Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Οι Τεχνοοικονομικές Πλευρές της Κυβερνοασφάλειας

Παρασκευή Κοντογιάννη

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Μάιος 2018

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Ασφάλεια Υπολογιστών και Δικτύων

Μεταπτυχιακή Διατριβή

Οι Τεχνοοικονομικές Πλευρές της Κυβερνοασφάλειας

Παρασκευή Κοντογιάννη

Επιβλέπων Καθηγητής
Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών
στ… ……..
από τη Σχολή …….
του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2018

Περίληψη

Διανύοντας τον 21ο αιώνα, η ανάπτυξη της τεχνολογίας και η χρήση του διαδικτύου είναι πλέον γεγονός. Ολοένα και περισσότεροι είναι οι χρήστες και οι συσκευές που συνδέονται καθημερινά στο διαδίκτυο ανταλλάσσοντας συνεχώς δεδομένα και πληροφορία. Οι χρήστες οι οποίοι μπορεί να είναι από μεγάλοι οργανισμοί και το κράτος μέχρι μικρές επιχειρήσεις και μεμονωμένες οντότητες, προσπαθούν να διαφυλάξουν την πληροφορία τους από κακόβουλες εισβολές. Παρόλα αυτά, καθημερινά αναφέρονται περιστατικά ασφάλειας που στόχο έχουν να προκαλέσουν οικονομική απώλεια, διακοπή υπηρεσίας ή διαρροή ευαίσθητων δεδομένων. Αυτές είναι οι λεγόμενες κυβερνοεπιθέσεις που πραγματοποιούνται σε παγκόσμιο επίπεδο και με αρκετά μεγάλο ποσοστό χρηστών να έχει βρεθεί μπροστά σε ένα τέτοιο περιστατικό. Οι κακόβουλοι χρήστες εκμεταλλευόμενοι αδυναμίες και τρωτά σημεία των συστημάτων, επιτίθονται με βασικό σκοπό τη συλλογή απόρρητων δεδομένων και την πρόκληση ζημιάς στο στόχο-θύμα. Φαίνεται λοιπόν ότι υπάρχει ένα κενό στον τομέα της ασφάλειας το οποίο πρέπει να καθοριστεί και να βρεθεί μια λύση. Γίνεται προσπάθεια προστασίας των πληροφοριακών συστημάτων με την εφαρμογή ποικίλων μέσων και τεχνικών. Τέτοιες υλοποιήσεις μπορεί να είναι μηχανισμοί κρυπτογράφησης, τείχη προστασίας και μοντέλα ανίχνευσης εισβολών χωρίς όμως να παρέχουν την πλήρη κάλυψη και ασφάλεια των συστημάτων.

Στα πλαίσια της παρούσας διατριβής μελετάται η ασφάλεια του κυβερνοχώρου, παρουσιάζονται και αναλύονται τα πιο δημοφιλή είδη επιθέσεων καθώς και οι τεχνικές που εφαρμόζονται για την προστασία των συστημάτων. Επιπλέον προτείνονται νέες μέθοδοι βασισμένες σε προηγμένη τεχνολογία όπως η τεχνητή νοημοσύνη, τα συστήματα ασφάλειας πληροφοριών που θα μπορούσαν να χρησιμοποιηθούν ως αντίμετρα. Ωστόσο πριν την εφαρμογή των κατάλληλων μέτρων προστασίας θα πρέπει να εκτιμηθούν και οι δαπάνες των επιχειρήσεων στον τομέα της ασφάλειας. Για το λόγο αυτό μελετώνται ακόμα οικονομικοί δείκτες, γίνονται ποιοτικές και ποσοτικές αναλύσεις και μέθοδοι που καθορίζουν με ποιον τρόπο θα πρέπει να επενδύουν οι επιχειρήσεις ώστε να εξοικονομούν χρήματα και να ελαχιστοποιούν τις ζημιές τους.

Η κυβερνοασφάλεια είναι θέμα μείζονος σημασίας και πρέπει να αποτελεί βασική προτεραιότητα για κάθε επιχείρηση.

Summary

Throughout the 21st century, the rapid development of technology and the increased use of Internet is a fact. More and more users and devices are connected on the internet, exchanging information. Users, form large organizations and the governance to small businesses and individual entities try to keep this information secure from malicious intrusions. However, security incidents are daily reported causing financial loss, service interruption and leakage of sensitive data. Malicious users exploiting weaknesses and vulnerabilities of the systems are attacked in order to collect confidential date and damage the victim. So it seems to be a security gap that be defined and be found a solution. There is an effort to protect information systems by applying tools and techniques such as encryption mechanisms, firewalls, intrusion detection models but unfortunately do not provide extra coverage and system security. In this dissertation, cybersecurity is studied, being analyzed the most popular types of cyberattacks and the safeguards been applied in order businesses protect their systems. In addition, new methods based on advanced technology are proposed, as artificial intelligence and security intelligence systems that could be used as countermeasures. Before businesses decide which countermeasure fit their needs, security firms' costs should also be assessed. For this reason, economic indicators and models are studied, qualitative and quantitative analyzes and methods are developed that determine how companies should invest in saving money and minimizing the losses. Nowadays, cybersecurity is a major issue a priority for every business.

Ευχαριστίες

Θα ήθελα να σημειώσω ότι χωρίς την βοήθεια και συμβολή του καθηγητή μου κ. Νικόλαο Σκλάβο καθώς και την υποστήριξη της οικογένειας και των φίλων μου, δεν θα είχε ολοκληρωθεί η εκπόνηση αυτής της διατριβής.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή του θέματος της διατριβής που θα μελετηθεί. Επισημαίνεται ο σκοπός και η αναγκαιότητα της έρευνας, γίνεται μια ιστορική αναδρομή των επιθέσεων στον τομέα της ασφάλειας του κυβερνοχώρου και δίνεται μια εξήγηση για το λόγο που αυξάνονται τόσο ραγδαία.

1.1 Εισαγωγή

Η ραγδαία ανάπτυξη της τεχνολογίας και των πληροφοριακών συστημάτων είναι γεγονός. Η ελεύθερη και γρήγορη μετάδοση της πληροφορίας, οι ευκολίες που παρέχει το διαδίκτυο και οι ηλεκτρονικές συναλλαγές έχουν στρέψει τις επιχειρήσεις ανεξαρτήτου μεγέθους στην εφαρμογή πληροφοριακών συστημάτων και διαδικτυακών εφαρμογών. Πολλοί οργανισμοί βασίζουν τη λειτουργία και την ανάπτυξή τους στα πληροφοριακά συστήματα. Έχουν πρωταγωνιστικό ρόλο στη συλλογή, επεξεργασία και αποθήκευση των δεδομένων της επιχείρησης. Η αξία τους όμως έχει προκαλέσει και πολλοί προσπαθούν να τη μειώσουν προκαλώντας ανεπανόρθωτες ζημιές. Τα τελευταία χρόνια έχει παρατηρηθεί ότι τα πληροφοριακά συστήματα είναι ευάλωτα σε διαφορετικού τύπου απειλές που προέρχονται από το εσωτερικό ή το εξωτερικό περιβάλλον του οργανισμού, όπως κατασκοπεία, ελαττωματικός εξοπλισμός και ανθρώπινα λάθη. Βασικός σκοπός των απειλών είναι η πρόκληση ζημιών οι οποίες δεν περιορίζονται μόνο στις οικονομικές επιπτώσεις αλλά και στη διακοπή λειτουργιών. Κάθε τέτοια περίπτωση δυσλειτουργίας, διακοπής και παράνομης πρόσβασης αυτόματα ισοδυναμεί με κόστος, κόστος που ορίζεται ως οικονομικές απώλειες, διαρροή ευαίσθητων δεδομένων, δυσφήμισης της επιχείρησης. Ιδιαίτερο πρόβλημα ασφάλειας αντιμετωπίζουν οι επιχειρήσεις που διαχειρίζονται ευαίσθητες πληροφορίες ή επεξεργάζονται σημαντικές λειτουργίες. Τα περιστατικά ασφάλειας συνεχώς αυξάνονται με αποτέλεσμα οι επιχειρήσεις να στρέφονται στην εύρεση νέων λύσεων για την προστασίας του. Όπως έχει πει και ο Robert Mueller, πράκτορας του FBI, υπάρχουν δυο είδη επιχειρήσεων «αυτές που έχουν ήδη δεχτεί μια επίθεση και αυτές που θα δεχτούν».

Η διατήρηση της ασφάλειας είναι αποτέλεσμα νομικών και κανονιστικών προκλήσεων στις οποίες υποχρεώνονται να συμμορφωθούν οι επιχειρήσεις ώστε να μην τους υποβάλλονται κυρώσεις. Έτσι λοιπόν οι νομικές διατάξεις, η χρήση νέων τεχνολογιών και η εμφάνιση νέων κινδύνων αποτελούν τα βασικά ζητήματα της ασφάλειας του κυβερνοχώρου. Η ανάλυση επικινδυνότητας βοηθά στον εντοπισμό, την εκτίμηση και την αξιολόγηση του κινδύνου καθώς και στη διαδικασία της λήψης των αποφάσεων για τον περιορισμό και την αποτροπή του. Στόχος είναι η προστασία του οργανισμού ώστε να λειτουργεί για το σκοπό για τον οποίο έχει δημιουργηθεί.

Επομένως είναι αναμφισβήτητη η ανάγκη για ασφάλεια και πρέπει να αποτελεί βασική προτεραιότητα για όσους σχεδιάζουν, υλοποιούν και διαχειρίζονται πληροφοριακά συστήματα ώστε να εξασφαλίζεται η εύρυθμη λειτουργία της επιχείρησης και η επιχειρησιακή της συνέχεια σε περίπτωση που διεξάγεται ένα περιστατικό ασφάλειας.

1.2 Ιστορικό επιθέσεων

Οι επιθέσεις στον κυβερνοχώρο έχουν αυξηθεί σημαντικά τα τελευταία χρόνια. Σύμφωνα με τον πάροχο ψηφιακής ασφάλειας Gemalto το πρώτο εξάμηνο του 2017 πραγματοποιήθηκαν 918 παραβιάσεις δεδομένων που αντιστοιχούν σε 2 δισεκατομμύρια στοιχεία δεδομένων που εκλάπηκαν ή διακυβεύτηκαν, αριθμός που αυξήθηκε κατά 164% συγκριτικά με τις παραβιάσεις που πραγματοποιήθηκαν στο ίδιο χρονικό διάστημα το έτος 2016. Ο Jason Harton επικεφαλής της εταιρείας Gemalto τονίζει το εξής:

"Security is no longer a reactive measure but an expectation from companies and consumers”

Στη συνέχεια ακολουθούν κάποια παραδείγματα επιχειρήσεων που επισημαίνουν την αναγκαιότητα για ασφάλεια. Είναι επιχειρήσεις που έπεσαν θύματα κυβερνοεπιθέσεων αφού δεν πρόλαβαν να αντιδράσουν έγκαιρα με αποτέλεσμα να υποστούν αρκετές ζημιές.

2009

Google China
Στις αρχές του 2010, η Google ανακοίνωσε ότι την προηγούμενη χρονιά είχε γίνει στόχος μιας σειράς κυβερνοεπιθέσεων στην Κίνα με τη χρήση κακόβουλου λογισμικού που χρησιμοποιείται για τη μόλυνση προσωπικών υπολογιστών. Περιλάμβανε προσπάθειες πρόσβασης σε λογαριασμούς Gmail Κινέζων ακτιβιστών για τα ανθρώπινα δικαιώματα ωστόσο μόνο σε δυο λογαριασμούς απέκτησαν πρόσβαση και όχι στο περιεχόμενό τους αλλά στα ονόματα των ιδιοκτητών τους και στην ημερομηνία δημιουργίας του λογαριασμού. Ως βασικό ύποπτο θεώρησαν την κυβέρνηση της Κίνας η οποία εδώ και αρκετά χρόνια παραβίαζε κατάφωρα τα ανθρώπινα δικαιώματα και για το λόγο αυτό αποφάσισες να μεταφέρει τους διακομιστές της στο Χονγκ Κονγκ ώστε να ξεφύγει από τις πολιτικές της Κίνας.

2011

Playstation Network Sony
Τον Απρίλιο του 2011, 77 εκατομμύρια λογαριασμοί του δικτύου της Playstation καταστράφηκαν με τις οικονομικές απώλειες να εκτιμώνται στα 171 εκατομμύρια δολάρια. Θεωρείται ότι είναι η χειρότερη επίθεση που γίνεται σε κοινότητα παιχνιδιών. Ως αποτέλεσμα της επίθεσης ήταν η πρόσβαση στους λογαριασμούς των παικτών, σε ονόματα, κωδικούς πρόσβασης, διευθύνσεις οικίας, αριθμούς πιστωτικών καρτών.

2013

Adobe
Η εταιρεία το 2013 δέχτηκε επίθεση με αποτέλεσμα οι εισβολείς να έχουν πρόσβαση σε 38 εκατομμύρια λογαριασμούς χρηστών. Αν και στην αρχή είχε αναφέρει ψευδή στοιχεία, ότι δηλαδή είχαν κλαπεί 3 εκατομμύρια κρυπτογραφημένα αρχεία πελατών που αφορούσαν πιστωτικές κάρτες και δεν είχε προσδιορίσει τον αριθμό των λογαριασμών που είχαν κλαπεί τα στοιχεία σύνδεσης, στη συνέχεια ανέφερε ότι οι ενεργοί χρήστες που επηρεάστηκαν είναι 38 εκατομμύρια παρόλο που σε αρχείο που δημοσιεύτηκε αργότερα φαίνεται να υπάρχουν 150 εκατομμύρια ζεύγη χρηστών και κωδικών πρόσβασης. Η Adobe χρειάστηκε να καταβάλει 1,1 εκατομμύριο δολάρια για νομικές αμοιβές και ένα άγνωστο ποσό στους χρήστες που είχαν υποστεί ζημιά.

2014

Yahoo
Η yahoo αποκάλυψε τον Οκτώβρη του 2017 ότι 3 χρόνια πριν ήταν θύμα μιας από τις μεγαλύτερες παραβιάσεις στον κυβερνοχώρο έχοντας υπονομευτεί 3 δισεκατομμύρια λογαριασμοί χρηστών και πληροφορίες που σχετίζονταν με αυτούς όπως ονόματα χρηστών, ημερομηνίες γέννησης, διευθύνσεις ηλεκτρονικών ταχυδρομείων και κωδικοί πρόσβασης. Αρχικά η εταιρεία είχε αποκρύψει τα πραγματικά στοιχεία της επίθεσης γιατί εκείνη την περίοδο διαπραγματευόταν την πώλησή της σε άλλη εταιρεία και αυτομάτως θα επηρεαζόταν και η τιμή της.
Ebay

Την ίδια χρονιά η εταιρεία Ebay δήλωσε ότι 145 εκατομμύρια χρήστες της επηρεάστηκαν από την κακόβουλη εισβολή που δέχτηκε εκθέτοντας ονόματα, ημερομηνίες γέννησης και κωδικούς πρόσβασης. Διαπιστώθηκε ότι η επίθεση πραγματοποιήθηκε από εισβολείς οι οποίοι για να εισέλθουν στο δίκτυο της εταιρείας χρησιμοποίησαν τα στοιχεία τριών υπαλλήλων και είχαν πρόσβαση στο σύστημα για 229 ημέρες. Η εταιρεία στη συνέχεια ζήτησε από όλους τους υπαλλήλους να αλλάξουν τα στοιχεία πρόσβασης και τους εγγυήθηκε ότι κανένα οικονομικό στοιχείο τους όπως αριθμοί πιστωτικών καρτών δεν έχουν αποκαλυφθεί. Αν και για κάποιο διάστημα είχε παρατηρηθεί πτώση των χρηστών τα έσοδα και τα κέρδη της ebay κατά το δεύτερο τρίμηνο αυξήθηκαν.

2016

Uber
Προς τα τέλη του 2016 η εταιρεία Uber διαπίστωσε ότι δύο κακόβουλοι χρήστες είχαν αποκτήσει πρόσβαση σε στοιχεία της εταιρείας που σχετίζονταν με τις προσωπικές πληροφορίες 57 εκατομμυρίων χρηστών Uber και 600 χιλιάδων οδηγών. Πιο συγκεκριμένα είχαν κλέψει διευθύνσεις ηλεκτρονικού ταχυδρομείου, αριθμούς κινητών τηλεφώνων όπως επίσης και αριθμούς άδειας οδήγησης των οδηγών της εταιρείας. Το θετικό ήταν ότι δεν κλάπηκαν στοιχεία πιστωτικών καρτών και αριθμοί κοινωνικής ασφάλισης. Όλα τα δεδομένα τα εντόπισαν οι χακέρς μέσω λογαριασμού που διατηρούσαν όπου βρήκαν ονόματα και κωδικούς πρόσβασης στο Github τα οποία χρησιμοποίησαν για να αποκτήσουν πρόσβαση στα δεδομένα της Uber . Η εταιρεία γνωστοποίησε την παραβίαση που δέχτηκε περίπου ένα χρόνο μετά όπου και πλήρωσε τους χάκερς 100.000 δολάρια για να καταστρέψουν τα δεδομένα που είχαν υποκλέψει χωρίς ωστόσο να μπορεί να επιβεβαιώσει ότι το έκαναν. Αυτή η επίθεση φαίνεται ότι έχει επηρεάσει την εταιρεία τόσο σε οικονομικό κόστος όσο και στη φήμη της όπου σε διαπραγματεύσεις που έγιναν για να πουληθεί μέρος των μετοχών της η τιμή έπεσε από τα 68 δισεκατομμύρια δολάρια στα 48, με την παραβίαση να αποτελεί πολύ σημαντικό παράγοντα στη διαμόρφωση της αξίας της.

2017

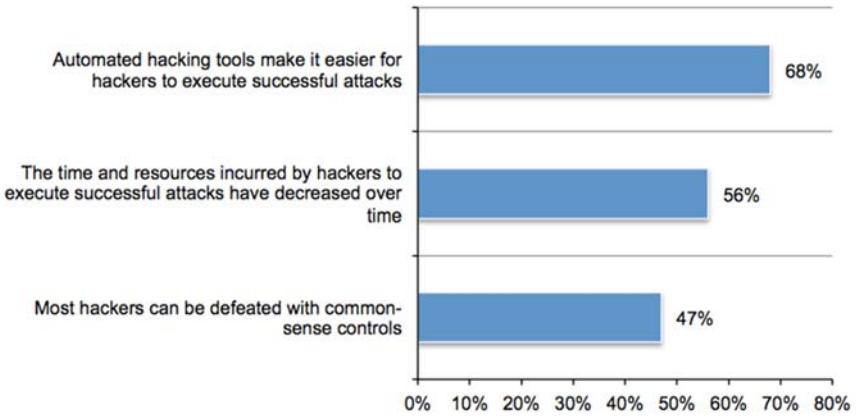
Equifax
Η εταιρεία ανακοίνωσε ότι τον Σεπτέμβριο του 2017 μια ευπάθεια στις εφαρμογές της έθεσε σε κίνδυνο περίπου 147,9 εκατομμύρια καταναλωτές αφού εκτέθηκαν προσωπικές τους πληροφορίες όπως αριθμός κοινωνικής ασφάλισης, ημερομηνία γέννησης, διευθύνσεις καθώς και δεδομένα πιστωτικών καρτών. Η παραβίαση ανακαλύφθηκε τον Ιούλιο αλλά πιθανόν να είχε ξεκινήσει από το Μάιο.

Αυτές θεωρούνται μερικές από τις πιο γνωστές παραβιάσεις του κυβερνοχώρου που πραγματοποιήθηκαν μέσα στον 21ο αιώνα. Ωστόσο η έναρξη των κυβερνοεπιθέσεων ξεκίνησε πολλά χρόνια πριν ακόμα την εφεύρεση των ηλεκτρονικών υπολογιστών. Το 1903 ο μάγος Nevil Maskelyne έστειλε προσβλητικά μηνύματα με σήματα Μορς κατά τη διάρκεια της παρουσίασης του John Ambrose Fleming για την ασφάλεια του ασύρματου τηλέγραφου του Γουλιέλμου Μαρκόνι. Λίγα χρόνια αργότερα, το 1932 τρεις Πολωνοί κρυπτολόγοι, ο Jerry Rozycki, ο Henryk Zygalski και ο Marian Rejewski κατάφεραν να σπάσουν τον κώδικα της μηχανής Enigma. Η ιστορία των επιθέσεων συνεχίζεται και εξελίσσεται στον τομέα της τηλεφωνίας ως τη στιγμή που ανακαλύφθηκε ο πρώτος υπολογιστής και κάθε μεγάλη επιχείρηση είχε αποκτήσει και έναν. Έτσι οι χάκερς εκείνης της εποχής βρήκαν αρκετά ενδιαφέρον το πως θα μπορούσαν να αποσπάσουν τις πληροφορίες που ήταν αποθηκευμένες εντός του υπολογιστή. Το πρώτο κακόβουλο λογισμικό εμφανίστηκε το 1988 με το όνομα Morris worm και θεωρείται ένας από τους πιο αναγνωρισμένους ιούς που επηρέασε την

ασφάλεια του κυβερνοχώρου. Ως αποτέλεσμα είχε να μολύνει 6.000 δικτυακούς υπολογιστές σε πανεπιστήμια, ερευνητικά κέντρα και κυβερνητικές εγκαταστάσεις. Σκοπός αυτού του ιού ήταν να μειώσει την επίδοση των υπολογιστών προκαλώντας και την τελική τους παύση. Αν και όπως αναφέρει ο δημιουργός του ιού Robert Tapan Morris ο αρχικός σκοπός της δημιουργίας του ιού του δεν ήταν να βλάψει τα υπολογιστικά συστήματα ωστόσο εκμεταλλευόμενος τις αδυναμίες του συστήματος κατάφερε να προκαλέσει ζημιά. Από εκείνη τη στιγμή ως τώρα πραγματοποιούνται καθημερινά επιθέσεις στα πληροφοριακά συστήματα που σκοπό έχουν να τους βλάψουν τόσο σε οικονομικό επίπεδο όσο και σε επίπεδο φήμης και υπόληψης. Επομένως πρέπει να επισημανθεί πόσο επιτακτική είναι η ανάγκη της ασφάλειας του κυβερνοχώρου ώστε να περιοριστούν και να εξαλειφθούν οι προσπάθειες παραβίασης.

1.3 Γιατί αυξάνονται οι επιτυχημένες επιθέσεις

Είναι γεγονός ότι τα περιστατικά ασφάλειας στον κυβερνοχώρο αυξάνονται με ταυτόχρονη σημαντική αύξηση και των επιτυχημένων επιθέσεων. Η αύξηση σημειώνεται λόγω της τεχνολογίας που εξελίσσεται με τη χρήση αυτοματοποιημένων εργαλείων hacking η οποία επιτρέπει την εκτέλεση περισσότερων επιθέσεων διευκολύνοντας την επιτυχημένη έκβαση της επίθεσης. Επιπλέον, έχει μειωθεί ο χρόνος και οι πόροι που χρησιμοποιούν για να εκτελέσουν μια επιτυχημένοι επίθεση μειώνοντας παράλληλα και το συνολικό κόστος της διαδικασίας. Οι επιθέσεις γίνονται από επαγγελματίες, έμπειρους και πιο ικανούς να φτάσουν στην επιτυχία. Έτσι λοιπόν, οι βελτιωμένες δεξιότητες των επιτιθέμενων, τα προηγμένης τεχνολογίας εργαλεία που χρησιμοποιούν, ο αυξημένος αριθμός των γνωστών ευπαθειών και τρωτών σημείων καθώς και η μείωση του χρόνου και του κόστους μια επίθεσης οδηγούν στην αποτελεσματική διείσδυση των εισβολέων στο σύστημα προκαλώντας αρνητικές συνέπειες στην επιχείρηση. Σε όλα αυτά θα πρέπει να συνυπολογίσουμε και τους μηχανισμούς άμυνας που είναι εξοπλισμένες οι επιχειρήσεις και να αντιμετωπίσουν τις επιθέσεις οι οποίοι πιθανόν να είναι παρωχημένοι σε νέους τύπους επιθέσεων λόγω της εξέλιξης της τεχνολογίας.[41]



Σχήμα 1.1: Οι λόγοι που συντελούν στην συνεχή αύξηση των επιτυχημένων επιθέσεων στον κυβερνοχώρο

Για να μπορέσουν οι επιχειρήσεις να περιορίσουν την επιτυχημένη δράση των κακόβουλων χρηστών θα πρέπει να λάβουν υπόψη όχι μόνο τεχνικά θέματα που θα δώσουν λύση στο πρόβλημα αλλά και τα κίνητρα των επιτιθέμενων καθώς και το περιβάλλον που θα εξελιχθεί η εισβολή. Ακολουθούν μερικά μέτρα που συνιστώνται για την ενίσχυση της ασφάλειας του κυβερνοχώρου:

- Δημιουργία ολιστικής προσέγγισης στην ασφάλεια του κυβερνοχώρου η οποία θα δίνει έμφασης σε τρεις σημαντικούς παράγοντες της ασφάλειας: άνθρωπος, διαδικασίες, τεχνολογίες.
- Εφαρμογή προγραμμάτων ευαισθητοποίησης και κατάρτισης που θα εκπαιδεύουν τους εργαζόμενους σχετικά με τα μέτρα ασφάλειας και τους τρόπους ταυτοποίησης.
- Δημιουργία μιας δυνατής και ικανής ομάδας να διαχειρίζεται αποτελεσματικά τις πολιτικές ασφάλειας και να ανταποκρίνεται επιτυχώς σε περιστατικά ασφάλειας.
- Επένδυση σε τεχνολογίες επόμενης γενιάς και σε ολοκληρωμένες πλατφόρμες ασφάλειας που μπορούν να αποτρέψουν επιθέσεις.

Η συνολική υποδομή του πληροφοριακού συστήματος θα πρέπει να είναι σχεδιασμένη με τρόπο ώστε να γνωρίζει ποιος και τι χρησιμοποιεί το δίκτυο. Επίσης να είναι ικανό να εντοπίζει κάθε ύποπτη ενέργεια και σε πραγματικό χρόνο να μπορεί να ανταλλάζει πληροφορίες επίθεσης ώστε να χρησιμοποιήσει τα κατάλληλα προστατευτικά μέτρα για να αποτρέψει την επίθεση.

1.4 Βασικά χαρακτηριστικά της διατριβής

1.4.1 Στόχος της διατριβής - Σπουδαιότητα και αναγκαιότητα της έρευνας

Η παρούσα διατριβή εντάσσεται στο ευρύτερο πλαίσιο της μελέτης της ασφάλειας του κυβερνοχώρου, ενός σχετικά νέου πεδίου έρευνας. Πιο συγκεκριμένα έχει σκοπό να μελετήσει τις βασικές έννοιες της κυβερνοασφάλειας δίνοντας σημαντική έμφαση στις τεχνοοικονομικές πλευρές της. Με δεδομένο ότι τα περιστατικά της ασφάλειας των πληροφοριακών συστημάτων ολοένα και αυξάνονται, οι επιχειρήσεις επενδύουν μεγάλα χρηματικά ποσά στην υλοποίηση αντιμέτρων για την ενίσχυση της ασφάλειας ώστε να μειώσουν τον κίνδυνο επίθεσης. Αν υπολογίσουμε ότι όσο και αν είναι το κόστος μιας τέτοιας επένδυσης δεν εξασφαλίζεται ολοκληρωμένη ασφάλεια και η πιθανότητα εμφάνισης ενός περιστατικού πάντα υπάρχει, οι επιχειρήσεις θα πρέπει να αποφασίσουν σε τι βαθμό θα επενδύουν λαμβάνοντας υπόψη το κόστος ως αντίκτυπος μιας επίθεσης. Για το λόγο αυτό θα επικεντρωθούμε στα κόστη της εφαρμογής αντίμετρων ασφάλειας, στις οικονομικές επιπτώσεις μιας παραβίασης καθώς και σε λύσεις που θα ελαχιστοποιήσουν τόσο τις δαπάνες όσο και τη ζημιά. Με λίγα λόγια παρουσιάζονται οι απειλές και οι επιθέσεις των πληροφοριακών συστημάτων, αναλύονται τα μέτρα που χρησιμοποιούνται για την προστασίας τους, κατηγοριοποιείται και αναλύεται το κόστος με το οποίο επιβαρύνονται οι επιχειρήσεις από την πραγματοποίηση μιας επιτυχημένης επίθεσης και προτείνονται νέα μέτρα που ταυτόχρονα θα έχουν καλύτερη απόδοση επένδυσης και θα παρέχουν αποτελεσματικότερη διασφάλιση με περιορισμό των επιθέσεων και των αρνητικών συνεπειών που προκύπτουν.

Η ραγδαία αύξηση και χρήση του διαδικτύου έχει δημιουργήσει ένα νέο είδος εγκληματικότητας, την ηλεκτρονική εγκληματικότητα. Τα θύματα τέτοιων επιθέσεων ολοένα και πολλαπλασιάζονται. Στόχος των κακόβουλων χρηστών μπορεί να είναι από μεγάλους οργανισμούς και κυβερνητικές οργανώσεις μέχρι μικρομεσαίες επιχειρήσεις και μεμονωμένοι χρήστες. Κάθε ένας προσπαθεί να προστατευτεί εφαρμόζοντας διαφορετικές τεχνικές ασφάλειας ώστε να μειώσει τις επιπτώσεις από μία επίθεση. Γνωρίζοντας πόσο δαπανηρή μπορεί να είναι μια τέτοια επένδυση, γίνεται προσπάθεια εύρεσης καινοτόμων λύσεων οι οποίες θα μειώσουν το κόστος και ταυτόχρονα θα επιφέρουν τα επιθυμητά αποτελέσματα.

1.4.2 Βασικά ερευνητικά ερωτήματα και Προτεινόμενη Μεθοδολογία

Η έρευνα προσεγγίζει το ζήτημα της κυβερνοασφάλειας από τεχνικής και οικονομικής άποψης. Η εξάπλωση των κακόβουλων επιθέσεων στον κυβερνοχώρο δημιουργεί την ανάγκη για εφαρμογή αντιμέτρων τα οποία αυτομάτως συνεπάγονται οικονομικό κόστος για την επιχείρηση. Τα βασικά ζητήματα μελέτης της διατριβής είναι:

- Τα μέτρα και οι τεχνολογίες ασφάλειας που εφαρμόζονται από τις επιχειρήσεις για την προστασία και αντιμετώπιση πιθανών επιθέσεων.
- Η οικονομική προσέγγιση και αξιολόγηση των θεμάτων που είναι σχετικά με την ασφάλεια του κυβερνοχώρου. Αναλύεται το κόστος/ όφελος και εξετάζεται το κατά πόσο μια επιχείρηση μπορεί να έχει κερδοφορία στην περίπτωση που δεν θα επενδύσει στην ασφάλεια.
- Η επιχειρηματική προσέγγιση για τη διατήρηση της ασφάλειας και την ελαχιστοποίηση των κακόβουλων ενεργειών και επιπτώσεων.

Όπως αναφέρθηκε και προηγουμένως, στόχος της έρευνας είναι η ανάλυση του κόστους μιας επένδυσης για την εφαρμογή συστημάτων ασφαλείας σε έναν οργανισμό, το κόστος των ζημιών που μπορεί να επιφέρει μια επίθεση στον οργανισμό. Θα πραγματοποιηθεί μελέτη του κόστους μια επίθεσης καθώς και μελέτη οικονομικών μοντέλων που εφαρμόζονται για τη λήψη των αποφάσεων στον τομέα της ασφάλειας. Η άντληση πληροφοριών και στοιχείων έγινε έπειτα από μελέτη ακαδημαϊκών άρθρων, επιστημονικών περιοδικών και βιβλίων. Οι βασικές μηχανές αναζήτησης που θα χρησιμοποιηθούν είναι IEEE, η βιβλιοθήκη του Πανεπιστημίου και το Google.

Κεφάλαιο 2
Οι βασικές έννοιες της κυβερνοασφάλειας

Σε αυτό το κεφάλαιο αναλύονται βασικές έννοιες που θα βοηθήσουν στην καλύτερη κατανόηση του προβλήματος της ασφάλειας. Στην αρχή του κεφαλαίου ορίζονται η κυβερνοασφάλεια, η κυβερνοεπίθεση και ο κυβερνοχώρος, έννοιες που χρησιμοποιούνται συνεχώς κατά την εκπόνηση της διατριβής. Στη συνέχεια γίνεται αναφορά στις κύριες απαιτήσεις της ασφάλειας του κυβερνοχώρου και στο τέλος του κεφαλαίου γίνεται ανάλυση της επικινδυνότητας με επεξήγηση βασικής ορολογίας που εστιάζει στο αντικείμενο της μελέτης μας.

2.1 Κυβερνοχώρος- Κυβερνοεπίθεση- Κυβερνοασφάλεια

Οι ανάγκες της σύγχρονης ψηφιακής εποχής έχουν οδηγήσει στη δημιουργία νέων εννοιών που μπορούν να εκφράσουν καλύτερα αυτό που βιώνουμε. Η συνεχής και εκτενής χρήση των πληροφοριακών συστημάτων, η χρήση κινητών τηλεφώνων και η σύνδεσή τους στο διαδίκτυο δημιούργησαν τον κυβερνοχώρο. Ο κυβερνοχώρος δεν έχει όρια και δεν μπορεί να καθοριστεί σε ένα πλαίσιο καθώς ολοένα και αυξάνονται οι χρήστες του. Μέχρι στιγμής υπάρχουν περίπου 3,8 δισεκατομμύρια χρήστες διαδικτύου, αριθμός που μέχρι το 2022 θα φτάσει στα 6 δισεκατομμύρια. Καθώς ο αριθμός των χρηστών αυξάνεται, αύξηση παρουσιάζεται και στις συσκευές που συνδέονται στο διαδίκτυο χωρίς να απαιτούν φυσική παρουσία και ανθρώπινη αλληλεπίδραση (IOT).[33]Οι συσκευές αυτές παράγουν και ανταλλάσσουν τεράστια ποσά πληροφορίας καθώς εφαρμόζονται σε διάφορους τομείς της καθημερινής ζωής. Εξαιτίας της αβεβαιότητας, το βασικό χαρακτηριστικό της πληροφορίας, και των αδυναμιών των συστημάτων, κακόβουλοι χρήστες προκαλούν επιθέσεις με διαφορετικές προθέσεις και στόχους κάθε φορά. Αυτή η κατάσταση έχει δημιουργήσει και ένα νέο τύπο εγκλημάτων, τις κυβερνοεπιθέσεις. Οι κακόβουλοι χρήστες εκμεταλλεύονται τα τρωτά σημεία του κυβερνοχώρου με σκοπό να κλέψουν ή να αλλοιώσουν πληροφορίες. Αυτό έχει ως αποτέλεσμα να πλήττεται η κυβερνοασφάλεια και να απειλούνται επιχειρήσεις, κυβερνητικές οργανώσεις και μεμονωμένες οντότητες.

Εικόνα 2.1: Βασικές έννοιες της ασφάλειας του κυβερνοχώρου

Κυβερνοχώρος

Σύμφωνα με το λεξικό, η λέξη κυβερνοχώρος προέρχεται από τις λέξεις κυβερνητική και χώρος. Ορίζεται ως ένας εικονικός και πλασματικός χώρος που δημιουργείται με τις εφαρμογές της κυβερνητικής σε σύνδεση με το διαδίκτυο. Η έννοιά του όμως δεν είναι καθορισμένη με σαφήνεια και πολλοί συγχέουν τον κυβερνοχώρο με το διαδίκτυο. Όμως το διαδίκτυο είναι ένα μόνο από τα στοιχεία αυτού. Πιο συγκεκριμένα ο κυβερνοχώρος αποτελείται από ένα σύνολο υπολογιστικών συστημάτων και περιφερειακών συσκευών τα οποία συνδέονται μεταξύ τους και με το διαδίκτυο. Περιλαμβάνει ένα σύνολο εσωτερικών δικτύων που λειτουργούν σε δημόσιους οργανισμούς και τράπεζες καθώς και μεμονωμένους προσωπικούς ηλεκτρονικούς υπολογιστές. Το πιο σημαντικό συστατικό του κυβερνοχώρου όμως είναι η πληροφορία που ανταλλάσσεται, επεξεργάζεται και αποθηκεύεται στα συστήματα και η απόκτηση ή η παραποίησή της αποτελεί το βασικό στόχο των κυβερνοεπιθέσεων. Μπορούμε να διακρίνουμε

τον κυβερνοχώρο σε τρία επίπεδα το φυσικό, το συντακτικό και το σημασιολογικό. Το φυσικό επίπεδο αποτελείται από τις συσκευές και τα καλώδια, το συντακτικό επίπεδο περιλαμβάνει τις οδηγίες και τις εντολές που δίνουν οι σχεδιαστές και οι χρήστες των συστημάτων για να λειτουργήσουν και να επικοινωνήσουν μεταξύ τους και το σημασιολογικό επίπεδο περιλαμβάνει τις πληροφορίες που είναι αποθηκευμένες σε μια συσκευή.[29] Συνήθως οι κακόβουλοι χρήστες επιτίθονται στον κυβερνοχώρο είτε για να αποκτήσουν τον έλεγχο των συστημάτων είτε για να αποκτήσουν πρόσβαση στην πληροφορία. Σύμφωνα με τον Timothy Luke, ο κυβερνοχώρος είναι ο αποκλειστικός χώρος της ψηφιακής πληροφορίας ενώ ο Βασίλειος Γιαννακόπουλος χαρακτηρίζει τον κυβερνοχώρο ως ένα προσβάσιμο παγκόσμιο χώρο, τον πέμπτο κοινό χώρο μετά τη θάλασσα, τον αέρα, τη γη και το διάστημα.

Κυβερνοεπίθεση
Η κυβερνοεπίθεση ορίζεται ως η εκμετάλλευση που πραγματοποιείται σε ένα υπολογιστικό σύστημα ή έναν προσωπικό υπολογιστή με σκοπό να βλάψει την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών που είναι αποθηκευμένες στο σύστημα-στόχος. Πιο αναλυτικά, αποτέλεσμα της επίθεσης είναι να αλλοιωθούν ή καταστραφούν πληροφορίες, να παραβιαστούν προσωπικά δεδομένα, να αποκτήσουν τον πλήρη έλεγχο των συστημάτων. Οι κυβερνοεπιθέσεις θέτουν σε κίνδυνο το σύστημα, δημιουργούν καταστροφικές συνέπειες και οδηγούν σε κυβερνοεγκλήματα.

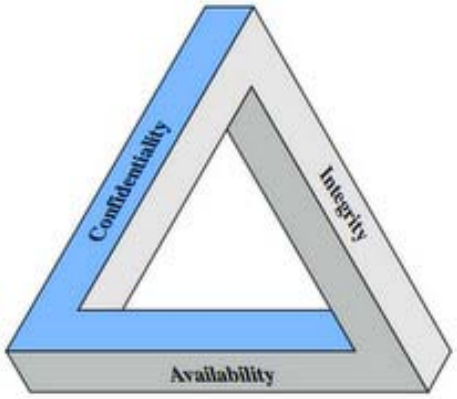
Κυβερνοασφάλεια
Η ασφάλεια του κυβερνοχώρου είναι η πρακτική της προστασίας των υπολογιστών και των διακομιστών, των ηλεκτρονικών συσκευών και των δικτύων από κακόβουλες επιθέσεις. Είναι γνωστή ως ασφάλεια των πληροφοριών και διασφαλίζει την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα της πληροφορίας. Περιλαμβάνει την ασφάλεια των υπολογιστών, την αποκατάσταση από καταστροφές του συστήματος και την εκπαίδευση των χρηστών. Η κυβερνοασφάλεια περιλαμβάνει τεχνικές, διαδικασίες και πρακτικές με σκοπό τον περιορισμό παράνομων ενεργειών και τη διαφύλαξη των περιουσιακών αγαθών μιας επιχείρησης. Οι κύριοι στόχοι που θα επιτευχθούν με τη διατήρηση της ασφάλειας του κυβερνοχώρου είναι:

- Η ασφαλής συλλογή και κοινοποίηση πληροφοριών για ακριβή λήψη απόφασης
- Η εύρεση και αντιμετώπιση ευπαθειών μέσω εφαρμογών
- Η διακοπή της μη εξουσιοδοτημένης πρόσβασης
- Η προστασία της ευαίσθητης πληροφορίας

2.2 Κύριες απαιτήσεις της ασφάλειας

Για να υλοποιηθούν οι παραπάνω στόχοι, οι επιχειρήσεις υιοθετούν τα αντίστοιχα μέτρα ασφάλειας που χαρακτηρίζονται από τρεις βασικές ιδιότητες α) εμπιστευτικότητα, β) διαθεσιμότητα και γ) ακεραιότητα. Για παράδειγμα, η μη εξουσιοδοτημένη πρόσβαση καταργεί την ασφάλεια, η τροποποίηση της πληροφορίας από μη εξουσιοδοτημένα άτομα καταστρέφει την ακεραιότητα, η διαγραφή δεδομένων κάνει αδύνατη τη διαθεσιμότητα. Είναι πρωταρχικής σημασίας η αναγνώριση των πραγματικών απαιτήσεων ασφάλειας των επιχειρήσεων για την αντιμετώπιση και επίλυση των προβλημάτων που θα εμφανιστούν.

Απαιτήσεις ασφάλειας



Σχήμα 2.2:Οι απαιτήσεις της ασφαλείας - Το τρίγωνο CIA

Το τρίπτυχο CIA

Εμπιστευτικότητα: Η ιδιότητα εκείνη του συστήματος που επιτρέπει τη διαθεσιμότητα της πληροφορίας σε εξουσιοδοτημένα άτομα και οντότητες. Διασφαλίζει ότι στην πληροφορία έχουν πρόσβαση μόνο όσοι έχουν τα απαραίτητα δικαιώματα για να το κάνουν. Άλλες προσεγγίσεις της εμπιστευτικότητας σχετίζονται με την ιδιωτικότητα και την προστασία δεδομένων προσωπικού χαρακτήρα που είτε ανήκουν σε κάποιο άτομο είτε στην επιχείρηση. Με λίγα λόγια εμπιστευτικότητα σημαίνει μη αποκάλυψη ευαίσθητης πληροφορίας σε μη εξουσιοδοτημένους χρήστες. Επιτυγχάνεται με την κρυπτογράφηση των δεδομένων και με ελέγχους πρόσβασης σε αυτά.

Ακεραιότητα: Η ιδιότητα που εξασφαλίζει ότι η πληροφορία που διατίθεται είναι ακριβής και σωστή, δεν έχει επεξεργαστεί, τροποποιηθεί ή καταστραφεί από καμία οντότητα. Μόνο με τη διατήρηση της αρχικής της κατάστασης η πληροφορία αποκτά αξία για αυτό και η οποιαδήποτε μεταβολή της επιτρέπεται μόνο από εξουσιοδοτημένα άτομα. Η τροποποίηση περιλαμβάνει τη δημιουργία, την εισαγωγή και τη διαγραφή δεδομένων. Η προστασία της ακεραιότητας επιτυγχάνεται με ψηφιακές υπογραφές, με μηχανισμούς αυθεντικοποίησης και με ελέγχους πρόσβασης.

Διαθεσιμότητα: Η ιδιότητα που καθιστά την πληροφορία διαθέσιμη όταν ζητείται από εξουσιοδοτημένες οντότητες μέσα σε έναν συγκεκριμένο χρόνο. Εξασφαλίζει ότι οι εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στην πληροφορία ανά πάσα στιγμή ώστε να λειτουργήσει σωστά η επιχείρηση. Βασικός σκοπός της ασφάλειας είναι η παρεμπόδιση των κακόβουλων επιθέσεων που στοχεύουν σε κώλυμα της πρόσβασης των νόμιμων χρηστών σε ένα πληροφοριακό σύστημα. Σε αυτή την κατηγορία των επιθέσεων ανήκουν οι επιθέσεις άρνησης παροχής υπηρεσιών. Οι συνήθεις δείκτες για τη διαβάθμιση της διαθεσιμότητας είναι ο χρόνος λειτουργίας και ο χρόνος διακοπής. Ο χρόνος λειτουργίας υποδηλώνει τον χρόνο που το σύστημα λειτουργεί φυσιολογικά χωρίς προβλήματα ή διαταραχές και ο χρόνος διακοπής υποδεικνύει το χρόνο που το σύστημα δεν είναι διαθέσιμο.

$$\text{Διαθεσιμότητα}=\frac{uptime}{uptime+downtime}$$

Ένας άλλος τρόπος για να υπολογιστεί η διαθεσιμότητα είναι ο χρόνος που χρειάζεται το σύστημα να για να επιδιορθωθεί και να είναι ξανά διαθέσιμο. Ο μέσος χρόνος που μεσολαβεί

μεταξύ δύο βλαβών ονομάζεται μέσος χρόνος μεταξύ βλαβών MTBF και ο χρόνος που απαιτείται για αποκατάσταση καλείται μέσος χρόνος για επισκευή MTTR.

$$\text{Διαθεσιμότητα}=\frac{MTBF}{MTBF+MTTR}$$

Η ασφάλεια δεν περιορίζεται μόνο σε αυτές τις απαιτήσεις αλλά πρέπει να καλύπτει και ζητήματα όπως η ταυτοποίηση, η αυθεντικότητα, η λογοδοσία. Επιπρόσθετες ιδιότητες της ασφάλειας είναι:

Αυθεντικότητα: Το πληροφοριακό σύστημα διασφαλίζει ότι η ταυτότητα που δηλώνει μια οντότητα είναι αυτή που ισχυρίζεται ότι είναι. Με τον έλεγχο της ταυτότητας επιτυγχάνεται η ακεραιότητα των δεδομένων και πιστοποιείται η πηγή προέλευσής τους. Κατά κύριο λόγο η επιβεβαίωση πραγματοποιείται από τρίτα μέρη που διαβεβαιώνουν την αυθεντικότητα των κλειδιών που χρησιμοποιούν οι οντότητες που επικοινωνούν.[33] Η εξακρίβωση της ταυτότητας γίνεται σε δύο κατηγορίες:

- Έλεγχος ταυτότητας σε πραγματικό χρόνο
- Έλεγχος ταυτότητας σε ένα πιο ελαστικό χρονικό πλαίσιο

Λογοδοσία: Η ιδιότητα που διασφαλίζει ότι όλες είναι ενέργειες μια οντότητας μπορούν να αποδοθούν σε αυτή την οντότητα. Υποδεικνύει ότι μια οντότητα πρέπει να είναι υπεύθυνη των πράξεων της.

Αξιοπιστία: Διασφαλίζει ότι μια οντότητα έχει συμπεριφορά και αποτελέσματα συνεπή με τα επιδιωκόμενα.

Μη αποποίηση της ευθύνης: Κάθε ενέργεια μπορεί να αποδειχθεί και κανένας χρήστης δεν μπορεί να αρνηθεί ότι το έκανε. Περιλαμβάνει τη μη αποποίηση αποστολής όπου καμία οντότητα δεν μπορεί να αμφισβητήσει τη συμμετοχή της σε κάποια συναλλαγή εφόσον υπάρχουν στοιχεία και τη μη αποποίηση παραλαβής που και στη συγκεκριμένη περίπτωση ο παραλήπτης δεν μπορεί να αμφισβητήσει ότι παρέλαβε δεδομένα λόγω της διαθεσιμότητας αδιάψευστων αποδείξεων.

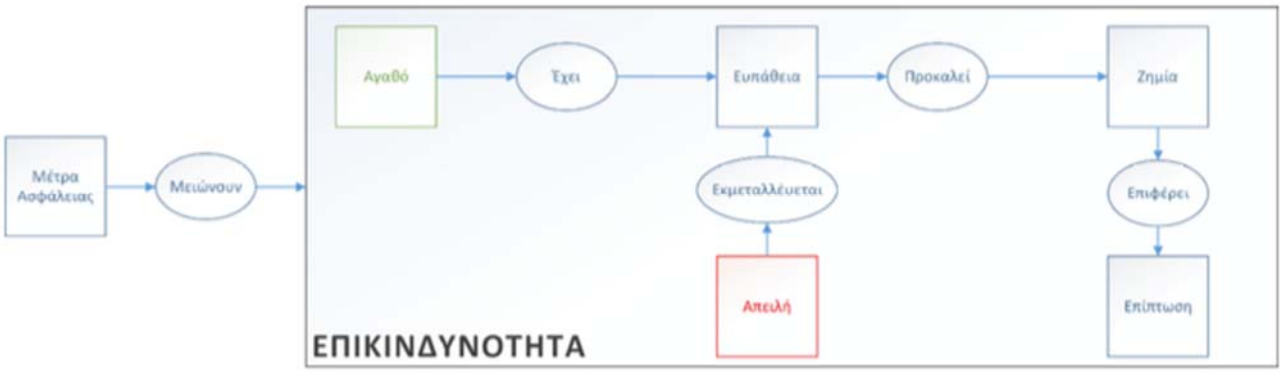
2.3 Ανάλυση της επικινδυνότητας

Η ανάλυση κινδύνου είναι η διαδικασία μελέτης και ανάλυσης της επικινδυνότητας ενός πληροφοριακού συστήματος. Σκοπός είναι να εντοπίζονται και να διαχειρίζονται πιθανά προβλήματα που προκαλούνται στις επιχειρήσεις. Η διαδικασία αυτή περιλαμβάνει αναγνώριση και κατηγοριοποίηση των ευπαθειών και των απειλών ενός συστήματος ώστε να εντοπιστούν οι αδυναμίες και να βρεθούν και να εφαρμοστούν τα κατάλληλα μέτρα προστασίας. Γενικά θα τη χαρακτηρίζαμε ως μια πολύπλοκη διαδικασία αφού πρέπει να εξετασθούν πολλοί παράγοντες όπως οικονομικά δεδομένα, πρωτόκολλα ασφάλειας, στρατηγικές της επιχείρησης ωστόσο τα οφέλη που θα αποκομίσει η επιχείρηση είναι πολλά και θα συμβάλει σε σημαντικό βαθμό στη μελλοντική λήψη αποφάσεων.

Η ανάλυση επικινδυνότητας στοχεύει στη γενικότερη βελτίωση της ασφάλειας. Εστιάζει στη βαθύτερη κατανόηση των κινδύνων υπολογίζοντας την πιθανότητα να πραγματοποιηθούν και στις δυνατότητες που έχουν καθώς και στην αναγκαιότητα για αντιμετώπισή τους περιορίζοντας όσο το δυνατόν τις αρνητικές συνέπειες που μπορεί να προκύψουν ως

αποτέλεσμα ενός περιστατικού ασφάλειας. Η διαδικασία αυτή αποτελεί κύριο όπλο στο σχεδιασμό και στη διαχείριση του κινδύνου και χάρη σε αυτή είναι πιο εύκολο να εξοικονομηθεί χρόνος και χρήμα. [22]

Η εκτίμηση του κινδύνου περιλαμβάνει τις παρακάτω υποδιεργασίες: την αναγνώριση των κινδύνων, την ανάλυση των κινδύνων και την αξιολόγησή τους. Η διαδικασία της αναγνώρισης έχει σκοπό να προσδιορίσει τι είναι πιθανό να προκαλέσει ζημιά σε ένα πληροφοριακό σύστημα και αποτελείται από τα ακόλουθα βήματα: την αναγνώριση των αγαθών, την αναγνώριση των απειλών, την αναγνώριση ευπαθειών, την αναγνώριση των υφιστάμενων μέτρων ασφάλειας και την αναγνώριση των συνεπειών. Ως αποτέλεσμα της αναγνώρισης είναι η καταγραφή των αγαθών από τα οποία απαρτίζεται το πληροφοριακό σύστημα του οργανισμού, η καταγραφή των απειλών από τις οποίες κινδυνεύουν τα αγαθά, η καταγραφή των αντιμέτρων που θα αντιμετωπίζουν τις απειλές, η καταγραφή των συνεπειών που θα προκληθούν από μια επίθεση.



