Μέτριο	16 έως 44
4	Υψηλό	45 έως 90
5	Πολύ υψηλό	91 έως 125

Σκοπός αυτής της κατάταξης είναι να βοηθήσει το αρμόδιο τμήμα ασφαλείας της εταιρείας να αναπτύξει και να εντάξει στην εταιρεία τα κατάλληλα μέτρα για την προστασία της από κυβερνοεπιθέσεις. Επιπλέον, λόγο της εποχής που ζούμε και λαμβάνοντας υπόψη την οικονομική κρίση που περνάμε, είναι πιθανών οι εταιρείες να μην μπορούν να διαθέσουν τα χρηματικό ποσό που απαιτείται για την πλήρη ασφάλεια της εταιρείας. Όμως χάρη στην κατάταξη κινδύνου, η εταιρεία είναι σε θέση να κρίνει που χρειάζεται την μεγαλύτερη προσοχή σε ασφάλεια και να επενδύσει περισσότερο σε αυτό το κομμάτι και λιγότερο σε αυτά που είναι χαμηλότερα στην κατάταξη. Με βάση την κατάταξη προκύπτουν τα εξής παρακάτω:

- Για όσα αποτελέσματα κατατάσσονται στην κατηγορία 4-5 (υψηλού και πολύ υψηλού κινδύνου) είναι απαραίτητο να ακολουθηθεί μια διαδικασία μετριασμού του κινδύνου.
- Για όσα αποτελέσματα κατατάσσονται στην κατηγορία 3 (μέτριου κινδύνου) θα πρέπει να ληφθούν μέτρα για τον περιορισμό του κινδύνου, ακολουθώντας της αρχή του "ALARP". Η αρχή αυτή αναφέρετε στους υπεύθυνους ασφαλείας και ο βασικός της σκοπός είναι η μείωση του βαθμού κινδύνου όσο τον δυνατόν πιο χαμηλά γίνεται.
- Για όσα αποτελέσματα κατατάσσονται στην κατηγορία 1-2 (χαμηλού και πολύ χαμηλού κινδύνου), οι υπεύθυνοι ασφαλείας θα πρέπει να αξιολογήσουν τους υπολειπόμενους κινδύνους πριν τους αποδεχτούν.

Ο παρακάτω πίνακας είναι ένα παράδειγμα αξιολόγησης κινδύνου το οποίο βασίζεται σε όσα έχουμε αναφέρει προηγουμένως και στοχεύει στην καλύτερη κατανόηση αυτής της ενότητας.

Πίνακας 5.3: Παράδειγμα αξιολόγησης κινδύνου

Πιθανά σενάρια απειλής	**Threat Rating**	**Vulnerability Rating**	**Impact Rating**	**Σύνολο βαθμού κινδύνου**	**Προφίλ Κινδύνου**	**Στρατηγική Διαχείρισης**
Σαμποτάζ	3	4	5	60	Υψηλό	Διαδικασία μετριασμού του κινδύνου
Ληστεία	2	4	5	40	Μέτριο	Αρχή του "ALARP"
Πυρκαγιά	2	4	5	40	Μέτριο	Αρχή του "ALARP"

Επίλογος

Συνοψίζοντας, στο πέμπτο και τελευταίο κεφάλαιο της παρούσας διπλωματικής, αναλύσαμε αρχικά τις βέλτιστες πρακτικές που θα πρέπει να ακολουθήσουν οι εταιρείας έτσι ώστε να διασφαλίσουν κατά το μέγιστο δυνατό την ασφάλεια των συστημάτων τους από κυβερνοεπιθέσεις. Οι πρακτικές αυτές αναφέρονται σε όλα τα πιθανά επίπεδα στα οποία μπορεί να δεχτεί επίθεση η εταιρεία. Στην συνέχεια, αφού εξηγήσαμε τον ρόλο του πλαισίου και την χρησιμότητά του, αναφερθήκαμε πιο ειδικά στο πλαίσιο NIST και στον τρόπο που αυτό λειτουργεί.

Κεφάλαιο 6: Μελέτη περίπτωσης

Στόχος αυτού του κεφαλαίου είναι η περιγραφή της έννοιας της ηλεκτρονικής τιμολόγησης (e-invoice), η καταγραφή των λόγων που είναι απαραίτητη, η ασφάλεια σε αυτά, η καταγραφή των θεμάτων ασφαλείας, η ανάλυση των απαιτήσεων που υπάρχουν για την ασφάλεια καθώς και μέτρα προστασίας για μεγαλύτερη ασφάλεια.

6.1 Ορισμός e-invoice

Σύμφωνα με την Τριανταφύλλου Δ. (2011), η ηλεκτρονική τιμολόγηση (e-invoice) είναι η ανταλλαγή τιμολογίων αλλά και άλλων εγγράφων όπως χρεωστικά και πιστωτικά σημειώματα, εμβάσματα καθώς και όρους πληρωμής μέσω ηλεκτρονικών διαδικασιών.

Με άλλα λόγια ένα e-invoice, όπως και ένα παραδοσιακό τιμολόγιο περιέχει ευαίσθητες πληροφορίες που αφορούν και τις δύο πλευρές (πωλητή - αγοραστή). Τέτοιες πληροφορίες είναι για παράδειγμα το Α.Φ.Μ του πωλητή και του αγοραστή, η διεύθυνση που εδρεύει η εταιρεία τους, στοιχεία επικοινωνίας όπως είναι ο αριθμός τηλεφώνου ή και κάποιο email αλλά και πολλά ακόμη.

Χάρη στην ραγδαία αύξηση των online αγορών αλλά και γενικά στην αύξηση της χρήσης των ηλεκτρονικών μέσων για την διεκπεραίωση διαδικασιών από την πανδημία και μετά, η χρήση του e-invoice αυξάνεται ολοένα και περισσότερο. Όπως όμως έχουμε αναφέρει προηγουμένως στην παρούσα διπλωματική, παράλληλα με την αύξηση των ηλεκτρονικών υπηρεσιών των επιχειρήσεων στις μέρες της πανδημίας παρατηρήθηκε και μεγάλη αύξηση των κυβερνοεπιθέσεων. Για τον λόγο αυτό, είναι σημαντικό η ανταλλαγή των e-invoice μεταξύ των πωλητών και των αγοραστών να προστατεύεται με όλους τους δυνατούς τρόπους.

6.2 Θέματα ασφαλείας

Λόγω του ότι τα e-invoicing μεταφέρονται ψηφιακά αυτό τα καθιστά πιο ευάλωτα σε πολλών ειδών επιθέσεις από ότι τα παραδοσιακά τιμολόγια. Μερικές από αυτές τις επιθέσεις είναι η επίθεση μέσω δικτύου, η επίθεση στο υλικό αποθήκευσης των e-invoicing αλλά και κλοπή των συσκευών που βρίσκονται αποθηκευμένα τα αρχεία της ηλεκτρονικής τιμολόγησης. Αν μπορούσαμε να κατατάξουμε τις τρείς αυτές επιθέσεις με βάση το ποια είναι πιο συχνή στο να συμβεί και με βάση τα όσα έχουμε μάθει από αυτήν την διπλωματική θα τις κατατάσσαμε ως εξής:

1. Επίθεση μέσω δικτύου
2. Επίθεση στο υλικό αποθήκευσης
3. Κλοπή υλικών αποθήκευσης

Αναλυτικότερα για την κάθε επίθεση:

Από τις επιθέσεις μέσω δικτύου, αυτές που αφορούν την κλοπή των e-invoicing κατά την μεταφορά τους είναι:

- Το sniffer attack, κατά το οποίο ο επιτιθέμενος μέσω μιας sniffer εφαρμογής ή συσκευής έχει την δυνατότητα να διαβάζει, να καταγράφει αλλά και να παρακολουθεί τα πακέτα που στέλνονται μέσω του δικτύου. Αν αυτά τα πακέτα που περιέχουν το e-invoice αρχεία δεν είναι κρυπτογραφημένα, ο επιτιθέμενος έχει πλήρη εικόνα των δεδομένων.

- Το compromised-key attack, κατά το οποίο ο επιτιθέμενος υποκλέβει το κλειδί που υπάρχει για την ασφαλή επικοινωνία μεταξύ του αποστολέα και του παραλήπτη και έτσι μπορεί να αποκρυπτογραφήσει τα δεδομένα που στέλνονται και
- Το Eavesdropping attack το οποίο μοιάζει αρκετά με την επίθεση sniffer. Ο επιτιθέμενος εντοπίζει τις πληροφορίες που θέλει να υποκλέψει ακούγοντας το μήνυμα που μεταδίδεται μέσω του δικτύου.

Από την άλλη, σχετικά με την επίθεση στο υλικό αποθήκευσης των e-invoicing, υπάρχουν πολλοί τρόποι για να καταφέρει ο επιτιθέμενος να αποκτήσει πρόσβαση σε αυτά. Δύο από αυτούς τους τρόπους είναι μέσω ενός κακόβουλου λογισμικού και μέσω φυσικής πρόσβασης στο σύστημα αποθήκευσης.

Τέλος, σχετικά με την κλοπή των υλικών αποθήκευση έχουμε να αναφέρουμε ότι είναι πιο δύσκολο να πραγματοποιηθεί από τις προηγούμενες δύο περιπτώσεις αλλά δεν παύει να υπάρχει. Ας υποθέσουμε ότι τα ηλεκτρονικά τιμολόγια στέλνονται μέσω email και έστω ότι ο πωλητής ή αντίστοιχα ο αγοραστής έχουν πρόσβαση στο email στο οποίο έγινε η αποστολή και παράδοση του ηλεκτρονικου τιμολογίου μέσω του κινητού τηλεφώνου τους. Σε περίπτωση κλοπής του κινητού ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στο email και άρα και στα e-invoice.

Βέβαια θα μπορούσε κανείς να πει ότι η κλοπή του υλικού αποθήκευσης μπορεί να πραγματοποιηθεί ακόμη και στην παραδοσιακή έκδοση των τιμολογίων. Παρόλα αυτά, η ηλεκτρονική μορφή τους τα καθιστά πιο ευάλωτα στην κλοπή γιατί μπορούν να υπάρχουν σε πολλών ειδών πλατφόρμες άρα είναι περισσότερο εκτεθειμένα.

6.3 Απαιτήσεις ασφαλείας

Για να μπορεί να λειτουργεί ομαλά η ηλεκτρονική τιμολόγηση και κυρίως να μπορεί να γίνει μέρος μιας εταιρείας θα πρέπει να τηρούνται κάποιες απαιτήσεις ασφαλείας. Είναι ζωτικής σημασίας η σωστή εφαρμογή των απαιτήσεων που θα αναλυθούν παρακάτω καθώς είναι απαραίτητη η διασφάλιση της αυθεντικοποίησης και της ακεραιότητας των e-invoicing σε όλη την διάρκεια ζωής τους. Επιπλέον, οι απαιτήσεις που θα αναλύσουμε, αναφέρονται τόσο στην διασφάλιση της ορθής μεταφοράς του ηλεκτρονικού τιμολογίου όσο και στην ορθή αποθήκευσή του. Σειρά έχει η ανάλυση αυτών των απαιτήσεων.

- Η πρώτη απαίτηση είναι η επαλήθευση της ταυτότητας προέλευσης. Αυτό έχει ως στόχο την εξασφάλιση ότι ο αποστολέας του τιμολογίου είναι πράγματι αυτός που ισχυρίζεται ότι είναι. Για να επιτευχθεί αυτό και για να μπορέσει η εφορία να κατονομάσει τα συμβαλλόμενα μέρη μιας φορολογικής συναλλαγής θα πρέπει, η φορολογική αρχή να πιστοποιήσει την ταυτότητα του φορολογούμενου.
- Η δεύτερη απαίτηση είναι η δυνατότητα της Μη-Αποποίησης της ευθύνης. Αυτό στοχεύει στην εξασφάλιση ότι ο εκδότης και ο παραλήπτης του ηλεκτρονικου τιμολογίου δεν μπορούν να αρνηθούν την πραγματοποίηση της συναλλαγής και της αποστολής του ηλεκτρονικού τιμολογίου.
- Η τρίτη απαίτηση είναι η διασφάλιση της ακεραιότητας του περιεχομένου του ηλεκτρονικού τιμολογίου. Αυτό έχει ως σκοπό να εξασφαλίσει ότι το περιεχόμενο του τιμολογίου δεν έχει τροποποιηθεί με κανέναν τρόπο. Η τροποποίηση αυτή, είτε πρόκειται για σκόπιμη ενέργεια είτε για τυχαία κατά την μεταφορά ή αποθήκευση του ηλεκτρονικού τιμολογίου πρέπει να

αποτρέπετε ρητά. Στόχος της τρίτης απαίτησης είναι η διαβεβαίωση των ενδιαφερόμενων για την ορθότητα του περιεχομένου.

- Η τέταρτη απαίτηση είναι η εξασφάλιση της εμπιστευτικότητας και της ιδιωτικότητας. Αυτό στοχεύει στην διαβεβαίωση ότι μόνο ο εκδότης και ο παραλήπτης μπορούν να διαβάσουν το περιεχόμενο του ηλεκτρονικού τιμολογίου.
- Η πέμπτη απαίτηση στοχεύει στην εξασφάλιση της ασφαλούς αποθήκευσης των ηλεκτρονικών τιμολογίων με τρόπο τέτοιον ώστε να διαβεβαιώνεται η ακεραιότητα, η αυθεντικοποίηση καθώς και η ανάγνωση του περιεχομένου κ άθολη την διάρκεια αποθήκευσης τους.
- Η έκτη απαίτηση είναι η εξασφάλιση της ακεραιότητας της ακολουθίας. Στόχος αυτής της απαίτησης είναι η αποφυγή των κενών στα ηλεκτρονικά τιμολόγια και η ενίσχυση του ελέγχου που πραγματοποιείται από τις φορολογικές αρχές.
- Η έβδομη και τελευταία απαίτηση είναι η διασφάλιση της διαθεσιμότητας της υπηρεσίας ηλεκτρονικής τιμολόγησης έτσι ώστε να είναι σε θέση να εκδώσει νέα ηλεκτρονικά παραστατικά ανά πάσα ώρα και στιγμή.

6.4 Μέτρα προστασίας

Γνωρίζοντας πλέον τους λόγους για τους οποίους είναι απαραίτητη η ασφάλεια των e-invoice, τα θέματα ασφαλείας που υπάρχουν καθώς και οι απαιτήσεις ασφαλείας που απαιτούνται για την υιοθέτηση και εφαρμογή των e-invoicing από μία εταιρεία, σειρά έχει η καταγραφή κάποιων βασικών μέτρων για την προστασία των ηλεκτρονικών τιμολογίων.

Τα μέτρα προστασίας που θα καταγράψουμε στην συνέχεια προέρχονται από τα μέτρα προστασίας που έχουμε αναφέρει στο κεφάλαιο των υφιστάμενων τεχνολογικών λύσεις.

Μέτρα προστασίας:

1. Αρχικά πρέπει να διασφαλιστεί η διαθεσιμότητα της υπηρεσίας. Για να επιτευχθεί αυτό συστήνεται η κατανόηση των πόρων με τους οποίους η υπηρεσία αυτή μπορεί να υπερφορτωθεί καθώς και τα όρια της πέρα από τα οποία η διαθεσιμότητας της κινδυνεύει να διακοπή. Επιπλέον, η υποδομή θα πρέπει να διαθέτει επαρκείς πόρους, όπως hardware, έτσι ώστε να είναι σε θέση να αντιμετωπίσει μια επίθεση DDoS. Επίσης, συστήνεται η ανάπτυξη ειδικών συστημάτων για την παρακολούθηση της διαθεσιμότητας και ανίχνευσης τυχόν επίθεσης DDoS.