Σχήμα 2.3: Ο συσχετισμός των βασικών όρων της ασφάλειας του κυβερνοχώρου

Αγαθά

Ως αγαθό μπορούμε να ορίσουμε οτιδήποτε έχει αξία για τον ιδιοκτήτη και το οποίο πρέπει να προστατέψει ώστε να μη μειωθεί η αξία του.

Ξεκινώντας από την καταγραφή των αγαθών, θα μπορούσαμε να τα διακρίνουμε σε δύο μεγάλες κατηγορίες:

1. Τα κύρια αγαθά, που περιλαμβάνουν πληροφορίες, και διεργασίες.
2. Τα υποστηρικτικά αγαθά, που περιλαμβάνουν το υλικό, το λογισμικό το διαδίκτυο, το ανθρώπινο δυναμικό, τις εγκαταστάσεις του οργανισμού. Πιο συγκεκριμένα το υλικό αποτελείται από τον βασικό εξοπλισμό του συστήματος καθώς και από τα περιφερειακά μέρη και τα μέσα αποθήκευσης, το λογισμικό περιλαμβάνει το λειτουργικό σύστημα, το λογισμικό διαχείρισης και υποστήριξης των διεργασιών, το ανθρώπινο δυναμικό αποτελείται από τα διοικητικά μέλη, τους απλούς χρήστες, το προσωπικό λειτουργίας και τέλος βασικά μέρη της εγκατάστασης είναι η τοποθεσίας, το περιβάλλον και οι υποδομές της επιχείρησης.

Για την καλύτερη διαχείριση των περιουσιακών στοιχείων της επιχείρησης υπάρχει ένα μοντέλο ταξινόμησης που εφαρμόζεται με σκοπό τη διευκόλυνση των αποφάσεων στα θέματα της ασφάλειας. [35] Τα αγαθά μπορούν να χαρακτηριστούν ως ασήμαντα, λιγότερο ασήμαντα, και κρίσιμα. Στην κατηγορία των κρίσιμων αγαθών περιλαμβάνονται πληροφορίες που είναι ευαίσθητες και εμπιστευτικές, αγαθά που η αποτυχία τους οδηγεί σε ανεπανόρθωτες

καταστροφές και σημαντικές οικονομικές απώλειες, αγαθά που η αποτυχία τους επηρεάζει και άλλα μέρη του συστήματος την ίδια χρονική στιγμή. Στην κατηγορία των αρκετά σημαντικών αγαθών ανήκουν πληροφορίες που χαρακτηρίζονται ως εμπιστευτικές, αγαθά που η αποτυχία τους θα προκαλέσει οικονομικές απώλειες αλλά υπάρχει επαναφορά του συστήματος στην αρχική του κατάσταση και αγαθά που επιδρούν σε ένα τμήμα του συστήματος. Στην επόμενη κατηγορία των λιγότερο σημαντικών αγαθών εμπεριέχονται πληροφορίες που χαρακτηρίζονται ως προσωπικές και αγαθά που η αποτυχία τους επηρεάζει έναν χρήστη χωρίς να δημιουργούν σημαντικές οικονομικές απώλειες. Οποιοδήποτε αγαθό ή πληροφορία δεν πληροί τα κριτήρια ώστε να ενταχθεί σε κάποια από τις προαναφερθείσες κατηγορίες, χαρακτηρίζεται ως ασήμαντο.

Ευπάθειες

Ως ευπάθεια ορίζεται η αδυναμία ή η σχεδιαστική ατέλεια ενός πληροφοριακού συστήματος σε επίπεδο εφαρμογής ή γενικότερης υποδομής του η οποία μπορεί να γίνει η αιτία για την παραβίαση της ασφάλειας ή της ακεραιότητας του συστήματος. Η ευπάθεια εκφράζεται με την ακόλουθη συνάρτηση:

Ευπάθεια = πιθανότητα να συμβεί μια απειλή × πιθανότητα να είναι επιτυχής

Γενικά οι ευπάθειες σχετίζονται με ό,τι εμπεριέχεται σε ένα πληροφοριακό σύστημα όπως φυσικό περιβάλλον, προσωπικό, διαδικασίες και ανάλογα με το αγαθό στο οποίο αναφέρονται κατατάσσονται στις κατηγορίες:

- Ευπάθειες υλικού και λογισμικού (πιθανές δυσλειτουργίες υλικού και λογισμικού που μπορεί να προκαλέσουν διακοπή παροχής υπηρεσιών όπως ευαισθησία στη σκόνη και την υγρασία, έλλειψη καθαριότητας και σωστής αποθήκευσης, έλλειψη ίχνους ελέγχου.)
- Ευπάθειες δικτύου (έλλειψη ασφάλειας αρχιτεκτονικής δικτύου, απροστάτευτες γραμμές επικοινωνίας οι οποίες αυξάνουν τον κίνδυνο διείσδυσης τρίτων μη εξουσιοδοτημένων οντοτήτων με σκοπό την υποκλοπή ή την καταστροφή των μεταδιδόμενων μηνυμάτων.)
- Φυσικές ευπάθειες (ευπάθειες που σχετίζονται με τα φυσικά φαινόμενα και με τις περιβαλλοντικές συνθήκες όπως σεισμοί, πλημμύρες, κεραυνοί, διακοπές ηλεκτρικού ρεύματος, υγρασία, σκόνη.)
- Ανθρώπινες ευπάθειες (εξαιτίας της κατάστασης ότι τα πληροφοριακά συστήματα χρησιμοποιούνται και διαχειρίζονται από ανθρώπους, αποτελούν αυτομάτως την μεγαλύτερη απειλή μέσα στο πληροφοριακό σύστημα. Η άγνοια σχετικά με τα θέματα ασφάλειας, η μη επαρκής εκπαίδευση, η απροσεξία και η επιπολαιότητα κατά τη χρήση αλλά και ο δόλος είναι οι πιο πιθανές ευπάθειες.)
- Οργανωτικές ευπάθειες (έλλειψη πολιτικών ασφαλείας, έλλειψη τακτικών ελέγχων, έλλειψη σχεδίων επιχειρησιακής συνέχειας, έλλειψη σχεδίου έκτακτης ανάγκης, ανεπαρκείς διαδικασίες ανάκτησης πληροφοριών.)

Επιγραμματικά μπορούμε να αναφέρουμε και άλλα παραδείγματα ευπαθειών όπως πληροφορίες που διαβιβάστηκαν από μη εξουσιοδοτημένα άτομα, ταινίες που χάθηκαν κατά τη μεταφορά και αποθήκευση, έλλειψη αντιγράφων ασφάλειας των πληροφοριών, έλλειψη εναλλακτικών επιλογών.[46]

Είδη απειλών

Ως απειλή ορίζεται ένα ανεπιθύμητο γεγονός που μπορεί να προκαλέσει αρνητικές επιπτώσεις στο πληροφοριακό σύστημα όπως είναι η μη διαθεσιμότητα του συστήματος και των υπηρεσιών, η καταστροφή των δεδομένων του συστήματος και η μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητες πληροφορίες.

Ανάλογα με το ποιος ευθύνεται για την πρόκληση των απειλών, μπορούμε να τις διακρίνουμε σε τρεις κατηγορίες. Περιβαλλοντικές είναι οι απειλές που προκύπτουν από τη φύση των συστημάτων ή από το περιβάλλον στο οποίο λειτουργούν, δεν προκαλούνται δηλαδή από τον ανθρώπινο παράγοντα (φυσικά φαινόμενα, διακοπή ηλεκτρικού ρεύματος). Στη δεύτερη κατηγορία ανήκουν εκείνες οι απειλές που προέρχονται από εσκεμμένες κακόβουλες ενέργειες με σκοπό την κατασκοπεία, την επεξεργασία ή την καταστροφή των πληροφοριακών δεδομένων ενώ στο τρίτο είδος απειλών είναι οι ακούσιες ή οι τυχαίες απειλές και αναφέρεται σε αυτές που προκύπτουν ως αποτέλεσμα λανθασμένων ενεργειών που κατά λάθος προκαλούν ζημιά στο πληροφοριακό σύστημα όπως λάθος χειρισμός του χρήστη, σφάλμα λογισμικού, αστοχία εξοπλισμού.

Ανάλογα με τον τύπο τους τις κατηγοριοποιούμε ως εξής :

- Φυσικές απειλές (νερό, φωτιά)
- Φυσικά φαινόμενα (σεισμός, πλημμύρα, ηφαιστειακή έκρηξη)
- Διακοπή υπηρεσιών κοινής ωφέλειας (διακοπή ηλεκτρική ισχύος)
- Παραβίαση της ασφάλειας των πληροφοριών (κλοπή, επεξεργασία, καταστροφή)
- Μη εξουσιοδοτημένες ενέργειες (μη εξουσιοδοτημένη χρήση, παράνομη αντιγραφή λογισμικού)
- Παραβίαση της ασφάλειας λειτουργιών (κατάχρηση δικαιωμάτων, σφάλμα χρήσης)

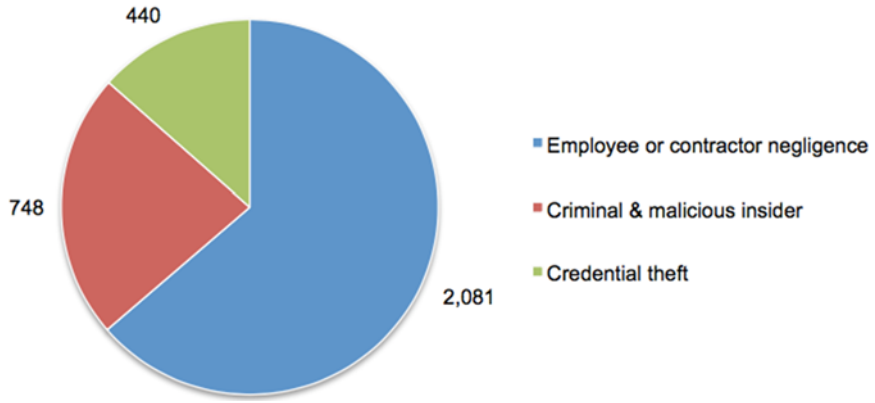
Σχήμα 2.4: Οι κίνδυνοι που αντιμετωπίζουν οι επιχειρήσεις

Φορείς των απειλών

Για την καλύτερη προστασία και ασφάλεια ενός πληροφοριακού συστήματος είναι καλό να προσδιορίσει η επιχείρηση ποιος θα ήθελε να τους παραβιάσει ή να τους κλέψει. Οι περισσότερες επιθέσεις δεν είναι τυχαίες αλλά υπάρχουν δόλια κίνητρα που υποκινούν τέτοιες ενέργειες. Για το λόγο αυτό η επιχείρηση οφείλει να μελετήσει τους πιθανούς φορείς και τους λόγους που θα τους οδηγούσαν στην εκτέλεση ενός περιστατικού.

Σύμφωνα με τον καθηγητή Martin Libicki, τα άτομα που μπορούν να πραγματοποιήσουν επιθέσεις στον κυβερνοχώρο χωρίζονται σε εσωτερικούς και εξωτερικούς. Οι εσωτερικοί αναφέρονται σε εκείνους που είναι είτε εργαζόμενοι στην επιχείρηση είτε έχουν άμεση σχέση με αυτή. Είναι εκείνοι δηλαδή που έχουν νόμιμη πρόσβαση στο δίκτυο (insiders). Ως εξωτερικές είναι οι επιθέσεις που προέρχονται από κάποιον δεν βρίσκεται εντός του δικτύου (hackers).

Έρευνες έχουν δείξει ότι το μεγαλύτερο ποσοστό επιθέσεων προκαλείται από εσωτερικούς χρήστες. Η συνηθέστερη αιτία είναι ένας δυσαρεστημένος υπάλληλος ή ένας πρώην υπάλληλος που θέλει να βλάψει την επιχείρηση. Πρώην υπάλληλος θεωρείται εκείνος που έχει παραιτηθεί ή απολυθεί και κάνοντας μια επίθεση θέλει να εκφράσει τη δυσαρέσκειά του ή να υποκλέψει πληροφορίες που μελλοντικά μπορεί να τις χρησιμοποιήσει για δικό του όφελος. Ο κίνδυνος θεωρείται μεγάλος γιατί οι εισβολείς έχουν γνώση του συστήματος και των εταιρικών πληροφοριών όπως και κάποιοι έχουν δικαιώματα πρόσβασης ως ένα επίπεδο κάτι που θα διευκόλυνε την επίθεσή τους. Μια άλλη αιτία που οδηγεί τους υπαλλήλους σε επιθέσεις είναι η άγνοια. Η ελλιπής εκπαίδευση και η απροσεξία τους οδηγούν σε σφάλματα ικανά να πλήξουν την ασφάλεια του συστήματος. [01]



Σχήμα 2.5: Αποτελέσματα έρευνας που επαληθεύουν ότι οι εσωτερικοί χρήστες αποτελούν τον μεγαλύτερο κίνδυνο σε μια επιχείρηση στον τομέα της ασφάλειας.

Όσον αφορά τις εξωτερικές επιθέσεις, προέρχονται από διαφορετικές αναλόγως τα κίνητρα με κοινό σκοπό να κερδίσουν κάτι. Σε αυτή την κατηγορία ανήκουν οι εξής ομάδες:

Hackers: Αποκτούν πρόσβαση σε ένα πληροφοριακό σύστημα ως πρόκληση στις δικές τους ικανότητες. Ένας hacker που βρίσκει μια αδυναμία στο σύστημα και προσπαθεί να την εκμεταλλευτεί και την δημοσιοποιεί ονομάζεται white hat, εκείνος που εκμεταλλεύεται το τρωτό σημείο της ασφάλειας για προσωπικό όφελος αποκαλείται black hat και εκείνοι που την ημέρα εργάζονται ως σύμβουλοι ασφάλειας και το βράδυ εκτελούν παράνομες επιθέσεις αποτελούν τους grey hat. Παρόλα αυτά τον όρο hacker τον χρησιμοποιούμε για να εκφράσουμε γενικά τον κακόβουλο χρήστη που προσπαθεί να αποκτήσει πρόσβαση σε ένα υπολογιστικό σύστημα χωρίς να έχει εξουσιοδότηση ανεξαρτήτως κινήτρων.

Hacktivists: Επιθέσεις με σκοπό την παροχή υπηρεσίας, τη δυσφήμιση συγκεκριμένων ιστοσελίδων και γενικότερα την προσέλκυση προσοχής και προβολής των ιδεών τους. Συνήθως έχουν κοινωνικοπολιτικό όφελος. Ο όρος προέρχεται από τις λέξεις hacker και activist.

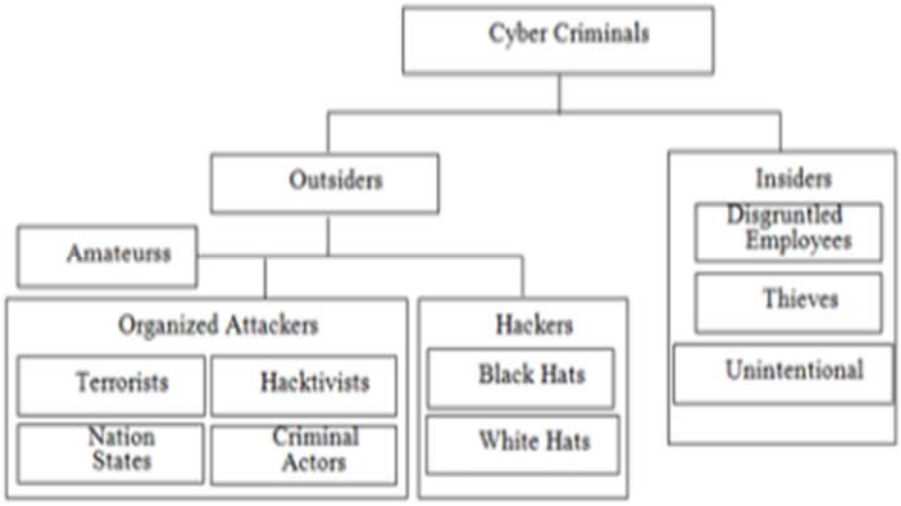
Κατάσκοποι (Spies): Χρήστες που επιδιώκουν την παράνομη απόκτηση πληροφοριών με απώτερο σκοπό το πολιτικό όφελος. Οι κατάσκοποι πληρώνονται για να επιτύχουν συγκεκριμένους στόχους. Είναι εξοπλισμένοι με εργαλεία τελευταίας τεχνολογίας, έχουν πολύ καλή τεχνογνωσία και με αρκετή υπομονή και επιμονή εργάζονται για να φτάσουν στο επιθυμητό αποτέλεσμα. Επίσης είναι ιδιαίτερα προσεκτικοί ώστε να περνούν απαρατήρητοι από τα συστήματα ασφάλειας και η δουλειά τους μπορεί να ολοκληρωθεί σε διάστημα μηνών ως και χρόνων.

Τρομοκράτες (Terrorists): Βασικός τους σκοπός είναι να διασπείρουν το φόβο σχετικά με πολιτικά ζητήματα χρησιμοποιώντας πληροφορίες που έχουν αποκτήσει με παράνομο τρόπο.

Βιομηχανικοί κατάσκοποι (Corporate raiders): Συμπεριφέρονται όπως οι κατάσκοποι αλλά ο σκοπός τους είναι να αποκτήσουν πρόσβαση σε πληροφορία ανταγωνιστικών εταιρειών προς δικό τους οικονομικό όφελος. Οι πιο καταστροφικές μορφές των κλεμμένων πληροφοριών περιλαμβάνουν κατασκευή και ανάπτυξη προϊόντων, πωλήσεις, δεδομένα κόστους, λίστες πελατών, έρευνα και σχεδιασμό. Η επίθεση μπορεί να περιλαμβάνει κλοπή στρατηγικών, και σχεδίων νέων προϊόντων ακόμα και οικονομικών στοιχείων της επιχείρησης.

Επαγγελματίες Εγκληματίες (professional criminals): Έχουν στόχο την παράνομη πρόσβαση και τροποποίηση της πληροφορίας ώστε να ικανοποιήσουν προσωπικά οικονομικά οφέλη.

Βάνδαλοι (Vandals): Πραγματοποιούν επιθέσεις με σκοπό την πρόκληση ζημιών με οποιοδήποτε τρόπο χωρίς κανένα κίνητρο. Στόχος τους είναι να προκαλέσουν όσο το δυνατόν περισσότερες ζημιές. Συνήθως εφαρμόζουν επιθέσεις άρνησης παροχής υπηρεσιών.

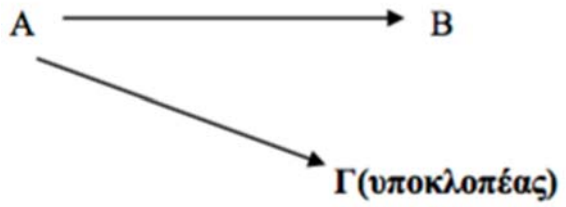


Σχήμα 2.6: Οι κατηγορίες των επιτιθέμενων

Τύποι Επιθέσεων

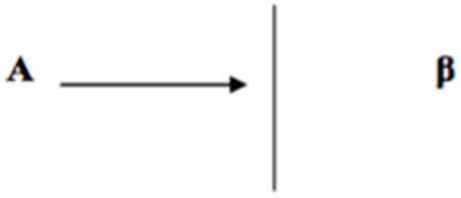
Κάθε κακόβουλος χρήστης αναλόγως το λόγο και το σκοπό που πραγματοποιεί την επίθεση ενάντια του στόχου του χρησιμοποιεί διαφορετικούς τρόπους δράσης. Στο σημείο αυτό αναλύονται οι 4 βασικοί τύποι επιθέσεων:

Μη εξουσιοδοτημένη πρόσβαση: Ο επιτιθέμενος έχει καταφέρει να προσπελάσει το πληροφοριακό σύστημα και έχει αποκτήσει πρόσβαση. Το στοιχείο που χρησιμοποιείται μπορεί να είναι ένα πρόγραμμα, ένα υπολογιστικό σύστημα ή ακόμα και ένας άνθρωπος. Σκοπός της επίθεσης είναι η κλοπή ή η καταστροφή ευαίσθητων πληροφοριών, η αντιγραφή αρχείων ή προγραμμάτων. Αυτό μπορεί να επιτευχθεί με διάφορους τρόπους. Ο εισβολέας μπορεί να αποκτήσει ελεύθερη πρόσβαση στο σύστημα επειδή κατάφερε να παρακάμψει όλους τους μηχανισμούς ασφάλειας. Προτού να αποκτήσει πρόσβαση, ο επιτιθέμενος πιθανόν να είχε μελετήσει και αναλύσει την κίνηση του δικτύου, συνέλεγε πληροφορίες με αποτέλεσμα να έβγαζε συμπεράσματα που θα τον διευκόλυναν στην έκβαση της επίθεσής του. Επιπλέον η μη εξουσιοδοτημένη πρόσβαση μπορεί να είναι αποτέλεσμα αποκάλυψης ευαίσθητης πληροφορίας εσκεμμένα ή κατά λάθος.



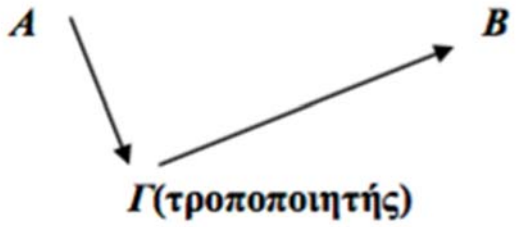
Σχήμα 2.7: Απεικόνιση της μη εξουσιοδοτημένης πρόσβασης

Διακοπή: Μια από τις πιο διαδεδομένες επιθέσεις είναι αυτή της διακοπής υπηρεσιών. Η επίθεση γίνεται με σκοπό να καταστραφούν πόροι του πληροφοριακού συστήματος ή να τεθούν ως μη διαθέσιμοι ώστε να διακοπεί και η λειτουργία της παροχής υπηρεσιών. Η διακοπή της λειτουργίας γίνεται λόγω αχρήστευσης (φυσική καταστροφή των πόρων του συστήματος), καταστροφής (κακόβουλες ενέργειες καταστρέφουν τους πόρους) και παρεμπόδισης (παρεμβολή ή υπερφόρτωση των πόρων του συστήματος).



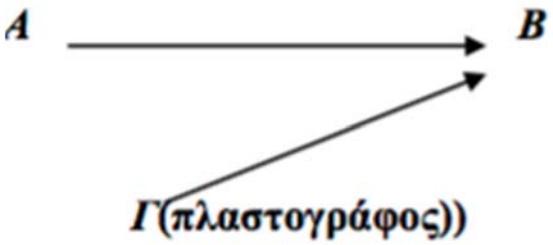
Σχήμα 2.8: Απεικόνιση της διακοπής

Τροποποίηση: Εφόσον ο κακόβουλος εισβολέας αποκτήσει πρόσβαση στο σύστημα έχει τη δυνατότητα να τροποποιήσει τα δεδομένα της πληροφορίας ή να αλλάξει τις τιμές τους. Επηρεάζεται η ακεραιότητα της πληροφορίας.

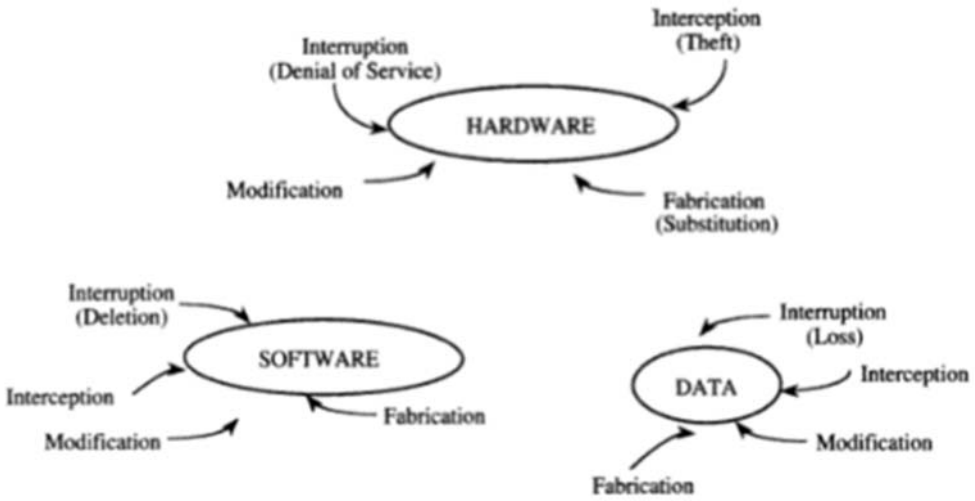


Σχήμα 2.9: Απεικόνιση της τροποποίησης

Πλαστογραφία: Το μη εξουσιοδοτημένο στοιχείο μπορεί να κατασκευάσει πλαστά αντικείμενα μέσα στο σύστημα, να εισάγει ψεύτικες συναλλαγές, να υποδυθεί κάποιον άλλον., να αλλάξει στοιχεία ή να προσθέσει καινούρια και λανθασμένα σε μια βάση δεδομένων. Το κατασκεύασμα αυτό συμπεριφέρεται σαν να είναι νόμιμο, παραπλανώντας τους νόμιμους χρήστες του συστήματος. Στην περίπτωση αυτή μπορεί να προσποιηθεί ότι είναι κάποιος άλλος χρησιμοποιώντας την ταυτότητα του άλλου.



Σχήμα 2.10: Απεικόνιση της πλαστογραφίας

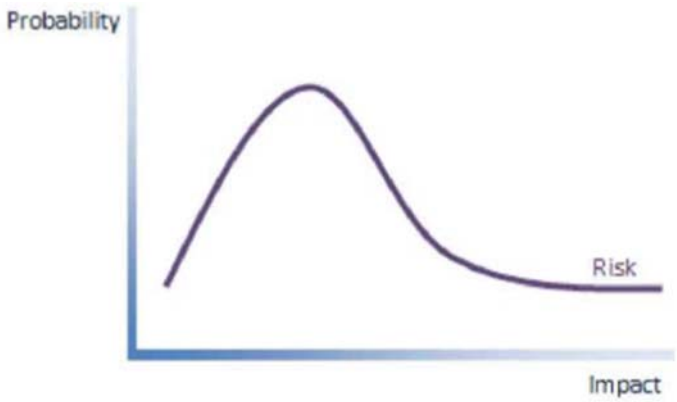


Σχήμα 2.11: Οι βασικοί τύποι επιθέσεων στα στοιχεία του πληροφοριακού συστήματος

Να αναφέρουμε επιπλέον και κάποια άλλα είδη επιθέσεων όπως είναι η επανεκπομπή μηνυμάτων (replay) η οποία έχει σκοπό τη μεταγενέστερη επανεκμπομπή μηνυμάτων τα οποία έχουν καταγραφεί μετά από παθητική παρακολούθηση καθώς και η ανάλυση της επικοινωνίας (traffic analysis) που στοχεύει στην παθητική παρακολούθηση ώστε να αναλυθεί η κυκλοφορία και η διακίνηση των δεδομένων και να εξαχθούν συμπεράσματα που θα βοηθήσουν σε επόμενες επιθέσεις.

Κίνδυνος

Ως κίνδυνος ορίζεται η πιθανότητα μια απειλή να εκμεταλλευτεί μια ευπάθεια. Η έννοια αυτή εκφράζει το ενδεχόμενο της απώλειας. Τύπος συνάρτησης
$R = I * p$



Σχήμα 2.12: Η σχέση πιθανότητας και επίπτωσης

Αντίμετρο

Μηχανισμός ή διαδικασία προστασίας που εφαρμόζεται για την αντιμετώπιση των απειλών. Ανάλογα με τον τύπο τους, χρησιμοποιούνται για ανίχνευση των απειλών, αναχαίτιση της επίθεσης, περιορισμό ή εξάλειψη των επιπτώσεων μιας απειλής.

2.4 Αρχές ασφάλειας

Για την καλύτερη και πιο αποτελεσματική διαχείριση της ασφάλειας του κυβερνοχώρου, οι ειδικοί που ασχολούνται με τέτοια ζητήματα θα πρέπει έκτος από την ανάλυση της επικινδυνότητας να λάβουν υπόψη κάποιες βασικές αρχές που ισχύουν στον κυβερνοχώρο.[11]

- Η αρχή της ευκολότερης διείσδυσης (principle of easiest penetration)
  Οι ειδικοί της ασφάλειας δεν πρέπει να ξεχνούν ότι ο επιτιθέμενος είναι ικανός να χρησιμοποιήσει οποιοδήποτε τρόπο για να αποκτήσει πρόσβαση στο σύστημα εκμεταλλευόμενος τις αδυναμίες του συστήματος που είτε είναι γνωστές και έχουν εφαρμοστεί μέτρα προστασίας είτε όχι.

- Η αρχή της επαρκούς προστασίας (principle of adequate protection)

Οι πόροι και τα αγαθά πρέπει να προστατεύονται στο επίπεδο που δικαιούνται και μόνο για το χρονικό διάστημα που έχουν αξία. Αυτό σημαίνει ότι αγαθά με λιγότερη αξία δεν χρήζουν υψηλά επίπεδα προστασίας όπως επίσης σε περίπτωση που χρησιμοποιούνται για μικρό χρονικό διάστημα να προστατεύονται μόνο για τότε.

- Η αρχή της αποτελεσματικότητας (principle of effectiveness)
  Κάθε μηχανισμός ελέγχου και προστασίας πρέπει να χρησιμοποιείται σωστά για να είναι αποτελεσματικός. "Use it or lose it ". Πρέπει να είναι εύχρηστος, κατάλληλος για να αντιμετωπίσει την επίθεση και επαρκής από πλευράς χρόνου, χώρου μνήμης και ανθρώπινης δραστηριότητας.

- Η αρχή του πιο αδύναμου συνδέσμου (principle of the weakest link)
  Η ασφάλεια δεν μπορεί να είναι πιο ισχυρή από τον αδύναμο σύνδεσμό της. Αυτό σημαίνει ότι μια οποιαδήποτε αποτυχία ελέγχου που πιθανόν να σχετίζεται με το υλικό, το λογισμικό ή ακόμα και τον άνθρωπο που τον σχεδιάζει και τον διαχειρίζεται μπορεί να οδηγήσει σε αποτυχία ασφάλειας.

Εκτός από τις βασικές αρχές της ασφάλειας υπάρχουν και κάποιες επιμέρους στις οποίες πρέπει να δίνεται η ίδια προσοχή και σημασία. Όλοι πρέπει να αντιμετωπίζονται ως εχθροί μέχρι να αποδείξουν το αντίθετο. Για το λόγο αυτό κάθε φορά θα πρέπει να γίνεται ταυτοποίηση του χρήστη και σε κάθε επικοινωνία να γνωρίζουμε ποιος είναι ο παραλήπτης. Επίσης είναι απαραίτητο να αναπτύσσονται σχέσεις εμπιστοσύνης μεταξύ των συνομιλητών και να επιβάλλεται η αναθεώρηση των σχέσεων σε τακτά χρονικά διαστήματα. Τέλος ακόμα και σε θέματα προστασίας είναι χρήσιμο να εφαρμόζονται δοκιμασμένες λύσεις που τα αποτελέσματα τους είναι γνωστά. Κάθε νέο μέτρο απαιτεί χρόνο και πολλές δοκιμασίες μέχρι να διαπιστωθεί ότι είναι ασφαλές να χρησιμοποιείται. Ακόμα όμως και με τις δοκιμασμένες μεθόδους οι χρήστες θα πρέπει να είναι συνεχώς σε επιφυλακή καθώς δεν υπάρχει κανένα προϊόν ή διαδικασία που να παρέχει 100% ασφάλεια. Κατασκευαστικά λάθη λογισμικού και υλικού καθώς και ασυνείδητες συμπεριφορές οδηγούν σε αντίθετα αποτελέσματα.

Κεφάλαιο 3

Η τεχνική προσέγγιση της κυβερνοασφάλειας

Το κεφάλαιο αυτό αναλύει την τεχνική πλευρά της μελετώντας τους τύπους των επιθέσεων που μπορεί να δεχτεί ένα υπολογιστικό σύστημα καθώς και τα τεχνικά μέτρα που θα πρέπει να εφαρμόζονται για την προστασία της ασφάλειας και την ελαχιστοποίηση των επιθέσεων

Καθημερινά, οι επιχειρήσεις ανά τον κόσμο έρχονται αντιμέτωπες με πολλούς και διαφορετικούς κινδύνους ενώ αρκετές από αυτές γίνονται στόχος κακόβουλων χρηστών που προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση και να προκαλέσουν ζημιές. Οι εγκληματίες για να ολοκληρώσουν με επιτυχία την επίθεση ακολουθούν συγκεκριμένα βήματα και η διαδικασία ονομάζεται cyber kill chain. Στη συνέχεια ακολουθεί ανάλυση της αλυσίδας και παρατίθενται οι πιο συνήθεις τρόποι που εφαρμόζουν οι επιτιθέμενοι για να δράσουν καθώς και τα αντίμετρα που χρησιμοποιούν οι επιχειρήσεις για να διασφαλίσουν τα αγαθά τους.

3.1 Cyber kill chain

Η αλυσίδα θανάτου του κυβερνοχώρου είναι μια ιδέα που περιγράφονται τα βήματα μιας επίθεσης ώστε να γίνει καλύτερα κατανοητός ο τρόπος που σκέφτονται και δρουν οι εισβολείς. Επιπλέον συμβάλλει στην προστασία και καλύτερη άμυνα των πληροφοριακών συστημάτων.[09] Να επισημάνουμε ότι όσο πιο κοντά στην αρχή της αλυσίδας αντιμετωπιστεί η επίθεση, τόσο λιγότερες είναι οι αρνητικές επιπτώσεις.

1. Reconnaissance
   Στο στάδιο αυτό οι επιτιθέμενοι επιλέγουν τον στόχο τους έχοντας πρώτα ελέγξει τα κενά και τις ευπάθειες που έχει, αν εμπεριέχει σημαντικές πληροφορίες και αν βέβαια αξίζει να πραγματοποιήσει την επίθεση αυτή. Επιγραμματικά εντοπίζουν κενά και ευπάθειες στο σύστημα- στόχος.
2. Weaoponize
   Οι αδυναμίες που εντοπίστηκαν, χρησιμοποιούνται για να αναπτυχθεί το κακόβουλο λογισμικό. Για παράδειγμα ο επιτιθέμενος μπορεί να δημιουργήσει ένα μολυσμένο αρχείο το οποίο θα στείλει μέσω ηλεκτρονικού μηνύματος (phising email) στο στόχο του ή μπορεί να δημιουργήσει ένα αυτοαναπαραγόμενο λογισμικό που θα διανεμηθεί μέσω μονάδας USB.
3. Delivery
   Το κακόβουλο λογισμικό μεταφέρεται στον υποψήφιο στόχο. Σε μερικές περιπτώσεις ιδιαιτέρα σε επιθέσεις κοινωνικής μηχανής ο άνθρωπος μπορεί να εντοπίσει την επίθεση και να τη σταματήσει όμως σε άλλες συνεχίζει την πορεία της.
4. Exploit
   Εκμετάλλευση του συστήματος. Εκπαιδευμένο προσωπικό διασφαλίζει ότι τα ευαίσθητα δεδομένα είναι ασφαλή και τα συστήματα είναι ενημερωμένα.
5. Installation
   Γίνεται εγκατάσταση του κακόβουλου λογισμικού στο στόχο .
6. Command and Control(C&C)
   Ο εισβολέας δημιουργεί ένα κανάλι μέσα από το οποίο ελέγχει το σύστημα απομακρυσμένα.
7. Actions
   Ο επιτιθέμενος εκτελεί απομακρυσμένα ενέργειες για να φτάσει στο επιθυμητό αποτέλεσμα ανάλογα με τα κίνητρα της επίθεσης. Τα κίνητρα του δράστη ενδέχεται να είναι πολιτικά, στρατιωτικά και οικονομικά για αυτό δεν μπορούν να καθοριστούν με ακρίβεια οι κινήσεις που θα κάνει.

Σχήμα 3.1: Η αλυσίδα θανάτου από τον Lockheed Martin

3.2 Περιστατικά

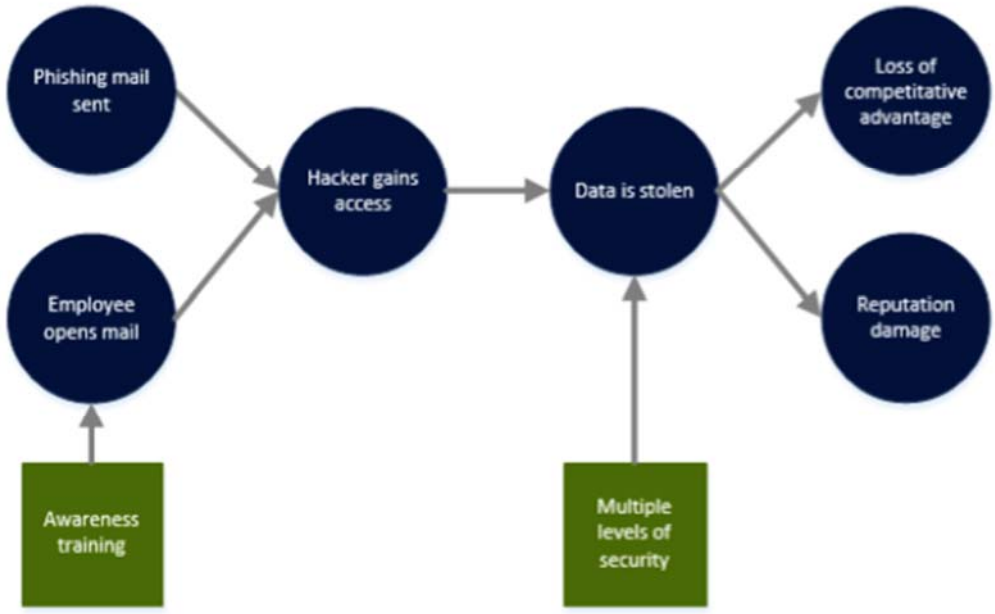
Οι κακόβουλοι χρήστες προκειμένου να παραβιάσουν την ασφάλεια των πληροφοριακών συστημάτων και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση χρησιμοποιούν ποικίλους τρόπους ανάλογα με το σκοπό της επίθεσης που πραγματοποιούν. Τα πιθανά περιστατικά μπορούν να χωριστούν στις ακόλουθες κατηγορίες.

Probe- Διερευνητική επίθεση
Ο κακόβουλος χρήστης σαρώνει τη συσκευή ή το δίκτυο για να ανιχνεύσει αδυναμίες και τρωτά σημεία που θα μπορούσε να τα εκμεταλλευτεί ώστε να θέσει σε κίνδυνο το σύστημα. Αυτού του είδους οι επιθέσεις μερικές φορές συνεπάγονται με την εμφάνιση σοβαρού περιστατικού ενώ κάποιες άλλες είναι αποτέλεσμα περιέργειας ή σύγχυσης.

Packet Sniffer- Παρακολούθηση δικτυακής κίνησης
Ο κακόβουλος χρήστης χρησιμοποιεί έναν sniffer για να συλλέξει πληροφορίες για το δίκτυο. Πιο συγκεκριμένα, το εργαλείο έχει τη δυνατότητα να συλλέγει τις πληροφορίες που μεταφέρονται στα πακέτα του δικτύου. Σε περίπτωση που τα πακέτα δεν είναι κρυπτογραφημένα μπορεί να τα διαβάσει. Οι επιτιθέμενοι καταγράφουν την κυκλοφορία του δικτύου, αναλύουν το περιεχόμενο των πακέτων και συλλέγουν τις ευαίσθητες πληροφορίες που χρειάζονται όπως ονόματα και κωδικοί πρόσβασης.

Denial of service attack (Άρνηση παροχής υπηρεσιών)
Ο κακόβουλος χρήστης με αυτή την επίθεση δεν έχει στόχο να αποκτήσει παράνομη πρόσβαση στο πληροφοριακό σύστημα αλλά να καταστήσει, προσωρινά ή μόνιμα, μη διαθέσιμους τους πόρους του δικτύου σε εξουσιοδοτημένους χρήστες. Αυτό επιτυγχάνεται με την πλημμύρα του συστήματος από περιττά αιτήματα με σκοπό να υπερφορτώσουν το σύστημα και να μην μπορεί να ανταποκριθεί είτε με την ανακατεύθυνση των δεδομένων. Συνήθως οι επιθέσεις πραγματοποιούνται σε διακομιστές που εξυπηρετούν εκατοντάδες χρήστες όπως τράπεζες και άλλα χρηματοπιστωτικά συστήματα.

Phising attack- Ηλεκτρονικό ψάρεμα
Ο κακόβουλης χρήστης με σκοπό να συλλέξει την πληροφορία που χρειάζεται, παρουσιάζεται ως μια έμπιστη και αξιόπιστη οντότητα ώστε να εξαπατήσει το θύμα και να του αποκαλύψει ευαίσθητα δεδομένα. Το ηλεκτρονικό ψάρεμα αποτελεί έναν τύπο κοινωνικής μηχανής και εφαρμόζεται για την κλοπή ονομάτων, κωδικών πρόσβασης και αριθμών πιστωτικών καρτών. Εμφανίζεται κυρίως με αποστολή ηλεκτρονικού ταχυδρομείου όπου ζητά από τον παραλήπτη να πατήσει έναν σύνδεσμο. Με τον τρόπο αυτό εγκαθίσταται κακόβουλο λογισμικό το οποίο συλλέγει τις ευαίσθητες πληροφορίες.



Σχήμα 3.2: Σχηματική απεικόνιση ηλεκτρονικού ψαρέματος μέσω ηλεκτρονικού ταχυδρομείου

Τα τελευταία χρόνια έχει παρατηρηθεί αύξηση των επιθέσεων στον κυβερνοχώρο με την εμφάνιση κακόβουλου λογισμικού. Η έρευνα Cybersecurity Ventures προβλέπει ότι μέχρι το 2019 οι επιχειρήσεις σε παγκόσμιο επίπεδο θα δέχονται ransomware επίθεση κάθε 14 δευτερόλεπτα. Ως κακόβουλο λογισμικό χαρακτηρίζεται ένα πρόγραμμα το οποίο εφόσον εγκατασταθεί μπορεί να βλάψει το πληροφοριακό σύστημα. Σκοπός του είναι είτε να προκαλέσει καταστροφικές συνέπειες στο σύστημα είτε να αποκτήσουν οι εισβολείς μη εξουσιοδοτημένη πρόσβαση. Ανάλογα το είδος του κακόβουλου λογισμικού μπορεί να λειτουργήσει ως παράσιτο μέσα σε άλλο πρόγραμμα. Συνήθως μεταφέρονται από συσκευή σε συσκευή όταν συνδεθούν μεταξύ τους ή μέσω ηλεκτρονικού ταχυδρομείου. Υπάρχουν διάφορα είδη κακόβουλου λογισμικού τα οποία και θα αναλυθούν παρακάτω:

Virus (ιός): Ο ιός είναι κακόβουλο λογισμικό που μολύνει και άλλα λογισμικά. Εγκαθίσταται πριν ή μετά τον εκτελέσιμο κώδικα ενός προγράμματος με σκοπό να βλάψει χρήσιμα αρχεία του θύματος. Εξαπλώνεται εύκολα και γρήγορα, και μεταδίδεται σε άλλους υπολογιστές με τη χρήση κάποιας εξωτερικής συσκευής USB, εξωτερικής μνήμης ή εξωτερικού σκληρού. Ένας ιός αποτελείται από τρία βασικά μέρη, τον μηχανισμό αναπαραγωγής, τον μηχανισμό που καθορίζει πότε θα ενεργοποιηθεί και το μέρος του κώδικα που δεν θα αναπαραχθεί και η διάρκεια ζωής του εκτείνεται σε τρεις φάσεις, Το πρώτο στάδιο είναι η λανθάνουσα

κατάσταση όπου ο ιός είναι απενεργοποιημένος και ορίζεται το πότε θα ενεργοποιηθεί, για παράδειγμα μετά από μια συγκεκριμένη ημερομηνία ή ένα συγκεκριμένο γεγονός. Η επόμενη φάση είναι να εγκατασταθεί ο ιός και τέλος να γίνει η ενεργοποίησή του όπως ορίστηκε στην πρώτη φάση. Οι συνέπειες ενός ιού περιλαμβάνουν από απλή διαγραφή δεδομένων μέχρι ολική καταστροφή του συστήματος.

Trojan Horses (δούρειος ίππος): Κακόβουλο λογισμικό που έχει ως στόχο την παρακολούθηση και όχι τη μόλυνση του συστήματος για αυτό το λόγο κιόλας δεν αναπαράγονται. Ουσιαστικά παριστάνουν ένα χρήσιμο στοιχείο για το σύστημα με σκοπό να αποκτήσουν τον έλεγχο του συστήματος ή να υποκλέψουν σημαντικές πληροφορίες. Ο κρυμμένος κώδικας που περιέχει ένα Trojan όταν εκτελείται επιτελεί λειτουργίες για τις οποίες δεν είναι εξουσιοδοτημένο.

Worm (σκουλήκι): Το σκουλήκι είναι ένας τύπος κακόβουλου λογισμικού το οποίο μπορεί να μεταδίδεται άμεσα και να πολλαπλασιάζεται με ταχύτατους ρυθμούς. Διαφέρει από τον ιό γιατί μπορεί και πολλαπλασιάζεται χωρίς τη χρήση φορέα. Η ενεργοποίηση του ξεκινά από τη στιγμή που φτάσει στον προορισμό-στόχο και η αναπαραγωγή του γίνεται μέσω ηλεκτρονικού ταχυδρομείου ή απομακρυσμένης εκτέλεσης.

Rootkit: Λογισμικό το οποίο εμπεριέχει κακόβουλα προγράμματα ώστε να μένει αόρατο από τα λογισμικά ασφαλείας του συστήματος. Η εγκατάστασή του μπορεί να γίνει είτε αυτόματα ή από τον εισβολέα που έχει αποκτήσει πρόσβαση στο σύστημα ως root. Συνήθως εισέρχονται στο σύστημα με τη μορφή Trojan ή με την παρέμβαση του επιτιθέμενου. Η ανίχνευσή του είναι ιδιαίτερα δύσκολη και περίπλοκη ,ειδικά σε περιπτώσεις που το Rootkit βρίσκεται στον πυρήνα, και απαιτείται συνδυασμός μεθόδων για να εντοπιστούν όπως μέθοδοι σάρωσης και ανάλυσης χωματερής μνήμης.

Backdoor/ Trapdoor: Η πίσω πόρτα ή αλλιώς η πόρτα παγίδα αποτελεί ένα μυστικό σημείο εισόδου ενός προγράμματος που επιτρέπει σε κάποιον να αποκτήσει πρόσβαση στο σύστημα παρακάμπτοντας μηχανισμούς ασφάλειας. Συχνά χρησιμοποιούνται για να εξασφαλίζουν απομακρυσμένη πρόσβαση ή να αποκτούν πρόσβαση σε κρυπτογραφημένα συστήματα. Ένα παράδειγμα backdoor μπορεί να είναι οι προεπιλεγμένοι κωδικοί πρόσβασης εφόσον αυτοί δεν έχουν αλλάξει από το χρήστη.

Logic Bomb (λογική βόμβα): Αποτελεί κακόβουλο λογισμικό με τη μορφή κώδικα το οποίο εισάγεται σε πρόγραμμα που εκτελεί νόμιμες λειτουργίες. Ενεργοποιείται υπό ορισμένες συνθήκες και θεωρείται από τα πιο παλιά είδη κακόβουλου λογισμικού.

Bot: Λογισμικό που καταλαμβάνει ένα σύστημα στο διαδίκτυο για να ξεκινήσει να κάνει επιθέσεις σε άλλα συστήματα που είναι συνδεδεμένα σε αυτό με τέτοιο τρόπο ώστε να μην μπορεί εύκολα να γίνει αντιληπτό από που προήλθε η επίθεση. Το bot εγκαθίσταται σε χιλιάδες συστήματα.

3.3 Αντιμετώπιση περιστατικών παραβίασης της ασφάλειας

3.3.1 Στάδια Αντιμετώπισης

Για να μπορέσει μια επιχείρηση να αντιμετωπίσει ένα περιστατικό ασφάλειας είναι καλό να ακολουθήσει μια σειρά βημάτων ανεξαρτήτως του είδους της επίθεσης που βιώνει. Οφείλει να έχει μια οργανωμένο σχέδιο δράσης στην περίπτωση εμφάνισης ενός περιστατικού το οποίο μπορεί να γλιτώσει την επιχείρηση από την πλήρη καταστροφή

- Προετοιμασία
  Κάθε επιχείρηση χρειάζεται να σχεδιάσει και να εφαρμόσει μεθόδους πρόληψης ώστε να περιορίσει τον κίνδυνο και να ελαχιστοποιήσει τη ζημιά μετά από μια ολοκληρωμένη και επιτυχημένη επίθεση. Η προετοιμασία σχετίζεται με την εφαρμογή αντιμέτρων όπως αποθήκευση αντιγράφων ασφάλειας, ενημέρωση και αναβάθμιση του λογισμικού, δημιουργία πολιτικών ασφάλειας και επιχειρησιακής συνέχειας.

- Αναγνώριση του είδους της επίθεσης
  Κάθε επιχείρηση πρέπει να είναι σε θέση κάθε φορά που γίνεται στόχος ενός περιστατικού να αναγνωρίζει από τα χαρακτηριστικά της, τον τύπο της επίθεσης που δέχεται ώστε να κάνει τις κατάλληλες ενέργειες για να την αντιμετωπίσει.

- Αντιμετώπιση της επίθεσης
  Κάθε επιχείρηση, αφού αναγνωρίζει το είδος της επίθεσης που δέχεται, πρέπει να μπορεί να πραγματοποιεί τις κατάλληλες ενέργειες για να αντιμετωπίσει τον εισβολέα, να προστατεύσει τα αγαθά της και να περιορίσει τη ζημιά της. Στο στάδιο αυτό κρίνεται απαραίτητο να καταγράφονται οι ενέργειες που εκτελούνται για κάθε περιστατικό ώστε να αξιολογηθούν ή και να εφαρμοστούν μελλοντικά για την αντιμετώπιση παρόμοιων επιθέσεων.

- Αποκατάσταση και ανάλυση
  Κάθε επιχείρηση, μόλις ολοκληρωθεί η επίθεση και η αντιμετώπιση της, κάνει μια αποτίμηση των ζημιών που υπέστη και μια ανάλυση της επίθεσης που δέχτηκε προσπαθώντας να εντοπίσει το λόγο που πραγματοποιήθηκε, αν αντιμετωπίστηκε έγκαιρα και με το σωστό τρόπο και ποιες εναλλακτικές θα μπορούσαν να εφαρμοστούν.

3.3.2 Αντίμετρα

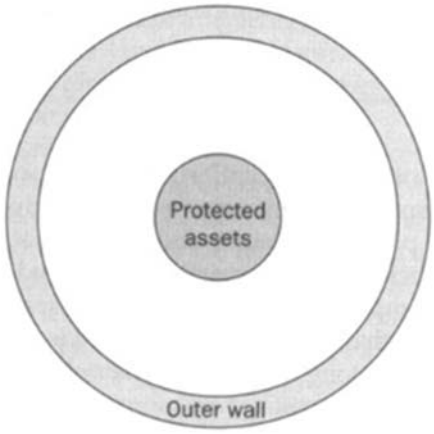
Η ασφάλεια των πληροφοριακών συστημάτων σχετίζεται με τους κινδύνους που έχουν να αντιμετωπίσουν και τους τρόπους με τους οποίους θα προστατεύσουν τα αγαθά τους και θα ελαχιστοποιήσουν τυχόν ζημιά που θα προκληθεί ύστερα από ένα περιστατικό ασφάλειας. Οι τεχνικές που εφαρμόζονται για να διασφαλίσουν την ακεραιότητα και εμπιστευτικότητα του συστήματος κατηγοριοποιούνται ως μέτρα ασφάλειας που σχετίζονται με:

- Πρόληψη: μέτρα που προσπαθούν να περιορίσουν ή να αποτρέψουν τον κίνδυνο που μπορεί να προκαλέσει ζημιά στο πληροφοριακό σύστημα.
- Ανίχνευση: μέτρα που προσπαθούν να ανιχνεύσουν πότε, πώς και από ποιον προκλήθηκε ένα περιστατικό. Περιλαμβάνει προγράμματα και τεχνικές για την έγκαιρη ανίχνευση και αντιμετώπιση περιστατικών.
- Αντίδραση: μέτρα για την αποκατάσταση και ανάκτηση του υπολογιστικού συστήματος.[44]

Σχήμα 3.3: Τα στάδια αντιμετώπισης των κινδύνων στον κυβερνοχώρο

Τα αμυντικά μοντέλα που εφαρμόζονται διακρίνονται σε δύο είδη :

- Το lollipop model το οποίο βασίζεται στη δημιουργία μιας ισχυρής περιμέτρου και συνήθως υλοποιείται με συσκευές ελέγχου πρόσβασης στην είσοδο και έξοδο από το δίκτυο. Στο μοντέλο αυτό ισχύει ο κανόνας ότι η περίμετρος είναι απαραβίαστη. Σε περίπτωση που παραβιαστεί όλα τα αγαθά που βρίσκονται στο εσωτερικό του δικτύου είναι εντελώς απροστάτευτα. Για την ασφάλεια της περιμέτρου χρησιμοποιούμε ξεχωριστά ή σε συνδυασμό τείχη προστασίας και συστήματα ανίχνευσης επιθέσεων.[27]



Σχήμα 3.4: Σχηματική αναπαράσταση του lollipop model

- Το onion model δεν περιορίζεται μόνο στην προστασία της περιμέτρου αλλά υλοποιείται από ένα σύνολο αντιμέτρων που εφαρμόζεται σε πολλαπλά επίπεδα και περιλαμβάνει τεχνικές όπως κρυπτογράφηση, ελέγχους πρόσβασης, ελέγχους ανίχνευσης και προστασία δικτυακών εφαρμογών. Αν ένας επιτιθέμενος παραβιάσει, θα πρέπει να αντιμετωπίζει τα αντίμετρα σε κάθε επίπεδο προστασίας.

Σχήμα 3.5: Σχηματική αναπαράσταση του onion model

Κάθε επιτιθέμενος ακόμα και αν καταφέρει να παραβιάσει την ασφάλεια της περιμέτρου έχει να αντιμετωπίσει στη συνέχεια όλα τα αντίμετρα που λειτουργούν στα υπόλοιπα επίπεδα προστασίας.

Κρυπτογράφηση

Ψηφιακά πιστοποιητικά

Ψηφιακές Υπογραφές

Τείχη προστασίας

Antivirus

Τεχνολογίες ανίχνευσης και αντιμετώπισης των εισβολών

Χρήση εικονικών ιδιωτικών δικτύων

Αντίγραφα ασφάλειας

Αρχεία καταγραφών

Διαδικασίες ταυτοποίησης και αυθεντικοποίησης

Βιομετρικά χαρακτηριστικά

Μηχανισμοί Ελέγχου πρόσβασης

Χρήση συνθηματικών

Τα συνθηματικά είναι ο πιο απλός, οικονομικός και σε ικανοποιητικό βαθμό ασφαλής τρόπος αυθεντικοποίησης. Το συνθηματικό είναι μια πληροφορία που δίνει ο χρήστης για να επιβεβαιώσει την ταυτότητά του και να αποκτήσει πρόσβαση στο σύστημα. Αναγράφει το χαρακτηριστικό του και στη συνέχεια το συνθηματικό του. Αν τα γράψει σωστά έχει επιτυχημένη πρόσβαση. Υπάρχουν περιπτώσεις που για λόγους ασφάλειας χρησιμοποιούνται μετρητές οι οποίοι καταγράφουν τις αποτυχημένες προσπάθειες που έγιναν από το χρήση για να αποκτήσει πρόσβαση, και μετά από έναν συγκεκριμένο αριθμό που έχει οριστεί από το σύστημα ο λογαριασμός κλειδώνει. Στη συνέχεια ο χρήστης θα πρέπει να ακολουθήσει μια διαφορετική διαδικασία ταυτοποίησης ή να επικοινωνήσει με το διαχειριστή του συστήματος για να τον ξεκλειδώσει ή να του δώσει νέο κωδικό. Υπάρχουν και συστήματα που απαιτούν επιβεβαίωση της ταυτότητας του χρήστη όχι μόνο στην αρχή για να εισέλθει στο σύστημα αλλά και κατά τη διάρκεια παραμονής εντός. Η επιλογή του κωδικού πρόσβασης πρέπει να γίνει προσεκτικά γιατί υπάρχει μεγάλος κίνδυνος υποκλοπής. Κάποιες φορές η επιλογή γίνεται από τον ίδιο τον διαχειριστή του πληροφοριακού συστήματος και άλλες φορές από τον ίδιο το χρήστη για αυτό και πρέπει για μεγαλύτερη ασφάλεια να ακολουθεί τα παρακάτω κριτήρια:

- Το συνθηματικό πρέπει να έχει ένα ελάχιστο και ένα μέγιστο μήκος.
- Καλό είναι να συνδυάζει αλφαριθμητικά σύμβολα, ειδικού τύπου χαρακτήρες, πεζά και κεφαλαία γράμματα.
- Δεν πρέπει να αναφέρονται σε προσωπικά στοιχεία (όπως ημερομηνία γέννησης, όνομα κάποιου αγαπημένου τους προσώπου) γιατί εύκολα μπορεί κάποιος να τα μαντέψει.
- Θα ήταν καλό αν δεν μπορεί ο χρήστης να τα απομνημονεύσει, να φυλάει το συνθηματικό σε σημείο που είναι αδύνατον να πλησιάσει κάποιος άλλος και να μην το αποκαλύπτει σε τρίτους.
- Απαιτείται αλλαγή του κωδικού πρόσβασης σε τακτά χρονικά διαστήματα.
- Χρήση διαφορετικού συνθηματικού σε διαφορετικούς λογαριασμούς του ίδιου χρήστη.
- Όχι χρήση έτοιμων φράσεων, έτοιμων λέξεων και επανάληψη χαρακτήρων.

Είναι απολύτως απαραίτητη η δημιουργία ενός κατάλληλου συνθηματικού που θα αποτρέπει μη εξουσιοδοτημένες προσβάσεις ακόμα και αν υπάρχουν επιθέσεις που έχουν στόχο την ανάκτηση αυτών. Οι πιο διαδεδομένες επιθέσεις είναι η επίθεση λεξικού και η μέθοδος εξαντλητικής αναζήτησης. Η επίθεση λεξικού βασίζεται στην ιδέα ότι ο χρήστης χρησιμοποιεί μια συνηθισμένη ακολουθία χαρακτήρων όπως 123456, abc123. Έτσι λοιπόν ο επιτιθέμενος δημιουργεί μια λίστα με τους πιθανούς κωδικούς πρόσβασης και έχοντας ως γνωστό το όνομα του λογαριασμού δοκιμάζει να συνδεθεί στο σύστημα. Η δεύτερη πιο διαδεδομένη επίθεση είναι αυτή της εξαντλητικής αναζήτησης κατά την οποία ο κακόβουλος χρήστης δοκιμάζει τον κάθε δυνατό συνδυασμό χαρακτήρων μέχρι να του δώσει το επιθυμητό αποτέλεσμα. Ο μόνος περιορισμός σε αυτό το είδος επίθεσης ότι ο χρόνος που θα χρειαστεί για την εύρεση του σωστού συνθηματικού είναι αρκετά μεγάλος.

Εικόνα 3.1: Χρήση συνθηματικών

Ψηφιακές υπογραφές

Η ψηφιακή υπογραφή είναι ένα μαθηματικό σύστημα που χρησιμοποιείται για να αποδειχθεί η γνησιότητα ενός ψηφιακού μηνύματος ή εγγράφου. Επιβεβαιώνει ότι το μήνυμα που στάλθηκε δημιουργήθηκε από τον ίδιο τον αποστολέα και δεν τροποποιήθηκε κατά τη μεταφορά του. Οι ψηφιακές υπογραφές χρησιμοποιούν συναρτήσεις κατακερματισμού και τεχνικές κρυπτογραφίας. Αποτελείται από τρεις αλγορίθμους α) ο αλγόριθμος δημιουργίας ιδιωτικού και δημόσιου κλειδιού ο οποίος χρησιμοποιεί μια γεννήτρια τυχαίων αριθμών και δημιουργεί τα κλειδιά, β) ο αλγόριθμος που χρησιμοποιείται για την προσθήκη της ψηφιακής υπογραφής στο μήνυμα, γ) ο αλγόριθμος που ελέγχει την αυθεντικότητα του μηνύματος (ποιος το έγραψε) και την ακεραιότητα του μηνύματος (δεν παραποιήθηκε το μήνυμα κατά τη μετάδοση).
Πιο απλά, η χρήση της ηλεκτρονικής υπογραφής περιλαμβάνει δύο βασικές διαδικασίες, τη δημιουργία της υπογραφής και την επαλήθευσή της. Στο πρώτο βήμα παράγεται μια μαθηματική σύνοψη του μηνύματος πρέπει να σταλεί με τη χρήση one way αλγορίθμων κατακερματισμού και στη συνέχεια με τη χρήση ενός ιδιωτικού κλειδιού κρυπτογραφείται η σύνοψη και δημιουργείται κατά αυτόν τον τρόπο η ψηφιακή υπογραφή. Στη συνέχεια η ψηφιακή υπογραφή προσαρτάται στο μήνυμα και στέλνεται μέσω του διαδικτύου. Εφόσον ο παραλήπτης λάβει το μήνυμα, εφαρμόζει τον ίδιο αλγόριθμο κατακερματισμού και δημιουργεί τη σύνοψη του μηνύματος την οποία αποκρυπτογραφεί με το δημόσιο κλειδί του αποστολέα και στο τέλος για να επαληθεύσει ότι το μήνυμά που έχει λάβει δεν έχει υποστεί κάποιου είδους αλλοίωση συγκρίνει τις δύο συνόψεις. Αν βρεθούν ίσες οι τιμές των συνόψεων, τότε το μήνυμα έφτασε στον παραλήπτη ακέραιο. Σε αντίθετη περίπτωση το μήνυμα έχει μεταβληθεί από μια τρίτη οντότητα και θα πρέπει να ελεγχθεί η ασφάλεια της επικοινωνίας.[45]

Ψηφιακά πιστοποιητικά

Τα ψηφιακά πιστοποιητικά αποτελούν μια ακόμα τεχνική που χρησιμοποιείται για την αυθεντικοποίηση του μηνύματος. Πρόκειται για ένα ηλεκτρονικό έγγραφο σε δυαδική μορφή που χρησιμοποιείται για την αναγνώριση μιας οντότητας και την ανάκτηση ενός δημόσιου κλειδιού. Το ψηφιακό πιστοποιητικό περιλαμβάνει το δημόσιο κλειδί του χρήστη, το όνομα του κατόχου, διάφορους αλγορίθμους. Για να είναι ένα πιστοποιητικό έγκυρο πρέπει να εκδοθεί από την Αρχή πιστοποίησης μετά από αίτηση του ενδιαφερόμενου. Το ψηφιακό πιστοποιητικό περιλαμβάνει τα εξής στοιχεία:

- Την έκδοση του πιστοποιητικού: κάθε νεότερη έκδοση περιλαμβάνει και επιπλέον πληροφορίες
- Ένα serial number: μια ακέραια, μοναδική τιμή που χαρακτηρίζει το πιστοποιητικό
- Το αναγνωριστικό του αλγορίθμου που περιγράφει ποιος αλγόριθμος χρησιμοποιήθηκε για τη δημιουργία της υπογραφής
- Το όνομα του εκδότη
- Το ονοματεπώνυμο καθώς και άλλες σημαντικές πληροφορίες του ιδιοκτήτη
- Το δημόσιο κλειδί του κατόχου του πιστοποιητικού
- Την περίοδο ισχύος η οποία περιλαμβάνει δύο ημερομηνίες την ημερομηνία έκδοσης και την ημερομηνία λήξης του πιστοποιητικού

Αυτά είναι τα βασικά συστατικά ενός ψηφιακού πιστοποιητικού σύμφωνα με το πρότυπο X.509 ωστόσο σε κάθε νέα έκδοση έχουν προστεθεί και άλλες πληροφορίες όπως το μοναδικό αναγνωριστικό του εκδότη και το αντίστοιχο μοναδικό αναγνωριστικό του ιδιοκτήτη. Κάποια άλλα πρότυπα είναι το SPKI και το PGP. Το PGP είναι ένα πρόγραμμα κρυπτογράφησης που παρέχει κρυπτογραφικό απόρρητο, προστασία της ιδιωτικής ζωής και έλεγχο ταυτότητας για την επικοινωνία δεδομένων. Χρησιμοποιείται για την υπογραφή, την κρυπτογράφηση και την αποκρυπτογράφηση κειμένων, ηλεκτρονικού ταχυδρομείου, αρχείων και καταλόγων. Το SPKI χρησιμοποιεί πιστοποιητικά όπου ο κώδικας αναφοράς στηρίζεται στο δημόσιο κλειδί αντί στα ονόματα. Είναι ευρέως διαδεδομένο και χρησιμοποιούνται κυρίως σε διάφορες ηλεκτρονικές κρυπτογραφημένες συναλλαγές οι οποίες πραγματοποιούνται μέσω του διαδικτύου. Φαίνεται ότι αποτελούν λύση στο πρόβλημα της διανομής δημόσιου κλειδιού καθώς συσχετίζουν το κλειδί με τον πραγματικό ιδιοκτήτη του μέσω μια τρίτης έμπιστης οντότητας.[45]

Εικόνα 3.2: Ψηφιακό πιστοποιητικό

Virtual private network (VPN)

Ένα εικονικό ιδιωτικό δίκτυο είναι ένα σύνολο λογικών συνδέσεων μέσω ενός δικτύου δημόσιας πρόσβασης όπως είναι το διαδίκτυο που δίνει τη δυνατότητα στους χρήστες να συνδέονται απομακρυσμένα στο κύριο δίκτυο. Ανάλογα με τον τρόπο που συνδέονται τα δύο άκρα τα εικονικά δίκτυα κατατάσσονται ως εξής:

Host to Host: όπου δημιουργούνται συνδέσεις μεταξύ των κόμβων
Host to Gateway: όπου δημιουργούνται συνδέσεις μεταξύ κόμβων και πυλών δικτύου
Gateway to gateway: όπου δημιουργούνται συνδέσεις μεταξύ πυλών διαφορετικών δικτύων

Τα εικονικά ιδιωτικά δίκτυα χαρακτηρίζονται από ασφάλεια καθώς εφαρμόζουν κρυπτογραφικές τεχνικές και πρωτόκολλα ασφάλειας όπως το SSH tunneling, το SSL και το IPsec ώστε να διασφαλίζουν τα δεδομένα και να αποτρέπουν τη διαρροή ιδιωτικών πληροφοριών από μη εξουσιοδοτημένος χρήστες. Κάποια βασικά πλεονεκτήματα της χρήσης εικονικών δικτύων είναι το χαμηλό κόστος, η ευελιξία και η ασφάλεια. Εξοικονομείται χρήμα εφόσον δε χρειάζεται μισθώσεις κυκλωμάτων, στηρίζεται στο ήδη υπάρχον δημόσιο δίκτυο στο οποίο απλά πρέπει να εφαρμοστεί το κατάλληλο υλικό και λογισμικό για να ξεκινήσει η εικονική σύνδεση. Και για το λόγο ότι αναφερόμαστε σε εικονικές συνδέσεις αφού δεν απαιτείται κάποιο φυσικό μέσο πρόσβασης και τα άκρα της σύνδεσης μπορούν να αλλάξουν, να μετακινηθούν ακόμα και να καταργηθούν.[40]

Δημιουργία αντιγράφων ασφαλείας

Η δημιουργία αντιγράφων ασφαλείας είναι η διαδικασία αντιγραφής και αποθήκευσης των δεδομένων ενός πληροφοριακού συστήματος ώστε να προστατευθούν από κάθε είδους απειλή και να μην υπάρξουν απώλειες. Η αποθήκευση συνίσταται να γίνει σε μια άλλη συσκευή, είτε είναι εξωτερικός σκληρός δίσκος είτε κάποια εξωτερική συσκευή όπως USB, δισκέτες, CD/DVD, μνήμες RAM. Η διαδικασία αυτή είναι ιδιαιτέρα σημαντική για δύο ξεχωριστούς λόγους. Πρώτον, αφού έχουν δημιουργηθεί αντίγραφα μπορούν να ανακτηθούν ανά πάσα στιγμή μετά από μια επιτυχημένη επίθεση που έχει δεχτεί το πληροφοριακό σύστημα και να μην υπάρξουν απώλειες λόγω διαγραφής ή καταστροφής τους. Ο δεύτερος εξίσου σημαντικός λόγος είναι ότι μπορούν να ανακτηθούν δεδομένα από προηγούμενη εποχή για να χρησιμοποιηθούν για επιχειρησιακούς σκοπούς.

Κάθε οργανισμός θα πρέπει να συντάσσει γραπτώς τους κανόνες που πρέπει να ακολουθούνται κατά το στάδιο της δημιουργίας των αντιγράφων. Θα πρέπει να ορίζονται με σαφήνεια:

- Η συχνότητα της δημιουργίας αντιγράφων
- Ο αριθμός των αντιγράφων
- Ο χρόνος κράτησής τους
- Οι τοποθεσίες που θα πρέπει να φυλάσσονται
- Τα άτομα που θα μπορούν να έχουν πρόσβαση σε αυτά

Η διαδικασίας της αντιγραφής και αποθήκευσης γίνεται με διάφορες τεχνικές όπως συμπίεση και κρυπτογράφηση. Ωστόσο υπάρχουν για κάποιοι κίνδυνοι που μπορεί να οδηγήσουν και σε απώλεια των δεδομένων όπως είναι η φυσική απώλεια, η κλοπή, κάποια αστοχία στη συσκευή να χαλάσει ή να απομαγνητιστεί, κάποια αστοχία στα κυκλώματα των σκληρών δίσκων. Τα αντίγραφα ασφάλειας πρέπει να λαμβάνονται κεντρικά από το file server, τον email sever και

τοπικά από τα έγγραφα που αποθηκεύει τοπικά κάθε χρήστης και από το email του χρήστη (για παράδειγμα το outlook).

Αρχεία καταγραφών

Τα αρχεία καταγραφών δημιουργούνται με σκοπό να καταγράφουν τη διαδρομή που ακολουθήσε ένας χρήστης για να αποκτήσει πρόσβαση καθώς και αν χρησιμοποίησε κάποιο δικαίωμα εγγραφής ή ανάγνωσης σε ευαίσθητα δεδομένα. Η διαδικασία αυτή βοηθά στον εντοπισμό μη εξουσιοδοτημένης δραστηριότητας και παραβίασης είτε σε πραγματικό χρόνο είτε μετά το συμβάν καθώς καταγράφονται πληροφορίες σχετικά με λάθη, συναγερμούς και κατάσταση. Το ημερολόγιο που καταγράφεται περιέχει επίσης και άλλα στοιχεία που θα βοηθούσαν στον εντοπισμό ενός γεγονότος όπως αυξημένη χρήση του επεξεργαστή που αποτελεί ένδειξη ότι υπάρχει πιθανότητα ιού. Κατά αυτό τον τόπο επηρεάζεται και η συμπεριφορά των χρηστών εφόσον κάθε τους κίνηση καταγράφεται και αποθηκεύεται με αποτέλεσμα να εργάζονται πιο συνειδητά.

Antivirus

Το antivirus είναι ένα λογισμικό που χρησιμοποιείται για τον εντοπισμό και την καταπολέμηση κακόβουλου λογισμικού όπως ιούς, trojans, spyware, backdoors, worms και άλλα τέτοια από τα οποία μπορεί να μολυνθεί ο υπολογιστής ή οποιοδήποτε πληροφοριακό σύστημα. Ένα τέτοιο λογισμικό συμβάλλει στην άμυνα του συστήματος καθώς μπορεί να αντιμετωπίσει πιθανές απειλές του συστήματος. Ελέγχει το σύστημα αν περιέχει μολυσμένα αρχεία και αν παρατηρηθεί κάτι τέτοιο καθαρίζει το σύστημα είτε καθαρίζοντας τον ιό από τα μολυσμένα αρχεία είτε διαγράφοντας τα αρχεία δεδομένων ή και τα προγράμματα που έχουν υποστεί βλάβη. Υπάρχουν όμως και κάποια αντιιικά λογισμικά που απλά δεν επιτρέπουν την εκτέλεση των μολυσμένων προγραμμάτων για να μην εξαπλώσουν τις συνέπειες και στο υπόλοιπο σύστημα. Τα προγράμματα αυτά έχουν τη δυνατότητα και σε πραγματικό χρόνο να προστατεύουν το σύστημα, ελέγχοντας κάθε κίνηση του χρήστη και όταν παρατηρούν κάτι κακόβουλο να προειδοποιούν το χρήστη και να παρεμποδίζουν το λογισμικό να εισέλθει στο σύστημα διαγράφοντάς το κατευθείαν. Οι δημιουργοί των κακόβουλων λογισμικών λαμβάνοντας υπόψη πως συμπεριφέρονται τα αντιιικά βρίσκουν τρόπους να εξουδετερώσουν και να απενεργοποιήσουν το αντιιικό ώστε να μολύνουν το σύστημα. Συνήθως είναι εγκατεστημένα σε σταθμούς εργασίας και ανιχνεύονται με υπογραφές και με τη συμπεριφορά τους και μεταξύ των δικτύων και ειδικότερα μεταξύ του ίντερνετ και του εσωτερικού δικτύου. Ωστόσο κάποιες φορές ίσως να δημιουργήσουν προβλήματα, όπως επιβράδυνση των συστημάτων, περιορισμένη προστασία λόγω μη αναβάθμισης του χρήστη και μη εντοπισμό νέων ιών. Σε επίπεδο δικτύου έχει παρατηρηθεί ότι δεν μπορούν να ανιχνεύσουν κακόβουλο λογισμικό στα κρυπτογραφημένα κανάλια SSH και σε άγνωστα πρωτόκολλα όπως το P2P. Γενικά το κόστος απόκτησης είναι χαμηλό ενώ ορισμένα διατίθενται και δωρεάν. Κάποια γνωστά λογισμικά είναι το Avast, το Norton, το AVG, το Kaspersky, το McAfee, το Bullguard και το TotalAV.

Firewalls

Ως τείχος προστασίας ορίζεται το υλικό και το λογισμικό που χρησιμοποιείται για την παρακολούθηση της εισερχόμενης και εξερχόμενης κυκλοφορίας δεδομένων ανάμεσα σε δύο δίκτυα. Η απαίτηση της σύνδεσης του δικτύου ενός οργανισμού με το διαδίκτυο δημιουργεί

ένα κανάλι αμφίδρομης επικοινωνίας το οποίο πρέπει να ελέγχεται συστηματικά για να αποφευχθούν κίνδυνοι όπως απόκτηση μη εξουσιοδοτημένης πρόσβασης. Ένα τείχος προστασίας επιτρέπει στο εσωτερικό δίκτυο πλήρη και ασφαλή επικοινωνία και πρόσβαση με ένα εξωτερικό δίκτυο και ταυτόχρονα επιτρέπει την πρόσβαση του εξωτερικού δικτύου σε ένα εσωτερικό με βάση ονόματα και συνθηματικά χρηστών, τις IP διευθύνσεις και τα Domain names. Θα λέγαμε πιο απλά ότι λειτουργεί ως εμπόδιο μεταξύ ενός αξιόπιστου εσωτερικού δικτύου και ενός μη αξιόπιστου εξωτερικού δικτύου. Για να επιτευχθεί ο σκοπός λειτουργίας των τειχών προστασίας, απαιτείται η σωστή ρύθμιση από τους διαχειριστές του δικτύου οι οποίοι θα πρέπει να έχουν μια ολοκληρωμένη άποψη για τις ανάγκες του και τους πιθανούς κινδύνους. Η σωστή πρακτική είναι να απορρίπτονται όλες οι συνδέσεις εκτός από εκείνες που έχουν οριστεί να επιτρέπονται.

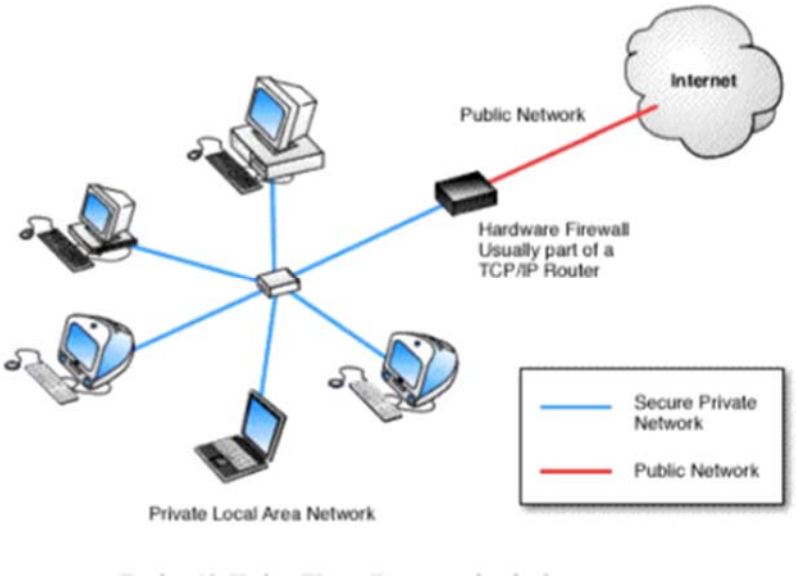
Τα τείχη προστασίας διακρίνονται σε δύο κατηγορίες, τα τείχη προστασίας δικτύου και τα τείχη προστασίας κεντρικού υπολογιστή. Η διαφορά τους έγκειται στο σημείο ότι τα πρώτα φιλτράρουν την κίνηση μεταξύ δύο ή περισσότερων δικτύων και τα δεύτερα εκτελούνται σε κεντρικούς υπολογιστές και ελέγχουν την κυκλοφορία μέσα και έξω από αυτούς. Επιπλέον μπορούμε να τα χωρίσουμε ως εξής:

Φίλτρα πακέτων: Φιλτράρει κάθε πακέτο που μεταδίδεται με βάση την πληροφορία που περιέχει ανεξάρτητα σε ποια σύνοδο ανήκει. Πιο συγκεκριμένα διαβάζει τα πακέτα δεδομένων και αν τα χαρακτηριστικά τους ταιριάζουν με τους κανόνες που έχει ορίσει ο διαχειριστής δικτύου απορρίπτει τα πακέτα ή τους επιτρέπει την πρόσβαση.
Τείχος προστασίας επιπέδου συνόδου - Πύλες κυκλώματος: Έχουν ως βασική αρχή λειτουργίας την απαγόρευση της απευθείας δημιουργίας συνδέσεων μεταξύ ενός εσωτερικού κόμβου και ενός εξωτερικού.

Πύλες εφαρμογών: Όταν ο πελάτης επιθυμεί πρόσβαση σε μια συγκεκριμένη υπηρεσία, στέλνει το αίτημα στον proxy server ο οποίος στη συνέχεια αφού αυθεντικοποιήσει το χρήστη θα προωθήσει τα πακέτα που έχει λάβει από τον πελάτη στον διακομιστή προορισμού.

Τείχη προστασίας NAT: Χαρτογραφεί όλες τις διευθύνσεις των εσωτερικών συστημάτων σε μια εξωτερική με κύριο σκοπό να επιτρέπει συνδέσεις που προέρχονται από το εσωτερικό.

Τείχη προστασίας Stateful: Συνδυάζουν τα χαρακτηριστικά και τις ικανότητες των τειχών προστασίας NAT, του επιπέδου συνόδου και του πληρεξούσιου φιλτράροντας πρώτα τα χαρακτηριστικά των πακέτων και στη συνέχεια αν επιτρέπεται η σύνοδος.
Καθώς κάθε ένα είδος τείχους προστασίας εκτελείται και σε διαφορετικό μοντέλο για διαφορετικό σκοπό. Για παράδειγμα στο πιο χαμηλό επίπεδο των μοντέλων OSI ή TCP/IP το firewall χρησιμοποιείται για να προσδιορίσει αν το πακέτο δεδομένων προέρχεται από έμπιστη πηγή χωρίς να ξέρει ποιο είναι το περιεχόμενό του και με ποια άλλα πακέτα μπορεί να συνδέεται. Σε άλλα επίπεδα όπως στο επίπεδο μεταφοράς το firewall ορίζει αν θα επιτρέψει ή απορρίψει την πρόσβαση. Αποτελούν κατά μια έννοια έναν μηχανισμό ελέγχου πρόσβασης αφού όλη η κίνηση του δικτύου πρέπει να διέρχεται από το firewall το οποίο θα είναι απαραβίαστο εκτός από συγκεκριμένες περιπτώσεις οι οποίες ορίζονται από τις πολιτικές που εφαρμόζει. [39]

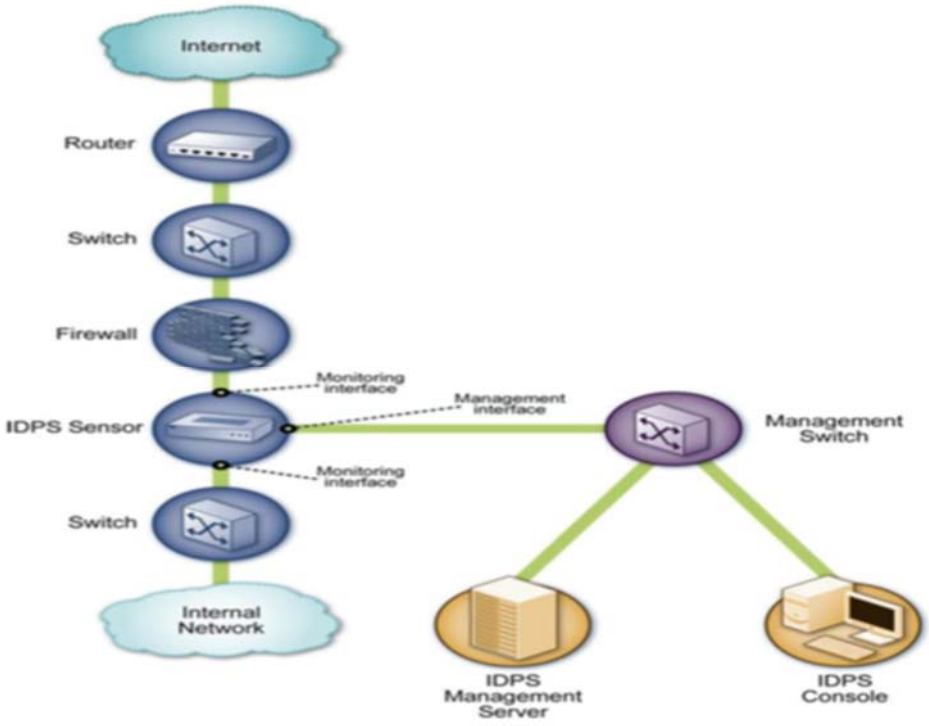


Σχήμα 3.6: Απεικόνιση τείχους προστασίας

Σύστημα πρόληψης εισβολών IPS

Το σύστημα πρόληψης εισβολών είναι μια τεχνολογία δικτύου που βοηθά στην πρόληψη απειλών ελέγχοντας την κυκλοφορίας του δικτύου με σκοπό την προστασία του από κακόβουλες δραστηριότητες. Οι συσκευές αυτές χρησιμοποιούνται για τον εντοπισμό και την πρόληψη κάθε τύπου κακόβουλης ενέργειας που θα μπορούσαν να επιφέρουν αρνητικές επιπτώσεις στο σύστημα. Είναι εγκατεστημένα σε κρίσιμα σημεία του δικτύου και εκτελούν σε πραγματικό χρόνο την ανάλυση της κίνησης του δικτύου. Τα συστήματα πρόληψης εισβολών θεωρούνται επεκτάσεις των συστημάτων ανίχνευσης και λειτουργούν με δύο τρόπους:

Inline (άμεσα) όπου το ίδιο το IPS απορρίπτει ή ανακατευθύνει πακέτα που εντοπίστηκαν στο δίκτυο με ύποπτη συμπεριφορά.
Έμμεσα όπου το IPS δίνει εντολή σε κάποιο άλλο σύστημα που συνδέεται με αυτό όπως το firewall να κάνει τις απαραίτητες ενέργειες για αναχαίτιση της επίθεσης.
Η χρήση τους είναι απαραίτητη για τη διατήρηση της ασφάλειας του δικτύου αφού προστατεύει και εμποδίζει την ανεπιθύμητη πρόσβαση και διακρίνονται σε τρεις βασικές κατηγορίες HIPS, NIPS και WIPS. Το WIPS ελέγχει την ασύρματη κίνηση δεδομένων με σκοπό την αποτροπή πρόσβασης και επίθεσης στο δίκτυο και στους πόρους που χρησιμοποιεί μια ασύρματη σύνδεση χρησιμοποιώντας αισθητήρες και κεραίες. Το NIPS χρησιμοποιείται για την ανίχνευση κακόβουλης δραστηριότητας και αρκετές φορές έχει τη δυνατότητα να εντοπίζει την επίθεση προτού φτάσει στο στόχο. Για να έχει τα επιθυμητά αποτελέσματα συνδυάζει υπογραφές επίθεσης και ανάλυση συμπεριφοράς. Τέλος το HIPS αναλύει τα γεγονότα που συμβαίνουν και όταν εντοπίσει μια κακόβουλη ενέργεια αναστέλλει τη λειτουργία και ενημερώνει το χρήστη για τα επόμενα βήματα που πρέπει να ακολουθήσει. Χρησιμοποιεί μια βάση δεδομένων αντικειμένων ενός συστήματος που παρακολουθείται για να εντοπίσει εισβολείς αναλύονται τις κλήσεις συστήματος τα αρχεία καταγραφής εφαρμογών και τις τροποποιήσεις του συστήματος αρχείο. Το HIPS έχει το πλεονέκτημα ότι αποφεύγει τους λανθασμένους συναγερμούς και διατηρεί σε μια καλή και ασφαλή κατάσταση το σύστημα και ακόμα έχει τη δυνατότητα να διαχειρίζεται πολλαπλές εφαρμογές ασφάλειας για την προστασία προσωπικών δεδομένων.



Σχήμα 3.7: Σύστημα ανίχνευσης εισβολών

Σύστημα ανίχνευσης εισβολών

Το σύστημα ανίχνευσης εισβολών είναι ένα σύστημα που παρακολουθεί και ελέγχει συμβάντα που λαμβάνουν χώρα στο δίκτυο. Στόχος είναι να εντοπίζονται πιθανές προσπάθειες εισβολής και στοιχεία που παραβιάζουν την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των πληροφοριακών πόρων. Οι λόγοι για τους οποίους συνιστάται η εγκατάσταση συστημάτων ανίχνευσης είναι η πρόληψη προβλημάτων, η ανίχνευση παραβιάσεων, η τεκμηρίωση υπαρκτών απειλών. Τα συστήματα χρησιμοποιούνται ως honeypots, σαν δολώματα για να προσελκύσουν τους επίδοξους εισβολείς και να αποσπάσει την προσοχή από το πραγματικό δίκτυο. Τα συστήματα IDS χωρίζονται σε δυο κατηγορίες τα ενεργά και τα παθητικά. Τα ενεργά IDS προσπαθούν να μπλοκάρουν τις επιθέσεις κατά τη διάρκεια της εξέλιξης της επίθεσης ενώ τα παθητικά καταγράφουν την εισβολή ή δημιουργούν ίχνη παρακολούθησης τα οποία είναι εμφανή μετά το τέλος της επίθεσης. Ενώ φαίνεται τα παθητικά συστήματα δεν είναι τόσο χρήσιμα στο να αποτρέπουν επιθέσεις, υπάρχουν ορισμένες επιθέσεις που γίνονται αντιληπτές μόνο εφόσον ολοκληρωθεί η επίθεση. Το βασικό χαρακτηριστικό των συστημάτων ανίχνευσης είναι ότι μπορούν και εντοπίζουν επιθέσεις και γενικότερα παραβιάσεις ασφαλείας οι οποίες δεν αναγνωρίζονται από άλλα μέτρα προστασίας. Κάθε επίδοξος εισβολέας μελετά το σύστημα, αναγνωρίζει τις αδυναμίες του και προσπαθεί να τις εκμεταλλευτεί ώστε να αποκτήσει πρόσβαση. Για το λόγο αυτό τα συστήματα ψάχνουν ίχνη εισβολής στο τοπικό δίκτυο του host και προσπαθούν να εντοπίσουν ασυνήθιστη δραστηριότητα στον host όπως log in παράξενη πρόσβαση σε αρχεία, μετατροπές σε δικαιώματα χρηστών. Αυτά είναι τα λεγόμενα συστήματα ανίχνευσης εγκατεστημένα σε υπολογιστή, υπάρχουν όμως και εκείνα που είναι εγκατεστημένα στο δίκτυο και αποτελούνται από δύο μέρη, τους αισθητήρες και τον σταθμό διαχείρισης. Οι αισθητήρες παρακολουθούν την κίνηση του δικτύου και αν εντοπίσουν κάτι ύποπτο το μεταφέρουν στο σταθμό

διαχείρισης ο οποίος θα στείλει αυτομάτως σήμα κινδύνου με τελικό προορισμό το διαχειριστή του συστήματος. Τα εν λόγω συστήματα ανιχνεύουν εισβολές σε επίπεδο δικτύου και επίπεδο κόμβου και η ανίχνευση μπορεί να γίνει με δύο τρόπους:

Την ανίχνευση υπογραφής: Για παράδειγμα ένας κανόνας θα μπορούσε να μην επιτρέπει στους χρήστες να τοποθετούν αρχεία σε home directory άλλων χρηστών. Ο κατασκευαστής παράγει μια λίστα από υπογραφές δηλαδή χαρακτηριστικά τμήματα που θεωρεί ότι είναι ύποπτα ή ενδεικτικά μιας επίθεσης οπότε το σύστημα ελέγχει αν υπάρχουν γνωστές υπογραφές και τις εντοπίσει στέλνει σήμα συναγερμού.

Την ανίχνευση συμπεριφοράς: όπου καταγράφονται συμπεριφορές που δεν ανταποκρίνονται στη φυσιολογική χρήση του συστήματος. Το IDS μαθαίνει ποια είναι η φυσιολογική συμπεριφορά από τότε που άρχισε να λειτουργεί. Έτσι λοιπόν αν το σύστημα παρατηρήσει απόκλιση συμπεριφοράς όπως αυξημένη δραστηριότητα, ασυνήθιστες αιτήσεις πρόσβασης ή αυξημένο αριθμό συνόδων, θεωρεί ότι γίνεται επίθεση. Συμπεριφέρονται πιο αποτελεσματικά όταν εφαρμόζονται σε στατικά περιβάλλοντα όπου υπάρχουν επαναλαμβανόμενα μοτίβα. Σε δυναμικά περιβάλλοντα ενδεχομένως να οδηγήσουν σε λανθασμένο συναγερμό αν η δραστηριότητα δεν έχει χαρακτηριστεί πρωτύτερα ως νόμιμη.

Είναι προτιμότερο και πιο αποτελεσματικό να εφαρμοστεί σε ένα πληροφοριακό σύστημα ο συνδυασμός των δύο συστημάτων πρόληψης και ανίχνευσης αφού διαπιστώνεται ότι το ένα συμπληρώνει το άλλο. Ένα σύστημα ανίχνευσης δεν είναι αρκετό για την πλήρη ασφάλεια του συστήματος καθώς εφόσον εντοπιστεί μια επίθεση χρειάζεται αρκετός χρόνος μέχρι να ενημερωθεί ο διαχειριστής του συστήματος με αποτέλεσμα οι επιπτώσεις που θα προκληθούν να είναι δυσμενείς για τον οργανισμό.

Αναφέραμε προηγουμένως ότι τα συστήματα ανίχνευσης λειτουργούν ως κυψέλες. Ουσιαστικά πρόκειται για ένα κόμβο δολώματος που σκοπίμως περιέχει ευπάθειες ώστε να δελεάσει τον μελλοντικό επιτιθέμενο και να τον προτρέψει να επιτεθεί σε αυτόν και όχι στα υπόλοιπα μέρη του συστήματος. Κατά αυτόν τον τρόπο η ζημιά που θα προκαλούσε μια επίθεση θα περιοριστεί στον κόμβο δόλωμα και επιπλέον το σύστημα θα ανιχνεύσει την επίθεση και θα εντοπίσει τον κακόβουλο εισβολέα.[19]

Κρυπτογραφία

Με τον όρο κρυπτογραφία εννοούμε τη μελέτη μαθηματικών τεχνικών που στοχεύουν στην εξασφάλιση θεμάτων που άπτονται της ασφάλειας μετάδοσης της πληροφορίας όπως εμπιστευτικότητας, ακεραιότητας και αυθεντικοποίησης. Πιο συγκεκριμένα είναι η διαδικασία κατά την οποία ένα μήνυμα μετασχηματίζεται σε μία άλλη μορφή με τη χρήση ενός κρυπτογραφικού αλγορίθμου και μπορεί να επιστρέψει στην αρχική μορφή μέσω της αντίστροφης διαδικασίας, της αποκρυπτογράφησης. Για να μετασχηματιστεί το αρχικό μήνυμα χρειάζεται έναν αλγόριθμο κρυπτογράφησης και ένα μυστικό κλειδί. Ο αλγόριθμος κρυπτογράφησης είναι ένας μαθηματικός τύπος που εφαρμόζεται στην πληροφορία για να την κρυπτογραφήσει και να την αποκρυπτογραφήσει. Όσο μεγαλύτερη είναι η πολυπλοκότητα του αλγορίθμου τόσο πιο δύσκολα κάποιος αποκτά πρόσβαση στο μήνυμα. Αν εφαρμόζεται ξεχωριστά για κάθε bit του μηνύματος χωρίς να το διαχωρίζουν σε τμήματα τότε αναφερόμαστε στη μέθοδο κρυπτογράφησης steam cipher (αλγόριθμος ροής) ενώ αν η κρυπτογράφηση γίνεται σε επίπεδο ομάδων δεδομένων συνήθως συγκεκριμένου μεγέθους τότε περιγράφουμε τη μέθοδο κρυπτογράφησης block cipher (αλγόριθμος δέσμης). [20,27]

Εκτός από τον αλγόριθμο κρυπτογράφησης, άλλοι βασικοί όροι που πρέπει να γίνουν κατανοητοί είναι:

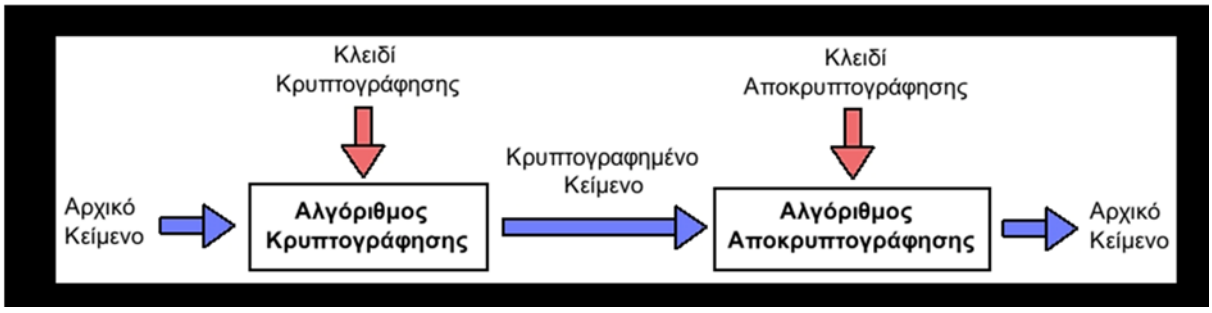
Plaintext: Το αρχικό μήνυμα.
CIphertext: Το κρυπτογραφημένο μήνυμα.
Key: Το κλειδί (δημόσιο ή ιδιωτικό) που αποτελείται από μια σειρά αριθμών και χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.
Encryption: Η διαδικασία κρυπτογράφησης ενός μηνύματος.
Decryption: Η διαδικασία αποκρυπτογράφησης ενός μηνύματος και επαναφοράς του στην αρχική μορφή με την αντίστροφη εφαρμογή του αλγορίθμου κρυπτογράφησης. [19]

Ανάλογα με είδος του κλειδιού που χρησιμοποιούν (δημόσιο ή ιδιωτικό) χωρίζονται σε δύο κατηγορίες:
Αλγόριθμοι συμμετρικού κλειδιού
Αλγόριθμοι ασύμμετρου(ή δημόσιου) κλειδιού

Συμμετρική κρυπτογράφηση

Η συμμετρική κρυπτογράφηση βασίζεται στην ύπαρξη ενός κοινού, μυστικού κλειδιού για την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος. Ο αποστολέας και ο παραλήπτης του μηνύματος πρέπει να έχουν συμφωνήσει από πριν ποιο θα είναι το κλειδί που θα χρησιμοποιήσουν. Η ανταλλαγή θα γίνει μέσω της αποστολής του κλειδιού από ένα ασφαλές κανάλι επικοινωνίας ή με τη φυσική τους παρουσία. Η διαδικασία που ακολουθείται είναι η εξής:
Ο αποστολέας χρησιμοποιώντας το μυστικό κλειδί και τον κατάλληλο αλγόριθμο, κρυπτογραφεί το μήνυμα και το στέλνει στον παραλήπτη.
Ο παραλήπτης λαμβάνει το μήνυμα, με το ίδιο μυστικό κλειδί αποκρυπτογραφεί το μήνυμα και το διαβάζει.

Η ασφάλειά του έγκειται στη μυστικότητα του κλειδιού. Αν για οποιοδήποτε λόγο η επικοινωνία πάψει να είναι μυστική και αποκαλυφθεί το κλειδί σε μια τρίτη οντότητα η διαδικασία της κρυπτογράφησης χάνει το νόημα. Στα πλεονεκτήματα της χρήσης του συμμετρικού κλειδιού είναι ότι οι διαδικασίες της κρυπτογράφησης και αποκρυπτογράφησης εκτελούνται γρήγορα και χωρίς να καταναλώνουν σημαντική υπολογιστή ισχύ. Οι πιο γνωστοί αλγόριθμοι είναι DES, 3DES, AES, RC2,RC4.



Σχήμα 3.8: Συμμετρική κρυπτογράφηση

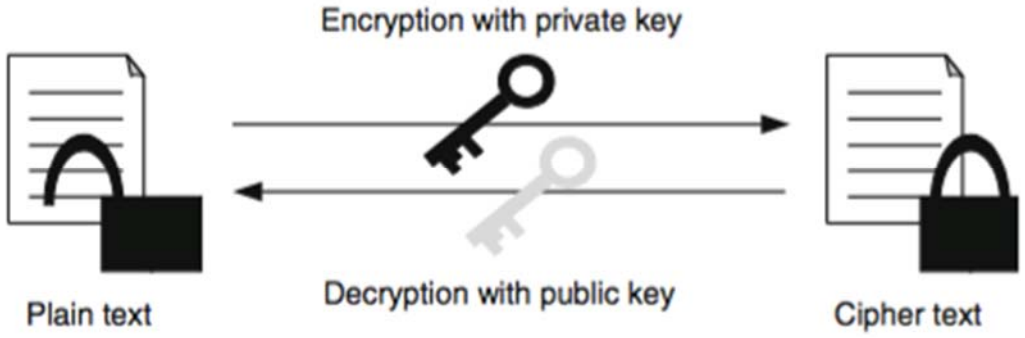
Ασύμμετρη κρυπτογράφηση

Η ασύμμετρη κρυπτογράφηση ή η κρυπτογράφηση δημόσιου κλειδιού βασίζεται στην ύπαρξη διαφορετικών κλειδιών για την κρυπτογράφηση και αποκρυπτογράφηση του μηνύματος. Σε αντίθεση με τη συμμετρική, ο αποστολέας και ο παραλήπτης δεν μοιράζονται το ίδιο κλειδί αλλά διαθέτουν δύο διαφορετικά, ένα δημόσιο και ένα ιδιωτικό. Το δημόσιο είναι διαθέσιμο σε όλους και μπορεί να είναι ανακοινωμένο σε όλη τη διαδικτυακή κοινότητα ή σε ορισμένους παραλήπτες. Το δημόσιο κλειδί χρησιμοποιείται για την κρυπτογράφηση του μηνύματος ενώ το ιδιωτικό κλειδί για την αποκρυπτογράφηση. Και τα δύο συνδέονται μέσω ενός μαθηματικού τύπου. Ο κάθε χρήστης έχει στην κατοχή του ένα ζευγάρι κλειδιών και η διαδικασία που ακολουθεί όταν θέλει να στείλει ένα μήνυμα είναι η ακόλουθη:

Ο Α θέλει να στείλει ένα μήνυμα στο χρήστη Β. Πριν το στείλει χρησιμοποιεί το δημόσιο κλειδί του Β για να το κρυπτογραφήσει και στη συνέχεια το στέλνει στον παραλήπτη.
Ο χρήστης Β λαμβάνει το κρυπτογραφημένο μήνυμα και χρησιμοποιώντας το ιδιωτικό του κλειδί, αποκρυπτογραφεί το μήνυμα και το διαβάζει.
Όποιος τρίτος ακούει τη σύνδεση δεν μπορεί να αποκρυπτογραφήσει το μήνυμα παρά μόνο αν έχει μάθει το ιδιωτικό κλειδί του παραλήπτη.