2. Επόμενο στόχος η προστασία του συστήματος όσον αφορά την επαλήθευση της ταυτότητας προέλευσης. Για να επιτευχθεί αυτό συστήνεται η χρήση ψηφιακών υπογραφών. Σύμφωνα με την Κουτίδου (2019), η ψηφιακή υπογραφή αποτελεί μια ηλεκτρονική τεχνική που συνδέεται με τα δεδομένα που έχουν υπογραφεί, με σκοπό να επιτρέπει την αναγνώριση του αποστολέα και την αμεσότητα της ανίχνευσης οποιασδήποτε αλλοίωσης. Για να μπορέσει όμως κάποιος να χρησιμοποιήσει μια ψηφιακή υπογραφή δεν αρκεί απλά να την δημιουργήσει αλλά θα πρέπει να την επαληθεύσει κιόλας. Η επαλήθευση γίνεται από τις αρμόδιες αρχές του κράτους και συγκεκριμένα για την Ελλάδα η αρμόδια αρχή είναι η ΑΠΕΔ.

3. Απαραίτητη είναι η προστασία της εμπιστευτικότητας και της ιδιωτικότητας του περιεχομένου. Για να επιτευχθεί αυτό συστήνεται η μέθοδος της κρυπτογράφησης. Υπάρχουν πολλοί μέθοδοι κρυπτογράφηση, αλλά εμείς προτείνουμε τον αλγόριθμό δημοσίου κλειδιού ο

οποίος έχει σχεδιαστεί με τέτοιον τρόπο ώστε το κλειδί που απαιτείται για την κρυπτογράφηση του περιεχομένου να είναι διαφορετικό από το κλειδί που απαιτείται για την αποκρυπτογράφηση του περιεχομένου. Έτσι ο εκδότης του ηλεκτρονικού τιμολογίου και ο παραλήπτης θα έχουν από ένα κλειδί για να μπορέσουν να αναγνώσουν το περιεχόμενο.

4. Απαραίτητη είναι επίσης η προστασία του δικτύου για την ασφαλή μεταφορά των ηλεκτρονικών τιμολογίων. Προτείνεται η εγκατάσταση ενός firewall για τον έλεγχο των κινήσεων μέσω δικτύου καθώς και για την δημιουργία κανόνων οι οποίοι θα αποτρέπουν τις κακόβουλες και μη εξουσιοδοτημένες κινήσεις στο δίκτυο.

5. Προκειμένου να είναι τα e-invoicing πάντα διαθέσιμα για μελλοντική ανάγνωση πρέπει να ληφθούν μέτρα για τη σωστή και ασφαλή αποθήκευσή τους. με τρόπο τέτοιον ώστε να είναι πάντα διαθέσιμα για μελλοντική ανάγνωση. Για τον λόγο αυτό προτείνεται η χρήση αντιγράφων ασφαλείας τα οποία θα βρίσκονται σε διαφορετικό χώρο και όχι συνδεδεμένα σε κάποιο δίκτυο, έτσι ώστε ακόμη και σε περίπτωση επίθεσης να υπάρχει διαθέσιμο για ανάκτηση το αρχείο αυτό.

6. Τέλος πρέπει να ληφθεί μέριμνα και για τα δικαιώματα πρόσβασης του προσωπικού της επιχείρησης, έτσι ώστε να είναι προσπελάσιμα τα e-invoice μόνο από το αρμόδιο προσωπικό και μόνο όταν αυτό απαιτείται για την ομαλή διεκπεραίωση των εργασιακών καθηκόντων

Επίλογος

Στην ενότητα αυτή επικεντρωθήκαμε στην ασφαλείας των ηλεκτρονικών τιμολογίων. Ο λόγος για αυτήν την ανάλυση είναι ότι τα ηλεκτρονικά τιμολόγια είναι αναπόσπαστο κομμάτι των ERP συστημάτων και συμπληρώνουν τις ηλεκτρονικές υπηρεσίες των επιχειρήσεων. Οι ευαίσθητες πληροφορίες που περιέχουν επιβάλλουν τη λήψη μέτρων προστασίας τους σε όλα τα στάδια της εφαρμογής τους.

Κεφάλαιο 7: Συμπεράσματα – Μελλοντικές επεκτάσεις

7.1 Συμπεράσματα

Έχοντας ολοκληρώσει την παρούσα μελέτη καταλήγουμε στο ότι οι ασφάλεια των δεδομένων που διαχειρίζεται μια εταιρεία στο ERP λογισμικό της είναι ζωτικής σημασίας. Επίσης είναι σημαντικό οι επιχειρήσεις να κατανοήσουν πολύ καλά τους λόγους που αναφέραμε σχετικά με το πόσο σημαντική είναι η ασφάλεια των δεδομένων που διαχειρίζεται ένα ERP σύστημα. Όσο καλύτερα κατανοήσουν αυτούς τους λόγους, τόσο πιο πιθανών είναι να συμμορφωθούν με τα απαραίτητα μέτρα για την προστασία του συστήματος τους.

Επιπλέον ο λόγος που κάναμε εκτενή αναφορά στις επιθέσεις που έχουν πραγματοποιηθεί, στα στάδια που χρειάζονται για την πραγματοποίηση μιας επίθεσης και στους τύπους των επιθέσεων που υπάρχουν στα ERP συστήματα, είναι για να καταδείξουμε την σοβαρότητα της κατάστασης καθώς και να βοηθήσουμε στον σχηματισμό μιας σφαιρικής αξιολόγησης των μέτρων προστασίας που πρέπει να λαμβάνονται υπόψη.

Επιπροσθέτως καταλήξαμε στο συμπέρασμα ότι οι συνέπειες που θα δεχτεί μια επιχείρηση σε περίπτωση κυβερνοεπίθεσης είναι πολύ μεγάλες. Πέραν των οικονομικών επιπτώσεων, αυτομάτως μειώνεται και η εμπιστοσύνη των πελατών και προμηθευτών της. Για τον λόγο αυτό, έχοντας κατανοήσει τα επιμέρους κεφάλαια αυτής της μελέτης, θα πρέπει όλες οι εταιρείες που σέβονται και νοιάζονται τους ανθρώπους με τους οποίους συναναστρέφονται, να τηρούν τα πρότυπα για την ασφάλεια του συστήματος από κυβερνοεπιθέσεις.

Είναι σημαντικό οι τεχνολογίες και τα πρότυπα που αναπτύσσονται για την διασφάλιση της προστασίας των προσωπικών δεδομένων από επιθέσεις να εξελίσσονται καθημερινά με σκοπό να είναι πάντα ενήμερα και άμεσα χρησιμοποιούμενα για την αντιμετώπιση νέων επιθέσεων και νέων μέσων για την πραγματοποίηση αυτών.

7.2 Μελλοντικές επεκτάσεις

Γνωρίζοντας την σημαντικότητα και την αναγνώριση που λαμβάνει στις μέρες μας το blockchain, σαν πρόταση βελτιστοποίησης της παρούσας διπλωματικής προτείναμε την ενσωμάτωση του blockchain με το ERP. Λόγος αυτής της πρότασης είναι η αυξημένη ασφάλεια που προσφέρει η χρήση του blockchain και η ανάγκη που υπάρχει για καλύτερη ασφάλεια των ευαίσθητων δεδομένων που επεξεργάζονται οι εταιρείες στα ERP λογισμικά τους. Στην συνέχεια θα αναφέρουμε κάποια γενικά χαρακτηριστικά που θα μας βοηθήσουν να καταλάβουμε καλύτερα την έννοια και την χρησιμότητα του blockchain καθώς και το πως αυτό βοηθάει στην αύξηση της ασφάλειας. Τέλος, θα αναφερθούμε στον τρόπο που αυτό ενσωματώνεται με το ERP.