Κατά αυτό τον τρόπο εξασφαλίζεται η εμπιστευτικότητα της επικοινωνίας και λύνεται το πρόβλημα της μεταφοράς του ιδιωτικού κλειδιού που αντιμετώπιζε η συμμετρική κρυπτογράφηση. Ωστόσο είναι πιο αργή σαν διαδικασία. Η διαδικασία της ασύμμετρης κρυπτογράφησης ήταν η αρχή για τη δημιουργία ψηφιακών υπογραφών και ψηφιακών πιστοποιητικών. Γνωστοί αλγόριθμοι ασύμμετρης κρυπτογράφησης είναι ο RSA, El Gamal και ο DSA.

Σε μια σύγχρονη εποχή που οι κακόβουλοι χρήστες κάνουν συνεχές πόλεμο, τα κρυπτογραφικά συστήματα πρέπει να εφαρμόζονται με τρόπο αποτελεσματικό, όσον αφορά την ταχύτητα, τους πόρους και την ενέργεια που καταναλώνουν.[29] Για να χαρακτηριστεί ένα σύστημα κρυπτογράφησης ασφαλές θα πρέπει να ικανοποιούνται κάποια κριτήρια. Πρώτον, το κόστος της παραβίασης του κρυπτομηνύματος (δηλαδή το κόστος που απαιτείται για την ανάκτηση του κλειδιού κρυπτογράφησης) να υπερβαίνει την αξία των πληροφοριών που λαμβάνονται μετά την αποκρυπτογράφηση του μηνύματος και δεύτερον ο χρόνος που απαιτείται για τη διαδικασία της κρυπτανάλυσης να υπερβαίνει την ωφέλιμη διάρκεια ζωής των ληφθέντων πληροφοριών.



Σχήμα 3.9: Ασύμμετρη κρυπτογράφηση

Βιομετρικά συστήματα

Βιομετρικά καλούνται τα συστήματα που χρησιμοποιούνται για την ταυτοποίηση των ατόμων μέσω της ανάλυσης σταθερών χαρακτηριστικών τους όπως του προσώπου, των δακτυλικών αποτυπωμάτων, της ίριδας. Οι βιομετρικές μέθοδοι μπορούν να χωριστούν σε δύο κατηγορίες: Εκείνες που στηρίζονται στην ανάλυση φυσικών ή γενετικών χαρακτηριστικών και σε εκείνες που στηρίζονται στην ανάλυση συμπεριφοράς, όπως φωνής, υπογραφής. Για να γίνει η βιομετρική αναγνώριση του ατόμου θα πρέπει να έχει προηγηθεί μια διαδικασίας λήψης βιομετρικού δείγματος το οποίο έχει αποθηκευτεί σε διάφορες συσκευές και όταν ο χρήστης απαιτήσει πρόσβαση στο σύστημα γίνεται σύγκριση με το αποθηκευμένο δείγμα. Οι τρόποι αποθήκευσης μπορεί να είναι το ίδιο το βιομετρικό σύστημα, μια κεντρική βάση δεδομένων, μια φορητή εξωτερική συσκευή. Πρόσβαση στο χρήστη θα δοθεί αν ταιριάζει με το βιομετρικό πρότυπο με μερικές αποκλίσεις που έχουν οριστεί ήδη από το σύστημα.[09]

Τα βιομετρικά συστήματα έχουν αναπτυχθεί για να καλύψουν τις ανάγκες ταυτοποίησης και αυθεντικοποίησης ενός πληροφοριακού συστήματος με ακρίβεια, αξιοπιστία και ταχύτητα. Είναι μια νέα τεχνολογία που αφήνει πίσω μεθόδους όπως κωδικοί πρόσβασης, log in, κάρτες εισόδου που ανά πάσα στιγμή μπορεί να κλαπούν. Η χρήση βιομετρικών μεθόδων απαιτεί τη φυσική παρουσία του ενδιαφερόμενου.[19]

Δακτυλικά αποτυπώματα

Τα δακτυλικά αποτυπώματα θεωρούνται εδώ και χρόνια ένας αξιόπιστος τρόπος αναγνώρισης και ταυτοποίησης προσώπων χρησιμοποιούμενος κυρίως από τις αστυνομικές αρχές. Μπορεί να είναι ένας παρεξηγημένος τρόπος αλλά δεν παύει να προτιμάται αφού τα χαρακτηριστικά των δακτυλικών αποτυπωμάτων είναι μοναδικά για τον καθένα. Τα βιομετρικά αυτά συστήματα χωρίζονται σε δύο κατηγορίες. Στην πρώτη κατηγορία ανήκουν εκείνα τα συστήματα που κάνουν εξακρίβωση ταυτότητας και στη δεύτερη αυτά που κάνουν απλά μια επιβεβαίωση. Για κάθε περίπτωση είναι η απαραίτητη η ανάγνωση του αποτυπώματος η οποία μπορεί να γίνει με τρεις διαφορετικούς τρόπους. Η πρώτη αναφέρεται στην οπτική ανάγνωση όπου ο χρήστης τοποθετεί το δάκτυλό του σε μια επιφάνεια και χρησιμοποιώντας τον κατάλληλο φωτισμό, γίνεται η λήψη της εικόνας. Ο δεύτερος τρόπος αναγνώρισης γίνεται με τη χρήση υπερήχων. Χωρίς να απαιτείται άμεση επαφή του δακτύλου με τον σαρωτή, ακουστικά κύματα φτάνουν στο δάκτυλο και μετρούν την πυκνότητα. Τέλος η τρίτη και πιο εξελιγμένη μέθοδος γίνεται με τη χρήση ενός αισθητήρα ο οποίος λαμβάνει τη θερμότητα ή την πίεση του δακτύλου και την μετατρέπει σε δεδομένα. Ωστόσο υπάρχουν και κάποιες δυσκολίες κατά την εφαρμογή αυτής της βιομετρικής μεθόδου. Η πιο δύσκολη είναι η ανάγνωση των δακτυλικών αποτυπωμάτων όταν υπάρχει κάποιος τραυματικός ή το δέρμα δεν είναι καθαρό ή αρκετά ξηρό ή λιπαρό. Επίσης λάθος καταγραφή μπορεί να γίνει από υπερβολική πίεση στο σύστημα.

Εικόνα 3.3: Δακτυλικά αποτυπώματα

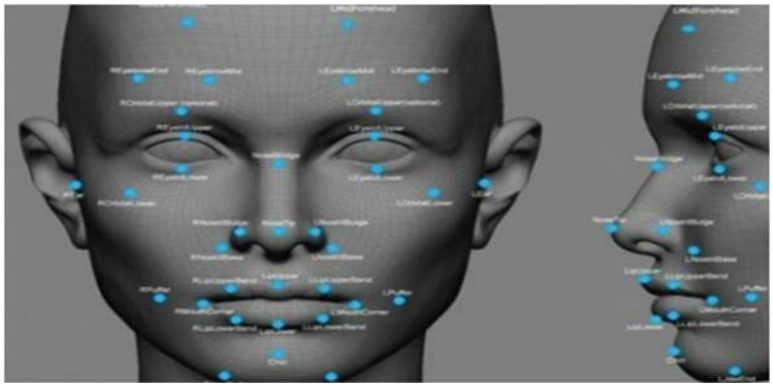
Ίριδα

Τα επόμενα βιομετρικά συστήματα σχεδιάστηκαν για να αναγνωρίζουν την ίριδα, ένα τμήμα του ματιού που διαθέτει μοναδικά, αμετάβλητα χαρακτηριστικά σε βάθος χρόνου και δεν είναι τόσο επιρρεπή σε εξωτερικούς παράγοντες που μπορεί να τα μεταβάλλουν. Η αναγνώριση της ίριδας αποτελεί τον πιο ασφαλή τρόπο ταυτοποίησης αλλά συγχρόνως και τον πιο ακριβό. Μπορεί να γίνει με δυο διαφορετικές τεχνικές. Η πρώτη είναι η ενεργητική διαδικασία κατά την οποία με τις υποδείξεις του προσωπικού, ο χρήστης τοποθετεί το κεφάλι του μπροστά σε μια κάμερα με τέτοιο τρόπο ώστε να εστιάζει στην ίριδα. Αντίθετα, η άλλη τεχνική που ονομάζεται παθητική περιλαμβάνει πολλές κάμερες οι οποίες εστιάζουν πρώτα στο πρόσωπο του χρήστη, έπειτα στο μάτι και τέλος στην ίριδα χωρίς ο χρήστες να έχει άμεση συμμετοχή.

Εικόνα 3.4: Ανάλυση της ίριδας του ματιού

Αναγνώριση προσώπου

Η αναγνώριση προσώπου είναι μια ακόμα βιομετρική μέθοδος που αναπτύχθηκε με σκοπό την ταυτοποίηση του ανθρώπου από τα χαρακτηριστικά του προσώπου του. Οι κάμερες του συστήματος καταγράφουν τα χαρακτηριστικά του προσώπου, μάτια, μύτη, στόμα βλέφαρα σε μέγεθος αλλά τις αποστάσεις που έχουν μεταξύ τους. Τα δεδομένα αυτά αποθηκεύονται σε μια βάση δεδομένων. Έτσι λοιπόν κάποιος που ζητά πρόσβαση, ελέγχεται το πρόσωπο του και αν ταιριάζει με το βιομετρικό πρότυπο που είναι αποθηκευμένο στη βάση δεδομένων, ταυτοποιείται και εισέρχεται. Μια ακόμα μέθοδος που χρησιμοποιείται για την αναγνώριση του προσώπου είναι η θερμογραφία. Κατά τη διαδικασία αυτή, μια υπέρυθρη κάμερα χαρτογραφεί τη ροή του αίματος κάτω από την επιφάνεια του δέρματος και οι σχηματισμοί που προκύπτουν δημιουργούν το πρότυπο που με τη σειρά του χρησιμοποιείται για την επιβεβαίωση της ταυτότητας του ανθρώπου. Ενώ είναι μια απλή και γρήγορη διαδικασία, η αναξιοπιστία της έγκειται στο γεγονός ότι τα χαρακτηριστικά του προσώπου αλλάζουν με το πέρασμα του χρόνου ή ο ίδιος ο άνθρωπος αποφασίσει να τα αλλάξει.



Εικόνα 3.6: Ανάλυση προσώπου

Smart cards

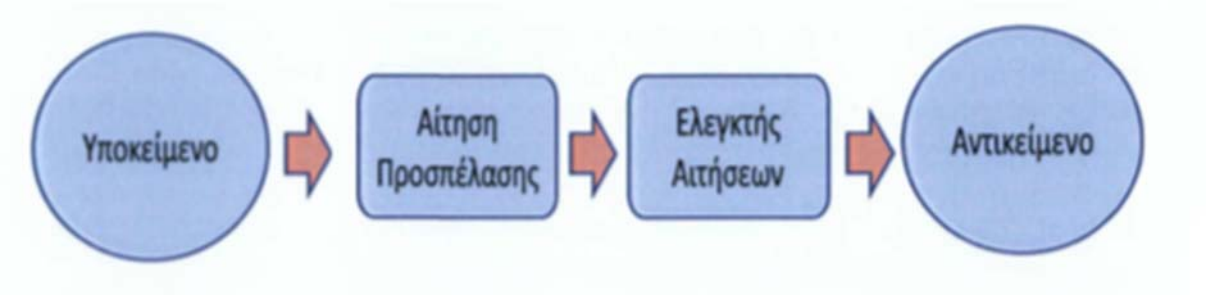
Ως έξυπνες κάρτες μπορούμε να ορίσουμε τις κάρτες που έχουν τη μορφή μιας πιστωτική κάρτας αλλά έχουν ενσωματωμένο ένα ολοκληρωμένο κύκλωμα το οποίο διαθέτει μνήμη και μικροεπεξεργαστή. Μπορούν να αποθηκεύουν και να επεξεργάζονται πληροφορίες με γρήγορο και ασφαλή τρόπο όποτε ζητηθεί. Ανάλογα με την ικανότητα επεξεργασίας διακρίνονται σε:
Κάρτες μνήμης/ κάρτες αποθήκευσης πληροφοριών (memory cards): δε διαθέτουν επεξεργαστή απλά περιέχουν κάποια μνήμη για να αποθηκεύουν ή να διαγράφουν τιμές.
Έξυπνε κάρτες (smart cards): έξυπνες κάρτες που έχουν ή και όχι μικροεπεξεργαστή ο οποίος αποθηκεύει με ασφάλεια τις πληροφορίες.
Έξυπνες κάρτες πολλαπλών εφαρμογών (multi-application smart cards): χρησιμοποιούνται όπως οι έξυπνες κάρτες με δυνατότητα να εκτελούν περισσότερες από μια εφαρμογές. Ο χρήστης με βάση τις ανάγκες του ορίζει για ποιες εφαρμογές θα την χρησιμοποιήσει.

Ανάλογα με τις δυνατότητες εισόδου/εξόδου οι έξυπνες κάρτες διακρίνονται σε:
Έξυπνες κάρτες με επαφές οι οποίες για να λειτουργήσουν πρέπει να τοποθετηθούν σε μια συσκευή ανάγνωσης.
Ασύρματες έξυπνες κάρτες οι οποίες έχουν ενσωματωμένη μια μικροσκοπική κεραία και μπορούν να επικοινωνούν απομακρυσμένα με την κεραία της συσκευής ανάγνωσης για να διαβάσουν ή να τροποποιήσουν την αποθηκευμένη πληροφορία.
Υβριδικές ή συνδυασμένες κάρτες οι οποίες έχουν συνδυάσει και τους δυο τρόπους επικοινωνίας και λειτουργούν ενσύρματα και ασύρματα.
Οι έξυπνες κάρτες έχουν πληθώρα εφαρμογών σε τομείς της καθημερινής ζωής. Εκτός από πρόσβαση σε κτίρια μέσω της ταυτοποίησης του ανθρώπου μπορεί να χρησιμοποιηθεί για πρόσβαση σε ανοιχτά και κλειστά δίκτυα αφού έχουν αποθηκευτεί πληροφορίες ελέγχου πρόσβασης και ψηφιακά πιστοποιητικά, για τραπεζικές συναλλαγές, ως κάρτα υγείας, ως κάρτες GSM ή τηλεκάρτες, ως δίπλωμα οδήγησης.

Μηχανισμοί ελέγχου πρόσβασης

Οι μηχανισμοί ελέγχου πρόσβασης αποτελούν πολιτικές ασφαλείας που έχουν δημιουργηθεί για να καλύψουν τις απαιτήσεις ενός πληροφοριακού συστήματος. Δεν πρέπει να ξεχνάμε ότι η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα είναι τα βασικά χαρακτηριστικά της ασφάλειας και δεν πρέπει να παραβιάζονται για κανέναν λόγο. Επομένως έχουν δημιουργηθεί κανόνες και οδηγίες που ελέγχουν την πρόσβαση του κάθε χρήστη καθώς και τις αρμοδιότητές του. Με τον έλεγχο προσπέλασης δίνεται στο χρήστη πρόσβαση στο σύστημα αφού πρώτα έχει ταυτοποιηθεί και στη συνέχεια αφού αποκτήσει νόμιμη πρόσβαση ανάλογα με τα δικαιώματα που έχει, αποκτά πρόσβαση και στην πληροφορία. [31] Οι μηχανισμοί ελέγχου περιλαμβάνουν:

Μηχανισμό αυθεντικοποίησης του χρήστη
Μηχανισμό διαχείρισης των δικαιωμάτων του χρήστη
Μηχανισμό ελέγχου και καταγραφής ενεργειών
Μηχανισμό λήψης απόφασης και εξουσιοδότησης
Μηχανισμό επιβολής του ελέγχου εξουσιοδότησης



Σχήμα 3.10: Μηχανισμός ελέγχου

Ουσιαστικά ο έλεγχος προσπέλασης αποτελείται από δυο τμήματα: από τον μηχανισμό που θα αποφασίσει αν θα δοθεί ή όχι η άδεια προσπέλασης και ένα μηχανισμό που ορίζει την απόφαση.

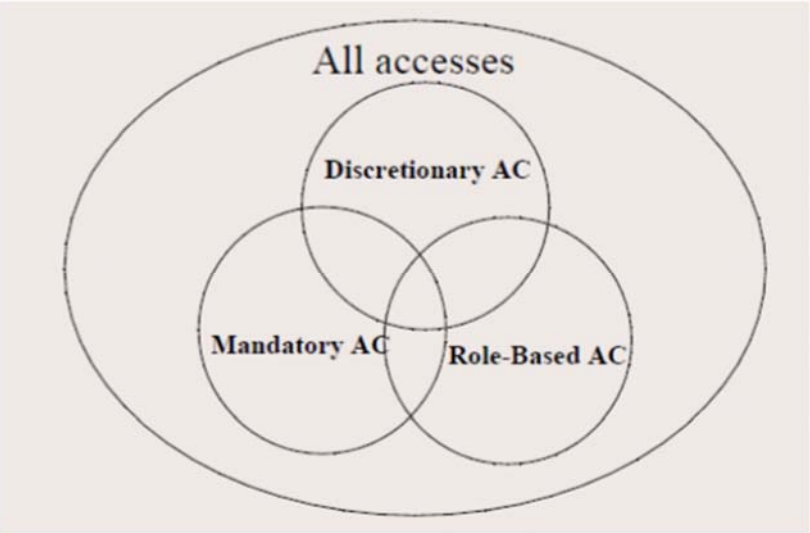
Οι πολιτικές αυτές ασφαλείας που εφαρμόζονται ανάλογα με το βαθμό εμπιστοσύνης και το βαθμό ευαισθησίας της πληροφορίας διακρίνονται σε:

Άκρως απόρρητο (top secret)
Απόρρητο (secret)
Εμπιστευτικό (confidential)
Αδιαβάθμητο (unclassified)

Σχήμα 3.11: Διαβάθμιση της ευαισθησίας της πληροφορίας

Υπάρχουν τρεις μηχανισμοί προσπέλασης

Κατ' απαίτηση
Κατά διάκριση
Βασισμένος σε ρόλους



Σχήμα 3.12: Απεικόνιση των μηχανισμών προσπέλασης

Προαιρετικός έλεγχος πρόσβασης-Κατά διάκριση

Το μοντέλο DAC καθορίζει τους κανόνες που ορίζουν ποιος έχει πρόσβαση, σε ποιο αντικείμενο και σε τι βαθμό. Το μοντέλο αυτό βασίζεται στη λογική του κατόχου-ιδιοκτησίας. Πιο συγκεκριμένα, ένας χρήστης πληροφοριακού συστήματος κατέχει κάποιους πόρους αυτού. Εφόσον είναι ιδιοκτήτης (υποκείμενο) των πόρων (αντικείμενα) ορίζει ο ίδιος ποια είναι τα δικαιώματα που έχει για τα αντικείμενα αυτά όπως επίσης έχει τη δυνατότητα να τα τροποποιήσει ή να τα αφαιρέσει τελείως. Επιπλέον μπορεί να τα παραχωρήσει και σε άλλους χρήστες. Ουσιαστικά ο μηχανισμός αυτός καθορίζει το πλήθος και το είδος των πόρων του κάθε χρήστη και το δικαίωμα εξουσιοδότησης που έχει σε αυτά. Χρήστες με ίδια δικαιώματα πρόσβασης ανήκουν στην ίδιο ομάδα υποκειμένων. Σε περίπτωση που δημιουργηθούν νέοι πόροι, ο χρήστης ακολουθεί την ίδια διαδικασία. Αφού ορισθούν οι κανόνες πρόσβασης, δημιουργείται στο σύστημα ένας πίνακας ελέγχου πρόσβασης που αποθηκεύει τα δεδομένα και τον συνδυασμό υποκείμενο-αντικείμενο-δικαίωμα μοντελοποιώντας τις πολιτικές εξουσιοδότησης της επιχείρησης. Για το λόγο όμως ότι οι πίνακες δύσκολα προσαρμόζονται στην εισαγωγή νέων εγγραφών που συνεπάγεται και αύξηση του μεγέθους και γενικότερα η σχετικά δύσκολη διαχείρισή τους οδήγησε στην υλοποίηση του μοντέλου με τη χρήση δύο λιστών. Η πρώτη λίστα ονομάζεται λίστα ελέγχου πρόσβασης και δίνει απάντηση στο ερώτημα ποια είναι τα δικαιώματα πρόσβασης στο αντικείμενο και η δεύτερη λίστα, λίστα δυνατοτήτων καταγράφει τι είδους δικαιώματα έχει το υποκείμενο.

Έστω ότι ένας χρήστης χ ζήτα πρόσβαση από τον ελεγκτή του συστήματος για το αντικείμενο α. Ο ελεγκτής με τη σειρά θα ελέγξει τον πίνακα για να διαπιστώσει ότι όντως ο χρήστης χ έχει δικαιώματα ως προς τον πόρο που ζήτησε. Αν τον εντοπίσει στο στον πίνακα τότε του επιτρέπει και την πρόσβαση αλλιώς την απορρίπτει και πιθανόν να εκτελέσει περαιτέρω ενέργειες ώστε το πληροφοριακό σύστημα να παραμείνει ασφαλές.

Κάθε φορά που ο χρήστης εκτελεί τροποποιήσεις σε δικαιώματα ή πόρους με την έννοια της προσθήκης, διαγραφής, ανάκλησης ή παραχώρησης οφείλει να ενημερώνει τον διαχειριστή του συστήματος για να παίρνει και την τελική έγκριση. Παρ' όλα αυτά δεν κρίνεται και τόσο ασφαλής ως μηχανισμός ελέγχου αφού ο ιδιοκτήτης του πόρου έχει τη μεγαλύτερη ευθύνη για τους πόρους που διαχειρίζεται.

Κατά απαίτηση

Το μοντέλο Κατά απαίτηση MAC ή ο υποχρεωτικός έλεγχος πρόσβασης βασίζεται σε διαβάθμιση της πληροφορίας. Κάθε πόρος του συστήματος κατατάσσεται σε διαφορετικά επίπεδα ασφάλειας ανάλογα με την αξία και τη σημαντικότητά του για το πληροφοριακό σύστημα που ανήκει όπως επίσης και με τις συνέπειες που θα αντιμετωπίσει η επιχείρηση σε περίπτωση που πληγεί η ασφάλειά του. Η διαβάθμιση αυτή που ουσιαστικά καθορίζει και την ευαισθησία της πληροφορίας υποδηλώνεται με τη χρήση ετικετών οι οποίες είναι οι εξής:
Άκρως απόρρητο (top secret)
Απόρρητο (secret)
Εμπιστευτικό (confidential)
Αδιαβάθμητο (unclassified)

Αντίστοιχη διάκριση υπάρχει και στα δικαιώματα που έχει ένας χρήστης πάνω στην πληροφορία με τη χρήση των παραπάνω ετικετών ασφάλειας. Αυτές οι ετικέτες προσδιορίζουν το βαθμό που ένας χρήστης έχει εξουσιοδότηση στην πληροφορία ώστε το σύστημα να μην διακυβεύονται τα βασικά χαρακτηριστικά της εμπιστευτικότητας, της ακεραιότητας και της αυθεντικότητας, και το σύστημα να παραμένει ασφαλές. Με τη χρήση του μοντέλου αυτού γίνεται καλύτερη και πιο ασφαλή διαχείριση της πληροφορίας εφόσον δεν είναι πλέον στη διακριτική ευχέρεια του χρήστη να ορίσει τις πολιτικές εξουσιοδότησης αλλά του ίδιου του συστήματος που είναι υπεύθυνο να επιβάλλει τους κανόνες προσπέλασης. Η πιο γνωστή υλοποίηση του μοντέλου στηρίζεται στο μοντέλο Bell Lapadula σύμφωνα με το οποίο εφαρμόζονται δύο βασικοί κανόνες.

1. Κανένα υποκείμενο δεν μπορεί να διαβάσει δεδομένα ενός υψηλότερου επιπέδου.
2. Κανένα υποκείμενο δεν μπορεί να γράψει δεδομένα σε ένα χαμηλότερο επίπεδο.

Για παράδειγμα αν ένας χρήστης που έχει χαρακτηριστεί ως απόρρητος μπορεί να διαβάσει την πληροφορία του εμπιστευτικού και του αδιαβάθμητου αλλά όχι του απόρρητου. Επιπλέον μπορεί να γράψει πληροφορία που θα χαρακτηριστεί απόρρητη ή άκρως απόρρητη αλλά όχι εμπιστευτική ή αδιαβάθμητη.

Υπάρχει μια ακόμα μοντελοποίηση, το μοντέλο Biba που εξασφαλίζει την ακεραιότητα και πληροφορίας και βασίζεται σε δύο βασικούς κανόνες.

Κανένα υποκείμενο δεν μπορεί να διαβάσει δεδομένα σε ένα χαμηλότερο επίπεδο.
Κανένα υποκείμενο δεν μπορεί να γράψει δεδομένα σε ένα υψηλότερο επίπεδο.

Για παράδειγμα, αν ο χρήστης έχει χαρακτηριστεί ως απόρρητος δεν μπορεί να γράψει πληροφορία άκρως απόρρητη αλλά μπορεί να δημιουργήσει νέα δεδομένα τα οποία θα προσδιοριστούν ως εμπιστευτικά ή αδιαβάθμητα και μπορεί να διαβάσει δεδομένα με τη διαβάθμιση απόρρητο ή άκρως απόρρητο αλλά όχι δεδομένα που ανήκουν στην εμπιστευτική ή αδιαβάθμητη κατηγορία.

Έλεγχος πρόσβασης με βάση τους ρόλους

Όπως λέει και το όνομά του, το μοντέλο αυτό βασίζεται σε ρόλους. Πιο συγκεκριμένα ανάλογα με τις αρμοδιότητες που έχει ένας χρήστης αποκτά διαφορετικά δικαιώματα ως προς τα αντίστοιχα αντικείμενα. Με τον τρόπο αυτό κάθε χρήστης μπορεί να έχει περισσότερους του ενός ρόλους και διαφορετικές εξουσιοδοτήσεις. Ακόμα, ένας ρόλος μπορεί να ανήκει σε περισσότερους του ενός χρήστες. Για το λόγο αυτό, τα δικαιώματα πρόσβασης σε ένα

αντικείμενο παραχωρούνται στους ρόλους επομένως όποιος χρήστης έχει αναλάβει τον συγκεκριμένο λόγο έχει και πρόσβαση στα αντίστοιχα αντικείμενα. Κάθε ρόλος έχει τα ίδια δικαιώματα πρόσβασης αλλά κληρονομεί και τα δικαιώματα πρόσβασης που βρίσκονται σε υψηλότερο επίπεδο από αυτός. Γίνεται δηλαδή μια διαβάθμιση των ρόλων η οποία ονομάζεται ιεραρχία.[39, 44]

Με τον τρόπο που είναι δομημένο το μοντέλο θα λέγαμε ότι συνδυάζει δυο σημαντικά χαρακτηριστικά των προηγούμενων μοντέλων:

Την ευελιξία του κατά διάκριση μοντέλου με την έννοια ότι σε κάθε χρήστη ανατίθενται ρόλοι που με τη σειρά τους καθορίζουν τα δικαιώματα πρόσβασης του χρήστη. Σε περίπτωση λοιπόν που για κάποιο λόγο χρειάζεται να διαγραφούν δικαιώματα του χρήστη απλά ανακαλείται ο ρόλος του που τα περιλαμβάνει και για οποιαδήποτε αλλαγή των δικαιωμάτων ανακαλούνται οι παλιοί και ορίζονται οι καινούριοι. Για κάθε νέες ενέργειες και αρμοδιότητες δημιουργούνται και νέοι ρόλοι που αναθέτονται στους κατάλληλους χρήστες. Να επισημάνουμε ότι τα δικαιώματα των χρηστών διαρκούν όσο είναι ενεργοί οι ρόλοι του. Τον έλεγχο της ροής της πληροφορίας του κατά απαίτηση μοντέλου με την έννοια ότι τα δικαιώματα πρόσβασης ορίζονται από το ίδιο το σύστημα στους ρόλους.

Πρωτόκολλο ίντερνετ IPsec

Το πρωτόκολλο ίντερνετ είναι μια συλλογή πρωτοκόλλων που μπορεί να εφαρμοστεί στο στρώμα του διαδικτύου με σκοπό την ασφάλεια της μετάδοσης της πληροφορίας αφού προστατεύει κάθε κυκλοφορία εφαρμογής που γίνεται μέσω δικτύου. Πιο συγκεκριμένα, στις λειτουργίες του περιλαμβάνει έλεγχο ταυτότητας, κρυπτογράφηση των πακέτων που στέλνονται εξασφαλίζοντας την ακεραιότητα και εμπιστευτικότητα των δεδομένων και την προστασία τους από παράνομη αναπαραγωγή. Εξασφαλίζει ακόμα την αυθεντικότητα, προστατεύεται ολόκληρο το φορτίο ή μόνο το ωφέλιμο και οι αλγόριθμοι που εφαρμόζει είναι md5 Rsa, sha (ακεραιότητα) και 3DES, AES (εμπιστευτικότητα). Χρησιμοποιούνται μεταξύ ενός ζεύγους πυλών ή ενός ζεύγους υποδοχών ή μεταξύ μίας πύλης και μιας υποδοχής. Λειτουργεί με δύο διαφορετικούς τρόπους. Το transport mode σύμφωνα με το οποίο κρυπτογραφείται μόνο το ωφέλιμο φορτίο του πακέτου και όχι οι επικεφαλίδες και τα επιμέρους τμήματα και το tunnel mode που κρυπτογραφείται όλο το πακέτο μαζί με τις επικεφαλίδες.

Κεφάλαιο 4

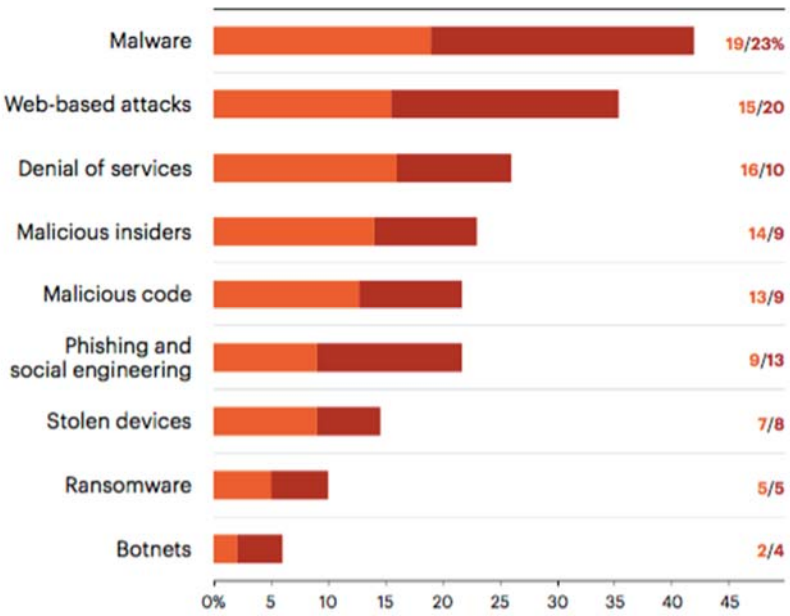
Η οικονομική προσέγγιση της κυβερνοασφάλειας

Οι επιχειρήσεις επενδύουν τεράστια χρηματικά ποσά για την προστασία των πληροφοριακών συστημάτων ωστόσο δεν είναι ικανά για την πλήρη κάλυψη των επιθέσεων με αποτέλεσμα να οδηγούνται σε οικονομικές απώλειες. Στο παρόν κεφάλαιο γίνεται ανάλυση των οικονομικών πτυχών της ασφάλειας του κυβερνοχώρου. Πιο συγκεκριμένα, κατηγοριοποιείται το κόστος που προκύπτει ως επένδυση των επιχειρήσεων και το κόστος που προκύπτει μετά την ολοκλήρωση ενός περιστατικού, περιγράφονται οικονομικοί δείκτες, ποσοτικοί και ποιοτικοί, που σχετίζονται με την ασφάλεια και την πιθανότητα πραγματοποίησης μιας επίθεσης καθώς και μοντέλα που ορίζουν τον τρόπο που οι υπεύθυνοι λήψης αποφάσεων θα πρέπει να λαμβάνουν τις σωστές αποφάσεις για την επιλογή και εφαρμογή των κατάλληλων εναλλακτικών για την ενίσχυση και βελτίωση της ασφάλειας του κυβερνοχώρου

Σύμφωνα με έρευνα που πραγματοποιήθηκε για το 2017, το μέσο παγκόσμιο κόστος των επιθέσεων στον κυβερνοχώρου αυξάνεται. Τα τρία πρώτα χρόνια ήταν σταθερή όμως το 2017 υπήρξε σημαντική αύξηση που άγγιξε το 27,4% συγκριτικά με την προηγούμενη χρονιά. Ο χρηματοπιστωτικός κλάδος και οι εταιρείες υπηρεσιών κοινής ωφέλειας και ενέργειας αντιμετωπίζουν το υψηλότερο ετήσιο κόστος σε αντίθεση με τις επιχειρήσεις που σχετίζονται με την εκπαίδευση και την φιλοξενία που υπέστησαν πολύ χαμηλότερο. Ωστόσο κάθε επιχείρηση ανεξαρτήτως τομέα και μεγέθους είναι καλό να διαχειρίζεται και αναλύει το κόστος μια δυνητικής επίθεσης καθώς και το κόστος επένδυσης πριν λάβει τη σωστή για εκείνη απόφαση. Αυτό έχει ως επακόλουθο οι ειδικοί να εστιάζουν σε τρόπους που θα οδηγήσουν στη μείωση των οικονομικών απωλειών. [21]

Σχήμα 4.1: Κόστος επιτυχημένων κυβερνοεπιθέσεων

Στη ίδια έρευνα καταγράφεται και το κόστος που προκύπτει στην επιχείρηση ανάλογα με το είδος της επίθεσης που δέχτηκε. Οι επιθέσεις από κακόβουλο λογισμικό τύπου malware προκαλούν το μεγαλύτερο κόστος με αμέσως επόμενες τις web-based attacks. Στο παρακάτω διάγραμμα παρουσιάζεται το αντίστοιχο κόστος.



Σχήμα 4.2: Κόστος ανά τύπο επίθεσης

4.1 Ανάλυση Κόστους

Έχοντας μελετήσει την ύψιστη σημασία της πληροφορίας και την άμεση ανάγκη των οργανισμών για προστασία από δυνητικές επιθέσεις, κάθε οργανισμός οφείλει τη λήψη αντιμέτρων για να είναι σε θέση να αντιμετωπίσει περιστατικά ασφαλείας. Προτού αξιολογήσει τις εναλλακτικές λύσεις και αποφασίσει ποιο είναι το κατάλληλο μέτρο που θα εφαρμόσει, θα πρέπει να υπολογίσει τα κόστη που θα προκύψουν στον οργανισμό τόσο κατά την εφαρμογή των μέτρων όσο και για τις οικονομικές επιπτώσεις που έρχονται ως αποτέλεσμα μιας επιτυχημένης επίθεσης. Μπορούμε να πούμε ότι κόστος είναι τα χρήματα που χρειάζονται για την ανάπτυξη, επένδυση, παραγωγή και αγορά.

Έτσι λοιπόν μπορούμε να χωρίσουμε το κόστος σε δύο μεγάλες κατηγορίες:

- Το προληπτικό κόστος
- Το κόστος μετά από μια εκδήλωση επιτυχημένης επίθεσης

4.1.1 Το προληπτικό κόστος

Ως προληπτικό κόστος ορίζουμε το κεφάλαιο που είναι διατεθειμένος ο οργανισμός να επενδύσει για να εξασφαλίσει ένα επίπεδο ασφαλείας το οποίο είναι ικανό να προστατεύσει, στο σημείο που έχει ορίσει, τα πληροφοριακά συστήματα της εταιρείας και να διασφαλίσει την επιχειρησιακή συνέχεια του οργανισμού. Τα έξοδα αυτά είναι καθόλη τη διάρκεια του κύκλου επένδυσης και διακρίνονται σε έξοδα λήψης αποφάσεων, κόστη σχεδιασμού, λειτουργίας, συντήρησης και αρχικού επενδυτικού κόστους. Σύμφωνα με έρευνα του Gartner ,υπολογίζεται ότι μέσα στο 2018 θα δαπανηθούν παγκοσμίως σε θέματα κυνερνοασφάλειας 96 δισεκατομμύρια δολάρια.

Κόστος διαδικασίας λήψης απόφασης: Ο υπεύθυνος λήψης απόφασης θα πρέπει να επενδύσει πολύ χρόνο και προσπάθεια για τον προσδιορισμό των προβλημάτων και την επιλογή της ιδανικής λύσης μεταξύ εναλλακτικών. Κατά τη διαδικασία αυτή γίνεται αξιολόγηση του

κινδύνου και του κόστους, εργασίες που απαιτούν αρκετή δουλειά τόσο από τους υπεύθυνους λήψης αποφάσεων όσο και από τους εμπειρογνώμονες.

Κόστος προγραμματισμού: Το κόστος προγραμματισμού περιλαμβάνει το κόστος σχεδιασμού της λύσης, την υλοποίηση και εφαρμογή της. Πρέπει να δοθεί ιδιαίτερη προσοχή σε αυτό το στάδιο γιατί οποιεσδήποτε παραλείψεις και αστοχίες μπορεί να οδηγήσουν σε επιπρόσθετο κόστος.

Κόστος ευκαιρίας: Πραγματοποιείται κάθε φορά που επενδύεται κεφάλαιο. Πιο συγκεκριμένα, όταν το κεφάλαιο επενδύεται για μια διασφάλιση, δεσμεύεται εκεί και δεν μπορεί να χρησιμοποιηθεί για άλλο σκοπό. Τα κέρδη που χάνονται από τη μη αξιοποίηση του κεφαλαίου σε άλλες εναλλακτικές ονομάζεται κόστος ευκαιρίας.

Κόστος συντήρησης: Περιλαμβάνει τα έξοδα που σχετίζονται με αλλαγές και βελτιώσεις στις υπάρχουσες διασφαλίσεις προκειμένου να προσαρμοστούν στις νέες ανάγκες του οργανισμού και στα σύγχρονα περιβάλλοντα και να ανταποκριθούν στους επιχειρηματικούς στόχους. Το ποσό που δαπανάται εξαρτάται από το είδος και την πολυπλοκότητα της αλλαγής. Πολλές φορές αυτές οι αλλαγές συνεπάγονται και αλλαγές που πρέπει να γίνουν σε εγχειρίδια χρήσης συστημάτων, σε εκπαιδευτικά σεμινάρια των εργαζόμενων με το αντίστοιχο κόστος.

Κόστος λειτουργίας: Το κόστος λειτουργίας εμπεριέχει δαπάνες σχετικά με όλες τις ενέργειες που γίνονται για να εξασφαλιστεί η ομαλή λειτουργία και αποτελεσματικότητα της διασφάλισης σε μελλοντικό χρόνο. Τέτοια έξοδα μπορεί να είναι η διαχείριση, η υποστήριξη και η χορήγηση αδειών.

- Διαχείριση: Η λειτουργία αυτή είναι ιδιαίτερα σημαντική γιατί συμβάλλει στη διαμόρφωση και ομαλή λειτουργία του συστήματος για να μπορεί να ανταποκρίνεται επιτυχώς στις όποιες αλλαγές γίνουν οι οποίες απαιτούν χειροκίνητες ενέργειες. Για παράδειγμα διαγράφει ή προσθέτει παλιούς και νέους χρήστες, αλλάζει τις ρυθμίσεις του συστήματος για να προσαρμοστεί στις νέες συνθήκες, περιλαμβάνει ακόμα και πλαίσιο συντήρησης.
- Υποστήριξη: Η υποστήριξη εκτείνεται σε δύο επίπεδα, την υποστήριξη χρηστών και την υποστήριξη της εταιρείας. Κατά την υποστήριξη του χρήστη, η εταιρεία θα πρέπει να δίνει τη δυνατότητα στους χρήστες να ζητήσουν βοήθεια σε τυχόν δυσκολίες που μπορεί να αντιμετωπίσουν. Για παράδειγμα αν ένας χρήστης έχει ξεχάσει τον κωδικό πρόσβασης σε ένα σύστημα το οποίο είναι απαραίτητο στην εργασία του, απευθύνεται στην ομάδα υποστήριξης για να τον εξυπηρετήσει. Όσο αφορά την υποστήριξη της εταιρείας, η επιχείρηση οφείλει να είναι σε θέση να αντιμετωπίσει προβλήματα τεχνικού επιπέδου που πιθανόν να προκύψουν στα συστήματα ασφαλείας και δεν μπορεί να τα διαχειριστεί εσωτερικά με τους πόρους που διαθέτει. Στρέφεται λοιπόν στους υπεύθυνους από τους οποίους προμηθεύτηκε το σύστημα για να αντιμετωπίσουν τα ενδεχόμενα προβλήματα.
- Χορήγηση αδειών: Κατά την απόκτηση μιας διασφάλισης, ειδικά σε περιπτώσεις απόκτησης καινούριου λογισμικού, είναι απαραίτητη και η αγορά της άδειας νόμιμης χρήσης. Αυτό μπορεί να είναι κόστος μιας φοράς, κατά την πρώτη δηλαδή αγορά, μπορεί να χρειάζεται να ανανεώνεται κατά κάποιο χρονικό διάστημα οπότε και να αποτελεί τακτικό κόστος. Σε κάθε περίπτωση είναι αναγκαία αυτή η αγορά καθώς αν παρατηρηθεί παράνομη χρήση συστημάτων η επιχείρηση οδηγείται σε νομικές κυρώσεις οι οποίες θα αποτελέσουν ένα επιπλέον έξοδο για αυτές.

Αρχικό κόστος επένδυσης: Τα αρχικά έξοδα προκύπτουν με την υλοποίηση της επένδυσης και περιλαμβάνουν κόστη που σχετίζονται με την απόκτηση του υλικού και του λογισμικού, κόστη εργασίας και κόστη που αφορούν αλλαγές στην οργάνωση της εταιρείας.

Τα πρώτα αναπόφευκτα έξοδα είναι για την αγορά του υλικού και του λογισμικού. Ο οργανισμός επενδύει σε ό,τι αφορά το πληροφοριακό σύστημα. Κεντρικές μονάδες επεξεργασίας, κεντρική πλακέτα, μνήμη τυχαίας προσπέλασης, μονάδα τροφοδοσίας είναι κάποια από τα βασικά αποτελούμενα μέρη του συστήματος. Στο υλικό περιλαμβάνονται και περιφερειακές συσκευές εισόδου και εξόδου όπως πληκτρολόγιο, οθόνη, ποντίκι, κάμερα, μικρόφωνο, σαρωτές, θύρες USB και θύρες δικτύου. Υπάρχουν και κάποιες φορές που ένα σύστημα καταφθάνει πλήρως ολοκληρωμένο με εγκατεστημένο το λειτουργικό σύστημα που χρειάζεται για να λειτουργήσει. Αν δεν συμβεί αυτό, ο οργανισμός οφείλει να συμπεριλάβει στο κόστος και τα έξοδα για την απόκτηση του λογισμικού το λειτουργικό σύστημα θα είναι το κατάλληλο για να ανταποκρίνεται επακριβώς στους επιχειρηματικούς στόχους της επιχείρησης. Σκοπός είναι η διαχείριση των εξαρτημάτων του υλικού και η σωστή κατανομή των πόρων του για να λειτουργεί το σύστημα κατά το βέλτιστο και αποδοτικό τρόπο.

Η εταιρεία, αφού αγοράσει τη διασφάλιση, θα δαπανήσει χρήματα για τη σωστή εγκατάστασή της. Η ενσωμάτωσή της στο δίκτυο απαιτεί νέους πόρους και ρυθμίσεις όπως διακόπτες, δρομολογητές, κόμβους και καλώδια τα οποία θα χρησιμοποιούν σωστά για τη μετάδοση των δεδομένων. Όλα αυτά πρέπει να μείνουν όσο το δυνατόν περισσότερο ανεπηρέαστα από εξωτερικούς παράγοντες. Για παράδειγμα μια διακοπή ρεύματος θα μπορούσε να έχει μοιραία κατάληξη για τον οργανισμό. Η εταιρεία οφείλει λοιπόν να προμηθευτεί τροφοδοτικά ρεύματος UPS. Ακόμα οι συνθήκες του περιβάλλοντος που είναι εγκατεστημένο το σύστημα θα ήταν καλό να προφυλάσσεται από υψηλές θερμοκρασίες, υγρασία και σκόνη. Συμπεραίνουμε λοιπόν ότι για να δημιουργηθούν οι ιδανικές συνθήκες που θα φιλοξενήσει τη νέα υποδομή απαιτούνται επιπρόσθετες δαπάνες.

Κόστος εργασίας: Η απόκτηση και εφαρμογή ενός συστήματος ασφαλείας οδηγεί πολλές φορές σε οργανωτικές αναδιαρθρώσεις εντός της επιχείρησης. Είναι πιθανόν να δημιουργηθούν νέες θέσεις εργασίας, νέες ομάδες που θα είναι υπεύθυνες για την ανάπτυξη, τη λειτουργία και τον έλεγχο της διασφάλισης. Αλλαγές ακόμα μπορεί να γίνουν σε οδηγίες και διαδικασίες οι οποίες θα πρέπει να γνωστοποιηθούν σε όλα τα μέλη του οργανισμού ώστε να ακολουθούν μια ενιαία πολιτική. Η ενημέρωση μπορεί να γίνει μέσω εκπαιδευτικών σεμιναρίων εντός της επιχείρησης ή μέσω διαδικτύου. Συνεπώς προκύπτουν και επιπλέον κόστη, τα λεγόμενα κόστη εργασίας τα οποία περιλαμβάνουν δαπάνες για την εγκατάσταση και τον έλεγχο των συστημάτων και της συνολικής υποδομής, ενέργειες που απαιτούν αρκετό χρόνο εργασίας, όπως επίσης και οι ώρες που δεσμεύονται από τους εργαζόμενους και τους εκπαιδευτές για την ενημέρωση και κατάρτιση των υπαλλήλων.

4.1.2 Το κόστος μετά από μια ολοκληρωμένη με επιτυχία επίθεση

Σε αυτή την κατηγορία, ως κόστος ορίζουμε τις οικονομικές επιπτώσεις που έχει υποστεί ο οργανισμός εφόσον εκδηλωθεί ένα περιστατικό ασφάλειας. Ο οικονομικός αντίκτυπος μπορεί να χωριστεί σε εσωτερικό και εξωτερικό κόστος. Το εσωτερικό σχετίζεται με τις δραστηριότητες του οργανισμού που θα υλοποιηθούν μετά την παραβίαση οι οποίες απαιτούν

εταιρικούς πόρους και αφορούν λειτουργίες όπως η ανίχνευση, η κλιμάκωση, η οργάνωση, η συγκράτηση , η έρευνα και η διόρθωση ενώ το εξωτερικό κόστος προέρχεται από εξωτερικούς παράγοντες που είναι μέρος της παραβίασης ή των άμεσων συνεπειών της. Διακρίνεται σε άμεσο και έμμεσο κόστος ή υλικό και άυλο, μόνιμο ή παροδικό. Η έρευνα του Ponemon Instiute αναφέρει ότι το συνολικό κόστος μετά από μια επιτυχημένη επίθεση υπολογίζεται στα 5 εκατομμύρια δολάρια όπου σε κάθε υπάλληλο αντιστοιχεί σε 301 δολάρια.

Εσωτερικό κόστος

Όπως αναφέραμε παραπάνω το εσωτερικό κόστος σχετίζεται με τις λειτουργίες που θα εκτελεστούν εντός του οργανισμού με την πραγματοποίηση μιας παραβίασης.

- Η ανίχνευση της παραβίασης είναι η πρώτη και πιο σημαντική ενέργεια ώστε να ακολουθήσουν και οι επόμενες. Χρησιμοποιώντας εργαλεία παρακολούθησης και καταγραφής εντοπίζεται η επίθεση, συλλέγονται και αναλύονται πληροφορίες ώστε οι διαχειριστές ασφαλείας να βεβαιωθούν ότι δεν είναι μόνο ενδείξεις αλλά πραγματικό περιστατικό.
- Η κλιμάκωση είναι επίσης ένα σημαντικό βήμα για την αντιμετώπιση της επίθεσης. Εφόσον ο υπάλληλος ανιχνεύσει την επίθεση, ενημερώνει τους υπεύθυνους και εκείνοι με τη σειρά τους την ανώτερη διοίκηση η οποία και θα αποφασίσει ποιοι πόροι και ενέργειες θα γίνουν για να αντιμετωπισθεί το περιστατικό.
- Η οργάνωση σχετίζεται στον προγραμματισμό των εργασιών και την ανάθεση των καθηκόντων στους εργαζόμενους. Πρέπει να έχει γίνει σωστή επιλογή του προσωπικού που εργάζεται σε θέματα ασφάλειας. Επιπλέον, καθώς ο χρόνος είναι πολύτιμος και δεν επιτρέπονται καθυστερήσεις, θα ήταν καλό να γνωστοποιείται η διαθεσιμότητα των εμπειρογνωμόνων ή να δημιουργούνται ομάδες έκτακτης ανάγκης ώστε να είναι πάντα σε αναμονή για την αντιμετώπιση των περιστατικών.
- Εφόσον έχει συνταχθεί η ομάδα αντιμετώπισης τίθενται σε περιορισμό και απενεργοποιούνται συστήματα που έχουν δεχτεί επίθεση και εκτελούνται εργασίες για να περιοριστούν και οι αρνητικές συνέπειες και οι ζημιές που προκλήθηκαν από την παραβίαση.
- Στη συνέχεια πραγματοποιείται έρευνα ώστε να αποφευχθούν παρόμοια περιστατικά στο μέλλον. Αναλύονται όλες οι πληροφορίες που συλλέχθηκαν από την επίθεση ώστε να γίνει πλήρως κατανοητό τι συνέβη και να πραγματοποιηθούν διορθωτικές ενέργειες που θα έχουν ως αποτέλεσμα την εξάλειψη της ευπάθειας, την ανάκτηση των πληροφοριακών συστημάτων και την αποφυγή τέτοιων επιθέσεων στο μέλλον.

Άμεσο κόστος

Το άμεσο κόστος είναι οι εμφανείς οικονομικές ζημιές οι οποίες προκύπτουν μετά την επίθεση και μπορούν να μετρηθούν και ποσοτικά. Τέτοιες είναι οι δαπάνες που αφορούν το κόστος εργασίας και υλικών που απαιτούνται για την αποκατάσταση των ζημιών, η απώλεια παραγωγικότητας και η έλλειψη διαθέσιμων πόρων καθώς και πρόστιμα που σχετίζονται με μη συμμόρφωση σε κανονισμούς. Πιο συγκεκριμένα, δημιουργούνται νέα έξοδα για την αποκατάσταση των ζημιών που προκλήθηκαν στα πληροφοριακά συστήματα και επαναφορά τους στην αρχική κατάσταση είτε με την επιδιόρθωση των υπαρχόντων είτε με την αγορά καινούριου εξοπλισμού. Η αγορά νέου εξοπλισμού, εκτός από την καταστροφή της

υπάρχουσας υποδομής πραγματοποιείται και έναν ακόμα λόγο, τη βελτίωση και αναβάθμιση των πληροφοριακών συστημάτων εφόσον αυτή η υποδομή σε επίπεδο υλικού και λογισμικού δεν επαρκεί για την αντιμετώπιση των επιθέσεων. Εκτός από τα υλικά που χρειάζονται για την αποκατάσταση των ζημιών, απαιτείται και επιπλέον χρόνος εργασίας από τους υπάλληλους του οργανισμού. Ο χρόνος μεταφράζεται σε κόστος για τον οργανισμό αφού πρέπει να πληρώσει τις υπερωρίες του ανθρώπινου δυναμικού που εργάζεται στα τμήματα τα οποία εμπλέκονται στα θέματα ασφαλείας της εταιρείας. Σημαντικό είναι ακόμα να αναφέρουμε ότι όσο διαρκεί η επίθεση και έως ότου αποκατασταθεί η ομαλή λειτουργία του οργανισμού ,προκύπτει ένα σύνολο δαπανών που σχετίζονται με τη διακοπή της λειτουργίας και περιλαμβάνουν απώλειες όπως απώλεια εσόδων, απώλεια παραγωγικότητας των εργαζομένων, απώλεια πωλήσεων. Η απώλεια εσόδων μπορεί να μετρηθεί συγκριτικά με τα έσοδα της προηγούμενης περιόδου της επίθεσης αλλά δεν είναι και απόλυτα σωστά. Οι απώλειες πωλήσεων μπορεί να είναι απλά προσωρινό γεγονός λόγω διακοπής υπηρεσιών, ωστόσο πιθανώς να έχει και μόνιμο χαρακτήρα αν οι πελάτες οριστικά επιλέξουν ανταγωνιστική επιχείρηση. Άλλο άμεσο κόστος θεωρείται και η απώλεια αξίας των περιουσιακών στοιχείων της εταιρείας που κλέβονται ή αλλοιώνονται κατά τη διάρκεια της επίθεσης ωστόσο είναι πιο δύσκολο να μετρηθούν καθώς η αξία ενός πληροφοριακού στοιχείου εξαρτάται πολλές φορές και από το ποιος κατέχει την πληροφορία. Υπάρχουν ποσοτικοί δείκτες που υπολογίζουν το βαθμό της ζημιάς που έχει υποστεί το περιουσιακό στοιχείο για αυτό θα ήταν χρήσιμο να γίνει ένας υπολογισμό πριν και μετά την παραβίαση. Τέλος, έξοδα εμφανίζονται στην περίπτωση που αναλάβουν την υπόθεση ανάλυσης και αντιμετώπισης της κυβερνοεπίθεσης εξωτερικοί συνεργάτες.

Έμμεσο κόστος

Το έμμεσο κόστος είναι οι οικονομικές συνέπειες μιας επιτυχημένης κυβερνοεπίθεσης σε άυλο επίπεδο οι οποίες δεν είναι τόσο εύκολο να ποσοτικοποιηθούν καθώς εξαρτώνται και από πολλούς παράγοντες αλλά έχουν ωστόσο σημαντικό αντίκτυπο στην επιχείρηση. Το έμμεσο κόστος περιλαμβάνει δαπάνες που αφορούν το αυξημένο κόστος της επιχείρησης, την απώλεια σήματος, την απώλεια εμπιστοσύνης.

Αναλυτικότερα, μια επίθεση ενδέχεται να κοστίσει σημαντικά στη φήμη του οργανισμού. Μια κακή φήμη δεν βλάπτει άμεσα την εταιρεία αλλά οδηγεί σε ανεπιθύμητες συνέπειες μακροπρόθεσμα. Οι πελάτες χάνουν την εμπιστοσύνη τους, στρέφονται σε ανταγωνιστικές εταιρείες με αποτέλεσμα να μειωθούν οι μελλοντικές χρηματορροές. Δυσκολία υπάρχει και στην προσέλκυση νέων πελατών λόγω της κακής ασφάλειας θεωρώντας τον οργανισμό μη φερέγγυο. Σε αυτή την περίπτωση το μέγεθος της επίπτωσης εξαρτάται από το είδος και το μέγεθος της επιχείρησης, δύσκολα όμως υπολογίζονται με αριθμούς. Επιπλέον αυτή η έλλειψη εμπιστοσύνης και η αύξηση της δυσπιστίας έχει επίδραση και στον τρόπο διαχείρισης της εταιρείας από τους μετόχους για εταιρείες που είναι εισηγμένες στο χρηματιστήριο. Ένα τέτοιο περιστατικό επηρεάζει αρνητικά την απόδοση των μετοχών, μειώνει την τιμή τους, μειώνει την κεφαλαιοποίηση της αγοράς που στη χειρότερη περίπτωση να οδηγήσει στην χρεωκοπία της επιχείρησης. Ως εκ τούτου η εταιρεία δεν πρέπει να ενδιαφέρεται μόνο για την πρόληψη και αντιμετώπιση των επιθέσεων αλλά και για την άποψη της κοινής γνώμης καθώς ακόμα και η υποψία περί παραβίασης μπορεί να επηρεάσει αρνητικά τους πελάτες.

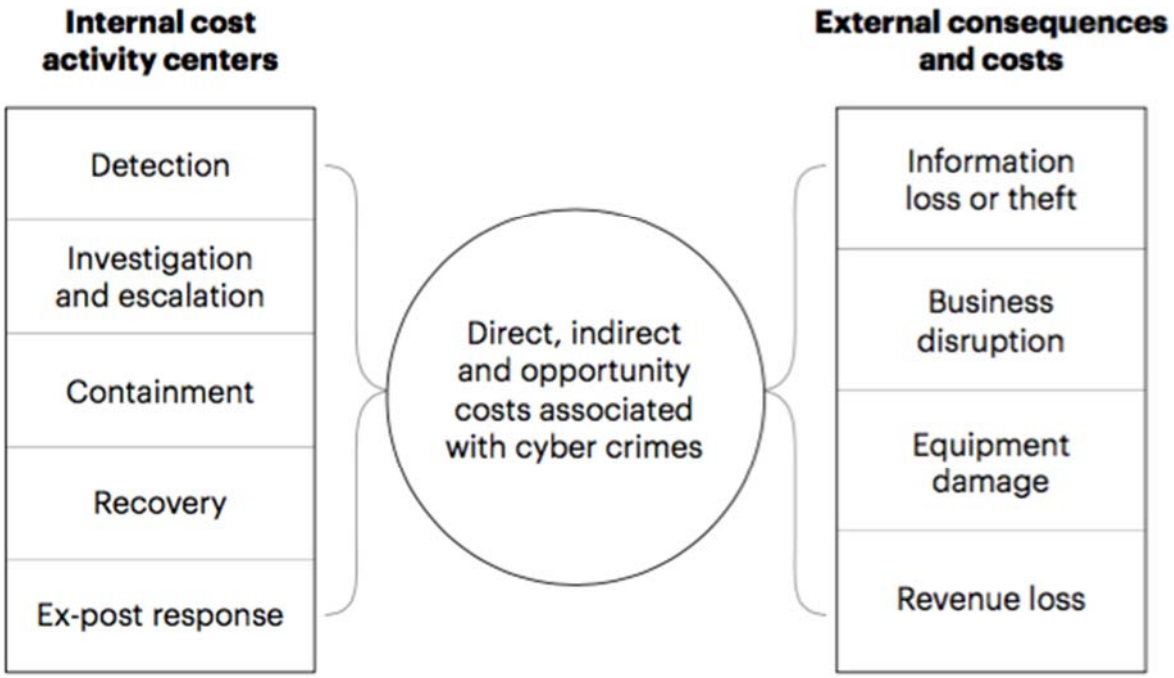
Μετά από μια παραβίαση, οι οργανισμοί πρέπει να είναι σε θέση να αντέξουν και το νομικό κόστος. Τέτοια έξοδα σχετίζονται με δικαστικές διενέξεις φυσικών και νομικών προσώπων που θεωρούν ότι έχουν υποστεί βλάβη από τη διαρροή προσωπικών και ευαίσθητων πληροφοριών. Αυτό έχει ως αποτέλεσμα όχι μόνο την υποβολή προστίμων προς την

επιχείρηση για συμμόρφωση αλλά και οικονομικές δαπάνες για αποζημίωση των προσβεβλημένων από την επίθεση.

Η διαρροή ευαίσθητων πληροφοριών επηρεάζει διαφορετικούς τομείς. Για παράδειγμα η διαρροή πληροφοριών που σχετίζεται με στρατηγικά θέματα του οργανισμού, επιχειρηματικούς στόχους και οικονομικά θέματα μπορεί να επηρεάσει αρνητικά την ανταγωνιστικότητα της και την εισροή κερδών. Ένα ακόμα παράδειγμα σχετίζεται με τους υπαλλήλους του οργανισμού. Η υγεία και η ζωή τους βρίσκεται σε κίνδυνο αν οι παραβιάσεις της ασφάλειας έχουν ως αποτέλεσμα δυσλειτουργίες μηχανημάτων και επικίνδυνων συνθηκών ιδιαίτερα αν στο στόχαστρο βρεθούν συστήματα που χρησιμοποιούνται στη δημόσια υγεία όπως στα νοσοκομεία. Αρνητικές επιπτώσεις ενδέχεται να υπάρξουν και στα οικονομικά των ανθρώπων καθώς μπορεί μετά από επίθεση να αλλοιωθούν τα στοιχεία τους ή να παραποιηθούν οι οικονομικές απολαβές τους. Τέλος άλλες έμμεσες απώλειες προκύπτουν ανάλογα με τις περιστάσεις και είναι η αδυναμία εκπλήρωσης συμβάσεων, καθυστερημένες παραδόσεις και έξοδα νομικού επιπέδου.

Με βάση την έρευνα του Ponemon Institute για το έτος 2017, το κόστος ενός κυβερνοεγκλήματος ποικίλει ανάλογα με το μέγεθος, τον τύπο της επίθεσης και τη χώρα που πραγματοποιείται όπως επίσης και από το είδος της επιχείρησης, την οργάνωση των ωριμότητα, και την αποτελεσματικότητα του οργανισμού στα θέματα ασφάλειας. Η έρευνα έδειξε ότι το κόστος μετά από επίθεση είναι μεγαλύτερο σε εταιρείες που σχετίζονται με οικονομικά όπως τράπεζες και χρηματοπιστωτικές υπηρεσίες καθώς και υπηρεσίες κοινής ωφέλειας και ενέργειας σε αντίθεση με εταιρείες που δραστηριοποιούνται στο χώρο της εκπαίδευσης ,της φιλοξενίας, της επιστήμης που υπέστησαν κατά μέσο όρο πολύ χαμηλότερο κόστος. Ανάλογα με το μέγεθος της επιχείρησης διαφοροποιείται και το είδος της επίθεσης. Για παράδειγμα σε μικροεπιχειρήσεις το κόστος που έχουν να υποστούν είναι υψηλότερο για επιθέσεις που βασίζονται στο διαδίκτυο, επιθέσεις ηλεκτρονικού ψαρέματος κοινωνικής δικτύωσης ενώ μεγάλοι οργανισμοί αντιμετωπίζουν ανάλογο κόστος σε επιθέσεις οι οποίες σχετίζονται με άρνηση παροχής υπηρεσιών, κακόβουλης πληροφορία και κακόβουλου κώδικα. Ανεξαρτήτως μεγέθους, σχεδόν όλοι οι οργανισμοί έχουν δεχτεί επιθέσεις τύπου ransomware, επιθέσεις όπως σκουλήκια, ιοί και trojans. Σε επίπεδο κόστους έχει παρατηρηθεί ότι οι πιο ακριβές επιθέσεις είναι εκείνες της άρνησης παροχής υπηρεσιών, του κακόβουλου κώδικα και των κακόβουλων εμπιστευτικών πληροφοριών αν και έχει διαπιστωθεί ότι οι περισσότερες εταιρείες επενδύουν περισσότερα χρήματα για την αντιμετώπιση τέτοιων επιθέσεων κακόβουλων λογισμικών και web και λιγότερο σε κλεμμένες συσκευές, botnets και ransomware. Οι συνέπειες ενός κυβερνοεγκλήματος κακόβουλου λογισμικού είναι πιο καταστροφικές διότι απαιτείται περισσότερος χρόνος για να αντιμετωπισθούν. Τέλος ιδιαίτερα σημαντικό είναι κόστος σε δραστηριότητες ανίχνευσης και περιορισμού της επίθεσης το οποίο φθάνει το 56% του συνολικού κόστους της επιχείρησης και ακολουθεί στη συνέχεια το κόστος ανάκτησης και έρευνας.

Με βάση τις συνέπειες μιας επίθεσης, η επιχείρηση αντιμετωπίζει το μεγαλύτερο κόστος με την απώλεια πληροφοριών, ακολουθεί το κόστος διακοπής της επιχείρησης, η μειωμένη παραγωγικότητα έργου, οι αποτυχίες επιχειρηματικών διαδικασιών και τέλος οι απώλειες εσόδων, ζημιών και εξοπλισμού.



Σχήμα 4.3: Άμεσα και Έμμεσα κόστη

4.1.3 Μοντέλο ICAMP (Incident Cost Analysis and Modelling Project)

Το πιο διαδεδομένο μοντέλο που χρησιμοποιείται για την ανάλυση του κόστους μια ενδεχόμενης επίθεσης είναι το μοντέλο ICAMP (Incident Cost Analysis Modelling Project). Σκοπός του μοντέλου είναι να αναπτύξει μια μεθοδολογία για την καλύτερη κατανόηση των παραγόντων που επηρεάζουν την τυχαιότητα και το κόστος των περιστατικών ασφάλειας των υπολογιστικών συστημάτων. Τα ζητήματα με τα οποία ασχολείται είναι:

Οι παράγοντες που είναι πιθανό να αυξήσουν τη συχνότητα των περιστατικών είναι ζητήματα ελλιπούς εκπαίδευσης, ελλιπούς σχεδιασμού πολιτικών ασφάλειας, ανοιχτή πρόσβαση στα συστήματα χωρίς περιορισμούς.

Οι παράγοντες που είναι πιθανό να αυξήσουν το κόστος ενός περιστατικού για παράδειγμα είναι η έλλειψη τεχνογνωσίας, η παλαιότητα συστημάτων, ο χρόνος εκδήλωσης περιστατικού, μη χρησιμοποίηση αποθηκευτικών μέσων.

Το κόστος παραβίασης ασφάλειας αναλύεται σε 4 κατηγορίες: κόστος σε χρήμα, κόστος σε ανθρώπινη εργασίας, κόστος που δεν είναι δυνατόν να προσδιορισθεί ποσοτικά και αριθμός χρηστών που επηρεάζονται από το περιστατικό.

Θεωρείται μια πολύ καλή προσέγγιση κυρίως επειδή αναλύει το κόστος στις παραπάνω κατηγορίες ωστόσο τα αποτελέσματα δεν γίνεται να είναι απόλυτα καθώς εξακολουθούν να υπάρχουν κατηγορίες κόστους που δεν ποσοτικοποιούνται ακριβώς.

4.2 Οικονομικοί δείκτες

Όπως αναφέραμε σε προηγούμενη ενότητα, κάθε επιχείρηση που έχει στόχο το κέρδος οφείλει να εκτιμά τα αγαθά της και να δίνει αξία σε αυτά. Αποδίδουν επομένως νομισματική αξία σε κάθε είδος αγαθών που απαρτίζει την επιχείρηση όπως εξοπλισμό, πληροφορία, εργατικό δυναμικό. Στη συνέχεια με τη χρήση οικονομικών δεικτών αξιολογεί την σημερινή κατάσταση, υπολογίζει το κέρδος αλλά και προβλέπει τόσο το κέρδος όσο και την οικονομική ζημιά της. Βοηθούν ακόμα στην αξιολόγηση των εναλλακτικών λύσεων στην ασφάλεια του κυβερνοχώρου για αυτό αποτελούν σημαντικό μέρος της διαδικασίας λήψης αποφάσεων. Ουσιαστικά βαθμολογούν τις εναλλακτικές επιλογές στα χαρακτηριστικά τους και εκείνη η λύση με την υψηλότερη κατάταξη ορίζεται και ως η καλύτερη επένδυση. Να επισημάνουμε ότι για την περίπτωση επένδυσης στην ασφάλεια του κυβερνοχώρου η έννοια του κέρδους δεν συνεπάγεται την αύξηση των εισροών αλλά τον μετριασμό του κινδύνου και τη μείωση των αναμενόμενων ζημιών.

4.2.1 Στατικοί δείκτες

Σύγκριση Κόστους

Ο δείκτης **T** εκφράζει το συνολικό κόστος της εναλλακτικής επένδυσης και υπολογίζεται από το άθροισμα των επιμέρους σχετικών δαπανών όπως το κόστος κεφαλαίου, οι αποσβέσεις και τα επιτόκια που προκύπτουν από το κεφάλαιο που δεσμεύεται. Τα κόστη σχετίζονται με κόστη εφαρμογής, λειτουργίας, συντήρησης καθώς και κόστη κεφαλαίου. Ο τύπος που υπολογίζεται το ανώτερο συνολικό κόστος είναι

$$T = V + n*D + I$$

Όπου

$\mathbf{T_n}$: το συνολικό κόστος στα n χρόνια

$\mathbf{V_n}$: τα ποικίλα κόστη για τα n χρόνια

N: η διάρκεια ζωής της επένδυσης

D: η γραμμική απόσβεση για κάθε χρόνο

Ο τύπος που υπολογίζει τη γραμμική απόσβεση είναι

$$D = \frac{A0 - Ln}{2}$$

A_0: το κόστος απόδοσης

Ln: η απόδοση ρευστοποίησης

Η προσέγγιση της γραμμικής απόσβεσης βασίζεται στην υπόθεση ότι το αντικείμενο χάνει την αξία του με την πάροδο του χρόνου ή όταν εκτελείται κάποια εργασία ή όταν μειώνεται η ουσία του.

$\mathbf{I_n}$: το τεκμαρτό επιτόκιο στα n χρόνια. Το τεκμαρτό επιτόκιο υπολογίζεται με βάση το μέσο κεφάλαιο που δεσμεύτηκε το οποίο εξαρτάται από την προσέγγιση της απόσβεσης. Αν η

απόδοση ρευστοποίησης είναι μηδέν, θα δεσμευτεί κατά μέσο όρο το μισό του κόστους απόκτησης. Αν η απόδοση ρευστοποίησης είναι μεγαλύτερη από το μηδέν, απόσβεση θα είναι χαμηλότερη και θα γίνουν περισσότερες δαπάνες.

$$I_n = \varnothing C_n * I_n$$

Όπου

$\varnothing C_n$: το μέσο δεσμευμένο κεφάλαιο στα n χρόνια

Η συνάρτηση που υπολογίζει το μέσο δεσμευμένο κεφάλαιο είναι

$$\varnothing C = \frac{A0 - Ln}{2} + Ln = \frac{A0 - Ln + 2Ln}{2} = \frac{A0 + Ln}{2}$$

Όπου

A0: το κόστος απόκτησης

L_n: η απόδοση ρευστοποίησης

I: το επιτόκιο

Σύγκριση Κερδών

Ο δείκτης **P_n** λαμβάνει υπόψη το κόστος και το όφελος της λύσης και ισούται με την αφαίρεση του κόστους από το σύνολο των εσόδων. Για να είναι σωστός ο υπολογισμός τα έσοδα και το κόστος θα πρέπει να αναφέρονται στο ίδιο χρονικό διάστημα.

$$P_n = R_n - T_n$$

Όπου
P_n: το κέρδος μετά από χρονικό διάστημα n
R_n: τα έσοδα περιόδου n
T_n: το κόστος περιόδου n

ROI- Return on Investment

Ο δείκτης **ROI** συγκρίνει το ποσό του εισοδήματος που προέρχεται από μια επένδυση με το κόστος της επένδυσης. Ορίζεται ως η απόδοση της επένδυσης και είναι γνωστή ως ο λόγος της κερδοφορίας διότι παρέχει πληροφορίες σχετικά με τις επιδόσεις της διοίκησης στη χρήση των διαθέσιμων πόρων για τη δημιουργία εισοδήματος. Πιο απλά, ο δείκτης αυτός εκφράζει μια πολύ βασική οικονομική αρχή που αναφέρεται στη χρήση όσο το δυνατόν λιγότερων πόρων με αποτέλεσμα την απόκτηση όσο των δυνατών περισσότερων πόρων .Υπολογίζεται από την ακόλουθη μαθηματική σχέση όπου τα μέλη της έχουν υπολογιστεί για την ίδια χρονική περίοδο του ενός χρόνου.

$$ROI = \frac{Pi}{Ti}$$

Όπου
ROI: η απόδοση της επένδυσης για το έτος i

P_i: το συνολικό κέρδος της χρονιάς i
T_i: το συνολικό κόστος της χρονιάς i

Αν οι τιμές αναφέρονται σε χρονικό διάστημα ακριβώς ενός έτους μπορεί μέσω του τύπου να υπολογιστεί και το ετήσιο επιτόκιο του κεφαλαίου που χρησιμοποιήθηκε

I_1= ROI - 1

Όπου
I_1: το ετήσιο επιτόκιο ενός χρόνου
ROI: η απόδοση της επένδυσης εντός του χρόνου

Αν το ετήσιο επιτόκιο είναι θετικό I>0 θα αποκτηθεί κέρδος ενώ αν είναι αρνητικό I<0 θα δημιουργηθεί ζημιά. Με βάση ένα δεδομένο επιτόκιο μπορεί το αποτέλεσμα να επηρεάσει μια διαδικασία επένδυσης, δηλαδή αν το επιτόκιο που υπολογίζεται για μια εναλλακτική είναι χαμηλότερο από το δεδομένο επιτόκιο τότε μπορεί να γίνει η επένδυση στη συγκεκριμένη λύση.

ROSI- Return on Security Investment

Ο δείκτης ROI ονομάζεται και **ROSI** όταν αναφέρεται σε επενδύσεις που σχετίζονται με την ασφάλεια. Ενσωματώνει τους κινδύνους και το κόστη που σχετίζονται με ένα περιστατικό ασφάλειας και τα συνδυάζει με τα αποτέλεσμα μιας λύσης ασφάλειας. Ο τύπος που υπολογίζει το δείκτη ROSI είναι

$$\text{ROSI} = \frac{Risk\ exposure * mitigatio\ ratio - Cost\ of\ solution}{Cost\ of\ solution} = \frac{ALE * mitigatio\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

Όπου
Risk exposure =ALE
ALE: η ετήσια προσδοκώμενη απώλεια και ισούται ALE=SLE*ARO

SPP Static Payback Period

Ο δείκτης **SPP** ορίζεται ως περίοδος στατικής αποπληρωμής και εκφράζει σε έτη το χρονικό διάστημα που απαιτείται για την απόσβεση του αρχικού κόστους. Υπολογίζεται από τη σχέση

$$N = \frac{Ti}{P\emptyset}$$

Όπου
n: η περίοδος σε χρόνια
T: το αρχικό κόστος επένδυσης
P∅ : το μέσο ετήσιο κέρδος

Καθώς οι στατικοί οικονομικοί δείκτες ποσοτικοποιούν αρκετές έννοιες που χρησιμοποιούνται στη διαδικασία λήψης αποφάσεων για την ασφάλεια του κυβερνοχώρου και αποτελούν κριτήριο απόφασης εναλλακτικής παρουσιάζουν κάποια μειονεκτήματα κατά της εφαρμογή τους.

Επανερχόμαστε στο δείκτη ROSI και θα αναλύσουμε όλα τα βήματα που ακολουθούνται για τον υπολογισμό του καθώς και τους παράγοντες που το επηρεάζουν. Αρχικά χωρίζεται σε δύο φάσεις την προετοιμασία και τον υπολογισμό κάθε μια από τις οποίες περιλαμβάνει ορισμένες ενέργειες.

1η φάση :Προετοιμασία

Σημείο εκκίνησης
Ο υπολογισμός του δείκτη ROSI βασίζεται σε υποθέσεις που αναφέρονται σε μελλοντικά ζητήματα ασφάλειας που πιθανόν να προκύψουν. Τέτοιες υποθέσεις μπορεί να είναι:

Η αξία των απειλών
Οι μελλοντικές επιθέσεις συνεχώς εξελίσσονται στο πλαίσιο δυνατοτήτων τους οπότε είναι αδιανόητο τι μπορεί να προκύψει. Αυτομάτως επηρεάζεται και ο αντίκτυπος που έχουν οι απειλές και με δυσκολία μπορεί να προβλεφθεί. Τέλος αν μια επιχείρηση ενσωματώσει νέα προϊόντα και υπηρεσίες υπάρχει περίπτωση οι ευπάθειές τους να είναι άγνωστες και τα υπάρχοντα μέτρα ασφαλείας να μην ανταποκρίνονται.

Κουλτούρα κινδύνου του οργανισμού
Τα δυο βασικά χαρακτηριστικά που μπορεί να προσδιορίσει η κουλτούρα κινδύνου είναι:
Η όρεξη για κίνδυνο και η αντίδραση για αρνητικά αποτελέσματα.. Έτσι λοιπόν μπορεί να χαρακτηριστεί ως συντηρητική όταν επιλέγει να αποφύγει τον κίνδυνο ενώ ως επιθετική όταν αποφασίζει να τον αναλάβει. Επιπλέον ανάλογα με τον τρόπο που αντιδρά στα αρνητικά αποτελέσματα είτε ξεκινά τα κατηγορώ και προσάπτει ευθύνες ή μαθαίνει από τα λάθη της και βελτιώνεται.

Η λογιστική φύση των προτεινόμενων δαπανών
Στο στάδιο αυτό θα πρέπει να προσδιοριστεί τι περιλαμβάνει η επένδυση και τι είναι το λειτουργικό κόστος. Κάθε επιχείρηση καθορίζει ποιες είναι οι οικονομικές τις δαπάνες καθώς και τον προϋπολογισμό της εφόσον κάθε μια έχει διαφορετικές ανάγκες. Τέλος θα ήταν χρήσιμο να γίνει και διάκριση των δαπανών που αφορούν αναβάθμιση μιας υπάρχουσας εγκατάστασης και αναβάθμισης που σχετίζεται με την αγορά νέου προϊόντος ή υπηρεσίας.

Ο χρόνος είναι κρίσιμος; Δαπάνες για προστασία ή διόρθωση
Οι προγραμματιστές λογισμικού γνωρίζουν ή πρέπει να μάθουν ότι το κόστος της πρώτης φοράς είναι πολύ μικρότερο από το κόστος της διόρθωσης ενός σφάλματος κατά τη διαδικασία ανάπτυξης.

Πολυδιάστατος αντίκτυπος
Κάθε επιχείρηση πρέπει να αναλύει τον αντίκτυπο που θα έχει μια επιτυχημένη επίθεση. Καθώς τα συστήματα πληροφοριών και οι τεχνολογίες χρησιμοποιούνται ευρέως, η απώλεια της εμπιστευτικότητας, της ακεραιότητας και η διακοπή υπηρεσιών της επιχείρησης δημιουργούν επιπτώσεις σε πολλούς τομείς. Εκτός από τις οικονομικές ζημιές οι συνέπειες μπορεί να είναι νομικές, παραγωγικότητας, καταστροφή φήμης. Όλες αυτές παρουσιάζονται από την αρχή του περιστατικού μέχρι να διαγνωστεί, να αντιμετωπιστεί και να επέλθει η πλήρης ανάκτηση. Ωστόσο υπάρχουν και μακροπρόθεσμες επιπτώσεις εξαιτίας της ανεπαρκούς διαχείρισης της κρίσης όπως συνέπειες με το νόμο και τις αρχές.

2η φάση Υπολογισμός

Εκτίμηση οικονομικών ζημιών
Έχοντας αναλύσει πρωτύτερα τα είδη των οικονομικών επιπτώσεων, θα αναφέρουμε εν συντομία ότι για να καθοριστεί ο δείκτης ROSI απαιτείται η ποσοτικοποίηση των ζημιών που θα προκύψουν από μια επιτυχημένη επίθεση ακόμα και αν πολλές φορές η φύση τους είναι τέτοια που δύσκολα μπορούν να μετρηθούν. Συνήθως αρνητικές επιπτώσεις προκύπτουν στη φήμη και στην απώλεια του εμπορικού σήματος. Έμμεσες απώλειες προκύπτουν ανάλογα με τις περιστάσεις όπως πρόστιμα, αποζημιώσεις, καθυστερημένες παραδόσεις και άμεσες απώλειες που σχετίζονται με τις διαδικασίες αντιμετώπισης του περιστατικού όπως τα έξοδα που δαπανώνται στο στάδιο της ανίχνευσης, της ανάκτησης και της συνέχισης της λειτουργίας της επιχείρησης.

Δημιουργία εσόδων από αναμενόμενα οφέλη
Σκοπός της επένδυσης στην ασφάλεια δεν είναι η δημιουργία κερδών όπως σε άλλους τομείς για αυτό και τα οφέλη προσδιορίζονται από μειωμένες οικονομικές ζημιές, μειωμένο κίνδυνο εμφάνισης περιστατικού.

Ιδιοκτησία των ωφελειών
Για να θεωρηθούν αξιόπιστα τα οφέλη που αναφέρονται στον υπολογισμό του δείκτη ROSI θα πρέπει να έχουν προσδιορίσει και τον ιδιοκτήτη τους.

Εκτίμηση κόστους
Κάθε προτεινόμενη λύση κοστίζει ένα συγκεκριμένο ποσό στον επενδυτή. Με το που αποφασίζεται η εναλλακτική υπάρχει το κόστος της εγκατάστασης, της διαμόρφωσης και τη ενσωμάτωσης με τα υπόλοιπα εργαλεία της επιχείρησης, υπάρχει το κόστος για τις εκπαιδεύεις που θα γίνουν καθώς και τα λειτουργικά κόστη που περιλαμβάνουν τη συντήρηση, την υποστήριξη και την αναβάθμιση του συστήματος.

Προϋποθέσεις
Για να γίνει πρέπει να πληρούνται οι παρακάτω προϋποθέσεις:
Το προϊόν/ η υπηρεσία ταιριάζει με τις πραγματικές ανάγκες της επιχείρησης.
Το προϊόν/ υπηρεσία έχει διαμορφωθεί και χρησιμοποιείται σωστά.
Το προϊόν/ υπηρεσία παραδόθηκε και λειτουργεί όπως ακριβώς το περιέγραψε ο πωλητής.

Υπολογισμός ROSI
Για τον υπολογισμό αυτού του δείκτη χρησιμοποιούνται διάφορα μοντέλα και εξισώσεις.

Ποιότητα ROSI
Αν και οι στατικοί δείκτες εκφράζουν μια εικόνα της οικονομικής κατάστασης της επιχείρησης και επηρεάζουν κατά ένα βαθμό στη διαδικασία λήψης απόφασης, δεν είναι αρκετοί και απολύτως έγκυροι καθώς έχουν κάποια αδύναμα στοιχεία. Για παράδειγμα ο δείκτης ROI δεν λαμβάνει υπόψη του συγκεκριμένες προϋποθέσεις όπως μεμονωμένες προτιμήσεις της επιχείρησης, διαφορετικοί χρόνοι εμφάνισης του κόστους και του κέρδους. Επίσης κατά τους υπολογισμούς του κόστους και του κέρδους για τη διαδικασία σύγκρισης οι χρονικές περίοδοι που επιλέγονται ίσως να είναι προβληματικές με την έννοια ότι μπορεί να παρουσιάζουν ασυνήθιστα κέρδη ή κόστη και να οδηγούν σε ένα μη αντιπροσωπευτικό αποτέλεσμα.[13]

4.2.2 Δυναμικοί Δείκτες

Εκτός από τη χρήση των στατικών δεικτών, στη διαδικασία λήψης απόφασης προστίθενται και οι δυναμικοί οικονομικοί δείκτες. Οι δυναμικοί δείκτες έχουν σκοπό να συμπληρώσουν τους στατικούς και να εξαλείψουν τα αδύναμα σημεία τους με πρώτο και σημαντικότερο το μειονέκτημα της έλλειψης θεώρησης της χρονικής προοπτικής. Γενικότερα λαμβάνουν υπόψη διαφορετικές χρονικές περιόδους, δεν χρησιμοποιούν μέσες τιμές και τα ποσά κέρδους και κόστους παράγονται σε διαφορετικά χρονικά διαστήματα.

NPV Net Present Value

Ο δείκτης **NPV** (καθαρή παρούσα αξία) είναι το συνολικό όφελος (κέρδος) που έχει ο επενδυτής από την εφαρμογή του χρόνου κατά τη συνολική διάρκεια της ζωής του. Υπολογίζει το πλεόνασμα ή την έλλειψη ταμειακών ροών σε σχέση με το κόστος του κεφαλαίου που χρησιμοποιήθηκε σε μια επένδυση. Οι επιχειρήσεις χρησιμοποιούν το μοντέλο της καθαρής τρέχουσας αξίας για να αναλύσουν το δίπτυχο ωφέλεια -κόστος σχετικά με τις δαπάνες που θα κάνουν για να προστατεύσουν τους πόρους τους. Υπολογίζεται από το ακόλουθο άθροισμα:

NPV= $\sum_{t=1}^{n}(Rt * dt - Tt * dt) - Ti + Ln * dn$

Όπου
NPV: η καθαρή παρούσα αξία μιας επένδυσης
R_t: η απόδοση τη χρονιά t
D_t: ο συντελεστής επιτοκίου προεξόφλησης κατά το έτος t
T_t: το συνολικό κόστος κατά το έτος t
T_i: το αρχικό κόστος της επένδυσης
L_n: η απόδοση ρευστοποίησης

Εναλλακτικά
NPV= $\sum_{t=1}^{n}\left(Bt - \frac{C}{1} + K\right)^t$
Όπου
B: το όφελος μιας επένδυσης τη χρονική περίοδο t
C: το συνολικό κόστος μια επένδυσης
K: το προεξοφλητικό επιτόκιο

Το καθαρό σημείο net είναι η διαφορά μεταξύ του συνολικού κόστους και της συνολικής ωφέλειας η οποία περιλαμβάνει κέρδη και αποταμιεύσεις.
Αν η συνολική ωφέλεια ενός πληροφοριακού συστήματος S είναι B και το συνολικό κόστος είναι C, στόχος είναι η διαφορά G(s)=B(s) – C(s) να μεγιστοποιηθεί. Η τιμή S που μεγιστοποιεί το G(s) αποδίδεται από την ακόλουθη εξίσωση:

$\frac{dG}{dS} = \frac{dB}{dS} - \frac{dC}{dS} = 0 \quad \frac{dB}{dS} = \frac{dC}{dS}$

Αν NPV > 0 τότε αποδεχόμαστε την επένδυση και η επιχείρηση είναι βιώσιμη.
Αν NPV < 0 απορρίπτουμε την επένδυση γιατί θα οδηγήσει σε ζημιά.
Αν NPV= 0 η επένδυση είναι αδιάφορη. Δεν προκαλεί όφελος αλλά ούτε και ζημιά.

Ο δείκτης αυτός θεωρείται ένα αρκετά χρήσιμο εργαλείο που χρησιμοποιείται από τις επιχειρήσεις για να καθορίσουν αν μια εναλλακτική είναι συμφέρουσα να χρηματοδοτηθεί ή όχι ώστε να υλοποιηθεί η επένδυση.

NFV Net Future Value

Ο **NFV** είναι η καθαρή μελλοντική αξία η οποία συσχετίζει τις ροές των πληρωμών σε μελλοντικό χρόνο αντί για την παρούσα χρονική στιγμή.
Συνήθως αυτός ο μελλοντικός χρόνος είναι το τέλος της επενδυτικής ζώνης. Η μαθηματική σχέση που προκύπτει είναι:
NFV= $\sum_{t=1}^{n}(Rt * ct - Tt * ct) - Ti * cn$ +Ln

Όπου
NFV: η καθαρή μελλοντική αξία
R_t: η απόδοση τη χρονιά t
C_t: ο συντελεστής επιτοκίου κατά το έτος t
T_t: το συνολικό κόστος κατά το έτος t
T_i: το αρχικό κόστος της επένδυσης
$L_{n:}$ η απόδοση ρευστοποίησης

EAA Equivalent Annual Annuity

Ο **EAA** αντιπροσωπεύει της αξία της επένδυσης

EAA= NPV * $ANF_{n,i}$

ANF = $\frac{(1+i)^n * i}{(1+i)^n - 1}$

Όπου
EAA: η ετήσια πρόσοδος μιας επένδυσης
NPV: η καθαρή παρούσα αξία
ANF: συντελεστής προσόδου
I: τεκμαρτό επιτόκιο
N: χρόνος ζωής

Αν EAA > 0 η επένδυση είναι λογική γιατί δημιουργεί κέρδη. Σε περίπτωση που υπάρχουν εναλλακτικές, καλύτερη για επένδυση θεωρείται εκείνη με το υψηλότερο EAA.
Είναι ένα πολύ χρήσιμο εργαλείο για να συγκριθούν επενδύσεις με διαφορετικές διάρκειες ζωής γιατί ο δείκτης EAA σχετίζεται με το χρονικό διάστημα ενός έτους και μπορεί να συγκριθεί ανεξάρτητα της διάρκειας των επενδύσεων.

IRR Internal Rate of Return

Ο I**RR** υποδηλώνει τον εσωτερικό ρυθμό απόδοσης και είναι εκείνο το επιτόκιο που θα κάνει το δείκτη NPV μηδέν. Αντιπροσωπεύει μια μέση ετήσια απόδοση η οποία προκύπτει από την επένδυση που έχει γίνει.
Αν το IRR είναι μεγαλύτερο ή ίσο από το συγκεκριμένο επιτόκιο τότε η επένδυση είναι λογική. Δεν υπάρχει συγκεκριμένος τύπος που να υπολογίζει τον συγκεκριμένο δείκτη. Για να βρεθεί η τιμή του, υπολογίζεται επαναληπτικά ο NPV για διαφορετικές τιμές επιτοκίου μέχρι να πάρει την τιμή μηδέν. Το επιτόκιο αυτό όπου NPV= 0 είναι και ο εσωτερικός ρυθμός απόδοσης.

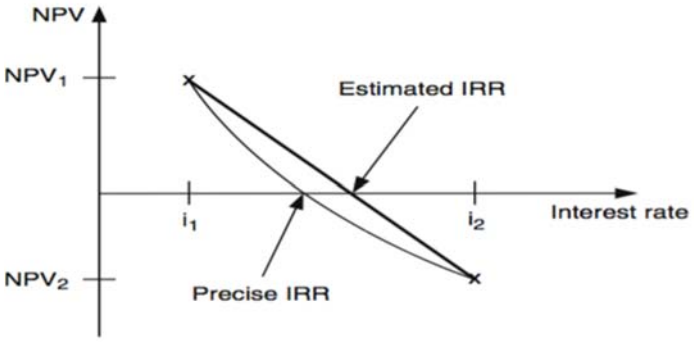
NPV= $\sum_{t=1}^{n}(Rt * dt - Tt * dt) - Ti + Ln * dn$

Όπου
d=($\frac{1}{1+IRR}$)^n = d^n

Το IRR υπολογίζεται μέσω του NPV
Για δεδομένα i, i
Αν i1<i2
IRR = i1 + $\frac{NPV1}{NPV1-NPV2}$ * (i2- i1)

Αν i>i

IRR = i1 + $\frac{NPV2}{NPV2-NPV1}$ * (i1- i2)



Σχήμα 4.4 : Ο δείκτης IRR

Το IRR χρησιμοποιείται για να συγκρίνουμε εναλλακτικές επενδύσεις με μια ενιαία ποσοστιαία τιμή. Αν το IRR είναι μεγαλύτερο ή ίσο του κόστους κεφαλαίου η επιχείρηση θα δεχτεί την επένδυση αλλιώς θα την απορρίψει.

VOFI Visualization of financial implications

Η μέθοδος **VOFI** απεικονίζει όλες τις εισροές και τις εκροές που πραγματοποιούνται στην επιχείρηση κατά κα διάρκεια της επένδυσης και τα επιτόκια υπολογίζονται όπως σε έναν τραπεζικό λογαριασμό. Έτσι τα επιτόκια είναι πιο ρεαλιστικά και ανταποκρίνονται στην πραγματική αγορά. Η απεικόνισή τους γίνεται με την καταγραφή σε έναν πίνακα όλων των ροών και των υπολογισμών των τόκων και των φόρων. Ο δείκτης VOFI θεωρείται ο ακριβέστερος οικονομικός δείκτης εφόσον υπολογίζονται με ακρίβεια οι φόροι και οι τόκοι με το μόνο αδύναμο σημείο να είναι το γεγονός ότι δεν είσαι σαφές αν οι κινήσεις των λογαριασμών σχετίζονται αποκλειστικά με τη συγκεκριμένη επένδυση ή αναφέρονται σε άλλες εσωτερικές ή εξωτερικές επενδύσεις της επιχείρησης.

Όπως και στους στατικούς οικονομικούς δείκτες έτσι και στους δυναμικούς εμφανίζονται κάποια κρίσιμα σημεία.

4.2.3 Ποσοτικοί δείκτες

Ο πρώτος σημαντικός δείκτης είναι ο κίνδυνος **R** και εκφράζεται ως το γινόμενο της επίπτωσης και της πιθανότητας να συμβεί ένα περιστατικό.

R = I * p

Όπου
R: ο κίνδυνος
I: η επίπτωση η οποία δείχνει από νομισματική άποψη την απώλεια ή τη ζημιά που θα προκύψει εφόσον η απειλή υλοποιηθεί και εκφράζεται από τον τύπο:

$I= a_v * e_f$

όπου
A: η αξία του αγαθού
E: ο παράγοντας έκθεσης

P: η μεταβλητή p ορίζεται ως την πιθανότητα να εμφανιστεί μια απειλή εντός καθορισμένης περιόδου d

$P = \frac{d}{365}$ ή $p = \frac{m}{1440}$

Όπου
d: οι μέρες
m: τα λεπτά

ALE annual loss expected

Ο δείκτης **ALE** ονομάζεται ετήσια προσδοκώμενη απώλεια και εκτιμά τον κίνδυνο που προκύπτει ως

ALE= αναμενόμενο ποσοστό απώλειας * αξία της απώλειας
Ή
ALE= επίπτωση του συμβάντος * συχνότητα εμφάνισης

ALE = SLE * ARO

Όπου
ALE: η ετήσια προσδοκώμενη απώλεια
SLE: μια μεμονωμένη προσδοκώμενη απώλεια
ARO: η εκτιμώμενη συχνότητα εμφάνισης της απειλής σε ένα έτος

Ο παράγοντας ARO είναι ένας ακέραιος αριθμός παρόλο που εκφράζεται ως ετήσιο ποσοστό εμφάνισης. Δεν υπάρχει περιορισμός στη μέγιστη τιμή που μπορεί να πάρει εφόσον μια απειλή μπορεί να εμφανιστεί από μια ως περισσότερες φορές κατά τη διάρκεια της ημέρας. Αν ARO = 0 σημαίνει ότι η απειλή δεν συμβαίνει ποτέ.

Ο παράγοντας SLE εκφράζει την απώλεια ενός αγαθού και υπολογίζεται από τη σχέση
SLE= A * E

Όπου
A: η αξία της πληροφορίας
E: παράγοντας έκθεσης ο οποίος περιγράφει την απώλεια που θα προκαλέσει μια απειλή στο περιουσιακό στοιχείο εκφρασμένη επί τις εκατό.
CTB Cost to Break

Ο δείκτης **CTB** υποδηλώνει το ελάχιστο αναμενόμενο κόστος που προκύπτει από τον οποιοδήποτε για να ανακαλύψει και να εκμεταλλευτεί μια ευπάθεια στο σύστημα. [31] Το ετήσιο κόστος εκφράζεται από τη σχέση

$CTB = C_D + C_v$

Όπου
CTB: το ετήσιο κόστος για τη διακοπή
C_D: το ετήσιο κόστος για να σπάσει τους αμυντικούς μηχανισμούς
C_v: το ετήσιο κόστος για να εκμεταλλευτεί τις ευπάθειες του συστήματος

Damage to Defence Mechanisms

Μετά από κάθε επίθεση που δέχεται το πληροφοριακό σύστημα, προκαλούνται ζημιές στους μηχανισμούς άμυνας. Το ετήσιο κόστος για την επισκευή των ζημιών ορίζεται ως

$D = D_D + D_I$

Όπου
D: το ετήσιο κόστος για την επισκευή των ζημιών
D_D: το κόστος ζημιών στον αμυντικό μηχανισμό
D_I: το κόστος ζημιών στην υποδομή του συστήματος

Είναι λογικό ότι ένας κακόβουλος χρήστης δεν είναι πρόθυμος να ξοδέψει περισσότερα χρήματα για να επιτεθεί από τα χρήματα που έχει επενδύσει η επιχείρηση στα συστήματα ασφάλειας. Αν E_s η ετήσια συνολική δαπάνη του οργανισμού για θέματα ασφάλειας, τότε το σύστημα θεωρείται ασφαλές αν ισχύει

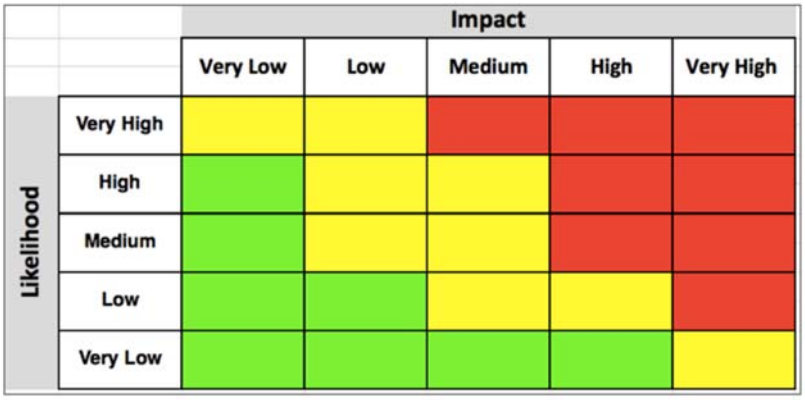
$CTB > E_s$

4.2.4 Ποιοτικοί δείκτες

Όπως αναφέραμε η ποιοτική ανάλυση του κινδύνου αποτελεί αναπόσπαστο τμήμα της λήψης αποφάσεων. Για να γίνει καλύτερα αντιληπτό χρησιμοποιούνται ποιοτικοί δείκτες που εστιάζουν στις ποιοτικές επιπτώσεις. Τέτοιοι είναι η κρίση των εμπειρογνωμόνων, η φήμη και η εμπειρία. Διάφορες τεχνικές μπορούν να χρησιμοποιηθούν για την ανάλυση της ποιοτικής πλευράς του κινδύνου όπως οι συνεντεύξεις των εμπειρογνωμόνων που χαρακτηρίζονται από εγκυρότητα, οι έρευνες με τη μορφή ερωτήσεων που δίνονται για να απαντηθούν από μεγάλες ομάδες. Οι ερωτήσεις είναι σχεδιασμένες με τρόπο που υποστηρίζουν τη συλλογή έγκυρων δεδομένων, η τεχνική του brainstorming κατά την οποία μέσα από αυθόρμητες απαντήσεις και σκέψεις οι συμμετέχοντες εκφράζουν τις απόψεις τους με δημιουργικότητα και με αυτό τον τρόπο μπορούν να προκύψουν νέες ιδέες και λύσεις, η τεχνική των Δελφών η οποία έχει τη

μορφή επανειλημμένης έρευνας στην οποία συμμετέχουν εμπειρογνώμονες και συλλέγονται οι απόψεις τους.

Εφόσον ολοκληρωθεί η ποιοτική ανάλυση των κινδύνων, τα αποτελέσματα που αναφέρονται στην εκτίμηση των κινδύνων καταγράφονται σε έναν πίνακα και η πιθανότητα και οι επιπτώσεις ενός περιστατικού κατατάσσονται σε κατηγορίες σε τρεις κατηγορίες υψηλό, μεσαίο και χαμηλό.



Πίνακας 4.1: Risk matrix

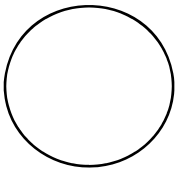
Σημαντικό ρόλο στην αναγνώριση και ποιοτική ανάλυση του κινδύνου έχουν οι ακόλουθες μεθοδολογίες.

Fault tree analysis model

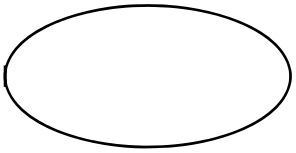
Η ανίχνευση δένδρων βλαβών είναι μια τεχνική ανάλυσης που χρησιμοποιείται για να προσδιορίσει τη ριζική αιτία που προκαλεί ένα συγκεκριμένο ανεπιθύμητο γεγονός. Η κατασκευή και η ανάλυση των δένδρων σφάλματος περιλαμβάνει εννέα βήματα ξεκινώντας από το ανώτερο επίπεδο στο χαμηλότερο ώστε να εντοπιστούν οι βασικές αιτίες που σχετίζονται με το συγκεκριμένο πρόβλημα. Όπως αναφέρθηκε προηγουμένως, η ανάλυση ξεκινά από το υψηλότερο επίπεδο, από την κορυφή δηλαδή και προς τα κάτω χρησιμοποιώντας Boolean λογική για να μπορέσει να συνδυάσει γεγονότα χαμηλότερου επιπέδου και να αποδοθεί καλύτερα μια ανεπιθύμητη κατάσταση. Το συμβάν κορυφής είναι και το τελικό αποτέλεσμα της βλάβης και αντιπροσωπεύει και το προς επίλυση πρόβλημα για το οποίο απαιτείται η απαραίτητη αξιοπιστία και διαθεσιμότητα. Η τεχνική αυτή χρησιμοποιείται κυρίως σε τομείς ασφάλειας και αξιοπιστίας, καθορίζει ποιοτικά και ποσοτικά την πιθανότητα αποτυχίας ενός πληροφοριακού συστήματος και διευκολύνει στην καλύτερη κατανόηση του τρόπου αποτυχίας του συστήματος, στον εντοπισμό καλύτερων τρόπων μείωσης του κινδύνου και στον προσδιορισμό των συμβάντων που προκαλούν συστηματικά ένα περιστατικό ασφάλειας.

Για την ανάπτυξη ενός δένδρου σφάλματος χρησιμοποιούνται λογικές πύλες οι οποίες σε συνδυασμό με τα βασικά συμβάντα και άλλα βασικά σύμβολα αποτελούν το συγκεκριμένο πρότυπο.
F= {BE, G, T, I)
Όπου
B: σύνολο βασικών συμβάντων
T: σύνολο πυλών
I: σύνολο εισόδων στις πύλες

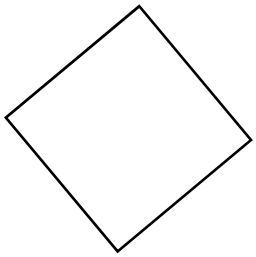
Βασικά σύμβολα



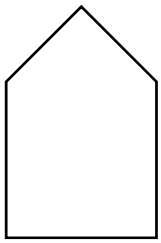
Βασικό συμβάν σφάλματος, δεν υπάρχουν άλλα από κάτω.