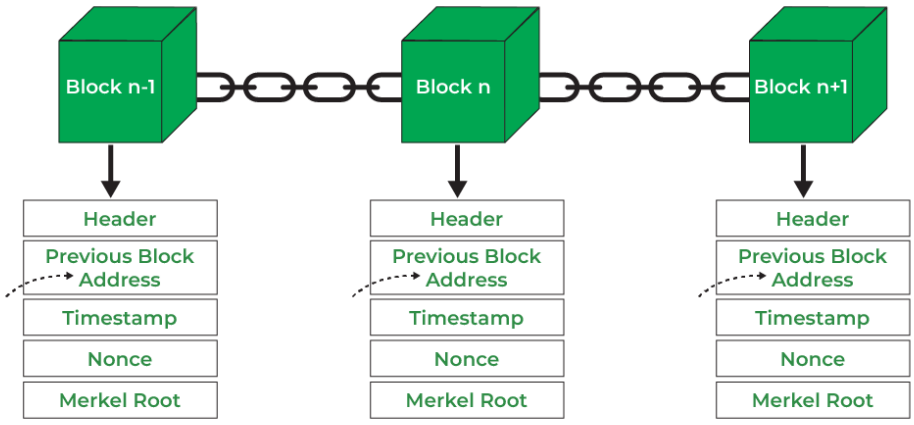
Το σημαντικότερο πλεονέκτημα του blockchain είναι ότι δεν έχει κεντρική βάση για την αποθήκευση των δεδομένων. Αντιθέτως, τα δεδομένα που θέλει να αποθηκεύσει κατανέμονται σε διασυνδεδεμένα μπλοκ, τα οποία συνδέονται μεταξύ τους σε μια αλυσίδα με τη χρήση περίπλοκων αλγορίθμων. Επιπλέον, κάθε μπλοκ αποθηκεύει ένα μικρό κομμάτι των δεδομένων. Υπάρχει η δυνατότητα της προσθήκης νέων μπλοκ στην αλυσίδα, αλλά είναι αδύνατο να τροποποιηθούν μετά την ενσωμάτωσή τους. Αυτός ο τρόπος παρέχει υψηλό επίπεδο ασφάλειας και προστασίας από επιθέσεις.

7.2.1 Χαρακτηριστικά του blockchain

Το blockchain, είναι μια τεχνολογία που βοηθά στην αποθήκευση και την ασφαλή κοινή χρήση ενός συνόλου δεδομένων. Δίνει την δυνατότητα στις εταιρείες να αποθηκεύουν μαζικά πληροφορίες σε ψηφιακή μορφή κάνοντας χρήση τα δομημένα κατανεμημένα block που υπάρχουν σε ένα δίκτυο blockchain. Τα block αυτά έχουν ορισμένη χωρητικότητα αποθήκευσης και όταν αυτό γεμίσει, κλείνει και συνδέεται με όλα τα προηγούμενα διαθέσιμα, σχηματίζοντας μια αλυσίδα.

Ο τρόπος δημιουργίας αυτών των block είναι και ο λόγος για τον οποίο το blockchain θεωρείται το ασφαλέστερο μέρος αποθήκευσης δεδομένων. Για την καλύτερη κατανόηση του τρόπου δημιουργίας των block ας υποθέσουμε ότι θέλουμε να πραγματοποιήσουμε μια συναλλαγή: Τα δεδομένα που είναι αποθηκευμένα σε μπλοκ μπορούν να προσπελαστούν με επαλήθευση, επικύρωση και συναίνεση από την αρχική οντότητα που θέλει να αποθηκεύσει ή να επεξεργαστεί τα δεδομένα. Για κάθε νέο αίτημα συναλλαγής και κάνοντας χρήση της τεχνολογία του blockchain, δημιουργούνται block πληροφοριών στο δίκτυο για την αποθήκευση των δεδομένων αυτής της συναλλαγής, η οποία στην συνέχεια μεταδίδεται σε ένα ομότιμο δίκτυο υπολογιστών. Έπειτα, στέλνοντας αυτό το block σε κάθε κόμβο στο κατανεμημένο δίκτυο, το δίκτυο αυτό καλείται να επικυρώσει την εγκυρότητα της συναλλαγής. Τέλος, μετά την επιβεβαίωση της εγκυρότητας, τα block συνδέονται μεταξύ τους και προστίθενται στην υπάρχουσα αλυσίδα.

Με άλλα λόγια, η αυξημένη ασφάλεια του blockchain προέρχεται από το γεγονός ότι καμία τροποποίηση δεν μπορεί να πραγματοποιηθεί αν δεν έχει πάρει έγκριση από την πλειοψηφία των block της αλυσίδας. Και επιπλέον, πέρα της έγκρισης που απαιτείται, γίνεται χρήση και ειδικών εξελιγμένων μαθηματικών πράξεων και τεχνολογιών λογισμικού πράγμα που καθιστά την τροποποίηση των block δύσκολη.



Σχήμα 7.1: Αρχιτεκτονική του blockchain

7.2.2 Ενσωμάτωση του blockchain με το ERP

Στόχος αυτής της ενσωμάτωσης είναι η παροχή αυξημένης ασφάλειας για την προστασία των ευαίσθητων δεδομένων που διαχειρίζεται ένα ERP σύστημα. Οι εταιρείες ανάπτυξης ERP λογισμικών παρέχουν την καλύτερη δυνατή ασφάλεια που μπορούν, όμως αυτό δεν είναι πάντα αρκετό. Γι΄αυτό τον λόγο η τεχνολογία του blockchain έρχεται να βοηθήσει τις εταιρείες στην παροχή αυξημένης ασφάλειας.

Επιπλέον, η ενσωμάτωση του blockchain με τα ERP συστήματα πέραν από την ασφάλεια που ήδη αναφέραμε ότι προσφέρει, προσφέρει επίσης και την δυνατότητα της ιχνηλάτισης των αρχείων, του ελέγχου πρόσβασης και του ελέγχου της ταυτότητας διαχείρισης, την δυνατότητα διαλειτουργικότητας των δεδομένων και τον διαμοιρασμό των πληροφοριών, την δυνατότητα συμμόρφωσης με τους κανονισμούς ασφαλείας (GDPR) και τέλος δίνει την δυνατότητα για βελτίωση των οικονομικών συναλλαγών. Αναλυτικότερα για το καθένα:

Αυξημένη ασφάλεια.

1. Το blockchain έχει την δυνατότητα να επικυρώνει τις συναλλαγές και παράλληλα να δημιουργεί αμετάβλητα αρχεία δεδομένων τα οποία διαμοιράζονται μεταξύ των διάφορων block. Αυτό παρέχει την δυνατότητα του άμεσου εντοπισμού οποιασδήποτε τυχόν αλλαγής μπορεί να γίνει στο περιεχόμενο των block.
2. Με την δυνατότητα που παρέχει για τον έλεγχο πρόσβασης και της ταυτότητας του προσώπου, αυξάνεται η ασφάλεια στην πρόσβαση των ευαίσθητων πληροφοριών της εταιρείας. Ο έλεγχος αυτός γίνεται με την χρήση ψηφιακών υπογραφών οι οποίες στηρίζονται στην κρυπτογράφηση του δημόσιου κλειδιού καθώς και στον έλεγχο ότι το ιδιωτικό κλειδί είναι σωστό. Με άλλα λόγια, κάτοχος της πληροφορίας είναι αυτός που έχει πρόσβαση στο ιδιωτικό κλειδί.
3. Επιπλέον, με την δυνατότητα της διαλειτουργικότητας των δεδομένων και τον διαμοιρασμό των πληροφορίων, παρέχετε στις εταιρείες ένα ασφαλές κανάλι ανταλλαγής δεδομένων. Ακόμη και αν τα ERP συστήματα που θέλουν να επικοινωνήσουν είναι διαφορετικά μεταξύ τους, το blockchain λειτουργεί ως ενδιάμεσος κόμβος και τους παρέχει την δυνατότητα επικοινωνίας. Επιπροσθέτως, εξασφαλίζεται ένα ανώτατο επίπεδο ελέγχου πρόσβασης και άρα η ανταλλαγή των πληροφοριών μέσω αυτού του καναλιού θεωρείται αξιόπιστη.
4. Όσον αφορά την συμμόρφωση με τους κανονισμούς ασφαλείας, το blockchain δίνει την δυνατότητα αποθήκευσης των ευαίσθητων πληροφοριών σε ένα ασφαλές μέρος αποτρέποντας έτσι την ανάγνωση αυτών από τρίτες εταιρείες για σκοπούς marketing.
5. Τέλος, η ενσωμάτωση του blockchain με το ERP παρέχει την δυνατότητα ασφαλέστερων και γρηγορότερων οικονομικών συναλλαγών. Επιπλέον χάρη στου ότι το blockchain παρέχει την δυνατότητα ιχνηλάτισης αρχείων, επιτρέπει την ευκολότερη παρακολούθηση και διαχείριση των συναλλαγών.