Προηγούμενη εκδήλωση, ειδικοί όροι ή περιορισμοί που ισχύουν για οποιαδήποτε λογική πύλη και κυρίως χρησιμοποιούνται με πύλες priority and και inhibit.



Αντιπροσωπεύει ένα γεγονός που δεν αναπτύσσεται πλέον είτε γιατί έχει ανεπαρκή συνέπεια ή επειδή οι πληροφορίες δεν είναι διαθέσιμες, περιέχει συμβολικά γεγονότα που δεν εμφανίζονται.



Εξωτερική εκδήλωση, ένα συμβάν που αναμένεται να συμβεί.

Root event - το γεγονός που θα αναλυθεί εκτενώς μέσω των λογικών πυλών και προκλήθηκε από προηγούμενες ενέργειες.

Λογικές πύλες

AND: υποδεικνύει ότι το γεγονός θα συμβεί όταν πραγματοποιηθούν όλα τα συμβάντα.

OR: υποδηλώνει ότι το παραπάνω γεγονός θα συμβεί αν πληρούνται ένα από τα παρακάτω γεγονότα.

Αποκλειστικό and: το γεγονός εξόδου θα γίνει αν όλα τα σφάλματα εισόδου εμφανιστούν σε συγκεκριμένη ακολουθία .

Αποκλειστικό or: το γεγονός θα συμβεί αν συμβεί ένα μόνο γεγονός εισόδου.

Inhibit: παρουσιάζεται σφάλμα εξόδου όταν το σφάλμα εισόδου εμφανίζεται μόνο μια συνθήκη ενεργοποίησης.

Σύμβολα μεταφοράς

Transfer in δηλώνει ότι το δένδρο αναπτύσσεται περαιτέρω

Transfer out δηλώνει ότι αυτό το τμήμα του δένδρου πρέπει να συνδεθεί στο αντίστοιχο transfer in.

Βασικοί όροι

Cut set: ένα σύνολο από αποτυχίες υλικού και λογισμικού που θα προκαλέσει βλάβη στο σύστημα.

Minimal cut set: το ελάχιστο σύνολο κοπής - ο ελάχιστος συνδυασμός των αποτυχιών υλικού και λογισμικού οι οποίες αν συμβούν όλες μαζί θα προκαλέσουν ένα συμβάν.

Failure - αποτυχία: ως αποτυχία ορίζεται ένα βασικό μη φυσιολογικό περιστατικό σε ένα υλικό ή λογισμικό. Θεωρείται η αδυναμία μιας λειτουργίας να ανταποκριθεί στις απαιτήσεις της.

Fault - βλάβη: μια ανεπιθύμητη κατάσταση που εμφανίζεται σε λάθος χρόνο.

Primary fault - κύριο σφάλμα: οποιαδήποτε βλάβη ενός συστατικού του υλικού και του λογισμικού που εμφανίζεται στο περιβάλλον για το οποίο έχει εξειδικευθεί να είναι.

Secondary fault - δευτερεύουσα βλάβη: οποιαδήποτε βλάβη σε ένα συστατικό του υλικού ή του λογισμικού το οποίο δεν σχεδιαστεί για το συγκεκριμένο περιβάλλον που βρίσκεται και η λειτουργία του υπερβαίνει τις προϋποθέσεις για τις οποίες σχεδιάστηκε.

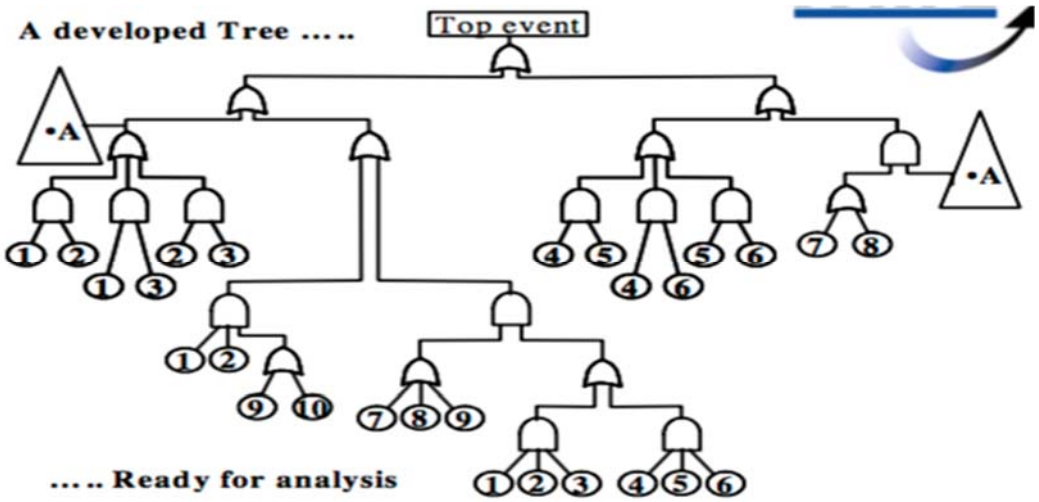
Command fault - σφάλμα εντολής: το σφάλμα εντολής αναφέρεται στη σωστή λειτουργία του εξαρτήματος του υλικού ή του λογισμικού αλλά σε λάθος χρόνο ή μέρος.

Undesirable event - ανεπιθύμητο γεγονός: το συμβάν του ανώτατου επιπέδου για το οποίο ξεκίνησε και η κατασκευή του δένδρου ανάλυσης σφαλμάτων.

Exposure time - χρόνος έκθεσης: είναι ο χρόνος λειτουργίας του συστήματος σε αποτυχία. Όσο μεγαλύτερη είναι η διάρκεια έκθεσης τόσο μεγαλύτερη είναι πιθανότητα αποτυχίας.

Τα βασικά συμβάντα που βρίσκονται στο κατώτερο μέρος συνδέονται με το συμβάν που είναι στην κορυφή μέσω πυλών AND και OR. Είναι πιθανόν πολλοί συνδυασμοί βασικών αιτιών να προκαλέσουν το επάνω συμβάν.
Κάθε κατηγορία σφάλματος περιγράφεται με ένα σύμβολο συμβάντος
Βασικό συμβάν – πρωτεύον σφάλμα
Ενδιάμεσο συμβάν – σφάλμα εντολής
Μη ανεπτυγμένο συμβάν – δευτερεύον σφάλμα

Σχεδιάγραμμα



Σχήμα 4.5: Fault tree analysis

Κανόνες

- Ακριβής περιγραφή του συμβάντος. Ποιο είναι το σφάλμα και πότε συμβαίνει.
- Αν στην ερώτηση το σφάλμα μπορεί να αποτελεί στοιχείο αποτυχίας η απάντηση είναι ναι, το σφάλμα κατατάσσεται στην κατηγορία σφάλμα κατάστασης συνιστωσών αλλιώς σφάλμα κατάστασης συστήματος.
- Κανένας κανόνας θαύματος. Αν η κανονική λειτουργία ενός στοιχείου έχει ως αποτέλεσμα την ακολουθία σφαλμάτων τότε θεωρούμε ότι το στοιχείο λειτουργεί κανονικά.
- Κανόνας πλήρους ανάλυσης. Όλες οι είσοδοι μια πύλης πρέπει να έχουν οριστεί πριν γίνει περαιτέρω ανάλυση.
- Κανόνας πύλη προς πύλη. Οι είσοδοι μιας πύλης πρέπει να είναι σφάλματα και όχι άλλες πύλες.

Η κατασκευή και η ανάλυση του δένδρου σφάλματος ακολουθεί την παρακάτω διαδικασία.

1. Ορισμός συστήματος: Στο πρώτο βήμα γίνεται ανάλυση του σχεδιασμού και της λειτουργίας του συστήματος.
2. Καθορισμός του ανεπιθύμητου, κορυφαίου συμβάντος: Στο δεύτερο βήμα ορίζεται το συμβάν το οποίο έχει γνωστοποιηθεί από προηγούμενη ανάλυση κινδύνου.
3. Καθορισμός ορίων: Ο αναλυτής του συστήματος καθορίζει τα όρια, τα υποσυστήματα, τις λειτουργίες και το περιβάλλον του βασικού συστήματος
4. Κατασκευή του δένδρου σφάλματος: Εφόσον έχει οριστεί ποιο είναι το ανεπιθύμητο συμβάν, ξεκινά η δημιουργία του δένδρου, αρχίζοντας από τη ν κορυφή χρησιμοποιώντας πύλες and και or για να ενώσει με τα ενδιάμεσα γεγονότα ώστε η ανάλυση να φτάσει στο κατώτερο επίπεδο όπου δεν θα υπάρχει άλλη αποσύνθεση του γεγονότος και θα είναι το βασικό γεγονός το οποίο θα αποτελεί και την κύρια αιτία του περιστατικού.

5. Επίλυση δένδρου σφάλματος: Στο σημείο αυτό γίνεται ποιοτική αξιολόγηση του δένδρου εφαρμόζοντας την Boolean άλγεβρα. Σε περίπτωση που ζητηθεί και ποσοτική αξιολόγηση, θα πρέπει να παρέχονται και δεδομένα που αφορούν το ρυθμό αποτυχίας για κάθε ένα από τα βασικά συμβάντα καθώς και να υπολογιστεί η πιθανότητα αποτυχίας του κορυφαίου γεγονότος.

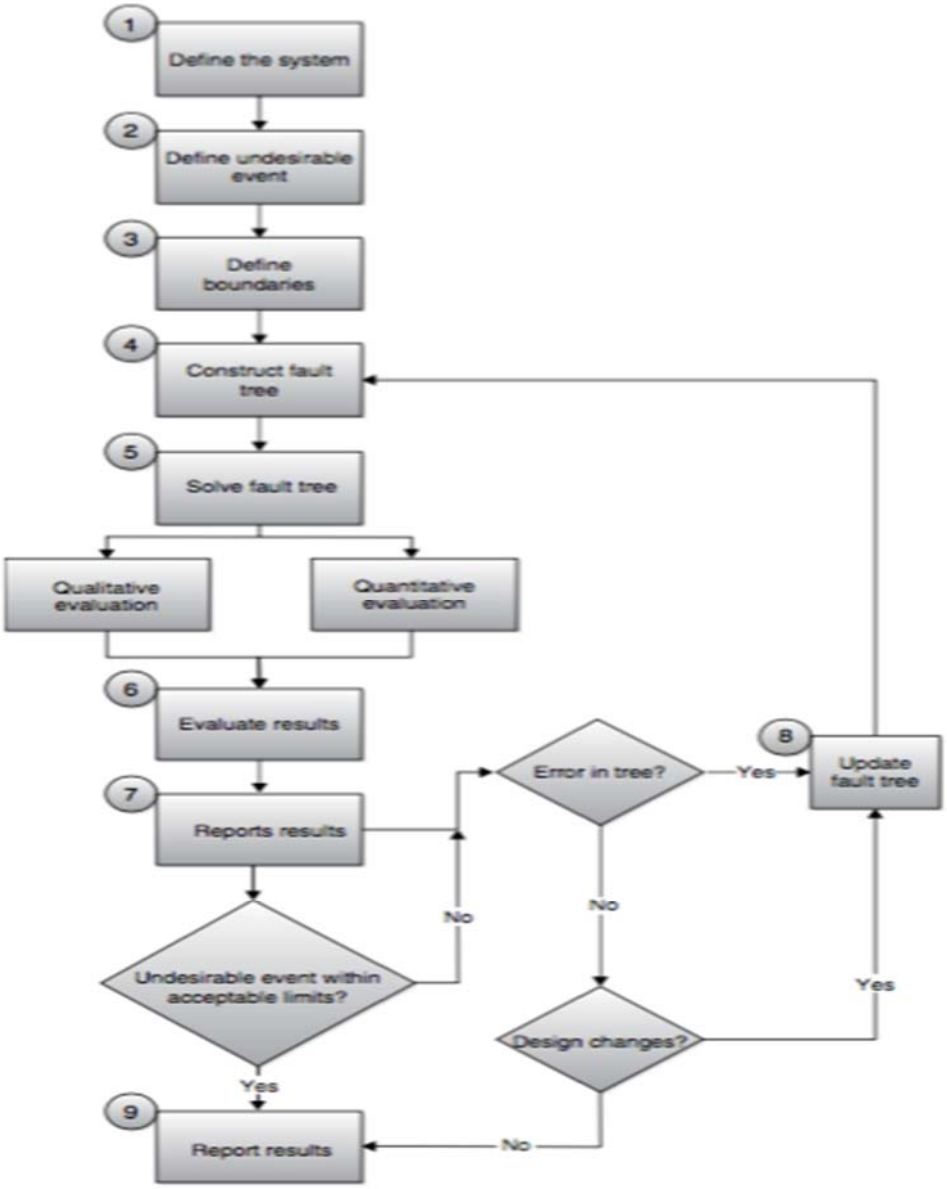
Η πιθανότητα αποτυχίας ορίζεται από τη συνάρτηση:

P=1-R=1-e^-λ
Όπου
R: η αξιοπιστία R= e^-λ
Λ: ο ρυθμός αποτυχίας
Τ: ο χρόνος έκθεσης αποτυχίας

Εφόσον καθοριστούν τα ποσοστά αποτυχίας για κάθε βασικό συμβάν μπορεί να υπολογιστεί και η πιθανότητα του κορυφαίου συμβάντος ξεκινώντας από το κατώτερο επίπεδο και ακολουθώντας τις λογικές πύλες θα υπολογιστεί το τελικό αποτέλεσμα ως εξής:

Για την πύλη AND η πιθανότητα αποτυχίας είναι
$P_f=P_a* P_b$
Ενώ για την πύλη OR η πιθανότητα αποτυχίας είναι
$P_f=P_a+P_b-(P_a*P_b)$
Όσο αφορά την ποιοτική αξιολόγηση του κινδύνου, το FTA μπορεί να αποτελέσει ένα μέσο για τον εντοπισμό και την καταγραφή της εκτίμησης και της διαχείρισης των συνεπειών μιας ανεπιθύμητης απειλής. Το ελάχιστο σύνολο κοπής αποτελεί το βασικό διαρθρωτικό στοιχείο που περιέχει τις ελάχιστες αποτυχίες του συστήματος που αν συμβούν θα προκαλέσουν περιστατικό ασφάλειας. Με το ελάχιστο σύνολο κοπής δημιουργείται μια δομημένη σχέση αιτίας και αιτιατού όπου μέσα από τις διαδρομές του δένδρου τα γεγονότα και οι αιτίες αλληλεπιδρούν δημιουργώντας μοναδικούς συνδυασμούς βασικών συμβάντων για την κατανόηση των βασικών τρωτών σημείων του συστήματος.

6. Αξιολόγηση αποτελεσμάτων: Ο αναλυτής αξιολογεί τα αποτελέσματα του προηγούμενου βήματος και καθορίζει ποιες θα είναι οι διορθωτικές ενέργειες που πρέπει να γίνουν στο σύστημα για να μετριαστεί ή ακόμα και να εξαλειφθεί η πιθανότητας εμφάνισης του κορυφαίου συμβάντος.
7. Αναφορά αποτελεσμάτων: Στο βήμα αυτό συντάσσεται αναφορά με τα αποτελέσματα που προήλθαν από το δένδρο ανάλυσης σφάλματος.
8. Ενημέρωση του δένδρου σφάλματος: Γίνεται ενημέρωση του δένδρου σε περίπτωση που υπάρχουν ακόμα σφάλματα ή επειδή έγιναν αλλαγές στο σύστημα.
9. Αναφορά αποτελεσμάτων: Στο τελευταίο βήμα συντάσσεται νέα αναφορά με τα αποτελέσματα της ενημέρωσης του δένδρου σφάλματος.[08]



Σχήμα 4.6: Διαδικασία σχεδιασμού και ανάλυσης ενός FTA

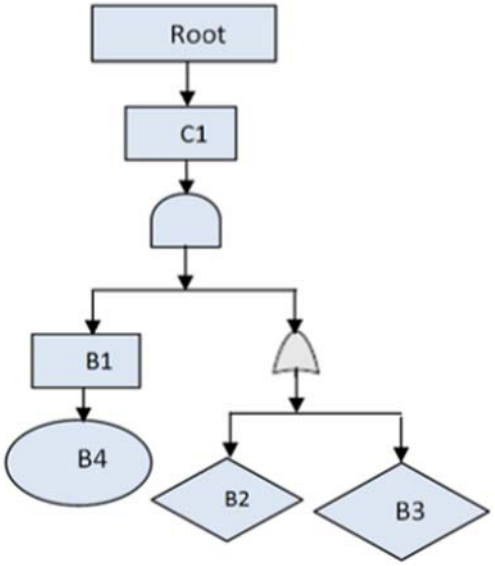
Σκοπός του μοντέλου του δένδρου ανάλυσης σφάλματος είναι να δώσει έμφαση στην αξιοπιστία του συστήματος δίνοντας προτεραιότητα στους συντελεστές που οδηγούν στην κορυφή του συμβάντος, να παρακολουθήσει τις επιδόσεις ασφάλειας αλλά και να βοηθήσει στην ελαχιστοποίηση και βελτιστοποίηση των πόρων, στο σχεδιασμό του συστήματος και στη διάγνωση των αιτιών του συμβάντος.

Για την καλύτερη κατανόηση της λειτουργίας του δένδρου σφάλματος θα περιγράψουμε το ακόλουθο παράδειγμα.

Συμβάν: Διαρροή δεδομένων από εξερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου.
Για να δημιουργηθεί το δένδρο σφάλματος θα πρέπει να αναλύσουμε τα σφάλματα που έχει κάνει ο υπάλληλος. Ο υπάλληλος πιθανόν να έστειλε email σε λάθος ηλεκτρονική διεύθυνση και δεν κατάφερε να επαληθεύσει τον αποδέκτη λόγω έλλειψης επιμέλειας. Επιπλέον, οι ανεπαρκείς τεχνικοί έλεγχοι όπως η κρυπτογράφηση και η χρήση κωδικών πρόσβασης θα μπορούσαν να αποτελέσουν βασικά αίτια διαρροής δεδομένων. [14]

Root event: Διαρροή δεδομένων
C1= λανθασμένη διεύθυνση

B1= αποτυχία επιβεβαίωσης διεύθυνσης παραλήπτη
B2: έλλειψη πολιτικών και διαδικασιών
B3: έλλειψη τεχνικών ελέγχων
B4: έλλειψη δέουσας επιμέλειας των υπαλλήλων



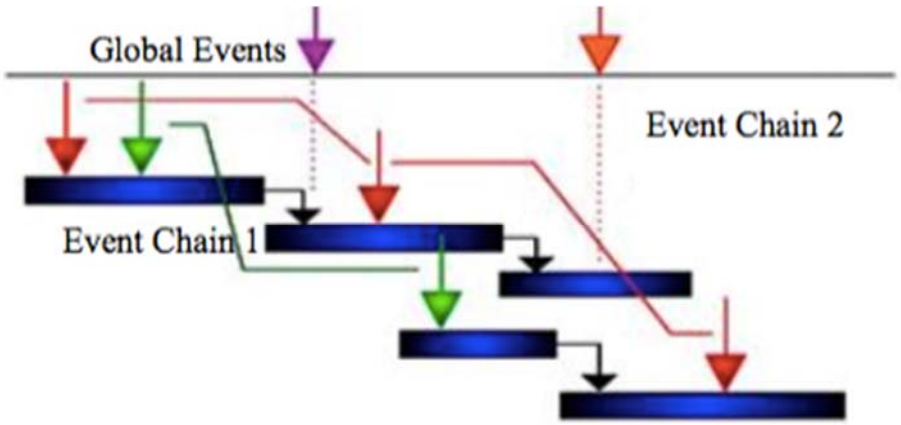
Σχήμα 4.7: FTA για διαρροή δεδομένων μέσω ηλεκτρονικού ταχυδρομείου

Η μέθοδος αυτή είναι μια αρκετά δημοφιλής και ισχυρή τεχνική που μπορεί να εφαρμοστεί σε διαφορετικούς τομείς και μπορεί να αναλύσει επιτυχώς πιθανά σενάρια που προκαλούν περιστατικά ασφάλειας τα οποία προέρχονται από ανθρώπινα σφάλματα. Η αξιολόγηση του ριζικού συμβάντος χαρτογραφεί διαφορετικά πρότυπα συμπεριφοράς και αναλύει και ερμηνεύει αποτελεσματικά την ανθρώπινη φύση.

Chain of events model

Το μοντέλο αυτό ασχολείται με τη διαχείριση των κινδύνων που μπορεί να προκύψουν από οποιαδήποτε μελλοντική επίθεση στον κυβερνοχώρο. Ταξινομεί χρονολογικά τους παράγοντες που είναι η αιτία για την πρόκληση συμβάντων σε αλυσίδες οι οποίες σε ορισμένες περιπτώσεις αντιπροσωπεύουν και απώλειες. Με το ακόλουθο παράδειγμα γίνεται καλύτερη κατανόηση του μοντέλου.

Η κλοπή μιας ταυτότητας είναι ένα παγκόσμιο γεγονός η οποία περιλαμβάνει απόκτηση ευαίσθητων προσωπικών δεδομένων όπως ονόματα, διευθύνσεις, αριθμούς πιστωτικών καρτών. Η αλυσίδα 1 του μοντέλου αποτελείται από όλες τις παράνομες πράξεις που οδηγούν στην κλοπή πληροφοριών. Αυτές οι πληροφορίες χρησιμοποιούνται από τους εγκληματίες με διαφορετικούς τρόπους για διαφορετικού σκοπούς. Επομένως η αλυσίδα 2 αποτελείται από τις πράξεις των εγκληματιών για να καταστρέψουν το θύμα- στόχο τους αφού έχουν αποσπάσει τις σημαντικές πληροφορίες. Ανάμεσα στις δυο αλυσίδες υπάρχουν οι στρατηγικές και οι τακτικές των εγκληματιών που υιοθετούν για να πετύχουν στο στόχο τους. [15]



Σχήμα 4.8: Chain of event model

Πλεονεκτήματα

- Εντοπίζονται γρήγορα περιστατικά με βάση την αλυσίδα γεγονότων οδηγώντας σε έγκαιρη εφαρμογή μέτρων αντιμετώπισης.
- Δίνει έμφαση σε επικίνδυνες συμπεριφορές και σε παράγοντες που συμβάλλουν σε γεγονότα αποτυχίας.

Μειονεκτήματα

- Ανεπαρκής πρόβλεψη για ευπάθειες.
- Χαμηλή πιθανότητα αντιμετώπισης όλων των γνωστών τρωτών σημείων.

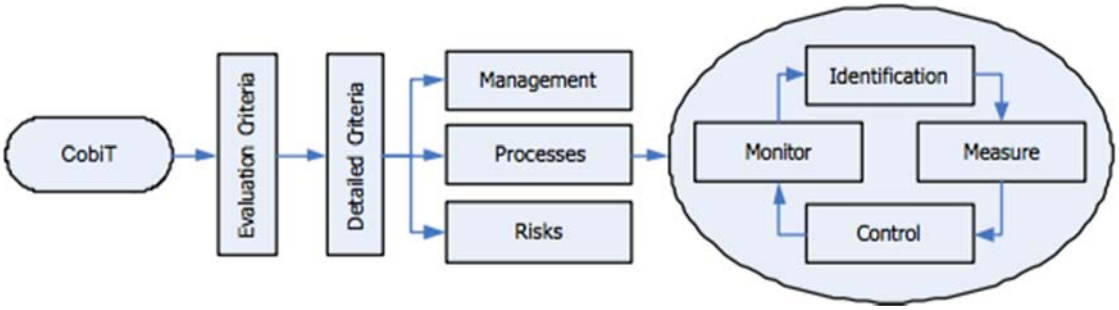
Μεθοδολογία αξιολόγησης κινδύνων

Ένα πολύ σημαντικό σημείο κατά τη διαδικασία λήψης απόφασης είναι η ανάλυση των απειλών και των κινδύνων. Υπάρχουν πολλές διαφορετικές μέθοδοι που εξυπηρετούν το σκοπό αυτό αλλά κάθε επιχείρηση εφαρμόζει εκείνη που ανταποκρίνεται καλύτερα τις ανάγκες της. Κάθε μέθοδος εστιάζει σε ένα συγκεκριμένο σκοπό και έχει διαφορετικά χαρακτηριστικά. Στη συνέχεια θα περιγράψουμε τις πιο διαδεδομένες μεθόδους διαχείρισης κινδύνου.

COBIT: Το πλαίσιο COBIT εφαρμόζεται γενικότερα για τη διακυβέρνηση της επιχείρησης και ένα μέρος του αποτελεί η διαχείριση των κινδύνων η οποία γίνεται με ποιοτικά μέτρα. Πρώτη ενέργεια είναι η κατανόηση των επιχειρησιακών στόχων και πως οι στόχοι της πληροφορικής ευθυγραμμίζονται με τους στόχους της επιχείρησης. Στη συνέχεια ορίζονται οι απειλές και οι ευπάθειες και χρησιμοποιούνται σενάρια κινδύνου και τον ευκολότερο προσδιορισμό του. Στη συνέχεια, αξιολογούνται οι κίνδυνοι και θέτονται προτεραιότητες που υποδεικνύουν σε ποιον κίνδυνο πρέπει να δοθεί περισσότερη προσοχή. Γενικότερα για κάθε κίνδυνο που υπάρχει, πρέπει να αποφασίζεται η κατάλληλη ενέργεια μεταξύ των παρακάτω επιλογών:

- Αποφυγή κινδύνου με τον τερματισμό της δραστηριότητας που προκαλεί τον κίνδυνο
- Μείωση του κινδύνου εφαρμόζοντας αλλαγές
- Μεταφορά του κινδύνου σε τρίτους
- Αποδοχή του κινδύνου και των συνεπειών του

Και αφού έχει αποφασιστεί ποια θα είναι η αντίδραση για κάθε κίνδυνο γίνεται παρακολούθηση και έλεγχος ώστε ο κίνδυνος να διατηρείται σε ανεκτό επίπεδο και συντάσσονται αναφορές σχετικά με τα αποτελέσματα των αποφάσεων που έχουν ληφθεί.[07]



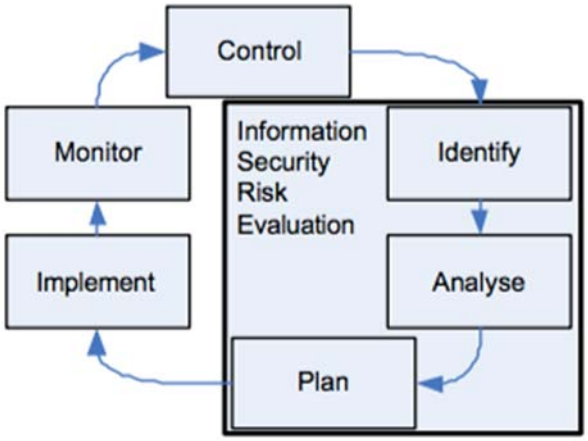
Σχήμα 4.8: Αξιολόγηση κινδύνου με τη χρήση του μοντέλου CobiT

CRAMM: Η μέθοδος CRAMM αναλύει τα περιουσιακά στοιχεία και μετριάζει του κινδύνους. Ακολουθεί τρία βασικά βήματα α) αναγνώριση των περιουσιακών στοιχείων και αποτίμηση αυτών με βάση τον αντίκτυπο και το κόστος μετά από ένα περιστατικό ασφάλειας, β) εκτίμηση και προσδιορισμός των απειλών, γ) επιλογή και εφαρμογή του κατάλληλου αντιμέτρου για τον περιορισμό των κινδύνων και την σωστή διαχείρισή τους. Στο πρώτο βήμα γίνεται αναγνώριση όλων των τύπων αγαθών και τους δίνεται μια αξία που προκύπτει από το κόστος που θα δημιουργούσε μια απώλεια, καταστροφή ή μια διαθεσιμότητα αυτών. Στο επόμενο βήμα εκτιμώνται οι απειλές και υπολογίζεται ο βαθμός κινδύνου της επιχείρησης και στο τέλος αποφασίζεται αν ο βαθμός αυτός είναι υψηλός για να δικαιολογήσει μια εφαρμογή ενός αντιμέτρου.[07]

FAIR: Διαδικασία διαχείρισης κινδύνου που στηρίζεται σε μαθηματικά και σε πολλές ποσοτικές μετρήσεις. Είναι μια ποσοτική ανάλυση του κινδύνου κατά την οποία προσδιορίζονται και αναλύονται οι απειλών των περιουσιακών στοιχείων, αξιολογείται η πιθανότητα εμφάνισης της απειλής και η πιθανότητα η απειλή να προκαλέσει απώλεια λόγω ευπαθειών, καθώς και το μέγεθος των πιθανών απωλειών και στη συνέχεια οι δύο προηγούμενες συνιστώσες συνδέονται με την έννοια του κινδύνου.

FRAAP: Βασιζόμενο στην άποψη ότι ο χρόνος είναι αυστηρά περιορισμένος, έχει σκοπό την επίτευξη γρήγορων αποτελεσμάτων σε πολύ σύντομο χρονικό διάστημα. Εστιάζει σε μεμονωμένα περιουσιακά στοιχεία και παρέχει καθοδήγηση για την αξιολόγηση των κινδύνων σε ώρες. Η μέθοδος FRRAP εστιάζει στην ποιοτική ανάλυση του κινδύνου. Η ομάδα που συντάσσεται εξετάζει τις απειλές και τα τρωτά σημείου του περιουσιακού στοιχείου που εξετάζεται, ανταλλάσσοντας ιδέες μεταξύ τους ώστε να προσδιορίσουν τις πιθανές απειλές και τις επιπτώσεις του στοιχείου και να καθορίσουν ένα επίπεδο κινδύνου για κάθε απειλή με βάση την πιθανότητα εμφάνισης. Στη συνέχεια αποφασίζουν ποιες απειλές πρέπει να γίνουν αποδεκτές και ποιες να ανατεθούν στον κατάλληλο μηχανισμό ελέγχου.

OCTAVE: Το μοντέλο OCTAVE παρέχει μια τεκμηριωμένη διαδικασία διαχείρισης κινδύνου η οποία επικεντρώνεται στην ανάλυση του κινδύνου από οικονομικής πλευράς. Υλοποιείται από μια εξειδικευμένη ομάδα που διαθέτει γνώσεις σχετικά με τις επιχειρηματικές διαδικασίες και τα υφιστάμενα μέτρα που εφαρμόζονται ήδη, η οποία εξετάζει τους κινδύνους από οικονομική προοπτική και αναπτύσσει τις αντίστοιχες στρατηγικές για την κυβερνοασφάλεια. Στην αρχή η ομάδα ορίζει την αξιολόγηση των επιπτώσεων, στη συνέχεια αναλύει ποιος έχει πρόσβαση σε κρίσιμα σημεία και στο τέλος εντοπίζει τους κινδύνους των κρίσιμων στοιχείων και δημιουργεί μια στρατηγική προστασίας για την επιχείρηση.[07]



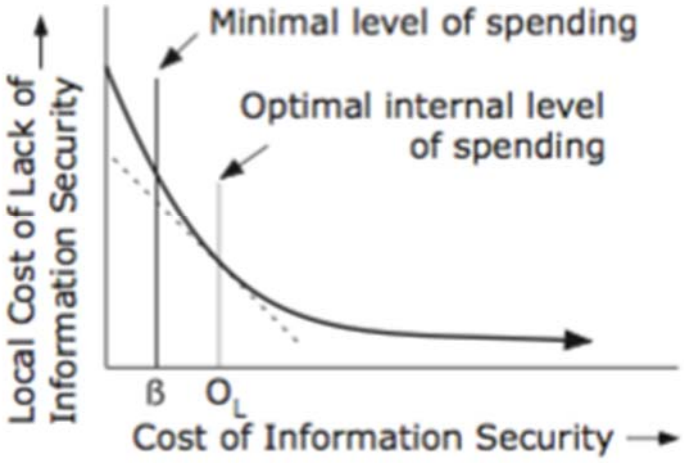
Σχήμα 4.9: Αξιολόγηση κινδύνου με χρήση του μοντέλου Octave

RMM: Το μοντέλο RMM δεν αντιμετωπίζει άμεσα τη διαχείριση κινδύνου αλλά βοηθά στην ανάπτυξη και βελτίωση των υφιστάμενων προγραμμάτων διαχείρισης αφού εξετάζει αν το πρόγραμμα ανταποκρίνεται στις προσδοκίες και στους στόχους της επιχείρησης.

ΤΑΡΑ: Στην αρχή δημιουργήθηκε για να χρησιμοποιηθεί από την Intel όμως με την πάροδο του χρόνου έγινε γνωστό και εφαρμόστηκε και από άλλες επιχειρήσεις δίνοντας μια ενδιαφέρουσα οπτική στη διαχείριση του κινδύνου. Στηρίζεται στη βασική ιδέα ότι δεν είναι λογικός και οικονομικά υποφερτός ο περιορισμός όλων των πιθανών κινδύνων για αυτό και διαχειρίζεται μόνο τις κρίσιμες καταστάσεις, δίνοντας ιδιαίτερη έμφαση στις απειλές, στα κίνητρα των επιτιθέμενων, στις μεθόδους που θα χρησιμοποιήσουν για να ξεκινήσουν την επίθεση καθώς και στους στόχους που θέλουν να επιτύχουν με την πρόκληση του συμβάντος.

4.3 Βέλτιστο επίπεδο επένδυσης

Κάθε επιχείρηση αφού έχει αξιολογήσει τους κινδύνους της, πρέπει να αποφασίσει ποιο επίπεδο ασφάλειας θα υιοθετήσει. Για κάθε επιχείρηση το επίπεδο είναι διαφορετικό διότι εξαρτάται από το μέγεθος, τον τομέα που ανήκει και τους επιχειρηματικούς της στόχους. Υπάρχει ένα βασικό επίπεδο επένδυσης που απαιτείται να εφαρμοστεί και το ονομάζεται βασική γραμμή ασφάλειας β. Πάνω από τη γραμμή ή πάνω στη γραμμή υπάρχει και το βέλτιστο επίπεδο επένδυσης και είναι το σημείο που το οριακό κόστος της ασφάλειας των πληροφοριών ισούται με την οριακή μείωση του κόστους που οφείλεται σε περιστατικά ασφάλειας. Επομένως οι επιχειρήσεις χρειάζεται να εκτιμήσουν τα πιθανά κόστη που προκύπτουν από την έλλειψη της ασφάλειας, τα χρήματα που απαιτούνται για να επενδύσουν σε θέματα ασφάλειας και την απόδοση από μια επένδυση καταλήγουν σε μία απόφαση. Το παρακάτω διάγραμμα συσχετίζει το ελάχιστο επίπεδο με το τοπικά βέλτιστο.[14]



Σχήμα 4.10:Βέλτιστο σημείο επένδυσης

4.3.1 Μοντέλο Gordon Label

Το μοντέλο Gordon Loeb είναι ένα μαθηματικό–οικονομικό μοντέλο που καθορίζει το βέλτιστο επίπεδο των επενδύσεων στον τομέα της ασφάλειας των πληροφοριών. Για να είναι προστατευμένη μια επιχείρηση πρέπει να επενδύσει σε λύσεις που θα της επιφέρουν το επιθυμητό αποτέλεσμα. Αυτή η επένδυση συνυπολογίζεται στα κόστη της επιχείρησης και δεν αποφέρει κέρδη. Κόστος όμως η επιχείρηση έχει και στην περίπτωση που δεχτεί μια επιτυχημένη επίθεση λόγω της απώλειας των δεδομένων αν αυτά χαθούν, αλλοιωθούν ή καταστραφούν. Για το λόγο αυτό σχεδιάστηκε το παρόν μοντέλο για να αναλυθεί μέχρι ποιο σημείο οι οργανισμοί πρέπει να επενδύουν σε αντίμετρα για να εξοικονομούν χρήματα και ταυτόχρονα να έχουν τις λιγότερες απώλειες. Οι βασικοί παράγοντες που επηρεάζουν το αποτέλεσμα είναι η αξία των αγαθών, η σημαντικότητα των αγαθών και η πιθανότητα της επίθεσης .
Ένα σύνολο πληροφοριών χαρακτηρίζεται από 3 παραμέτρους:

Την **απώλεια λ** ως αποτέλεσμα μιας επίθεσης
Την **πιθανότητα τ** να πραγματοποιηθεί η επίθεση
Την **πιθανότητα υ** η επίθεση να χαρακτηριστεί επιτυχημένη

Πιο συγκεκριμένα, ως **λ** ορίζεται η χρηματική απώλεια της επιχείρησης που προήλθε από παραβίαση της ασφάλειας ων πληροφοριών. Αυτή η απώλεια σχετίζεται με παραβίαση της εμπιστευτικότητας, της ακεραιότητας, της άρνηση παροχής υπηρεσιών. Ως **τ** ορίζεται η πιθανότητα απειλής, δηλαδή η πιθανότητα μιας απόπειρας παραβίασης ενός συνόλου δεδομένων $\tau \in (0,1)$. Τέλος η παράμετρος $\upsilon \in (0,1]$ δηλώνει την ευπάθεια με την έννοια ότι μια απειλή, χωρίς καμιά επιπρόσθετη ασφάλεια ,θα γίνει επίθεση και θα προκαλέσει απώλεια λ . Τόσο η πιθανότητα απειλής όσο και η ευπάθεια πρέπει να κυμαίνονται μεταξύ των τιμών $0<\tau<1$ και $0<\upsilon<1$.

Αν υ=0, η πληροφορία είναι αόρατη και συμβαίνει στην περίπτωση που η πληροφορία είναι εντελώς απρόσιτη.
Αν υ=1, η πληροφορία είναι εντελώς ευάλωτη.

Για ένα συγκεκριμένο σύνολο, η πιθανότητα απώλειας που συχνά αποκαλείται κίνδυνος απώλειας, είναι το προϊόν της πιθανότητας αδυναμίας και της πιθανότητας απειλής. Το προϊόν

αυτό δείχνει την προσδοκώμενη απώλεια που σχετίζεται με το σύνολο των δεδομένων και δεν εξαρτάται από την επένδυση που έγινε στην ασφάλεια των πληροφοριών. Για οποιοδήποτε τ>0 η αναμενόμενη ζημιά αυξάνεται με την ευπάθεια.

Οι επενδύσεις που γίνονται σε μια επιχείρηση έχουν σκοπό να επηρεάσουν τις ευπάθειες και όχι να μειώσουν την απειλή.

$L=\tau^*\lambda$

Μια ακόμα παράμετρος είναι η **z.** Ορίζεται ως η **χρηματική επένδυση** που θα κάνει η επιχείρηση στον τομέα της ασφάλειας για να προστατεύσει το σύνολο των πληροφοριών. Η μονάδα μέτρησης του z είναι ίδια με του λ και εκφράζεται με νομισματική αξία. Σκοπός της z επένδυσης είναι να ελαχιστοποιήσει την πιθανότητα παραβίασης η οποία εκφράζεται από τη συνάρτηση S(z,υ) και ορίζεται ως η πιθανότητα ενός συνόλου δεδομένων με ευπάθεια υ να παραβιαστεί με δεδομένο ότι η επιχείρηση έχει επενδύσει z για να προστατεύσει την πληροφορία.
Διακρίνουμε τις εξής περιπτώσεις :

Περίπτωση ν 1
S(z,0) για όλες τις τιμές z. Αν η πληροφορία είναι εντελώς άτρωτη, παραμένει ασφαλής για κάθε τιμή του z ακόμα και τη μηδενική δηλαδή η επιχείρηση να μην έκανε καμία επένδυση.

Περίπτωση ν2
S(0,u) για όλα τις τιμές υ. Αν ζ=0, δηλαδή δεν έχουν δαπανηθεί χρήματα για την προστασία των πληροφοριών, τότε η πιθανότητα παραβίασης της ασφάλειας η οποία εξαρτάται από την πραγματοποίηση μιας απειλής είναι η εγγενής ευπάθεια του συνόλου των πληροφοριών.

Περίπτωση ν3
$S(z,u)>0$ και $S(z,u)<0$ για όλα τα z και $\upsilon(\in\in 0,1)$

Καθώς αυξάνεται η επένδυση z, είναι λογικό οι πληροφορίες να γίνονται πιο ασφαλείς αλλά με μειωμένο ρυθμό. Επιπλέον αν υποθέσουμε ότι για όλα τα υ(0.1) το $\lim S(z,u) \to 0$ καθώς το $z\to\infty$ έτσι επενδύοντας επαρκώς στη ασφάλεια, η πιθανότητα παραβίασης τ πολλές φορές μπορεί να γίνει αυθαίρετα κοντά στο μηδέν.

Από όλα τα παραπάνω συμπεραίνουμε ότι ακόμα και μια πολύ μικρή επένδυση για την ασφάλεια των πληροφοριών μπορεί να μειώσει την πιθανότητα παραβίασης της ασφάλειας. Ωστόσο καμία επένδυση δεν μπορεί να θέσει απόλυτα ασφαλή μια ευάλωτη πληροφορία. Καθώς η επιχείρηση δεν γνωρίζει από την αρχή το κόστος ασφάλειας των πληροφοριών το οποίο δεν είναι και σταθερό, προτού πάρει οποιαδήποτε απόφαση για το ποσό που πρέπει να επενδύσει στην ασφάλεια και δεδομένου ότι είναι ουδέτερη σε σχέση με τον κίνδυνο, συγκρίνει τα αναμενόμενα οφέλη της επένδυσης με το αντίστοιχο κόστος της.

Τα αναμενόμενα οφέλη της επένδυσης υποδηλώνονται με τον όρο
EBIS και ισούνται

$EBIS(z)=[\upsilon-S(z,u)]L$

Με τη μείωση της αναμενόμενης ζημιάς της επιχείρησης που αποδίδεται στην επιπρόσθετη ασφάλεια

ENBIS(z)=[u,S(z,u)]L-z

Ως βέλτιστη απόδοση ορίζουμε το z*(u)
Το σύνολο των πληροφοριών δεν είναι πλήρες ευάλωτο ούτε πλήρες άτρωτο 0<υ<1

Θεωρητικά αν ένα σύνολο πληροφοριών είναι τελείως άτρωτο, η βέλτιστη επένδυση στην ασφάλεια τους είναι μηδέν z*(0)=0

Ο κάθε οργανισμός πρέπει να επενδύει στην ασφάλεια μόνο μέχρι το σημείο που το οριακό όφελος ισούται με το οριακό κόστος

S(z*,u)L=1

Η αξία ενός συνόλου πληροφοριών μετριέται από τη δυνητική απώλεια που σχετίζεται με το σύνολο των πληροφοριών. Επιπλέον μπορούμε να πούμε ότι για ένα δεδομένο επίπεδο ευπάθειας το βέλτιστο ποσό z* που θα επενδυθεί για την ασφάλεια πληροφοριών αυξάνεται καθώς αυξάνεται και η αξία του συνόλου της πληροφορίας (με αύξηση της απειλής t ή της απώλειας λ).Σε κάθε περίπτωση το βέλτιστο ποσό που πρόκειται να επενδυθεί είναι μικρότερο από το uL

Τέλος το βέλτιστο επίπεδο επένδυσης είναι ίσο με το μηδέν αν το οριακό όφελος σε z=0 είναι μικρότερο ή ίσο του οριακού κόστους μιας τέτοιας επένδυσης.

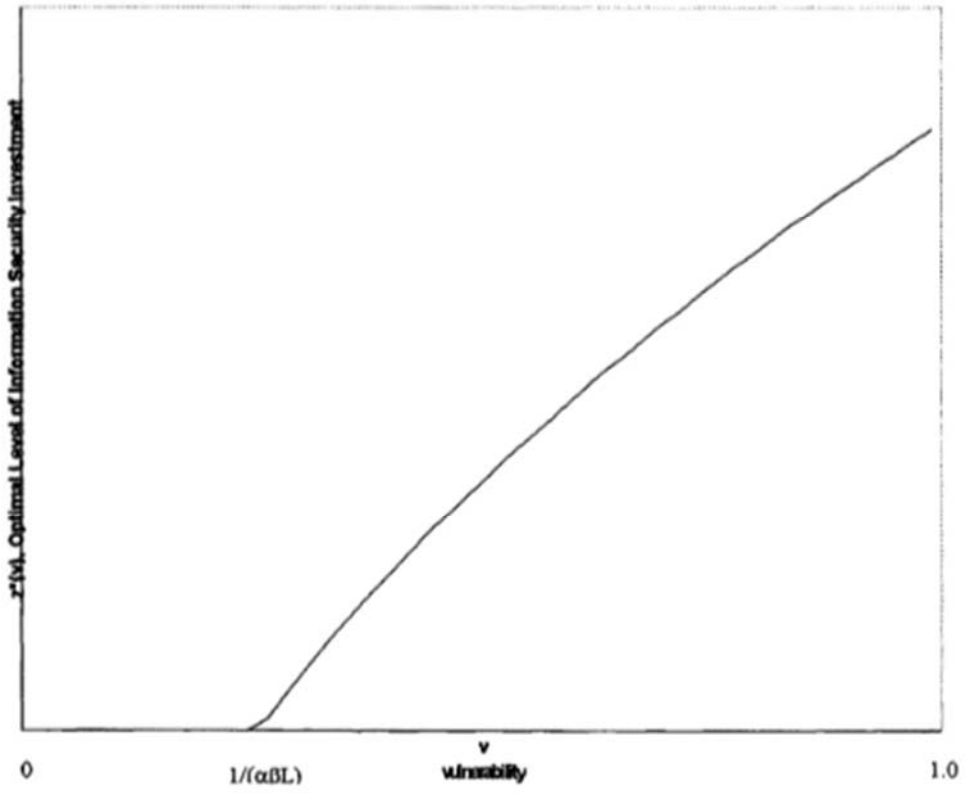
$L \leq \frac{1}{Sz(0,u)}$

Όπως αναφέρθηκε και προηγουμένως, αν το σύνολο των πληροφοριών δεν είναι απολύτως άτρωτο u=0 δεν υπάρχει λόγος να πραγματοποιηθεί κάποια επένδυση στον τομέα της ασφάλειας, δηλαδή z*(0)=0. Σε κάθε άλλη περίπτωση που το σύνολο των πληροφοριών παρουσιάζει υψηλότερο ποσοστό ευπάθειας, είναι αναγκαίο να πραγματοποιηθεί μια επένδυση ώστε να μειωθεί η πιθανότητα απώλειας και κατ' επέκταση η αναμενόμενη απώλεια. Σε κάποιο βαθμό n η αύξηση της ευπάθειας οδηγεί και σε αύξηση των επενδύσεων.

Πρώτη τάξη λειτουργιών παραβίασης

$Z^{I*}(\upsilon) = \frac{\frac{(\upsilon\beta\alpha L))^1}{\beta+1} - 1}{\alpha}$

Η βέλτιστη επένδυση ισούται με μηδέν μέχρι $\upsilon = \frac{1}{\alpha\beta L}$



Σχήμα 11: Βέλτιστη τιμή επένδυσης ως συνάρτηση ευπάθειας για την πρώτη τάξη λειτουργιών

Ο τύπος που εκφράζει το εσωτερικό βέλτιστο επίπεδο ασφάλειας είναι

$Z^{II*}(\upsilon) = \frac{\ln(1/-a\upsilon L(ln\upsilon)}{aln\upsilon}$

Δεύτερη τάξη λειτουργιών

Σχήμα 4.12: Βέλτιστη τιμή επένδυσης ως συνάρτηση της ευπάθειας για τη δεύτερη τάξη λειτουργιών

$S^{II}(z,\upsilon) = \upsilon^{\alpha z+1}$

Όπου α: μέτρο παραγωγικότητας της ασφάλειας.

Οι Gordon Loeb προτείνουν αυτό το μαθηματικό μοντέλο σύμφωνα με το οποίο για κάθε δεδομένη ευπάθεια υπάρχουν διαφορετικά επίπεδα ασφάλειας πληροφοριών τα οποία μπορούν να εφαρμοστούν όταν ένα υψηλότερο επίπεδο ασφάλειας θα προκαλέσει πτώση της αναμενόμενης απώλειας αυτής της ιδιαίτερης ευπάθειας. Αυτό διαμορφώνεται ως συνάρτηση του επιπέδου ασφάλειας σε μια αναμενόμενη ευπάθεια στη μείωση της απειλής. Έδειξαν ακόμα ότι για ένα ευρύ φάσμα λειτουργιών πιθανότητας παραβίασης, το βέλτιστο ποσό που θα επενδύσει η επιχείρηση δεν πρέπει να υπερβαίνει το 36,8% της αναμενόμενης ζημιάς που θα προκαλέσει η παραβίαση της ασφάλειας. [01]Ο Willemsot αμφισβήτησε το όριο αυτό και ως απαιτούμενο όριο επένδυσης έδωσε το 50%. Τέλος το μοντέλο αυτό εξετάζει τον τρόπο με τον οποίο η ευπάθεια και η απώλεια επηρεάζουν το βέλτιστο επίπεδο των πόρων που πρέπει να αφιερωθούν για τη διασφάλιση των πληροφοριών.

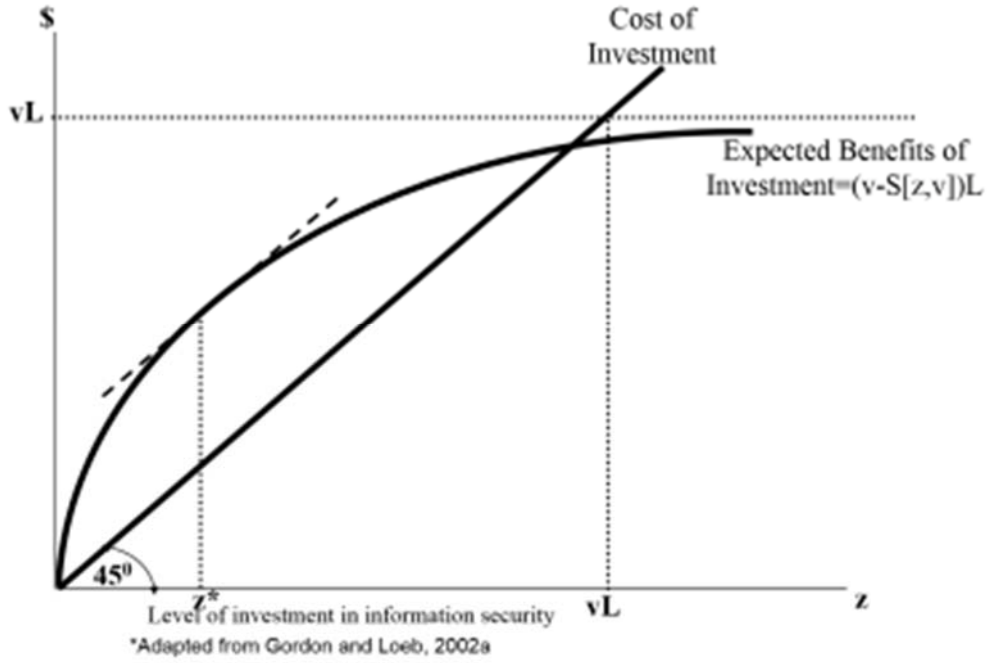
Έτσι λοιπόν οι διαχειριστές της ασφάλειας πρέπει να διαιρούν τα σύνολα της πληροφορίας σε χαμηλά, μεσαία και υψηλά επίπεδα ευπάθειας και ανάλογα με το επίπεδο στο οποίο βρίσκονται να αποφασιστεί το αντίστοιχο ποσό της επένδυσης.

Υπάρχουν τρία βασικά στοιχεία που υπογραμμίζουν τον τρόπο με τον οποίο μια επιχείρηση θα κάνει την βέλτιστη επένδυση στην ασφάλεια του κυβερνοχώρου.

1.Το πρώτο σημαντικό στοιχείο είναι να προσδιορίσει και να αποτιμήσει το σύνολο των πληροφοριών της. Η αξίας της πληροφορίας αντιπροσωπεύει την δυνητική απώλεια στην περίπτωση που βιώσει οποιουδήποτε τύπου παραβίαση.

2.Το δεύτερο σημαντικό στοιχείο είναι να εκτιμήσει ο οργανισμός την πιθανότητα να δεχτεί μια επίθεση ένα σύνολο πληροφοριών. Η εκτίμηση αυτή γίνεται με βάση την ευαισθησία του συνόλου των πληροφοριών.

3.Και το τρίτο σημαντικό στοιχείο σχετίζεται με τον τρόπο που η επένδυση στην ασφάλεια θα μειώσει την ευπάθεια ενός συνόλου πληροφοριών σε μια παραβίαση. Ουσιαστικά αναφέρεται στην παραγωγικότητα της επένδυσης η οποία πιθανώς να διαφέρει για διαφορετικά σύνολα πληροφοριών.



Σχήμα 4.13: Ανάλυση κόστους όφελους

Συνοψίζοντας, το μοντέλο Gordon Loeb εμπεριέχει ένα σύνολο βημάτων που πρέπει να ακολουθεί ο κάθε οργανισμός προτού λάβει απόφαση σε ποιο επίπεδο θα επενδύσει για την ασφάλεια του κυβερνοχώρου. Στη αρχή κάθε οργανισμός καθορίζει την αξία κάθε πληροφορίας καθώς και την πιθανή ζημιά της από τυχόν επιτυχημένη παραβίαση. Στη συνέχεια ο οργανισμός εκτιμά την πιθανότητα παραβίασης του κάθε συνόλου πληροφορίας με βάση την ευπάθεια του συνόλου αυτό και δημιουργεί ένα πλέγμα όλων των δυνατών συνδυασμών l,z. Τέλος, καθορίζει το επίπεδο επένδυσης στον κυβερνοχώρο και την κατανομή των πόρων που θα δεσμεύσει για την προστασία της πληροφορίας.

Ωστόσο κατά την εφαρμογή του συγκεκριμένου πλαισίου για τη λήψη της απόφασης προκύπτουν και κάποιοι περιορισμοί που πρέπει να μην αγνοηθούν. Ο πρώτος περιορισμός αναφέρεται στην αβεβαιότητα που συνδέεται με την αποτίμηση του συνόλου των πληροφοριών που προσπαθεί να προστατεύσει και στην εκτίμηση της πιθανότητας της παραβίασης του συνόλου αυτού. Ο δεύτερος περιορισμός έγκειται στο γεγονός ότι θεωρείται μια εντελώς adhoc προσέγγιση η οποία δεν λαμβάνει υπόψη τις ποιοτικές πτυχές και ανησυχίες της επιχείρησης, για παράδειγμα τη γενική στρατηγική του οργανισμού πριν την τελική λήψη της απόφασης επένδυσης.

Σε καμία περίπτωση το μοντέλο που μελετάμε δεν παρέχεται ως λύση στο μείζον ζήτημα της ασφάλειας που είναι εκτεθειμένες οι επιχειρήσεις. Θεωρείται ως μια ορθολογική οικονομική διαδικασία η οποία είναι μέρος της συνολικής διαδικασίας λήψης αποφάσεων και βοηθά τις επιχειρήσεις να αποφασίσουν πόσα χρήματα θα επενδύσουν στον τομέα της ασφάλειας υπό το πρίσμα του κινδύνου που έχουν να αντιμετωπίσουν. Η προσέγγιση κόστους οφέλους που

αναλύεται μέσω του μοντέλου θεωρείται ένα καλό σημείο εκκίνησης για τις επενδυτικές αποφάσεις της επιχείρησης.[17,18,28]

4.4 Μεθοδολογίες υποστήριξης αποφάσεων

Κάθε οργανισμός έχει ως βασικό σκοπό να δώσει προτεραιότητα στην οργάνωση της άμυνας, να εξετάσει ποιες είναι οι απειλές από τις οποίες κινδυνεύει περισσότερο και να μειώσει τις ευπάθειες και τα αδύναμα σημεία της ασφάλειας στον κυβερνοχώρο. Δεδομένου ότι η μεγαλύτερη πρόκληση που έχουν να αντιμετωπίσουν είναι ο χαμηλός προϋπολογισμός και η έλλειψη χρηματοδότησης τα οποία δεν επαρκούν για να καλύψουν τις ευπάθειες, κάθε οργανισμός καλείται να βρει μια ισορροπία για να υπερασπιστεί το σύστημά του. Στη διαδικασία της λήψης της σωστής απόφασης για το πως και που θα επενδυθεί το διαθέσιμο χρηματικό πόσο στα θέματα ασφάλειας συμβάλλει ενεργά η προσέγγιση της θεωρίας παιγνίων που ακολουθούν οι συμμετέχοντες. Το μοντέλο της θεωρίας παιγνίων είναι ένα μαθηματικό πλαίσιο για τη μοντελοποίηση των συγκρούσεων και τη συνεργασία δύο ή περισσότερων ατόμων. Υπάρχουν τρεις διαφορετικές μεθοδολογίες που μπορούν να εφαρμοστούν:

1. Θεωρία καθαρού παιχνιδιού: αποτελείται από ένα μεγάλο παιχνίδι που περιλαμβάνει όλους τους ελέγχους και όλες τις απειλές.
2. Υβριδική μεθοδολογία: εμπεριέχει όλες τις λύσεις για κάθε παιχνίδι και σε συνδυασμό με τον αλγόριθμο σακιδίου Knapshack προτείνει τη βέλτιστη επενδυτική στρατηγική.
3. Συνδυαστική τεχνική: αποτελείται από μια στρατηγική πολλαπλών στόχων-πολλαπλών επιλογών σε συνδυασμό με τον αλγόριθμο του σακιδίου.

Κατά την εφαρμογή του μοντέλου διαμορφώνονται οι αλληλεπιδράσεις των συμπεριφορών των παικτών. Ορίζουμε ως A-attacker (επιτιθέμενος) και ως D-defender (αυτός που αμύνεται). Αναλυτικότερα, ο D μπορεί να είναι ο διαχειριστής ασφάλειας του κυβερνοχώρου σε μια επιχείρηση και ο στόχος του είναι να υπερασπίσει τα περιουσιακά στοιχεία του οργανισμού από κλοπή και καταστροφή, να μετριάσει τη δυνητική επιχειρηματική συμπεριφορά καθώς και να διατηρήσει τη φήμη του οργανισμού. Για να τα πετύχει όλα αυτά, έχει στη διάθεσή του έναν προϋπολογισμό B που θέλει να επενδύσει για να παραμείνει το σύστημά του ασφαλές. Οι έλεγχοι ασφάλειας που εφαρμόζει για την επίτευξη του στόχου του βρίσκονται σε διαφορετικά επίπεδα. Ισχύει ότι όσο υψηλότερο είναι το επίπεδο, τόσο μεγαλύτερος είναι ο βαθμός που εφαρμόζεται ο έλεγχος. Κάθε έλεγχος φέρνει ορισμένα πλεονεκτήματα, φέρνει όμως και άμεσες και έμμεσες δαπάνες.[17]

Μερικές έννοιες που χρησιμοποιούνται είναι οι ακόλουθες:

Βάθος στοιχείου: ορίζουμε τη θέση του περιουσιακού στοιχείου μέσα στον οργανισμό. Ουσιαστικά καθορίζει τη σημασία του αγαθού όταν ο οργανισμός το χάσει μετά από μια επιτυχημένη επίθεση. Όσο μεγαλύτερο είναι το βάθος τόσο μεγαλύτερη αξία και πιο εμπιστευτικά είναι τα δεδομένα. Αγαθά του ίδιου βάθους έχουν και την ίδια αξία για την επιχείρηση. Έκτος από την ίδια αξία έχουν και τις ίδιες ευπάθειες.

T= το σύνολο των στόχων ασφάλειας μέσα σε έναν οργανισμό $T=\{t_ι\}$

V= το σύνολο των ευπαθειών που απειλούνται από επιθέσεις μέσα στον οργανισμό $V=\{v_z\}$

D= το σύνολο των βαθών $D=\{d_x\}$

L= το σύνολο των επιπέδων που υλοποιείται ο έλεγχος ασφάλειας L={lk}. Όσο υψηλότερο είναι το επίπεδο τόσο μεγαλύτερος είναι ο βαθμός που εφαρμόζεται ο έλεγχος.

Ένας στόχος ασφάλειας στον κυβερνοχώρο ορίζεται ως το ζεύγος ευπάθειας-βάθους $t=\{v_z, d_x\}$. Επίσης συνδέεται με μια αξία κρούσης που εκφράζει το επίπεδο ζημιών που προκαλούνται στον D αν ο A καταφέρει να επιτεθεί επιτυχώς σε αυτόν τον στόχο. Τέτοιες επιπτώσεις μπορεί να είναι η απώλεια δεδομένων, η διακοπή της επιχείρησης, η φθορά της φήμης. Ο συντελεστής της επίπτωσης αυτής εξαρτάται από το βάθος που στοχεύει η επίθεση καθώς και από τη συχνότητα των επιθέσεων που κινήθηκαν ενάντια στο συγκεκριμένο στόχο.

Επομένως ορίζουμε
S(I,t)= I(t)*T(t)[1-E(lt)]

Την αναμενόμενη ζημιά όπου θα υποστεί ο D ύστερα από μια επιτυχημένη επίθεση όταν ο έλεγχος είχε εφαρμοστεί στο επίπεδο I.

E=L*T [0,1] ορίζεται ως η αποτελεσματικότητα του επιπέδου ελέγχου

Τέλος σε επίπεδο I ορίζεται το έμμεσο κόστος C:L->Z+

Παιχνίδια ελέγχου

Στο παιχνίδι ελέγχου οι συμμετέχοντες είναι δύο. Ο D που εκπροσωπεί τον υπεύθυνο για την λήψη αποφάσεων στον κυβερνοχώρο και ο A που εκπροσωπεί οποιονδήποτε κάνεις επιθέσεις. Στόχος του D είναι να προστατεύσει τα περιουσιακά του στοιχεία και να ελαχιστοποιήσει τις αναμενόμενες απώλειες σε αντίθεση με τον A που στοχεύει να επωφεληθεί στο μέγιστο από μια επίθεση. Για το λόγο αυτό επιλέγει να εκμεταλλευτεί μια ευπάθεια με σκοπό να μεγιστοποιήσει τη ζημιά που θα προκαλέσει. Ο κάθε παίχτης δρα διαφορετικά χωρίς να ξέρει την κίνηση του άλλου, Ο D επιλέγει να εφαρμόσει τον έλεγχο ασφάλειας στο επίπεδο I και ο A επιλέγει να εκμεταλλευτεί μια ευπάθεια t={v,] .Το παιχνίδι ακολουθεί συγκεκριμένους κανόνες και ο κάθε παίχτης πρέπει να επιλέξει και να εφαρμόσει μια συγκεκριμένη στρατηγική από ένα σύνολο συμπεριφορών με στόχο να βελτιστοποιήσει το αποτέλεσμα του παιχνιδιού.

- Όταν η μείωση της βλάβης που επιτυγχάνεται στο επίπεδο I′ έναντι του I είναι μεγαλύτερη από το έμμεσο κόστος που παράγει το I', τότε ο D επιλέγει το I'.

- Όταν η ζημιά που προκαλεί ένας στόχος είναι μεγαλύτερη από εκείνη που προκαλεί ο τ τότε ο επιτιθέμενος επιλέγει τον τ.

- Ανεξάρτητα από τη στρατηγική που ακολουθεί ο επιτιθέμενος ο defender εγγυάται ένα ανώτατο όριο αναμενόμενης ζημιάς.

- Το κέρδος ενός επιτιθέμενου δεν ισούται με την απώλεια που υφίσταται ο υπερασπιστής.

- Η πληρωμή του επιτιθέμενου δεν σχετίζεται με τις έμμεσες δαπάνες του υπερασπιστή.

.

Διαδικασία λήψης απόφασης SAW (simple addictive weighting)

Η διαδικασία SAW ή αλλιώς η μέθοδος σταθμισμένου αθροίσματος χρησιμοποιείται κατά τη διαδικασίας λήψης απόφασης αφού βοηθά στην αξιολόγηση των εναλλακτικών και τον εντοπισμό της καλύτερης λύσης. Για κάθε εναλλακτική, υπολογίζεται η συνολική βαθμολογία ως άθροισμα των χαρακτηριστικών της και εκείνη με την υψηλότερη βαθμολογία επιλέγεται για να εφαρμοστεί. Πριν υπολογιστεί το άθροισμα, κάθε χαρακτηριστικό της εναλλακτικής πολλαπλασιάζεται με το βάρος το οποίο δηλώνει τη σημαντικότητα του χαρακτηριστικού. [02] Έτσι το τελικό αποτέλεσμα προκύπτει από τη γραμμική συνάρτηση όπου W ∈(0,1).[02]

$$\mathbf{O_y} = \sum_{z=1}^{n} \boldsymbol{WzSyz}$$

Διαδικασία λήψης απόφασης AHP (analytic hierarchy process)

Η μέθοδος της αναλυτικής ιεραρχίας χρησιμοποιείται για την διαδικασίας λήψης απόφασης αφού αξιολογούνται όλες οι πιθανές εναλλακτικές και τα χαρακτηριστικά τους. Στη συνέχεια δημιουργείται ένας πίνακας που περιέχει τις αξίες για κάθε ένα από τα χαρακτηριστικά της εναλλακτικής. Η συνολική βαθμολογία για κάθε λύση προκύπτει από το άθροισμα των υποβαθμολογιών που έχουν δοθεί στα χαρακτηριστικά . Η διαφορά στο τελικό αποτέλεσμα της απόφασης συγκριτικά με την προηγούμενη διαδικασία SAW είναι ότι προκύπτει από συγκρίσεις μεταξύ ζευγών. Η τιμή από κάθε σύγκριση ζευγών εισάγεται στον πίνακα

$$A = \begin{bmatrix} a11 & a1n \\ & \\ an1 & ann \end{bmatrix}$$

όπου ∀i ,j=1,….,n: α , ∀i=j : α , όπου ∀i ,j=1,….,n : α

Το άθροισμα για κάθε στήλη προκύπτει από τη συνάρτηση $\sum_{i=1}^{n} aij$

Η κανονικοποίηση του πίνακα

$$N=\begin{bmatrix} \frac{a11}{\sum_{i=1}^{n} ai1} & \frac{a1n}{\sum_{i=1}^{n} ain} \\ & \\ \frac{an1}{\sum_{i=1}^{n} ai1} & \frac{ann}{\sum_{i=1}^{n} ain} \end{bmatrix}$$

$$V_{i=}\frac{\sum_{j=1}^{n} \alpha ijnorm}{n} \qquad \alpha_{ij}{}^{norm}=\frac{aij}{\sum_{i=1}^{n} ij1}$$

4.5 Δυσκολίες κατά τη διαδικασία λήψης αποφάσεων

Κάθε οργανισμός έχοντας αναλύσει και αξιολογήσει όλους τους πιθανούς κινδύνους που διατρέχει και εκτιμώντας τα αγαθά που διαθέτει βρίσκεται στο κρίσιμο σημείο να αποφασίσει σε ποια μέτρα ασφάλειας θα επενδύσει ώστε να περιορίσει στο ελάχιστο το κίνδυνο. Κατά τη σημαντική αυτή διαδικασία της λήψης της απόφασης, η επιχείρηση έρχεται αντιμέτωπη και με κάποιες δυσκολίες που δυσχεραίνουν την επιλογή της εναλλακτικής λύσης, επηρεαζόμενη από τις πτυχές του κόστους, του χρόνου και της ποιότητας. [04]

Πτυχές κόστους

Πολλές φορές η εταιρεία επικεντρώνεται μόνο στο κόστος που θα προκύψει από την ίδια την επένδυση και όχι από το κόστος που απαιτείται για την επιλογή της καλύτερης επένδυσης. Η καλύτερη απόφαση έχει ιδιαίτερη αξία για την εταιρεία. Για παράδειγμα, μπορεί να επιλεγεί μια εναλλακτική λύση με την ίδια λειτουργικότητα και τα ίδια χαρακτηριστικά και να είναι λιγότερο δαπανηρή. Αν το κόστος της λήψης απόφασης υπερβαίνει την αξία της απόφασης δεν έχει νόημα να γίνει η επένδυση. Θα πρέπει να διασφαλιστεί ότι τα έξοδα της λήψης της απόφασης δεν θα πρέπει να υπερβαίνουν την ίδια την απόφαση. Ωστόσο είναι δύσκολο να προσδιοριστεί η ακριβής αξία της απόφασης πριν την ολοκλήρωσή της. Εκτός από την αξία της απόφασης θα πρέπει να ληφθούν υπόψη και άλλοι παράγοντες που συμμετέχουν στη διαδικασία λήψης της απόφασης. Ο ανθρώπινος παράγοντας αποτελεί σημαντικό μέρος της διαδικασίας καθώς αποτελεί υψηλό παράγοντα κόστους. Για να ολοκληρωθεί σωστά και με ακρίβεια αυτή η διαδικασία, συμμετέχουν περισσότεροι του ενός άνθρωποι οι οποίοι είτε έχουν θέση ευθύνης στην επιχείρηση, είτε είναι εξωτερικοί σύμβουλοι που συνεργάζονται με την εταιρεία για πιο εξελιγμένες και διεξοδικές αναλύσεις ώστε να επιτευχθεί το καλύτερο αποτέλεσμα. Εκτός από τους συμμετέχοντες στη διαδικασία της λήψης της απόφασης, κόστος εμφανίζεται και από το εξοπλισμό που χρειάζεται να χρησιμοποιηθεί εκείνη τη χρονική στιγμή που περιλαμβάνει είτε επιτραπέζιους και φορητούς υπολογιστές είτε το λογισμικό και το λειτουργικό σύστημα που χρειάζεται για τα τεστ περιβάλλοντα.

Πτυχές χρόνου

Η σημασία του χρόνου που χρειάζεται για να ολοκληρωθεί η διαδικασίας της λήψης απόφασης είναι ιδιαίτερα υψηλή. Καθυστερήσεις που επηρεάζουν τη διαδικασία μπορεί να οφείλονται σε αλλαγές και ελλείψεις διαδικασιών και πόρων. Οι αλλαγές προέρχονται συνήθως από εσωτερικούς παράγοντες όπως οργάνωση, στόχους, απόψεις εταιρείας και χρήστες καθώς και από εξωτερικούς παράγοντες όπως νέες συμπεριφορές, νέοι κανονισμοί και νέες τεχνικές οι οποίες έγιναν αρκετά δημοφιλείς με εξαιρετικά αποτελέσματα διασφάλισης και εξοικονόμησης κόστους όπως το cloud computing. Οπότε κάθε φορά που γίνονται αλλαγές απαιτούνται και περισσότεροι χρήστες για να τις αναλύσουν και να τις αξιολογήσουν επηρεάζοντας την τρέχουσα διαδικασίας που κάποιες φορές μπορεί να οδηγήσει και στην πλήρη αναθεώρησή της. Όσο αφορά τις ελλείψεις των πόρων, κάποιοι πόροι μπορεί να μην είναι διαθέσιμοι κατά τη διαδικασία με αποτέλεσμα να δημιουργείται ένας ανεπιθύμητος χρόνος αναμονής. Για το λόγο αυτό θα πρέπει από πριν να έχουν προσδιοριστεί ποιοι πόροι χρειάζονται και για ποιο σκοπό στη συγκεκριμένη διαδικασία. Ανεπαρκής διαθεσιμότητα ή χωρητικότητα οδηγεί σε καθυστερήσεις ή ακυρώσεις. Ο υπεύθυνος της διαδικασίες πρέπει να είναι έτοιμος να αντιμετωπίσει τέτοιες καταστάσεις που προήλθαν επειδή κάποιοι πόροι προέκυψαν ελαττωματικοί ή προορίζονταν για άλλα έργα όποτε και θα ήταν απαραίτητο να αντικατασταθούν για να ολοκληρωθεί η διαδικασία. Υπάρχουν και περιπτώσεις που κρίνεται αναγκαία η ακύρωση της διαδικασίας. Αυτό οφείλεται όταν τα συστήματα δεν πληρούν όλες τις απαιτήσεις ή δεν είναι έτοιμα για δοκιμαστικές λειτουργίες ή ακόμα επειδή η λειτουργία

τους έχει ανατεθεί σε εξωτερικούς συνεργάτες. Τέλος για να αντιμετωπισθούν οι ελλείψεις των διαδικασιών και να μην υπάρξουν επιπλέον καθυστερήσεις και αναμονές κρίνεται απαραίτητο να καταργηθούν περιττές διαδικασίες οι οποίες δεν προσφέρουν κανένα όφελος κατά τη διαδικασία της απόφασης ή να γίνει συνδυασμός των δραστηριοτήτων όπου είναι εφικτό για να είναι επαρκείς οι πόροι.

Πτυχές ποιότητας

Η ποιότητα της απόφασης ορίζει σε μεγάλο βαθμό την αποτελεσματικότητα της επένδυσης. Αν η λήψη αποφάσεων σχετίζεται με σφάλματα δεν θεωρείται καλή επιλογή. Η ποιότητα ωστόσο επηρεάζεται τόσο από τον παράγοντα κόστος όσο και από τον χρόνο. Για παράδειγμα, ανειδίκευτοι υπάλληλοι είναι γρήγοροι αλλά λιγότερο ακριβείς σε αντίθεση με εκπαιδευμένο και εξοικειωμένο προσωπικό με τη διαδικασία λήψης απόφασης του οποίου τα κίνητρα είναι υψηλά και στοχεύουν στην καλύτερη απόδοση των αποτελεσμάτων. Επιπλέον είναι σημαντική η επικοινωνία μεταξύ των ενδιαφερομένων, να γίνεται σωστή συλλογή δεδομένων, ανταλλαγή πληροφορίας και διαχωρισμός της σε χρήσιμη και άχρηστη, έγκαιρη γνωστοποίηση της κατάστασης ώστε να οδηγηθούν οι εμπλεκόμενοι σε αξιόπιστα αποτελέσματα. Σημαντικό ρόλο στην ποιότητα της απόφασης παίζει η ανάθεσή της σε τρίτους. Πιο συγκεκριμένα, η εξωτερική ανάθεση της διαδικασίας ναι μεν μπορεί να επιτύχει υψηλά επίπεδα ποιότητας αλλά θα πρέπει να δημιουργηθούν και οι σωστές διασυνδέσεις μεταξύ της επιχείρησης και του παρόχου της υπηρεσίας με την έννοια ότι αν σημαντικά καθήκοντα εκτελούνται από τρίτους, η επιχείρηση δεν θα μπορεί να βελτιώσει ή να αλλάξει από μόνη της τη διαδικασίας λήψης απόφασης στο μέλλον. Τέλος σε περιπτώσεις που οι επενδύσεις αγοράζονται από κάποιον πωλητή συχνά συνοδεύονται από όπου και συμφωνίες οι οποίες έχουν δυσμενείς επιπτώσεις για την επιχείρηση. Για παράδειγμα, όροι που αφορούν την ανάληψη ευθύνης σε περίπτωση ζημιάς από μια επιτυχημένη επίθεση ασφάλειας του κυβερνοχώρου εξαιτίας ενός ελαττωματικού προϊόντος με αποτέλεσμα η επιχείρηση να μην μπορεί να αποζημιωθεί.

4.6 Ο κύκλος ζωής της επένδυσης στην ασφάλεια του κυβερνοχώρου

Όλα όσα μελετήθηκαν σε αυτό το κεφάλαιο σχετικά με την οικονομική πλευρά της κυβερνοασφάλειας και το πως πρέπει να γίνονται οι επενδύσεις στον τομέα αυτό αποτελούν τα βασικά στάδια του κύκλου ζωής της επένδυσης στον κυβερνοχώρο.[04] Για την καλύτερη κατανόηση της διαδικασίας παρουσιάζονται συνοπτικά τα βήματα που απαιτούνται:

Έναρξη: Η επιχείρηση κρίνει επιθυμητή την επένδυση ως αποτέλεσμα ενός εσωτερικού ή εξωτερικού συμβάντος. Μια παραβίαση που πραγματοποιήθηκε και είχε σημαντικό αρνητικό αντίκτυπο στην ασφάλεια της επιχείρησης, η προσδοκία των πελάτων της σχετικά με την προστασία των δεδομένων και τον υπεύθυνο χειρισμό τους, η επιβολή νομοθεσιών και βασικών προτύπων καθώς και μια νέα τεχνολογία που θα έχει ως αποτέλεσμα τη βελτίωση του επιπέδου προστασίας και μείωση του κόστους της είναι κάποιοι από τους βασικούς παράγοντες που επηρεάζουν την επιχείρηση ώστε να αποφασίσει να ξεκινήσει μια τέτοια επένδυση.

Χορηγία: Κάθε επένδυση για να υλοποιηθεί χρειάζεται και την απαραίτητη χρηματοδότηση. Ο χορηγός που αναλαμβάνει το έργο της ασφάλειας είναι σημαντικό να έχει μια θέση ευθύνης μέσα στην επιχείρηση, να γνωρίζει τη συνολική στρατηγική της επιχείρησης, να είναι ικανός να αποδείξει ότι η επένδυση είναι προς όφελος της εταιρείας, να έχει πρόσβαση σε όλους τους

πόρους και να μπορεί να του κατανέμει σωστά, να συμμετέχει σε όλα τα στάδια του έργου και να έχει υποστηρικτικό έργο κατά τη διάρκεια της επένδυσης.
Αναγνώριση προβλημάτων απόφασης: Σε αυτό το στάδιο πρέπει να προσδιοριστούν τα προβλήματα που πιθανόν να εμφανιστούν από τον κάθε έναν που συμμετέχει στη διαδικασία λήψης απόφασης ώστε να υπάρχει πλήρης κατανόηση της κατάστασης, να αναγνωριστούν πλήρως κρίσιμες πτυχές του προβλήματος.

Αναγνώριση χαρακτηριστικών: Στη φάση αυτή εξετάζονται και αναλύονται τα λειτουργικά, τεχνικά χαρακτηριστικά της εναλλακτικής για να καθοριστεί αν όντως είναι η κατάλληλη επιλογή. Προσδιορίζονται ακόμα και τα οικονομικά χαρακτηριστικά όπως κόστη και οφέλη τα οποία παίζουν σημαντικό ρόλο στη λήψη απόφασης. Για την καλύτερη και πιο αντικειμενική αναγνώριση των χαρακτηριστικών συμμετέχουν μαζί με τους υπεύθυνους λήψης απόφασης και εμπειρογνώμονες που εξετάζουν τα πρότυπα και τις πρακτικές για το καλύτερο αποτέλεσμα.

Αξιολόγηση χαρακτηριστικών: Η αξιολόγηση χαρακτηριστικών έχει αξία όταν αυτά δεν είναι σημαντικά στη λήψη της απόφασης. Οι δύο συνηθισμένες τεχνικές για τη λήψη αποφάσεων είναι η μέθοδος AHP, SAW.

Εναλλακτική αξιολόγηση: Στο βήμα αυτό προσδιορίζονται και αξιολογούνται τα χαρακτηριστικά των εναλλακτικών δημιουργώντας ένα συνολικό άθροισμα το οποίο επιτρέπει την κατάταξη των επιλογών ώστε να ληφθεί η τελική απόφαση. Η εναλλακτική με την υψηλότερη βαθμολογία κρίνεται και ως πιο κατάλληλη για την εταιρεία.

Επιλογή της καλύτερης εναλλακτικής: Αφότου έχουν αξιολογηθεί οι εναλλακτικές, εκείνη που συγκεντρώνει την υψηλότερη βαθμολογία επιλέγεται. Σε περίπτωση που βρεθούν περισσότερες του ενός με την ίδια ο υπεύθυνος της λήψης απόφασης θα πρέπει να βρει επιπλέον χαρακτηριστικά ώστε να ξεχωρίσει τη μια καλύτερη.

Έγκριση: Η επιλογής μιας εναλλακτικής δεν οδηγεί πάντα σε υλοποίηση της επένδυσης και για το λόγο αυτό αφού επιλεχθεί η εναλλακτική παρουσιάζεται στα ανώτερα στελέχη της εταιρείας τα οποία θα πρέπει να δώσουν την τελική τους έγκριση.

Προγραμματισμός: Στο στάδιο αυτό προσδιορίζεται ο τρόπος που θα γίνει η εφαρμογή της διασφάλισης που έχει επιλεχθεί. Καθορίζεται η εγκατάσταση της διασφάλισης καθώς και ρυθμίσεις που πρέπει να γίνουν επιπλέον κατά το σχεδιασμό, προσδιορίζονται και οι εκπαιδεύσεις των χρηστών με τα νέα εργαλεία και τις διαδικασίες ασφάλειας.

Εφαρμογή: Η εφαρμογή της διασφάλισης συνίσταται να γίνεται σταδιακά για να μειωθεί ο κίνδυνος που μπορεί να προκύψει με την υλοποίησή της. Αρχικά μπορεί να εφαρμοστεί σε μια μικρή ομάδα χρηστών, μετά από λίγες μέρες σε μεγαλύτερη ομάδα και εφόσον διαπιστωθεί ότι δεν υπάρχει κάποιος κίνδυνος που μπορεί να οδηγήσει σε επιχειρηματική διακοπή να εφαρμοστεί σε όλη την επιχείρηση.

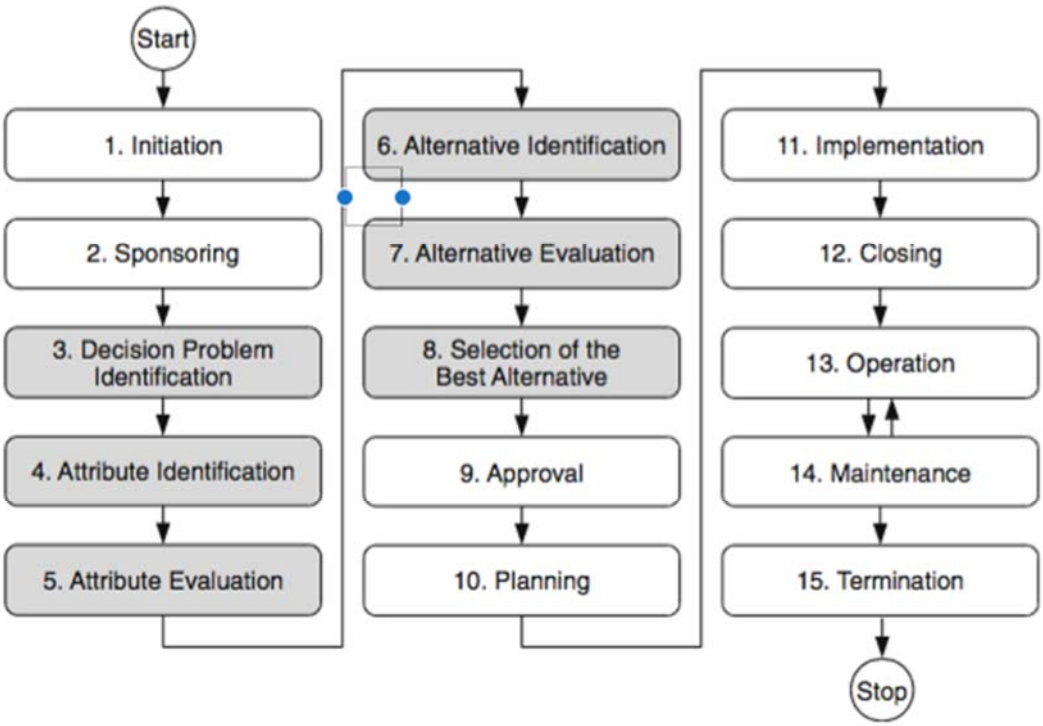
Κλείσιμο: Στο βήμα αυτό ολοκληρώνεται η εφαρμογή της διασφάλισης και περιλαμβάνει αναθεώρηση τελική έγκριση του χορηγού. Ο διαχειριστής του έργου εξετάζει τις πληροφορίες που έχουν συλλεχθεί ώστε να ελέγξει αν οι στόχοι της επένδυσης υλοποιήθηκαν επαρκώς.

Λειτουργία: Στο στάδιο αυτό ξεκινά και επίσημα η λειτουργία της διασφάλισης η οποία περιλαμβάνει την αντιμετώπιση περιστατικών, την απόδοση των αντιμέτρων, την αξιόπιστη εξασφάλιση. Στο πλαίσιο της λειτουργίας γίνεται υποστήριξη των χρηστών για τη βελτίωση

της χρήσης των συστημάτων και την εξάλειψη τυχόν προβλημάτων, παρακολούθηση όλου του συστήματος για τον εντοπισμό περίεργων δεικτών που θα οδηγούσαν σε πρόβλημα του παρελθόντος ή σε επικείμενη επίθεση και αιτήματα χρηστών για αλλαγές που θα περιόριζαν τυχόν προβλήματα.

Συντήρηση: Εφόσον η διασφάλιση χρησιμοποιείται καθημερινά, ανά τακτά χρονικά διαστήματα πρέπει να γίνεται έλεγχος για να διαπιστώνεται ότι συνεχίζει να λειτουργεί σωστά και να παρέχει υψηλό επίπεδο προστασίας. Βασικός σκοπός της συντήρησης είναι η μείωση των σφαλμάτων, η αύξηση της απόδοσης και η γενικότερη βελτίωση του συστήματος.

Τερματισμός: Κατά τον τερματισμό απομακρύνεται κάθε στοιχείο της διασφάλισης και παύει να χρησιμοποιείται. Οι λόγοι που μπορεί να προκαλέσουν τερματισμό είναι η πτώχευση της εταιρείας ή η ανάπτυξη ενός καινούριου προϊόντος που παρέχει καλύτερα αποτελέσματα στην προστασία των αγαθών, το υπερβολικό κόστος επένδυσης καθώς και η φθορά του υλικού.



Σχήμα 4.14: Ο κύκλος ζωής της επένδυσης

Και για να ξεκινήσει ο επενδυτικός κύκλος οι υπεύθυνοι ασφάλειας θα πρέπει να έχουν μια σταθερή βάση που θα τους βοηθήσει στη διαδικασία λήψης αποφάσεων και η οποία περιλαμβάνει έξι βασικές αρχές που δεν πρέπει να αγνοούν.[44]

Επενδυτική αρχή ν .1
Η εφαρμογή ελέγχων ασφαλείας για απειλές χαμηλού ως μέτριου κινδύνου είναι απαραίτητη και οικονομικά συμφέρουσα.

Επενδυτική αρχή ν.2
Εστίαση σε ασφάλεια πέρα από τους βασικούς ελέγχους για αντιμετώπιση εξελιγμένων επιθέσεων.

Επενδυτική αρχή ν.3

Για τις πιο εξελιγμένες επιθέσεις οι επιχειρήσεις πρέπει να παίρνουν το ρίσκο για τις λειτουργίες που έχουν χαμηλό αντίκτυπο και όπου το κόστος δεν υπερβαίνει το όφελος.

Επενδυτική αρχή ν.4
Τα οικονομικά οφέλη από τη συμμετοχή της επιχείρησης σε διαδικασίες ανταλλαγής πληροφοριών που σχετίζονται με την ασφάλεια και την αντιμετώπιση των απειλών είναι πολύ υψηλά.

Επενδυτική αρχή ν.5
Επιπλέον επενδύσεις για την αντιμετώπιση εξελιγμένων απειλών πρέπει να είναι προσαρμοσμένες στα χαρακτηριστικά των απειλών.

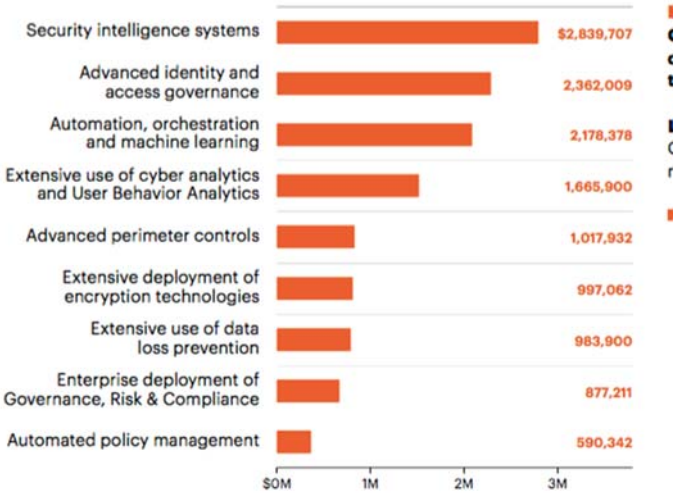
Επενδυτική αρχή ν.6
Η αντιμετώπιση των εξελιγμένων απειλών απαιτεί επενδύσεις που ανταποκρίνονται με τις τεχνολογικές εξελίξεις και είναι σε θέση να προβλέψουν τις απειλές και να τις αντιμετωπίσουν αποτελεσματικά.

Κεφάλαιο 5
Νέα αντίμετρα

Στο κεφάλαιο 5 προτείνονται και αναλύονται νέες ιδέες και λύσεις που μπορούν να εφαρμοστούν στα πληροφοριακά συστήματα με σκοπό την ενίσχυση της κυβερνοασφάλειας και της ταυτόχρονης μείωσης του κόστους επένδυσης και τον περιορισμό των οικονομικών επιπτώσεων που προκαλεί μια κυβερνοεπίθεση. Οι λύσεις αυτές σύμφωνα με την έρευνα του Ponemon Institute έχουν καλύτερα αποτελέσματα απόδοσης στον τομέα επένδυσης. Κάποιες από αυτές είναι security intelligence, big data analytics, access govenance tools και artificial intelligence.

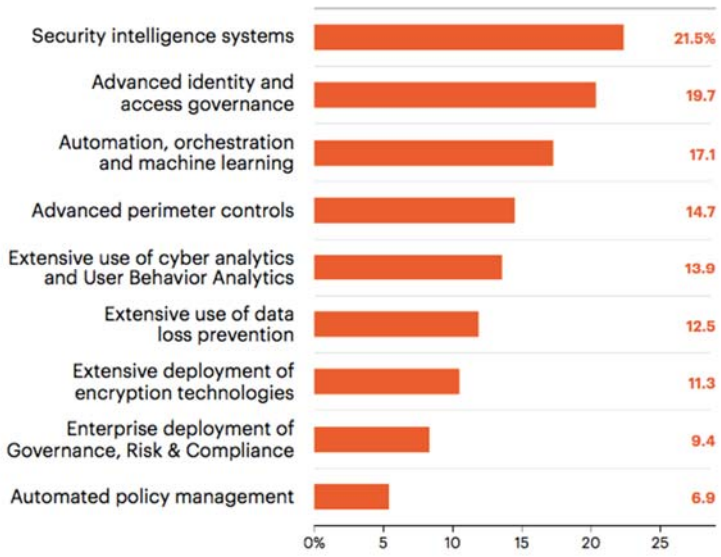
Είναι πλέον γνωστό ότι οι κυβερνοεπιθέσεις συνεχώς αυξάνονται και θα συνεχίσουν να αυξάνονται με ραγδαίο ρυθμό. Οι επιτιθέμενοι χρησιμοποιούν προηγμένες τεχνικές και βρίσκουν πιο αποτελεσματικούς τρόπους για να διαπράξουν την επίθεσή τους. Ως εκ τούτου οι επιχειρήσεις πρέπει να είναι πάντα σε θέση να προστατεύσουν τα περιουσιακά στοιχεία, τα δεδομένα και τους εργαζομένους. Σε προηγούμενο κεφάλαιο μελετήθηκαν ενδελεχώς όλα τα τεχνικά μέτρα προστασίας που λαμβάνουν οι επιχειρήσεις για την προστασία τους από τις απειλές του κυβερνοχώρου. Ωστόσο, καθώς η τεχνολογία εξελίσσεται και οι δυνατότητές της αυξάνονται, τα μέτρα αυτά δεν είναι ικανά να αντιμετωπίσουν τις κακόβουλες επιθέσεις και θεωρούνται κάπως παρωχημένα. Για το λόγο αυτό προτείνονται νέες μεθοδολογίες που σε συνδυασμό με τις υφιστάμενες λύσεις θα οδηγήσουν στο επιθυμητό αποτέλεσμα. Αν και ακόμα εφαρμόζονται σε χαμηλό βαθμό, οι παρακάτω μέθοδοι έχουν δείξει ότι μπορούν να εξοικονομηθούν πολλά χρήματα με την εφαρμογή τους. Σύμφωνα με έρευνα που πραγματοποιήθηκε για το έτος 2017 από το Ponemon Institute διαπιστώθηκε ότι τεχνολογίες όπως τα συστήματα ασφάλειας πληροφοριών, έχουν θετικά αποτελέσματα στον τομέα της ασφάλειας.

Εκτός από τη διατήρηση της ασφάλειας του κυβερνοχώρου οι επιχειρήσεις στοχεύουν και στην εξοικονόμηση χρημάτων. Η απόφαση της καλύτερης εναλλακτικής είναι εκείνη που συνδυάζει στο μέγιστο ασφάλεια και μείωση του κόστους επένδυσης. Το παρακάτω διάγραμμα αναφέρει τα χρηματικά ποσά που έμειναν στην επιχείρηση όταν αποφάσισαν να επενδύσουν σε μια από τις εννέα νέες μεθόδους και τεχνολογίες. Για παράδειγμα, επιχειρήσεις που επένδυσαν σε συστήματα πληροφοριών έσωσαν περίπου $2,8million και $2,3million εκείνες που εφάρμοσαν εργαλεία πρόσβασης διακυβέρνησης.



Σχήμα 5.1: Εξοικονόμηση χρημάτων ανά τεχνολογία

Συνοψίζοντας, η εκτιμώμενη απόδοση επένδυσης (δείκτης ROI) αγγίζει το 21,5% στις επιχειρήσεις που εφαρμόζουν πληροφοριακά συστήματα ασφάλειας, πολύ σημαντική απόδοση σε σχέση μ τις άλλες κατηγορίες. Στη συνέχεια ακολουθούν, οι επιχειρήσεις που επενδύουν σε προηγμένη τεχνολογία διακυβέρνησης και μηχανικής μάθησης. Για όλες τις κατηγορίες η μέση εκτιμώμενη απόδοση επένδυσης είναι περίπου στο 14,1%. [21]



Σχήμα 5.2: Ο δείκτης ROI

5.1 Security intelligence systems

Οι ειδικοί στον τομέα της ασφάλειας του κυβερνοχώρου προσπαθούν να προστατεύσουν τις επιχειρήσεις παίζοντας καθοριστικό ρόλο στην επιλογή των σωστών μεθόδων. Στην προσπάθειά τους να φτάσουν στο επιθυμητό αποτέλεσμα και με δεδομένο ότι δεν γνωρίζουν τους τρόπους που επιλέγουν οι εγκληματίες να επιτεθούν, εφαρμόζουν νέες τεχνικές. Τα συστήματα ασφάλειας πληροφοριών είναι μια τέτοια λύση, όπου τα σύστημα σχεδιάζονται για να συλλέγουν τεράστιες ποσότητες πληροφορίας για τις απειλές από τις οποίες κινδυνεύουν οι επιχειρήσεις. Κίνητρα, προθέσεις, ικανότητες και τεχνικές επιτιθέμενων είναι οι βασικές πληροφορίες που συλλέγουν και αναλύουν οι ειδικοί για να παρέχουν σωστές υπηρεσίες ασφαλείας. Συνδυάζει μεθόδους όπως διαχείριση αρχείων καταγραφής, προβολή δικτύου, εργαλεία συλλογής δεδομένων και ανίχνευσης της απειλής με προηγμένες δυνατότητες. Οι βασικές λειτουργίες των συστημάτων εστιάζουν στη συλλογή και επεξεργασία των δεδομένων. Πρώτα από όλα συλλέγονται τα δεδομένα από πολλές πηγές και πλατφόρμες που θα χρησιμοποιηθούν για ενδελεχή έρευνα. Η ανάλυση των δεδομένων γίνεται σε πραγματικό χρόνο κάτι το οποίο διευκολύνει στην άμεση και έγκαιρη αντιμετώπιση των απειλών. Ένα γεγονός που εντοπίζεται καθυστερημένα είναι πολύ πιθανόν να έχει ήδη προκαλέσει αναπόφευκτες ζημιές στην επιχείρηση. Τέλος έχει τη δυνατότητα να συσχετίζει διαφορετικά γεγονότα και συμβάντα ώστε να μπορεί να εντοπίζει και να επιλύει συγκεκριμένες απειλές πιο αποτελεσματικά.

Η διαδικασία που μετατρέπει τα δεδομένα σε χρήσιμες πληροφορίες ονομάζεται κύκλος πληροφοριών και είναι απαραίτητος για την επίτευξη των στόχων της επιχείρησης. Τα βήματα που περιλαμβάνει αυτή η επαναλαμβανόμενη διαδικασία είναι:

- Προγραμματισμός και κατεύθυνση. Στο πρώτο βήμα ορίζεται ποιος είναι ο στόχος για τον οποίο θα συλλεχθούν τα δεδομένα. Έστω ότι ο στόχος είναι ένα κακόβουλο λογισμικό τύπου malware. Οι πληροφορίες που θα μπορούσαν να συλλεχθούν και να είναι χρήσιμες για την αντιμετώπιση τέτοιων επιθέσεων στο μέλλον είναι ο εντοπισμός

των servers από τους οποίους προέρχονται, ο τύπος των συστημάτων που χρησιμοποιούν οι επιτιθέμενοι.

- Συλλογή πληροφοριών. Στο δεύτερο βήμα συλλέγονται οι απαραίτητες πληροφορίες από πηγές όπως το διαδίκτυο, τα αρχεία καταγραφών, τα τείχη προστασίας.
- Επεξεργασία πληροφοριών. Στο τρίτο βήμα οι πληροφορίες που συλλέχθηκαν μετατρέπονται σε κάτι χρήσιμο. Παράδειγμα επεξεργασίας είναι η μετατροπή των δυαδικών δεδομένων σε δεδομένα που είναι κατανοητά από τον άνθρωπο.
- Παραγωγή. Στο τέταρτο βήμα ο αναλυτής που είναι υπεύθυνος για τη διαχείριση των δεδομένων μετατρέπει τα δεδομένα σε χρήσιμη πληροφορία και δημιουργεί αναφορές που θα πρέπει να ικανοποιούν τον αρχικό στόχο που τέθηκε στο πρώτο βήμα ή οποιαδήποτε άλλη ανάγκη.
- Διάδοση. Στο πέμπτο βήμα διατίθεται το προϊόν πληροφορίας που δημιουργήθηκε στους χρήστες και στους άμεσα ενδιαφερόμενους. Δεν υπάρχει λόγος να προηγείται η παραπάνω διαδικασία αν οι χρήστες δεν έχουν πρόσβαση στο τελικό αποτέλεσμα.

Πλεονεκτήματα

Αν οι επιχειρήσεις εφαρμόσουν την τεχνολογία αυτή έχουν να επωφεληθούν σε πολύ σημαντικό βαθμό σε διάφορα επίπεδα. Η στρατηγική νοημοσύνη αξιολογεί διαφορετικά κομμάτια πληροφορίας, σχηματίζει ολοκληρωμένες απόψεις τις οποίες ενημερώνει στους υπευθύνους της επιχείρησης για τη λήψη αποφάσεων και τη δημιουργία νέων πολιτικών για την έγκαιρη προειδοποίηση και αντιμετώπιση των απειλών στον κυβερχνοχώρο. Σε επίπεδο λειτουργίας η ομάδα που διαχειρίζεται τα συγκεκριμένα συστήματα συλλέγει πληροφορίες για τις μεθόδους, τους στόχους και τις προθέσεις των επιτιθέμενων τα οποία θα βοηθήσουν την έρευνα καθώς και θα χρησιμοποιηθούν για την παρεμπόδιση μελλοντικών επιθέσεων. Τέλος, σε επίπεδο τακτικής, παρέχεται συνεχή επιχειρησιακή υποστήριξη αφού σε πραγματικό χρόνο αξιολογούνται γεγονότα και δραστηριότητες, δίνονται προτεραιότητες σε εκείνους του συναγερμούς που χρήζουν άμεση αντιμετώπιση και σε ποια τρωτά σημεία είναι πιο επικίνδυνα και χρήζουν άμεση θα διόρθωση.

Συμπεραίνουμε λοιπόν τη σπουδαιότητα της συγκεκριμένης τεχνολογίας καθώς προσφέρει καλύτερη διαχείριση κινδύνου και ελαχιστοποιεί την πιθανότητα μεγάλων οικονομικών προβλημάτων. Είναι επιτακτική ανάγκη η εφαρμογή της καθώς μόνο τέτοιου είδους τεχνολογίες θα μπορέσουν να αντιμετωπίσουν τους εγκληματίες που χρησιμοποιούν τεχνολογίες επόμενης γενιάς για να επιτεθούν. Επομένως κρίνεται απαραίτητη για την αντιμετώπιση των απειλών και τη διασφάλιση των συστημάτων.

5.2 Threat Intelligence sharing

Threat Information: Ως πληροφορία απειλής ορίζουμε κάθε πληροφορία που σχετίζεται με μια απειλή και συντελεί στην προσπάθεια του οργανισμού να προστατευτεί από αυτή ή να ανιχνεύσει δραστηριότητες που θα οδηγούσαν σε αυτή και θα την περιόριζαν. Υπάρχουν διάφοροι τύποι πληροφορίας απειλής:

- Οι δείκτες που είναι στοιχεία τα οποία υποδηλώνουν μια επικείμενη επίθεση ή μια επίθεση που βρίσκεται σε εξέλιξη.
- Οι τεχνικές, οι πρακτικές και οι διαδικασίες.
- Οι ειδοποιήσεις ασφάλειας - τεχνικές ειδοποιήσεις σχετικά με τις ευπάθειας και άλλα ζητήματα ασφάλειας του οργανισμού.

- Οι αναφορές πληροφοριών των απειλών. Εφόσον έχει συγκεντρωθεί η απαραίτητη πληροφορίας απειλής, γίνεται η ερμηνεία και η ανάλυση ώστε να χρησιμοποιηθεί κατά τη διαδικασία λήψης των αποφάσεων.