Επιπροσθέτως, χάρης του ότι το blockchain αποθηκεύει τα δεδομένα με την μορφή αλυσίδας και χάρη στη χρήση της κρυπτογραφίας και της επικύρωσης, παρέχει την δυνατότητα της αποτροπής τυχόν διαρροής των δεδομένων από μη εξουσιοδοτημένους χρήστες

Σχήμα 7.2: Λόγοι ενσωμάτωσης του blockchain με το ERP

Για όλους αυτούς τους λόγους, πιστεύεται ότι η ενσωμάτωση της blockchain τεχνολογίας με τα ERP συστήματα θα βοηθήσει θετικά στην βελτιστοποίηση της ασφάλειας των επιχειρησιακών λογισμικών.

Βιβλιογραφία

[1] A. Elragal and M. Haddara, "The Future of ERP Systems: look backward before moving forward," *Procedia Technology*, vol. 5, pp. 21-30, 2012.

[2] Τσώνης Χ.. SAP ERP «Η ΧΡΗΣΗ ΤΟΥ ΚΑΙ Η ΕΞΕΛΙΞΗ ΤΟΥ ΣΤΙΣ ΣΥΓΧΡΟΝΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ». (Πτυχιακή εργασία). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ- ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ.*

[3] Καραμπίνης Ν.. ΒΙΟΜΗΧΑΝΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑ. (Διπλωματική Διατριβή). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ- ΣΧΟΛΗ ΝΑΥΤΙΛΙΑΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΑΣ.*

[4] What is ERP?. *ORACLE*, 2023. https://www.oracle.com/erp/what-is-erp/ Επίσκεψη 20/2/2023.

[5] What is ERP?. *SAP*. https://www.sap.com/products/erp/what-is-erp.html Επίσκεψη 20/2/2023.

[6] What is ERP?. *MICROSOFT DYNAMIC 365*. https://dynamics.microsoft.com/en-us/erp/what-is-erp/ Επίσκεψη 20/2/2023.

[7] Entersoft Business Suite. https://www.entersoft.gr/products/business-suite/?gclid=Cj0KCQiAsdKbBhDHARIsANJ6-jcCdLB-vNGGu0auHWfKbkilFsy9QO8tcr-xl0WcZaTKKrM5Zduo8a8aAtFSEALw_wcB Επίσκεψη 20/2/2023.

[8] Καρτσάνης Χ.. (2020). Η Χρήση Εργαλείων Επιχειρηματικής Ευφυΐας SAP στη Διαδικασία Λήψης Αποφάσεων. (Μεταπτυχιακή εργασία). *Εθνικό Μετσόβιο Πολυτεχνείο- ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ.*

[9] F. Jingga and N. Limantara, "The Implementation of ERP Systems using ASAP Methodology," In Proc. International Conference on Information Management and Technology, 2016, pp. 23-28.

[10] S. Nagpal, S. K. Khatri and A. Kumar "Comparative study of ERP implementation strategies," In Proc. Long Island Systems, Applications and Technology, 2015, pp. 1-9.

[11] A. Elragal and E.M. Kommos, "In-house versus In-cloud ERP systems: A comparative study," *Journal of Enterprise Resource Planning Studies*, 2012.

[12] H. Tuttle, D. Fiddick and M.M. Katzman, "Critical Success Factors In Implementing

SAP ERP Software," *Engineering Management Field Project*, 2009.

[13] S. Matende and P. Ogao, "Enterprise Resource Planning (ERP) System Implementation: A Case for User Participation," *Procedia Technology*, vol. 9, pp. 518-526, 2013.

[14] M. Ali and L. Miller, "ERP system implementation in large enterprises: a systematic literature review," *Journal of Enterprise Information Management*, vol. 30, pp. 666-692, 2017.

[15] K. Jagoda and P. Samaranayake, "An integrated framework for ERP system implementation," *International Journal of Accounting & Information Management*, vol. 25, pp. 91-109, 2017.

[16] Μανώλη Α. και Σιδηροπούλου Ι.. (2017). ΥΛΟΠΟΙΗΣΗ ΕΚΠΑΙΔΕΥΤΙΚΩΝ ΣΕΝΑΡΙΩΝ ΧΡΗΣΗΣ ΥΠΟΣΥΣΤΗΜΑΤΩΝ ΤΟΥ CLOUD ERP ΣΥΣΤΗΜΑΤΟΣ SOFTONE. (Διπλωματική εργασία). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ*.

[17] Φιτσιλής Π.. (2015). Σύγχρονα Πληροφοριακά Συστήματα Επιχειρήσεων. *Εθνικό Μετσόβιο Πολυτεχνείο- Ελληνικά ακαδημαϊκά ηλεκτρονικά συγγράμματα και βοηθήματα ΕΚΔΟΣΕΙΣ kallipos*

[18] Atlantis E.R.P. *SOFTONE*. https://eatlantis.softone.gr/pages/loadpage.asp?id=1272 Επίσκεψη 2/3/2023.

[19] Τσολέκα Α.. (2017). ΔΙΑΧΕΙΡΙΣΗ ΒΑΣΕΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΑ ERP ΠΡΟΓΡΑΜΜΑΤΑ ΚΑΙ ΣΧΕΔΙΑΣΗ ΕΚΤΥΠΩΣΕΩΝ(SOFT1, ATLANTIS ΚΑΙ ODOO). (Διπλωματική εργασία). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ*.

[20] W.Y. Alhayek and R.A.A. Oden, "Cloud ERP VS On-Premise ERP," *International Journal of Applied Science and Technology*, vol. 10, pp. 55-60, 2020.

[21] M.J. Lee, W.Y. Wong and M.H. Hoo, "Next Era Rf Enterprise Resource Planning System review on traditional on-premise ERP versus cloud-based ERP: Factors influence decision on migration to cloud-based ERP for Malaysian SMEs/SMIs," In Proc. IEEE Conference on Systems, Process and Control, 2017, pp. 48-53.

[22] How Cloud ERP Compares to On-premise ERP. *ORACLE*, 2016. https://www.netsuite.com/portal/resource/articles/cloud-saas/on-premise-cloud-erp.shtml Επίσκεψη 4/3/2023

[23] Καλογερά Ε.. (2021). Συστήματα ERP Συγκριτική Μελέτη & Ανάλυση. (Διπλωματική εργασία). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ*.

[24] Σαραντίδης Α.. (2011). ΕΦΑΡΜΟΓΕΣ ΛΟΓΙΣΜΙΚΟΥ ERP ΣΤΗΝ ΠΑΡΑΓΩΓΙΚΗ ΔΙΑΔΙΚΑΣΙΑ ΓΡΑΦΙΚΩΝ ΤΕΧΝΩΝ ΤΗΣ «ARTION ΑΒΕΕΕ». (Πτυχιακή εργασία). *ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ- ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ*.

[25] Καντσού Ε.Α.. (2016). ΔΙΕΡΕΥΝΙΣΗ ΤΩΝ ΠΑΡΑΓΟΝΤΩΝ ΠΟΥ ΣΥΜΒΑΛΟΥΝ ΣΤΗΝ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΧΡΗΣΗ ΤΩΝ ERP ΣΥΣΤΗΜΑΤΩΝ ΣΤΟΝ ΚΛΑΔΟ ΤΟΥ ΛΙΑΝΙΚΟΥ ΕΜΠΟΡΙΟΥ ΕΝΔΥΣΗΣ. *Τ.Ε.Ι ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ- ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ*.

[26] Λούκης Ε., Ανδριτσάκης Α., Διαμαντοπούλου Β.. (2009). Ολοκληρωμένη Μηχανογραφική Υποστήριξη Επιχειρήσεων με SAP. *NewTech Pub ΕΚΔΟΣΕΙΣ ΝΕΩΝ ΤΕΧΝΟΛΟΓΙΩΝ*. 13-34.

[27] ΠΑΠΑΔΟΠΟΥΛΟΣ Γ.. (2012). Η ΕΠΙΔΡΑΣΗ ΤΩΝ ΣΥΣΤΗΜΑΤΩΝ ERP (ENTERPRISE RESOURCE PLANNING) ΣΤΟΝ ΕΣΩΤΕΡΙΚΟ ΕΛΕΓΧΟ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ. (Διπλωματική εργασία). *ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ*.

[28] Πένος Π.. (2010). ΕΠΙΛΟΓΗ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ(ERP). (Διπλωματική εργασία). *ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ*.

[29] What is data security? *IBM*. https://www.ibm.com/topics/data-security Επίσκεψη 10/3/2023.

[30] What is data security? The ultimate guide. *TechTarget*. https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know Επίσκεψη 10/3/2023

[31] Μπαριτάκη Μ.. (2020). Η ΣΥΓΚΡΟΥΣΗ ΤΗΣ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ ΜΕ ΤΑ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ. (Διπλωματική εργασία). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ*.

[32] Αθανασάκη Γ.. (2012). ΔΗΜΟΣΙΑ ΑΝΟΙΧΤΑ ΔΕΔΟΜΕΝΑ: ΠΡΩΤΟΒΟΥΛΙΕΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ. (Διπλωματική εργασία). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ*.

[33] Reducing the risks of cybersecurity threats. *Infor*. https://webassets.infor.com/resources/Infographics/Reducing-risks-of-cybersecurity-threats.pdf?mtime=20200219072247&focal=none&_ga=2.27196981.988468769.1626360758-2037298304.1620864820&fbclid=IwAR2IZdBoSiwql3gB2o9S6kxbb3QE7SnYo-ydfxez2Mfc0yFrEAl9IKK1_dk Επίσκεψη 12/3/2023.

[34] 10 most powerful ERP vendors today. *CIO*, 2022. https://www.cio.com/article/304902/10-most-powerful-erp-vendors-today.html Επίσκεψη 15/3/2023.

[35] Database Security Guide. *ORACLE*, 2017. https://docs.oracle.com/database/121/DBSEG/vpd.htm#DBSEG007 Επίσκεψη 16/3/2023.

[36] Oracle Corporation, "Oracle Database Security Guide," 2003.

[37] Security Policy. *SAP*. https://help.sap.com/docs/INTELLIGENT_SALES_EXECUTION/97d2089d85b543089bd4e59be5c5f1e5/bc0bf033dbf1403bab90946ba7411b39.html?locale=en-US&q=security%20policy Επίσκεψη 20/3/2023.

[38] Workday Security and Data Privacy. *Workday*, 2019. https://www.workday.com/content/dam/web/en-us/documents/datasheets/datasheet-workday-security.pdf Επίσκεψη 20/3/2023.

[39] Infor cloud security. *Infor*, 2023. https://trust.infor.com/ Επίσκεψη 20/3/2023.

[40] Security Policies Properties. *MICROSOFT LEARN*, 2018. https://learn.microsoft.com/en-us/dynamicsax-2012/developer/security-policies-properties Επίσκεψη 20/3/2023.

[41] Ensure ERP security with trusted software from Sage. *Sage*. https://www.sage.com/en-gb/erp/security/ Επίσκεψη 20/3/2023.

[42] M. Heikkila, A. Rattya, S. Pieska and J. Jamsa, "Security challenges in small- and medium-sized manufacturing enterprises," In Proc. International Symposium on Small-scale Intelligent Manufacturing Systems, 2016, pp. 25-30.

[43] I.M. Lopes, T. Guarda and P. Oliveira, "How ISO 27001 Can Help Achieve GDPR Compliance," In Proc. 14th Iberian Conference on Information Systems and Technologies, 2019, pp. 1-6.

[44] I. Stankov and G. Tsochev, "Vulnerability and Protection of Business Management Systems: Threats and Challenges," *BULGARIAN ACADEMY OF SCIENCES*, vol. 72, pp. 29-40, 2020.

[45] Ασφάλεια ERP σε έναν κόσμο ηλεκτρονικού εγκλήματος. *SAP*. https://wwwa.sap.com/greece/insights/erp-security.html Επίσκεψη 25/3/2023.

[46] Top ERP Security Problems and Best Practices. *ORACLE*, 2022. https://www.netsuite.com/portal/resource/articles/erp/erp-security-best-practices.shtml?fbclid=IwAR2QY4qqB8-HDG4ON3nfBdL-Lz-vGEcmeyaasJNPl8e7EH3CIIjM0BTC6EI Επίσκεψη 25/3/2023.

[47] CVE. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=erp Επίσκεψη 30/3/2023.

[48] Exploit Database. https://www.exploit-db.com/ Επίσκεψη 30/3/2023.

[49] Δημητριάδης Α.. (2017). Αξιοποίηση της ηλεκτρονικής εγκληματολογίας για την προληπτική αντιμετώπιση εκτεταμένων απειλών. (Διπλωματική εργασία). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ*.

[50] I. Tarnowski, "How to use cyber kill chain model to build cybersecurity?," *European Journal of Higher Education IT*, 2017.

[51] W. G. Mueller, A. Memory and K. Bartrem, "Causal Discovery of Cyber Attack Phases," In Proc. 18th IEEE International Conference On Machine Learning And Applications, 2019, pp. 1348-1352.

[52] T. Yadav and A.M. Rao, "Technical Aspects of Cyber Kill Chain," In Proc. Security in Computing and Communications-Communications in Computer and Information Science, 2015, pp. 438-452.

[53] D. Kiwia, A. Dehghantanha, K.L.R. Choo and J. Slaughter, "A cyber kill chain-based taxonomy of banking Trojans for evolutionary computational intelligence," *Journal of Computational Science*, vol. 27, pp. 394-409, 2018.

[54] T. Dargahi, A. Dehghantanha, P.N. Bahrami, M. Conti, G. Bianch and L. Benedetto, "A Cyber-Kill-Chain based taxonomy of crypto-ransomware features," *J Comput Virol Hack Tech, vol.* 15, pp. 277–305, 2019.

[55] P.N. Bahrami, A. Dehghantanha, T. Dargahi, R.M. Parizi, K.K.R. Choo and H.H.S. Javadi, "Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures," *Journal of Information Processing Systems*, vol. 4, pp. 865-889, 2019.

[56] T. Gunasekhar, K. T. Rao and M.T. Basu, "Understanding insider attack problem and scope in cloud," In Proc. International Conference on Circuits, Power and Computing Technologies, 2015, pp. 1-6.

[57] A. J Duncan, S. Creese and M. Goldsmith, "Insider Attacks in Cloud Computing," In Proc. IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 857-862.

[58] Μπαμπούρης Μ.. (2022). Attack Surface Management and Penetration Testing with Sn1per. (Μεταπτυχιακή Διπλωματική εργασία). *Πανεπιστήμιο Δυτικής Αττικής*.

[59] J. R. C. Nurse, O. Buckley, P.A. Legg, M. Goldsmith, S. Creese, G.R.T. Wright and M. Whitty, "Understanding Insider Threat: A Framework for Characterising Attacks," In Proc. IEEE Security and Privacy Workshops, 2014, pp. 214-228.

[60] S. Mathew, M. Petropoulos, H.Q. Ngo and S. Upadhyaya, "A Data-Centric Approach to Insider Attack Detection in Database Systems," In Proc. Recent Advances in Intrusion Detection, 2010.

[61] Z.M. Yusop and J. Abawajy "Analysis of Insiders Attack Mitigation Strategies," *Procedia - Social and Behavioral Sciences*, vol. 129, pp. 581-591, 2014.

[62] A. Georgiadou, S. Mouzakitis and D. Askounis, "Detecting Insider Threat via a Cyber-Security Culture Framework," *Journal of Computer Information Systems*, vol. 62, pp. 706-716, 2022.

[63] Capella University, "EXPLORING THE APPLICATION OF INFORMATION SECURITY GOVERNANCE IN MITIGATING INSIDER NEGLIGENCE THREATS: A QUALITATIVE ANALYSIS". 2019.

[64] A. Munshi, P. Dell and H. Armstrong, "Insider Threat Behavior Factors: A Comparison of Theory with Reported Incidents," In Proc. 45th Hawaii International Conference on System Sciences, 2012, pp. 2402-2411.

[65] G. Maclachlan, "Scandal, Spyware and Trust," *Infosecurity*, vol. 8, pp. 45, 2011.

[66] K. M. Sudar, P. Deepalakshmi, P. Nagaraj and V. Muneeswaran, "Analysis of Cyberattacks and its Detection Mechanisms," *Fifth International Conference on Research in Computational Intelligence and Communication Networks* 2020, pp. 12-16.

[67] S. R. Subramanya and N. Lakshminarasimhan, "Computer viruses," *IEEE Potentials*, vol. 20, pp. 16-19, 2001.

[68] East Carolina University, "Computer Worms: Past, Present, and Future," 2005.

[69] M. Conti, N. Dragoni and V. Lesyk "A Survey of Man In The Middle Attacks," *IEEE Communications Surveys & Tutorials*, vol. 18, pp. 2027-2051, 2016.

[70] H. Teymourlouri, "Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users," *World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering*, vol. 9, pp. 678-684, 2015.

[71] Γεωργιάδου Μ. και Ζιαζιάς Α.. (2007). Ασφάλεια στα διαδίκτυο. (Διπλωματική εργασία). *ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ.*

[72] Διαβάτη Παρασκευή.. (2021). Κυβερνοτρομοκρατία. (Διπλωματική εργασία). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ.*

[73] M. Raza, M. Iqbal, M. Sharif and W. Haider, "A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication," *World Applied Sciences Journal*, vol. 19, no. 4, pp. 439-444, 2012.

[74] Μπασδάρας Π.. (2017). Εκτιμώντας τις συνέπειες των κυβερνοεπιθέσεων σε μια εταιρεία και την προστασία της. (Διπλωματική εργασία). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ.*

[75] H. Saini, Y.S. Rao and T.C. Panda, "Cyber-Crimes and their Impacts: A Review," *International Journal of Engineering Research and Applications,* vol. 2, pp. 202-209, 2012.

[76] C.H. Ganan, M. Ciere and M.V Eeten, "Beyond the pretty penny: the Economic Impact of Cybercrime," In Proc NSPW, 2017, pp. 35-44.

[77] S. Das and T. Nayak T. "Impact of Cyber Crime: Issues and challenges*," International Journal of Engineering Sciences & Emerging Technologies*, vol. 6, pp. 142-153, 2013.

[78] Elamin A.. (2020). Ανάλυση Οικονομικών Επιπτώσεων Κυβερνοεπίθεσης σε Διεθνείς Οργανισμούς και Επιχειρήσεις & Μέθοδοι Προστασίας Προσωπικών Δεδομένων. *Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης*.

[79] Hamilton Place Strategies Report, "Cybercrime costs more than you think," 2016.

[80] N.K. Popli and Dr. A. Girdhar, "THE HARMFUL EFFECTS OF CYBER CRIME IN BUSINESS AND ECONOMIC SUSTAINABILITY," *ABS International Journal of Management*, vol. 5, pp. 74-76, 2017.

[81] H. Saleh, A. Rezk and S. Barakat, "THE IMPACT OF CYBER CRIME ON E-COMMERCE," *International Journal of Intelligent Computing and Information Science*, vol. 17, no. 3, pp. 85-96 2017.

[82] A. D. Smith, "Cybercriminal impacts on online business and consumer confidence," *Online Information Review*, vol. 28, no. 3, pp. 224-234, 2004.

[83] J. B. Hill, & N. E. Marion, *Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century*. PSI Textbooks- PRAEGER SECURITY INTERNATIONAL. 2016.

[84] What is data security? The ultimate guide. *TechTarget*. https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know Επίσκεψη 10/3/2023.

[85] 8 ERP security best practices to implement now. *TechTarget*. 8 ERP security best practices to implement now | TechTarget Επίσκεψη 10/3/2023.

[86] Εγχειρίδιο Κυβερνοασφάλειας. *Ελληνική Δημοκρατία.* https://mindigital.gr/wp-content/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf Επίσκεψη 10/4/2023.

[87] R. S. Sandhu and P. Samarati, "Access control: principle and practice," *IEEE communications magazine*, vol. 32, no. 9, pp. 40-48, 1994.

[88] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," 2020.

[89] National Institute of Standards and Technology, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". 2020.

[90] Using the Information Security Manual. *Australian Cyber Security Center*, 2023. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/using-information-security-manual Επίσκεψη 13/4/2023.

[91] P. Samarati, and S.C. Vimercati, "Access control: Policies, models, and mechanisms," In Proc. Foundations of Security Analysis and Design, 2001, pp. 137-196.

[92] S. Osborn, R. Sandhu and Q. Munawer, "Configuring role-based access control to enforce mandatory and discretionary access control policies," *ACM Transactions on Information and System Security*, vol. 3, no. 2, pp. 85-106, 2000.

[93] D. Dasgupta, A. Roy, and A. Nag, "Advances in user authentication," *Springer International Publishing*, 2017.

[94] J.M. Kizza, "Guide to computer network security," *Springer Nature Switzerland*, 2013.

[95] M. Ciampa, *Security+ Guide to Network Security Fundamentals*. PREPARING-TOMORROW'S-INFORMATION SECURITY PROFESSIONAL 2012.

[96] C. Theisen, N. Munaiah, M. Al-Zyoud, J. C. Carver, A. Meneely and L. Williams "Attack surface definitions: A systematic literature review," *Information and Software Technology*, vol. 104, pp. 94-103, 2018.

[97] UNITED STATES OF AMERICA, "NATIONAL SECURITY AGENCY - CYBERSECURITY INFORMATION," 2018.

[98] CISA, "Guidance for Securing Video Conferencing," 2020.

[99] Λιάγκου Β.. (2008). Ασφαλή και Έμπιστα Πρωτόκολλα Επικοινωνιών με Χρήση Κρυπτογραφίας και Κρυπτανάλυσης. (Διδακτορική Διατριβή). *Πανεπιστήμιο Πατρών.*

[100] Μπατσάρης Π.Δ.. (2006). Η επιστήμη της κρυπτογραφίας και ο κρυπταλγόριθμος RSA. (Μεταπτυχιακή εργασία). *Πανεπιστήμιο Μακεδονίας.*

[101] Μπρεχού Δ.. (2022). Στρατηγική της Κυβερνοασφάλειας στην ΕΕ. (Διπλωματική εργασία). *ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ.*

[102] Enisa.. (2021). Συνεργασία για την αύξηση της ευαισθητοποίησης σχετικά με τις κυβερνοαπειλές: ευρωπαϊκός μήνας κυβερνοασφάλειας 2021. *Europian Commission.*

[103] Μαυρίδης Ι.. (2015). Ασφάλεια Πληροφοριών στο Διαδίκτυο. *ΕΚΔΟΣΕΙΣ Kallipos*, 223.

[104] J. Thomas and G. Galligher, "Improving backup system evaluations in information security risk assessments to combat ransomware," *Computer and Information Science*, vol. 11, no. 1, 2018.

[105] Y. Wang, B. Rawal, Q. Duan, and P. Zhang, "Usability and security go together: A case study on database," In Proc. Second International Conference on Recent Trends and Challenges in Computational Models, 2017, pp. 49-54.

[106] S.M. Hawkins, D.C. Yen, and D.C. Chou, "Disaster recovery planning: a strategy for data security," *Information management & computer security*, vol. 8, no. 5, pp. 222-230, 2000.

[107] E. Politou, A. Michota, E. Alepis, M. Pocs and C. Patsakis, “Backups and the right to be forgotten in the GDPR: An uneasy relationship,” *Computer Law & Security Review*, vol. 34, no. 6, pp. 1247-1257, 2018.

[108] UNITED STATES COMPUTER EMERGENCY READINESS TEAM, “Data Backup Options,” 2012.

[109] Γκουτζαμάνης Ι.. (2018). Κακόβουλο Λογισμικό - Πολιτικές Ασφάλειας & Μέτρα Προστασίας Μελέτη περίπτωσης σε Πληροφοριακό Σύστημα. (Διπλωματική εργασία). *Πανεπιστήμιο Θεσσαλίας-Σχολή Θετικών Επιστημών.*

[110] Βατικιώτης Φ.. (2015). Υπολογιστική ανάλυση και μοντελοποίηση της συμπεριφοράς καταγραφής συμβάντων ιστοσελίδων του διαδικτύου με τεχνικές εξόρυξης δεδομένων (Data Mining). (Διπλωματική εργασία). *Εθνικό Μετσόβιο Πολυτεχνείο*.

[111] J. Srinivas, A.K. Das and N. Kumar, “Government regulations in cyber security: Framework, standards and recommendations,” *Future generation computer systems*, vol. 92, pp. 178-188, 2019.

[112] B. Krumay, E.W. Bernroider, and R. Walser “Evaluation of cybersecurity management controls and metrics of critical infrastructures: A literature review considering the NIST cybersecurity framework,” In Proc. Secure IT Systems: 23rd Nordic Conference, 2018, pp. 369-384.

[113] J. Webb and D. Hume, “Campus IoT collaboration and governance using the NIST cybersecurity framework,” In Proc. Living in the Internet of Things: Cybersecurity of the IoT-2018, 2018, pp. 1-7.

[114] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” 2018.

[115] L.A. Gordon, M.P. Loeb and L. Zhou, “Integrating cost-benefit analysis into the NIST Cybersecurity Framework,” *Journal of Cybersecurity*, pp. 1-8, 2020.

[116] C. Liu, C.K. Tan, Y.S. Fang and T.S. Lok, “The security risk assessment methodology,” *Procedia Engineering*, vol. 43, pp. 600-609, 2012.

[117] Κουναλάκης Ν.Α. και Χαρίτος Ε.Δ.. (2022). Κυβερνοασφάλεια στην Ναυτιλία. (Μεταπτυχιακή Διπλωματική Εργασία). *Πανεπιστήμιο Δυτικής Αττικής*.

[118] M. Jones-Lee and T. Aven, “ALARP- What does it really mean?,” *Reliability Engineering & System Safety*, vol. 96, no. 8, pp. 877-882, 2011.

[119] Τριανταφύλλου Δ.Ν.. (2011). Το ηλεκτρονικό εμπόριο ως εργαλείο εξέλιξης. (Πτυχιακή εργασία). *Τεχνολογικό εκπαιδευτικό ίδρυμα Κρήτης.*

[120] Τσαμπίκος Ρ.Μ και Χατζηπαναγιώτου Ε.. (2014). Ηλεκτρονική τιμολόγηση. (Πτυχιακή εργασία). *Τεχνολογικό εκπαιδευτικό ίδρυμα Κρήτης.*

[121] Z. Vanjak, V. Mornar and I. Magdalenic, “Deployment of e-invoice in Croatia,” In Proc. International Conference on Software and Data Technologies, 2008, pp. 348-354.

[122] Σαρηγιαννίδης Α.. (2022). Ασφάλεια δικτύων και επικοινωνιών. *Διεθνές πανεπιστήμιο της Ελλάδος*.

[123] P. Anu and S. Vimala, "A survey on sniffing attacks on computer networks," In Proc. 2017 International Conference on Intelligent Computing and Control, 2017, pp. 1-5.

[124] E. Padma, "A servey on Botnet Attack," *International journal of information and computing sciensce*, vol. 6, no. 4, pp. 72-77, 2019.

[125] H.N. Dai, Q. Wang, D. Li and R.C.W. Wong, "On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas," *International Journal of Distributed Sensor Networks*, vol. 9, no. 8, 2013.

[126] Τζωρτζάκος Φ.Π.. (2013). Ηλεκτρονική τιμολόγηση στα κινητά περιβάλλοντα. (Μεταπτυχιακή Διατριβή). *Πανεπιστήμιο Πειραιώς.*

[127] Ζυγούρη Χ.. (2013). Ηλεκτρονική τιμολόγηση στον Ενιαίο χώρο Πληρωμών σε Ευρώ. (Μεταπτυχιακή Διατριβή). *Πανεπιστήμιο Πειραιώς.*

[128] Κοκώνη Α.. (2021). ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ ΜΕ ΒΑΣΗ ΤΟ ΕΛΛΗΝΙΚΟ ΚΑΙ ΕΥΡΩΠΑΪΚΟ ΝΟΜΟΘΕΤΙΚΟ ΠΛΑΙΣΙΟ - Ο ΒΑΘΜΟΣ ΑΝΑΠΤΥΞΗΣ ΤΩΝ ΨΗΦΙΑΚΩΝ ΥΠΟΓΡΑΦΩΝ ΣΤΟΝ ΔΗΜΟΣΙΟ ΚΑΙ ΙΔΙΩΤΙΚΟ ΤΟΜΕΑ. (Διπλωματική εργασία). *Πανεπιστήμιο Αιγαίου.*

[129] Κουτίδου Σ.. (2019). Ψηφιακή υπογραφή και κρυπτογραφία. (Διπλωματική εργασία). *Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.*

[130] R. Stephen and A. Alex, "A Review on BlockChain Security," In Proc. IOP Conference Series: Material Science and Engineering, 2018, vol. 396.

[131] D. Rodeck and B. Curry, "What is Blockchain," *Forbes*, 2022.

[132] S. Demirkan, I. Demirkan and A. McKee, "Blockchain technology in the future of business cyber security and accounting," *Journal of Management Analytics*, vol. 7, no. 2, pp. 189-208, 2020.

[133] T.K. Dasaklis, T.G. Voutinas and A. Mihiotis, "Integrating blockchain with Enterprise Resource Planning systems: benefits and challenges," *Laboratory of Management and Public Administration, School of Social Sciences, Hellenic Open University Patra*, 2021.

[134] Z. Wang, Z. Zheng, W. Jiang and S. Tang, "Blockchain-Enabled Data Sharing in Supply Chains:Model, Operationalization, and Tutorial," *Production and Operations Management Society*, vol. 30, no. 7, pp. 1965-1985, 2021.

[135] T. Parikh, "The ERP of the Future : Blockchain of Things," *Department of Computer Science - Gujarat Technological University*, vol. 4, no. 1, pp. 1341-1348, 2018.

[136] T. Kitsantas, "Exploring Blockchain Technology and Enterprise Resource Planning System: Business and Technical Aspects, Current Problems, and Future Perspectives," *School of Information Sciences, Department of Applied Informatics, University of Macedonia*, vol. 14, 2022.

[137] A. Faccia and P. Petratos, "Blockchain, enterprise resource planning (ERP) and accounting information systems (AIS)," *Applied Sciences (Switzerland)*, vol. 11, no. 15, 2021.

Εικόνες

[138] Insider Threat. *Impreva*. https://www.imperva.com/learn/application-security/insider-threats/ Επίσκεψη 20/3/2023

[139] Sap B1 ERP Implementation. *SAP*. https://www.leapingfrogconsulting.com/erp-services/implementation Επίσκεψη 20/2/2023

[140] What is a Firewall and How does it Work?. *Wallarm*. https://www.wallarm.com/what/the-concept-of-a-firewall Επίσκεψη 16/3/2023

[141] What is multifactor authentication (MFA)?. *Wallarm*. https://www.wallarm.com/what/what-is-multifactor-authentication-mfa Επίσκεψη 16/3/2023

[142] Κώδικας του Καίσαρα. *ΒΙΚΙΠΑΙΔΕΙΑ*. 2023. https://el.wikipedia.org/wiki/%CE%9A%CF%8E%CE%B4%CE%B9%CE%BA%CE%B1%CF%82_%CF%84%CE%BF%CF%85_%CE%9A%CE%B1%CE%AF%CF%83%CE%B1%CF%81%CE%B1 Επίσκεψη 16/3/2023

[143] Συστήματα ERP: Γιατί είναι τόσο σημαντικά για τις επιχειρήσεις;. *TSOUK.GR*. 2022. https://www.tsouk.gr/systimata-erp-giati-einai-toso-simantika-gia-tis-epicheiriseis/ Επίσκεψη 20/2/2023

[144] Blockchain Structure. *Geeksforgeeks*. 2022. https://www.geeksforgeeks.org/blockchain-structure/ Επίσκεψη 18/5/2023

[145] Why Integrating ERP Systems into Blockchain Is a Great Idea?. *EOS Costa Rica*. 2019. https://eoscostarica.medium.com/why-integrating-erp-systems-into-blockchain-is-a-great-idea-e384b298a4a8 Επίσκεψη 18/5/2023