Κάθε πληροφορία είναι χρήσιμη ακόμα και αν τη στιγμή που τη λαμβάνουμε φαίνεται ότι δεν τη χρειαζόμαστε εφόσον μπορούμε να την αξιοποιήσουμε σε άλλη χρονική στιγμή. Είναι μια πηγή μάθησης αρκεί η πληροφορία που λαμβάνουμε να είναι οργανωμένη, σωστά επεξεργασμένη και διαθέσιμη στους κατάλληλους ανθρώπους ώστε να την αξιοποιήσουν κατάλληλα και να λάβουν τις σωστές αποφάσεις. Ειδικά στον τομέα της ασφάλειας του κυβερνοχώρου, η πρόληψη και η άμυνα από επιδέξιους επιτιθέμενους μπορεί να γίνουν πιο αποτελεσματικές αν υπάρξει συνεργασία των οργανισμών για την προστασία και αντιμετώπιση παρόμοιων απειλών. Μια τέτοια συνεργασία θα οδηγήσει στην ανταλλαγή πληροφοριών για το χειρισμό παρόμοιων καταστάσεων με σκοπό τη μείωση του κινδύνου αλλά και τη βελτίωση της υπάρχουσας ποιότητας της ασφάλειας. Κατά αυτό το λόγο υπάρχουν πολλά οφέλη που θα αποκομίσουν οι οργανισμοί αν εφαρμόσουν στις πρακτικές τους την κοινή χρήση της πληροφορίας των απειλών.

«one organization's detection to become another's prevention"

- Κοινή συνειδητοποίηση της κατάστασης: Η ανταλλαγή της πληροφορίας επιτρέπει στους οργανισμούς να μελετούν και να αναλύουν συλλογικά κοινή πληροφορία, και παρόμοιες εμπειρίες κάτι το οποίο βοηθά τους συμμετέχοντες να διεύρυνση της αναλυτικής τους σκέψης και στην πιο αποτελεσματική λήψη απόφασης με σκοπό την ενίσχυση των αμυντικών δυνατοτήτων του οργανισμών.
- Βελτίωση στάσης ασφάλειας: Ο διαμοιρασμός της πληροφορίας βελτιώνει τον τρόπο που αντιμετωπίζει ο οργανισμός το ζήτημα της ασφάλειας. Πλέον είναι σε θέση να κατανοούν καλύτερα το περιβάλλον της απειλής, να μετριάζουν τις απειλές, να ενημερώνουν τις πολιτικές και τις διαδικασίες για την άμυνα και διαχείριση των κινδύνων.
- Μεγαλύτερη αμυντική ευκινησία. Οι επιτιθέμενοι προκειμένου να αποφύγουν τα μέτρα ασφάλειας του οργανισμού και να εκμεταλλευτούν τις ευπάθειές του αλλάζουν τεχνικές, τακτικές και διαδικασίες. Οι οργανισμοί που συμμετέχουν στην ανταλλαγή πληροφοριών ενημερώνονται πιο γρήγορα για τις αυτές τις αλλαγές και για το πόσο σημαντικό είναι να δράσουν ταχύτατα και αποτελεσματικά ώστε να ανιχνεύσουν τον κίνδυνο και να τον αντιμετωπίσουν με αποτέλεσμα να μειώνεται η πιθανότητα επιτυχημένης επίθεσης. Ταυτόχρονα αυξάνεται και το κόστος των επιτιθέμενων για να αναπτύξουν νέα TTPs.

Σαφώς και τα πλεονεκτήματα είναι αρκετά για έναν οργανισμό που συμμετέχει στην κοινή χρήση της πληροφορίας για θέματα ασφάλειας ωστόσο υπάρχουν και κάποιες προκλήσεις που θα πρέπει να λάβει σοβαρά υπόψη ώστε να έχει μόνο οφέλη από αυτή τη διαδικασία. Πρώτο και σημαντικό είναι να αναπτύξει και να συντηρήσει σχέσεις εμπιστοσύνης με τους υπόλοιπους οργανισμούς που θα αποτελέσουν γερά θεμέλια στη διαδικασία ανταλλαγής που θα ακολουθήσει. Στη συνέχεια θα πρέπει να είναι σε θέση να αποφασίσει ποιες είναι οι πληροφορίες που μπορεί να μοιραστεί ώστε να διαφυλάξει τις ευαίσθητες πληροφορίες. Έτσι λοιπόν οι οργανισμοί πρέπει να ορίσουν πολιτικές, διαδικασίες και ελέγχους για να διαχειριστούν τους κινδύνους που προκύπτουν από την τυχόν διαρροή ευαίσθητων πληροφοριών οι οποίες θα μπορούσαν να οδηγήσουν σε οικονομικές απώλειες, νομικές ενέργειες και απώλεια φήμης. Παραδείγματα τέτοιων πληροφοριών που μπορεί να εκθέσουν ανεπανόρθωτα έναν οργανισμό είναι η ανταλλαγή πληροφοριών που σχετίζεται με τα αρχεία

καταγραφής ασφάλειας ή αποτελέσματα σάρωσης. Εφόσον κρίνουν ποιες πληροφορίες μπορούν να κοινοποιήσουν χωρίς να διατρέχουν κίνδυνο, με τη χρήση των κατάλληλων εργαλείων, της σωστής υποδομής και του εκπαιδευμένου προσωπικού γίνεται η δημοσίευση της πληροφορίας. Από την άλλη πλευρά, οι οργανισμοί χρειάζεται να έχουν την κατάλληλη υποδομή για να λάβουν πληροφορία από εξωγενείς παράγοντες και να τις ενσωματώσουν στη διαδικασία λήψης της απόφασης. Κάθε λαμβάνουσα πληροφορία, προτού χρησιμοποιηθεί, πρέπει να αξιολογείται ότι είναι η σωστή, η απειλή είναι σχετική και οι κίνδυνοι που ελοχεύουν από τη χρήση ή με χρήση της πληροφορίας είναι κατανοητοί. Ιδιαίτερη προσοχή θα πρέπει να δοθεί σε περιπτώσεις που οι πηγές που συμμετέχουν στην ανταλλαγή πληροφοριών είναι ανώνυμες αφού μπορεί να είναι χρήστες λιγότερης εμπιστοσύνης και οι οργανισμοί οφείλουν να είναι πιο επιφυλακτικοί απέναντι σε πληροφορία που ανέρχεται από άγνωστη πηγή. [24,25,26]

Αναλύοντας τόσο τα πλεονεκτήματα όσο και τα αδύναμα σημεία που θα πρέπει να προσέξουν οι οργανισμοί κατά την κοινή χρήση της πληροφορίας της ασφάλειας θα λέγαμε ότι αποτελεί μια πολύ καλή λύση για την ενίσχυση της ασφάλειας του κυβερνοχώρου. Τα σενάρια εφαρμογής που ακολουθούν, επιβεβαιώνουν ότι η ανταλλαγή των πληροφοριών αυξάνει την αποδοτικότητα και αποτελεσματικότητα της ασφάλειας.

Σενάριο ν.1
Επίθεση μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου τα οποία φέρουν κακόβουλο λογισμικό

Μια από τις πιο συνηθισμένες επιθέσεις είναι εκείνες που πραγματοποιούνται με την αποστολή ενός ηλεκτρονικού μηνύματος. Οι οργανισμοί που συμμετέχουν στην ανταλλαγή πληροφοριών και έχουν δεχτεί τέτοια επίθεση, μπορούν να δημοσιεύσουν πληροφορίες που σχετίζονται με αυτή όπως τις διευθύνσεις των αποστολέων των ηλεκτρονικών μηνυμάτων, τις διευθύνσεις URL, κάποια δείγματα του κακόβουλου λογισμικού που περιέχουν. Όλες αυτές οι πληροφορίες διαμοιράζονται με σκοπό οι οργανισμοί που θα συλλέξουν την πληροφορία να είναι σε θέση να προστατευτούν γρήγορα και αποτελεσματικά από παρόμοιες επιθέσεις.

Σενάριο ν.2
DDOS επιθέσεις

Οι πληροφορίες που μπορούν να δημοσιευτούν κατά την επίθεση της άρνησης παροχής υπηρεσιών σχετίζονται με την παρακολούθηση του δικτύου , τις υπηρεσίες , αναγνωρίζουν τη φυσιολογική κυκλοφορία του. Συμβάλλουν στην ανάπτυξη υπηρεσιών που θα ενισχύσει την ανεκτικότητα της αρχιτεκτονικής του συστήματος κατά των DDOS.

Σενάριο ν.3
Ανάλυση καμπάνιας

Κάθε εταιρεία κάνει ανεξάρτητη ανάλυση των επιθέσεων, παρατηρεί πρότυπα, δείκτες και άλλα χαρακτηριστικά με αποτέλεσμα να συμπεραίνουν ότι οι επιθέσεις δεν είναι τυχαίες αλλά αποτελούν μέρος ενός μεγαλύτερου και συντονισμένου συνόλου ενεργειών.[25]

Για να γίνει πιο αποτελεσματική η διαδικασία ανταλλαγής πληροφοριών είναι απαραίτητο κάθε οργανισμός να ενσωματώσει τη διαδικασία αυτή στον κύκλο ζωής του συστήματος. Πιο συγκεκριμένα οφείλει εφαρμόσει ένα σχέδιο ανταλλαγής πληροφοριών το οποίο θα συλλέγει, θα εξετάζει και θα αναλύει τις πληροφορίες τόσο από τις εξωτερικές πηγές όσο και από εκείνες

που προήλθαν από εσωτερικά του οργανισμού. Η χρήση αυτοματοποιημένων μεθόδων και πρωτοκόλλων μεταφοράς επιτρέπει την γρηγορότερη ανταλλαγή, επεξεργασίας και ανάλυσης της απειλής κάνοντας τον οργανισμό να δράσει έγκαιρα και να εφαρμόσει τα κατάλληλα προστατευτικά μέτρα.

5.3 Τεχνητή νοημοσύνη

Η τεχνητή νοημοσύνη είναι αποτέλεσμα ενός λογισμικού το οποίο προσπαθεί να δημιουργήσει έναν μηχανισμό απόφασης παρόμοιο με τον εκείνον του ανθρώπινου εγκεφάλου. Διαπιστώνοντας όμως πόσο δύσκολη είναι η ακριβής απομίμηση του εγκεφάλου εφόσον είναι υπερβολικά περίπλοκος, η τεχνητή νοημοσύνη επικεντρώθηκε σε μηχανισμούς λήψης αποφάσεων για συγκεκριμένα θέματα με σκοπό την επίλυση των προβλημάτων σε πολύ μικρό χρονικό διάστημα. Γνωρίζοντας ήδη το τεράστιο ζήτημα της ασφάλειας στον κυβερνοχώρο οι ερευνητές εστιάζουν στη ενσωμάτωση της τεχνητής νοημοσύνης στον τομέα της ασφάλειας με σκοπό την παροχή γρήγορων και επιτυχημένων λύσεων.

Οι επιθέσεις στον κυβερνοχώρο συνεχώς αυξάνονται προκαλώντας καταστροφικές ζημιές στους επιχειρηματικούς και χρηματοπιστωτικούς κλάδους. Σύμφωνα με την έκθεση της Cybersecurity ventures οι οικονομικές ζημιές που οφείλονται από κυβερνοεγκλήματα θα ανέλθουν μέχρι το 2021 στα $ 6 τρισεκατομμύρια δολάρια. Είναι σαφές ότι η οι επιχειρήσεις δεν μπορούν να βασίζονται μόνο στην ανθρώπινη δύναμη για να ανταπεξέλθουν στις επικείμενες απειλές αλλά ούτε και οι τεχνικές ασφαλείας επαρκούν για να αποτρέψουν τον κίνδυνο. Στρέφονται ως αυτού σε νέους τρόπους άμυνας με σκοπό τον εκσυγχρονισμό της τεχνολογίας που χρησιμοποιούν αλλά και τον περιορισμό των απωλειών ως αποτέλεσμα μια επιτυχημένης επίθεσης. Εκτός από το cloud computing η έννοια της τεχνητής νοημοσύνης εμφανίζεται στη μάχη κατά των επιθέσεων στον κυβερνοχώρο. Οι επιχειρήσεις χρησιμοποιώντας αυτόνομα συστήματα και με την κατάλληλη υποδομή προσπαθούν να εντοπίσουν και να καταπολεμούν ταχύτερα και αποτελεσματικά τις απειλές στις οποίες εκτίθενται αποκομίζοντας πολλά οφέλη κατά την εφαρμογή τους.

Πλεονεκτήματα

Η χρήση της τεχνητής νοημοσύνης στον τομέα της ασφάλειας του κυβερνοχώρου μόνο θετικά μπορεί να προσφέρει σε διαφορετικά τμήματα της ασφάλειας. Για αρχή βοηθά στην ευκολότερη διαχείριση των δεδομένων που λαμβάνουν οι επιχειρήσεις διευκολύνοντας τους αναλυτές να εξάγουν γρηγορότερα και με ακρίβεια αποτελέσματα που σχετίζονται με τους κινδύνους που διατρέχουν. Επιπλέον λόγω των εκατοντάδων απειλών που δέχονται, αυτοματοποιημένα πια είναι εφικτό να κατηγοριοποιούνται οι απειλές κάτι το οποίο βοηθά τόσο στην προστασία του οργανισμού όσο και στη χρησιμοποίηση των δεδομένων αυτών σε μελλοντικές αναλύσεις. Αυτή η κατηγοριοποίηση διευκολύνει και την ταξινόμηση των επιθέσεων με βάση το επίπεδο απειλής. Η τεχνητή νοημοσύνη πολλές φορές αντικαθιστά τους εργαζομένους στην ασφάλεια αφήνοντας του περισσότερο χρόνο ελεύθερο να ασχοληθούν και με άλλα ζητήματα. Μηχανήματα τεχνητής νοημοσύνης χρησιμοποιούνται για να τον εντοπισμό απλών επιθέσεων όπου ταυτόχρονα παρέχουν και λύσεις με αποτέλεσμα αρκετές φορές να είναι ικανά να αποκαθιστούν το πρόβλημα της επίθεσης μόνα τους χωρίς να εμπλέκεται ο ανθρώπινος παράγοντας. Αρκετές φορές είναι δυνατόν να εντοπίσουν επιθέσεις που προέρχονται από κακόβουλα λογισμικά νέες γενιάς, κάτι που τα συμβατικά πρωτόκολλα ασφάλειας και οι κοινές λύσεις ασφάλειας δεν είναι σε θέση να αντιμετωπίσουν. Οι μηχανές τεχνητής νοημοσύνης έχουν την ιδιότητα να χρησιμοποιούν δεδομένα από προηγούμενες

επιθέσεις με αποτέλεσμα να μπορούν να ανταποκριθούν έγκαιρα σε νεότερους και παρόμοιους κινδύνους. Ακόμα και αν μια επίθεση γίνει η τεχνητή νοημοσύνη συμβάλλει και στην εργασία των εμπειρογνωμόνων αυξάνοντας την αποτελεσματικότητά τους. Ακόμα και αν οι επιτιθέμενοι προσπαθούν να βρουν τρόπους για να μπερδέψουν τα μοντέλα, η τεχνητή νοημοσύνη μπορεί να εντοπίσει ανωμαλίες και μοτίβα σε μια κανονική δραστηριότητα τα οποία υποδηλώνουν δυνητική επίθεση που μπορούν να αποτρέψουν. Ο αναλυτής επιλέγει ένα υποσύνολο ανωμαλιών, χρησιμοποιώντας τους κατάλληλους αλγορίθμους έχει τη δυνατότητα να καθορίσει σε κλάσματα του χρόνου αν η ανωμαλία είναι μια πραγματική επίθεση ή μια γνωστή ευπάθεια.

Η χρήση της τεχνητής νοημοσύνης συμβάλλει στην ανίχνευση, την προστασία, την πρόβλεψη και τον τερματισμό μιας επίθεσης.

Ανίχνευση: Επιτρέπει στις επιχειρήσεις να παρακολουθούν ανώμαλη συμπεριφορά στην κίνηση ενός δικτύου σε πραγματικό χρόνο, να επεξεργάζονται και να αναλύουν περίεργα δεδομένα. Από ακαδημαϊκές έρευνες φαίνεται ότι το ποσοστό επιτυχίας της ανίχνευσης των επιθέσεων με τη χρήση της τεχνητής νοημοσύνης κυμαίνεται μεταξύ 85% - 99%.

Προστασία: Δίνει τη δυνατότητα να εντοπίζονται και δίνονται προτεραιότητα στις ευπάθειες. Παρέχει προστατευτικά μέτρα σε προληπτικό πλαίσιο μειώνοντας το κόστος που θα προέκυπτε από μια πετυχημένη επίθεση αλλά και εντοπίζει ευθέως ευπάθειες κυρίως χαμηλού επιπέδου όπως το phising τις οποίες και μπορεί να εξαλείψει. Επιτρέπει έναν αμυντικό μηχανισμό που θα εντοπίζει και θα κλείνει εισβολέας γρηγορότερα και ευκολότερα.

Πρόβλεψη: Ένα σύστημα τεχνητής νοημοσύνης μπορεί να προβλέψει και να σχεδιάσει άγνωστες τεχνικές και στρατηγικές πριν εμφανιστούν διατηρώντας την επιχείρηση ένα βήμα μπροστά από τους επιτιθέμενους. Επίσης προβλέπει από που μπορεί να έρθει η επόμενη επίθεση βοηθώντας στην καλύτερη κατανόηση του αντιπάλου και συμβάλλοντας στην ταχύτερη αντιμετώπιση της επίθεσης.

Τερματισμός: Είναι σε θέση να σταματήσει κυβερνοεπιθέσεις προτού καταστραφεί ανεπανόρθωτα το σύστημα. Καθώς εξελίσσεται και η τεχνολογία της τεχνητής νοημοσύνης οι αλγόριθμοι εξελίσσονται, μαθαίνουν από την επίθεση που δέχτηκε το σύστημα και προσπαθούν να αναπτύξουν νέες τεχνικές για την προστασία από το κακόβουλο λογισμικό σε δυνητική επίθεση.

Γενικότερα τα συστήματα τεχνητής νοημοσύνης μπορούν να αναχαιτίσουν πολλά προβλήματα μέσω των χαρακτηριστικών του ορθολογισμού και της αυτοματοποίησης που διαθέτουν διευκολύνοντας ταυτόχρονα και τη δράση των αναλυτών ασφάλειας οι οποίοι μπορούν να χρησιμοποιούν τους διαθέσιμους πόρους τους πιο αποδοτικά και αποτελεσματικά. Κατά συνέπεια, όταν συνδυάζεται ένα προηγμένο προϊόν τεχνολογίας με ένα έξυπνο και σωστά καταρτισμένο προσωπικό, τα αποτελέσματα είναι ενθαρρυντικά δίνοντας ένα σαφές πλεονέκτημα στους υπερασπιστές της ασφάλειας του κυβερνοχώρου έναντι των επιτιθέμενων. Επίσης μπορεί και λειτουργεί ταυτόχρονα σε διαφορετικά καθήκοντα παρακολουθώντας και προστατεύοντας ένα τεράστιο αριθμό συσκευών και συστημάτων μετριάζοντας επιθέσεις μεγάλης κλίμακας. Τέλος έχοντας επισημάνει πρωτύτερα πόσο σημαντικό ρόλο διαδραματίζει ο ανθρώπινος παράγοντας στα θέματα ασφάλειας, η τεχνητή νοημοσύνη εξαλείφει το ανθρώπινο λάθος αφού λειτουργεί με ακριβή τρόπο.

Σύμφωνα με την έρευνα της ESG σχετικά με τους λόγους που οδηγούν τις επιχειρήσεις σε υιοθέτηση της τεχνητής νοημοσύνης στον τομέας της ασφάλειας φαίνεται ότι:

- Το 29% θέλει να χρησιμοποιήσει τη συγκεκριμένη τεχνολογία για να επιταχύνει την ανίχνευση των περιστατικών.
- Το 27% θέλει να χρησιμοποιήσει τη τεχνολογία της τεχνητής νοημοσύνης για να επιταχύνει την αντίδραση εφόσον εμφανιστεί μια επίθεση. Αυτό μπορεί να σημαίνει βελτίωση των λειτουργιών, ιεράρχηση περιστατικών και αυτοματοποίηση των εργασιών αποκατάστασης.
- Το 24% θέλει να χρησιμοποιήσει την τεχνητή νοημοσύνη στην ασφάλεια του κυβερνοχώρου γιατί πιστεύει ότι θα τη βοηθήσει στην καλύτερη οργάνωση και τον εντοπισμό του επιχειρηματικού κινδύνου ταξινομώντας τα τρωτά σημεία του συστήματος και απομονώνοντας εκείνα που βρίσκονται σε υψηλό κίνδυνο.
- Το 22% θέλει να χρησιμοποιήσει την τεχνητή νοημοσύνη για να κατανοήσει καλύτερα τι πραγματικά συμβαίνει στον κυβερνοχώρο δίνοντας μια καλύτερη εικόνα για την κατάσταση ασφαλείας του.

Η ίδια έρευνα δείχνει ότι μόνο το 30% εκείνων που εργάζονται σε θέματα ασφάλειας αισθάνονται πλήρως ενημερωμένοι για την εφαρμογή της τεχνητής νοημοσύνης στον κυβερνοχώρο. Δεν ενδιαφέρονται να εμβαθύνουν αλλά να πετύχουν τους στόχους τους. Αν μπορεί να ανταποκριθεί στη βελτίωση της ασφάλειας και την αποτελεσματική διαχείρισή της τότε μπορεί και να υιοθετηθεί από τις επιχειρήσεις.[34]

Η τεχνητή νοημοσύνη όπως χρησιμοποιείται από τους οργανισμούς για την εξάλειψη των κινδύνων κατά αυτό τον τρόπο που μπορεί να αξιοποιηθεί και από τους επιτιθέμενους. Ο Maude υποστηρίζει ότι η τεχνητή νοημοσύνη στον κυβερνοχώρο αποτελεί δίκοπο μαχαίρι καθώς οι εγκληματίες μπορούν να χρησιμοποιήσουν καινοτόμες επιθέσεις που θα μπορούσαν να προκαλέσουν σοβαρές συνέπειες στην επιχείρηση.

Παρά τις προκλήσεις, οι ειδικοί στον τομέα της κυβερνοασφάλειας προβλέπουν ένα λαμπρό μέλλον για τη χρήση της τεχνητής νοημοσύνης καθώς η τεχνολογία ολοένα και βελτιώνεται. Θα αναπτυχθούν σύντομα μηχανές που θα λειτουργούν όπως τα ανθρώπινα όντα στον τρόπο που αντιμετωπίζουν και μελετούν τις διαφορετικού τύπου επιθέσεις. Επιπλέον θα μπορούν να εξαπατούν τον αντίπαλο δημιουργώντας ψεύτικους στόχους για τον αντίπαλο όπως αρχεία και συστήματα που ενώ φαίνονται πραγματικά δεν είναι. Κατά αυτό τον τρόπο όχι μόνο θα προβλέπουν το κακό αλλά θα ακολουθούν και μια αμυντική στρατηγική. Με τα σημερινά δεδομένα όμως συνίσταται να χρησιμοποιείται ως μέρος μιας συνολικής άμυνας εφόσον δεν μπορεί μόνο η τεχνολογία να είναι η μόνη μέθοδος ασφάλειας της επιχείρησης.

Laidlaw advises: "Know where your crown jewels are, and protect what is most valuable, using AI as part of that." [43]

5.4 Cyber Insurance

Η cyber insurance είναι ένα ασφαλιστικό προϊόν που χρησιμοποιείται για την προστασία των επιχειρήσεων από κινδύνους που σχετίζονται με το διαδίκτυο. Προσφέρει κάλυψη για ζημιές που προήλθαν από κλοπή, καταστροφή, πειρατεία, άρνηση παροχής υπηρεσιών, κάλυψη ευθύνης σε περιπτώσεις απώλειας φήμης και αδυναμίας διασφάλισης δεδομένων καθώς και κάλυψη δαπανών που αφορούν νομικές υποθέσεις. Είναι αρκετά χρήσιμη αφού χρηματοδοτεί τις επιχειρήσεις με σκοπό να ανακάμψουν από μεγάλες απώλειες.
Κάλυψη πρώτου μέρους

Ασφάλεια: Ασφάλιση κατά των επιθέσεων χάκερ στον κυβερνοχώρο
Δικαστική έρευνα: Καλύπτει νομικές, τεχνικές ή ιατροδικαστικές υπηρεσίες που είναι απαραίτητες για να εκτιμηθεί η επιδρομή στην κυβερνοχώρο, να εκτιμηθεί ο αντίκτυπος της επίθεσης και να τερματιστεί η επίθεση.
Επιχειρηματική διακοπή: καλύπτει το χαμένο εισόδημα και τις συναφείς δαπάνες όταν η επιχείρηση δεν είναι σε θέση να ασκήσει επιχειρηματική δραστηριότητα εξαιτίας ενός περιστατικού ασφάλειας.
Εκβιασμός: καλύπτει το κόστος που σχετίζεται με τους εκβιαστές που απειλούν ότι θα αποκτήσουν και θα αποκαλύψουν ευαίσθητες πληροφορίες
Απώλεια και αποκατάσταση δεδομένων και υπολογιστών: καλύπτει τη φυσική ζημιά ή την απώλεια περιουσιακών στοιχείων που αφορούν υπολογιστικά συστήματα όπως το κόστος ανάκτησης και αποκατάστασης δεδομένων, υλικού, λογισμικού ή άλλων πληροφοριών που υπέστησαν ζημιές ή καταστράφηκαν.
Κλοπή και απάτη: καλύπτει την καταστροφή και απώλεια δεδομένων ως αποτέλεσμα δόλιας συμπεριφοράς στον κυβερνοχώρο

Κάλυψη από τρίτους

Διαδικασία επίλυσης διαφορών και κανονιστικών ρυθμίσεων: καλύπτει έξοδα που συνδέονται με πολιτικές αγωγές, κυρώσεις που απορρέουν από ένα περιστατικό ασφάλειας.
Κόστος κοινοποίησης: καλύπτει το κόστος για την ενημέρωση των πελατών, των εργαζομένων και των θυμάτων που έχουν πληγεί από την επίθεση στον κυβερνοχώρο.
Διαχείριση κρίσεων: καλύπτει δαπάνες στο πλαίσιο των δημόσιων σχέσεων που πραγματοποιήθηκαν για την εκπαίδευση των πελατών σχετικά με ένα περιστατικό ασφάλειας.
Παρακολούθηση πιστώσεων: καλύπτει έξοδα για την παρακολούθηση της πίστωσης, της απάτης ή άλλων υπηρεσιών σε πελάτες που πλήττονται από τον κυβερνοχώρο.
Ευθύνη για τα μέσα: καλύπτει την ευθύνη των μέσων ενημέρωσης συμπεριλαμβάνοντας και την κάλυψη σε περιπτώσεις παραβιάσεις πνευματικών δικαιωμάτων και εμπορικών σημάτων.[05]

Η καινοτομία των ασφαλιστικών προϊόντων πηγάζει από την παροχή υπηρεσιών διαχείρισης συμβάντων σε συνεργασία με παρόχους υπηρεσιών ψηφιακής εγκληματολογίας, νομικούς, επικοινωνιολόγους με σκοπό την αποτελεσματική διαχείριση των περιστατικών και τη μείωση των συνεπειών στην εταιρική φήμη.[03]

Παρόλο που τα οφέλη είναι αρκετά θα πρέπει να σημειώσουμε ότι τα έξοδα για τα ασφάλιστρα είναι πολλά. Για το λόγο αυτό πρέπει πρώτα να γίνει αξιολόγηση των αγαθών που θέλουν να προστατεύσουν οι επιχειρήσεις και τα οποία δεν μπορούν οι ίδιες να προστατεύσουν και των απειλών από τις οποίες κινδυνεύουν. Άλλοι παράγοντες που επηρεάζουν τα κόστη ασφάλισης είναι η δραστηριότητα της εταιρείας, το μέγεθος των εσόδων, ο όγκος και ο τύπος των δεδομένων της, η εμπειρία της σε προηγούμενη επίθεση αλλά και η εμπειρία της ασφαλιστικής εταιρείας στην αντιμετώπιση περιστατικών.

Οι δύο παράγοντες που επηρεάζουν τις οικονομικές συνέπειες μια παραβίασης είναι

- Η συμμετοχή της εκτελεστικής εξουσίας στην στρατηγική ασφάλειας της επιχείρησης και στην ανταπόκριση της παραβίασης δεδομένων.
- Η αγορά ασφάλισης στον κυβερνοχώρο για τον περιορισμό του κόστους παραβίασης των δεδομένων.

Για την καλύτερη λήψη αποφάσεων θα πρέπει να ληφθούν υπόψη πέντε βασικές αρχές οι οποίες θα αποτρέψουν συμβάντα, θα προστατεύσουν τη φήμη, το εμπορικό σήμα και τις δαπανηρές κυρώσεις και τις απώλειες εσόδων. Με αυτό τον τρόπο οι επιχειρήσεις θα είναι σε θέση να υιοθετήσουν νέες τεχνολογίες και τρόπους εργασίας που θα συμβάλλουν στην αύξηση της παραγωγικότητας, της ανταγωνιστικότητας με τρόπο ασφαλές ώστε να επιτύχουν τους στόχους του.

- Διασφάλιση κουλτούρας ασφάλειας η οποία θα πρέπει να καλύπτει κάθε εργαζόμενο ανεξάρτητα από το ρόλο του και να εκτείνεται ως τους επιχειρηματικούς εταίρους με εκπαίδευση, δοκιμή επιπέδου συνειδητοποίησης, ασκήσεις phising για να ελέγχουν πόσο καλά ανταποκρίνονται στις απειλές.
- Προετοιμασία για γρήγορη ανταπόκριση. Εκτός από την πρόληψη οι επιχειρήσεις πρέπει να είναι προετοιμασμένοι, να έχουν σχεδιάσει, εξασκηθεί και βεβαιωθεί ότι έχουν τα κατάλληλα εργαλεία ασφάλειας.
- Προστασία BYOD. Έχοντας συμβεί πολλά περιστατικά ασφάλειας εξαιτίας της τακτικής bring your own device, θα ήταν απαραίτητο να παρθούν μέτρα προστασίας για τη χρήση κινητών συσκευών. Καμία συσκευή δεν θα επιτρέπεται να συνδέεται στο δίκτυο αν δεν έχει εγκατεστημένο λογισμικό ασφάλειας και δεν έχει ελεγχθεί ότι συμμορφώνεται πλήρως σε πολιτικές που επιτρέπουν την πρόσβαση σε ευαίσθητη πληροφορία.
- Προστασία περιουσιακών στοιχείων. Για την καλύτερη διαχείριση του κινδύνου και την προστασία των αγαθών συνίσταται η ταξινόμηση και η ιεραρχία των στοιχείων που πρέπει να προστατευτούν.
- Μείωση της ασφάλειας των πληροφοριών με σκοπό να γίνει ανάλυση των δεδομένων ώστε να υπάρχει καλύτερη και πιο κατανοητή εικόνα της κατάστασης της ασφάλειας του οργανισμού το οποίο θα οδηγήσει σε πιο ουσιαστικές αποφάσεις.

5.5 Access governance

Η διακυβέρνηση πρόσβασης είναι μια πτυχή της διαχείρισης της ασφάλειας που έχει σκοπό να μειώσει τους κινδύνους που προέρχονται από τους τελικού χρήστες οι οποίοι έχουν περιττά δικαιώματα πρόσβασης. Συνδυάζει τον έλεγχο πρόσβασης με τη δυνατότητα πρόσβασης επιβάλλοντας ένα σύνολο δικαιωμάτων πρόσβασης για επιχειρηματικούς ρόλους. Βοηθά τους διαχειριστές στην επιβολή της αρχής του ελάχιστου προνομίου, ειδικά σε περιπτώσεις που οι χρήστες αλλάζουν ευθύνες και ενώ δεν είναι πλέον κατάλληλοι για τις προσβάσεις συνεχίζουν να τις έχουν. Η ανάγκη για διακυβέρνηση πρόσβασης έχει αποκτήσει ιδιαίτερη σημασία αφού οι επιχειρήσεις προσπαθούν να συμμορφωθούν και διαχειριστούν τον κίνδυνο με στρατηγικό τρόπο. Σημαντικό ρόλο παίζει στη μείωση του κόστους και της προσπάθειας σε ό,τι αφορά την επίβλεψη και την επιβολή πολιτικών και διαδικασιών πρόσβασης. Τα εργαλεία που χρησιμοποιούνται για αυτό το σκοπό συμμετέχουν στην παρακολούθηση της πρόσβασης την επικύρωση των αιτημάτων αλλαγής, στην αυτοματοποίηση της επιβολής πολιτικών πρόσβασης με βάση τους ρόλους ή των χαρακτηριστικών. Επιπλέον επιτρέπει την παρακολούθηση λογαριασμών σε όλα τα είδη συστημάτων όπως βάσεις δεδομένων, αντίγραφα ασφάλειας, κωδικοί πρόσβασης, συσκευές δικτύου και τον εντοπισμό ευπαθών λογαριασμών, λογαριασμών υπερβολικής πρόσβασης με σκοπό να καθορίσει τις επόμενες κινήσεις για προβλήματα που εντοπίστηκαν. Βοηθά στον εντοπισμό παλιών λογαριασμών που ανήκουν σε άτομα που έχουν φύγει από την επιχείρηση, ορφανών λογαριασμών που δεν φαίνεται να ανήκουν σε κάποιον, κοινόχρηστων λογαριασμών χωρίς κανένα άτομο που οποιαδήποτε θα μπορούσε να διεκδικήσει ευθύνη για τη χρήση τους. Τέλος πραγματοποιεί ελέγχους ασφάλειας που μπορεί να αναθεωρήσουν ολόκληρο το σύστημα. Η διακυβέρνηση της

πρόσβασης σταδιακά αντικαθιστά τη διαχείριση της ταυτότητας και υπόσχεται θεαματικά αποτελέσματα στον τομέα της ασφάλειας ειδικά σε μεγάλες και πολύπλοκες επιχειρήσεις στις οποίες πολλές ομάδες διαχειρίζονται πολλά συστήματα και πόρους.

5.6 Big Data analytics

Η κυβερνοασφάλεια είναι ένα γιγαντιαίο πρόβλημα όσο αφορά το μέγεθος και την πολυπλοκότητά του και δεν μπορεί να αντιμετωπιστεί από τα παραδοσιακά εργαλεία ασφάλειας. Για το λόγο αυτό προτείνεται η διαδικασία ανάλυσης μεγάλων δεδομένων τα οποία μπορούν να δώσουν λύσεις στην πρόληψη και αντιμετώπιση επιθέσεων σε πραγματικό χρόνο. Σύμφωνα με τη Gartner, ως μεγάλα δεδομένα ορίζουμε δεδομένα μεγάλης ταχύτητας και ποικιλομορφίας που απαιτούν ανάλυση για να είναι χρήσιμα για την επιχείρηση. Η χωρητικότητα υπολογίζεται σε terabyte, petabyte, exabyte. Είναι δομημένα και αδόμητα δεδομένα που ενώ φαίνονται ασήμαντα και άγνωστα δυνητικά παράγουν χρήσιμες πληροφορίες. Το Google, το Facebook, οι συσκευές IoT και τα αρχεία καταγραφών των διακομιστών και των εφαρμογών είναι πηγές που παράγουν τεράστια δεδομένα. Κυρίως χρησιμοποιούνται για την κατανόηση και βελτιστοποίηση των επιχειρηματικών διαδικασιών, των χρηματικών συναλλαγών, την καλύτερη διαχείριση των πελατών, τη βελτίωση της υγειονομικής περίθαλψης και των μεταφορών. Στην ασφάλεια του κυβερνοχώρου, των μεγάλων δεδομένων επικεντρώνεται στη συλλογή τεράστιων ποσοτήτων ψηφιακής πληροφορίας με σκοπό την ανάλυσή τους ώστε να αναπτυχθούν νέες ιδέες για την πρόληψη, αντιμετώπιση και τερματισμό των επιθέσεων.[34]

Πιο συγκεκριμένα η ανάλυση των μεγάλων δεδομένων βοηθά στον τομέα της κυβερνοασφάλειας ως εξής:

- Με την εξόρυξη χρήσιμων πληροφοριών από μεγάλα δεδομένα δίνουν καλύτερη και ευρύτερη εικόνα των αδυναμιών και των κινδύνων της επιχείρησης.
- Τα εργαλεία που χρησιμοποιούνται για την ανάλυση των μεγάλων δεδομένων μπορούν να χειριστούν την πολυπλοκότητα και τον όγκο των δεδομένων του δικτύου τα οποία βοηθούν στην ανάλυση της ασφάλειας του κυβερνοχώρου.
- Τα μεγάλα δεδομένα σε συνδυασμό με τη μηχανική μάθησης μπορούν να προβλέψουν περίεργη συμπεριφορά πολύ νωρίτερα και η εύρεση ανωμαλιών γίνεται ευκολότερη.
- Επιπλέον τα δεδομένα που προέρχονται από το διαδίκτυο και τη βιομετρία θα χρησιμοποιηθούν για την πρόληψη της τρομοκρατίας.
- Ο όγκος των δεδομένων που επεξεργάζονται βοηθούν στον εντοπισμό των παραβιάσεων ή κακόβουλου λογισμικού. [23]

Εφόσον τα εργαλεία μεγάλων δεδομένων μπορούν γρήγορα να επαναλάβουν δεδομένα να δημιουργήσουν μοντέλα και να δώσουν γρήγορη ανάλυση, η δουλειά των ανθρώπων γίνεται ευκολότερη στην καθημερινότητα τους αφού πρέπει να αναλύουν εκατομμύρια αρχεία. Επίσης θα έχουν μια δύναμη πρόβλεψης ώστε να ξεχωρίζουν την κανονική κίνηση του δικτύου από μια ύποπτη και κακόβουλη κίνηση που θα οδηγήσει σε κυβερνοεπίθεση ή κακόβουλου λογισμικού.[06]

Σχήμα 5.3: Big Data Analysis

Η εισαγωγή της επιστήμης των δεδομένων στις υπάρχουσες ροές πρέπει να γίνει σταδιακά. Στην αρχή τα βήματα θα υλοποιηθούν ανεξάρτητα μόνο μεταξύ μιας ομάδας του και επιστήμονα. Μόνο α ντα αποτελέσματα που θα ληφθούν είναι ικανοποιητικά και ακριβή θα συνεχίσει η εφαρμογή της. Αυτό συμβαίνει γιατί η ανάλυση δεδομένων είναι κάτι καινούριο, υπάρχει αβεβαιότητα των αποτελεσμάτων και έλλειψη τεχνογνωσίας εις βάθος.

Για το λόγο αυτό η εφαρμογή μιας λύσης ανάλυσης προτείνεται να γίνει βάση των ακόλουθων βημάτων:
1.Ανάπτυξη επιχειρησιακής στρατηγικής .
2.Συμμετοχή σε εκπαιδευτικές δραστηριότητες και σε εργαστήρια. Απαραίτητη η συμμετοχή σε σεμινάρια και εργαστήρια ώστε να γίνονται πειραματισμοί σε τεχνικές Big Data μπορούν να αποκτήσουν βαθιά γνώση για το πως λειτουργεί και για τα αποτελέσματα που παράγει ώστε να βοηθήσουν την ανάπτυξη της στρατηγικής τους ανάλυσης.
3.Εφαρμογή κεντρικής υποδομής διαχείρισης δεδομένων.
4.Εφαρμογή πλατφόρμας όπου θα υποστηρίξει πειραματισμούς με ένα ποικίλο αριθμό εργαλείων, τεχνικών και αλγορίθμων για την αποθήκευση απόκτηση των δεδομένων.
5.Πρόσληψη επιστήμονα δεδομένων ο οποίος καθοδηγεί την εκτέλεση της ανάλυσης σε όλα τα στάδια.
6.Εφαρμογή ενός επιπέδου παρακολούθησης δικτύου .
Παρακολουθεί τις ροές του δικτύου και χρησιμοποιεί την ανάλυση δεδομένων
7.Εφαρμογή ενός επιπέδου Layer alert .
Περιλαμβάνει όλα τα μέτρα που απαιτούνται για να διασφαλιστεί η ασφάλεια του κυβερνοχώρου πχ κλείδωμα πρόσβασης, έλεγχος ταυτότητας χρήστη. Λειτουργεί ακόμα και αν η πλατφόρμα ανάλυσης δεν χρησιμοποιείται εκείνη την στιγμή.

Η μεγαλύτερη εφαρμογή των αναλύσεων ασφάλειας είναι η παρακολούθηση των απειλών και των περιστατικών. Εστιάζει στην ανακάλυψη και εκμάθηση γνωστών και άγνωστων προτύπων επιθέσεων που αναμένεται να επηρεάσουν την ταχύτερη και αποτελεσματικότερη αναγνώριση των κρυφών απειλών και να προβλέψουν μελλοντικές επιθέσεις με αυξανόμενη ακρίβεια.

Κεφάλαιο 6
Επίλογος

Το κεφάλαιο 6 είναι ο επίλογος της διατριβής όπου επισημαίνονται τα βασικά σημεία της έρευνας, εξάγονται συμπεράσματα και το πως θα μπορούσε να χρησιμοποιηθεί στο μέλλον.

6.1 Συμπεράσματα

Η ασφάλεια του κυβερνοχώρου είναι ένα σύνολο απαιτήσεων και αναγκών για κάθε επιχείρηση. Ωστόσο κανένα πληροφοριακό σύστημα δεν χαρακτηρίζεται από ολοκληρωμένη ασφάλεια και για αυτό και δίνεται ένας διαφορετικός ορισμός για την αυτή την έννοια. Ως ασφαλές ορίζεται ένα πληροφοριακό σύστημα για το οποίο απαιτείται μεγάλο χρονικό διάστημα και αρκετά χρήματα για να παραβιαστεί.

Επομένως οι επιχειρήσεις επενδύουν ορισμένο κεφάλαιο για την διασφάλισή τους. Με τη λήψη και εφαρμογή όλων των προτεινόμενων μέτρων για την ενίσχυση της ασφάλειας στον κυβερνοχώρο, οι επιχειρήσεις μπορούν να επωφεληθούν σε σημαντικό βαθμό. Ωστόσο τα οφέλη που θα αποκομίσουν δεν πρέπει να συνδέονται με κέρδη. Κέρδος είναι το οικονομικό όφελος που προκύπτει ύστερα από την επένδυση ενός κεφαλαίου στις παραγωγικές διαδικασίες της επιχείρησης σε αντίθεση με το όφελος που έχει μια γενικότερη έννοια που ουσιαστικά είναι η βελτίωση της ασφάλειας με σκοπό τον περιορισμό ή την εξάλειψη των κινδύνων.

Benefits= initially expected losses- residual expected losses

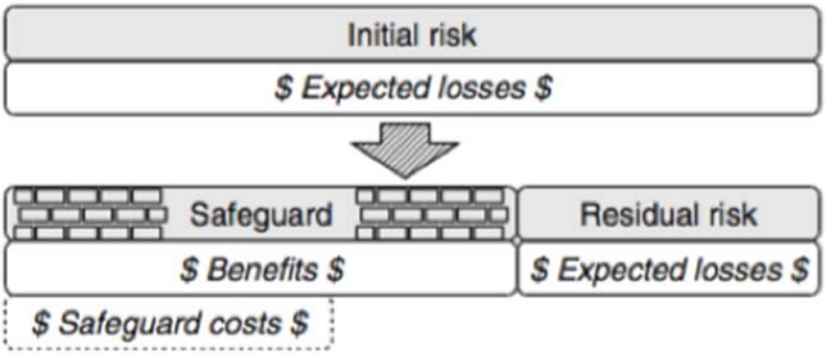
Ως όφελος στην ασφάλεια του κυβερνοχώρου ορίζεται η διαφορά των αρχικών αναμενόμενων ζημιών πριν την εφαρμογή της διασφάλισης και τις ζημιές που επέμειναν μετά την εφαρμογή της διασφάλισης. Οι αρχικές ζημιές υπολογίζονται από τον αρχικό κίνδυνο και την εκτίμησή του.

Επομένως, οι επενδύσεις στην ασφάλεια του κυβερνοχώρου δεν χρησιμοποιούνται για τη δημιουργία κερδών. Βοηθούν μόνο στη διασφάλιση των περιουσιακών στοιχείων και στην αποφυγή διακοπών και οικονομικών απωλειών ως συνέπεια μια επίθεσης. Λειτουργούν προληπτικά στις αρνητικές επιπτώσεις που θα εμφανιστούν μετά την επιτυχημένη κυβερνοεπίθεση. Ωστόσο οι επιχειρήσεις για να επιτύχουν τη μεγαλύτερη απόδοση της επένδυσης θα πρέπει λάβουν υπόψη, κατά τη διαδικασία λήψης απόφασης, τα έξοδα που προκύπτουν από την εφαρμογή της διασφάλισης. Πρέπει να γίνει αντιστάθμιση του κόστους και των παροχών των εναλλακτικών για τη λήψη της επενδυτικής απόφασης. Σε περίπτωση που το κόστος είναι μεγαλύτερο από το όφελος, η επένδυση δεν πραγματοποιείται οπότε και η επιχείρηση δέχεται τις απώλειες που θα προκύψουν από την επίθεση. Ακόμα και αν προκύψουν οικονομικές απώλειες θα είναι λιγότερες από την αρχική επένδυση της διασφάλισης όποτε η επιχείρηση θα μπορεί να ανταπεξέλθει σε αυτό το κόστος.

Οι επενδύσεις στον τομέα της ασφάλειας έχουν έμμεσο όφελος. Εξασφαλίζουν τα περιουσιακά στοιχεία και τη συνεχή λειτουργία της επιχείρησης, μειώνουν τις αναμενόμενες ζημιές επηρεάζοντας έμμεσα τα κέρδη της. Κάθε επιχείρηση ξεκινά τη λειτουργία της με ένα αρχικό κεφάλαιο που παρέχεται είτε από τους ίδιους του μετόχους είτε από τρίτους εκτός επιχείρησης. Το κεφάλαιο αυτό χρησιμοποιείται ανάλογα με τις ανάγκες της εκάστοτε επιχείρησης. Κάθε μέτοχος εστιάζει και βρίσκει τρόπους για να αυξήσει τα κέρδη της επιχείρησης που ανήκει. Η επένδυση στην ασφάλεια δεν πολλαπλασιάζει το αρχικό κεφάλαιο αλλά προσπαθεί να το διατηρήσει στα ίδια επίπεδα περιορίζοντας τις οικονομικές απώλειες. Ωστόσο όπως έχουμε αναφέρει και πρωτύτερα μια επένδυση στην ασφάλεια δεν είναι μόνο το αρχικό κόστος της αγοράς της διασφάλισης αλλά περιλαμβάνει και πάγια έξοδα λειτουργίας και συντήρησης τα οποία για μια επιχείρηση που δεν έχει επενδύσει σε μια διασφάλιση τα χρήματα μένουν σε αυτή. [04]

Συμπερασματικά, κάθε επιχείρηση ανάλογα με το τι πρεσβεύει και τους στόχους της ακολουθεί τη δική της επενδυτική στρατηγική. Τα ανώτατα στελέχη αποφασίζουν αν θα ακολουθήσουν μια τακτική ρίσκου χωρίς να επενδύσουν το κεφάλαιο στον τομέα της ασφάλειας και απλά να λειτουργούν με την πιθανότητα ότι ίσως δεχτούν κυβερνοεπίθεση άλλες επιχειρήσεις προκειμένου να διατηρήσουν την ασφάλεια λειτουργούν συντηρητικά και επενδύουν μέρος του αρχικού τους κεφαλαίου στον τομέα της ασφάλειας με σκοπό την προστασία των αγαθών της και την ελαχιστοποίηση των άμεσων και έμμεσων συνεπειών της επιτυχημένης επίθεσης,

Έρευνες έδειξαν ότι μέχρι το 2021 οι ζημιές που θα προκληθούν ως συνέπεια των κυβερνοεγκλημάτων θα ανέρχονται ετησίως στα 6 τρισεκατομμύρια δολάρια, ποσό που θα έχει διπλασιαστεί σε σχέση με το 2015. Επιπλέον οι επιχειρήσεις παγκοσμίως συνολικά θα δαπανήσουν ένα τρισεκατομμύριο δολάρια σε προϊόντα και υπηρεσίες στον τομέα της ασφάλειας για να καταπολεμήσουν το κυβερνοέγκλημα.



Σχήμα 6.1: Σχηματική απεικόνιση του όφελους σε σχέση με τις αναμενόμενες απώλειες

6.2 ΠΡΟΤΑΣΕΙΣ

Όσο και αν η τεχνολογία εξελίσσεται και οι επιχειρήσεις εφαρμόζουν νέα εργαλεία και λογισμικά για να διατηρήσουν την ασφάλεια στον κυβερνοχώρο, η εκπαίδευση των εργαζομένων παραμένει απολύτως αναγκαία για την αντιμετώπιση των απειλών. Καθώς το περιβάλλον μεταβάλλεται οι εργαζόμενοι παραμένουν σταθεροί στην πρώτη γραμμή για να περιορίσουν τον κίνδυνο δημιουργώντας μια ισχυρή κουλτούρα ασφάλειας. Σύμφωνα με τον Touhill, συγγραφέα του «Cybersecurity for executives», σε ερώτηση που του τέθηκε για το πως θα ξόδευε περισσότερα χρήματα για την ασφάλεια του κυβερνοχώρου απάντησε ότι θα τα ξόδευε για την καλύτερη εκπαίδευση των ανθρώπων. Συνεχίζει λέγοντας ότι ένα πολύ καλά ενημερωμένο και εκπαιδευμένο ανθρώπινο δυναμικό είναι έτοιμο να βοηθήσει στην ασφάλεια του κυβερνοχώρου. Μόνο με μεγάλη προσπάθεια, σωστή καθοδήγηση και εκπαίδευση θα είναι πιο αποτελεσματική η ασφάλεια στον κυβερνοχώρο. Σε αντίθετη περίπτωση, εμφανίζονται ρωγμές που θα οδηγήσουν και σε δυσοίωνα περιστατικά στο μέλλον.Για το λόγο αυτό οι επιχειρήσεις πρέπει να εστιάσουν στην εκπαίδευση των εργαζομένων σε βάθος. Προφανώς και υπάρχει μια κατάρτιση των εργαζομένων στα θέματα ασφάλειας για την αποφυγή λαθών για παράδειγμα “μην πατάτε σε αυτό τον ύποπτο σύνδεσμο στο ηλεκτρονικό σας ταχυδρομείο” ή “μη γράφετε τον κωδικό σας πρόσβασης σε χαρτί” αλλά αυτό δεν είναι αρκετό. Υπάρχουν και

άλλοι λόγοι ζωτικής σημασίας που οι εργαζόμενοι πρέπει να αντιληφθούν ώστε να φροντίσουν για την ασφάλεια.

1.Η ταχύτητα αντιμετώπισης
Με καλύτερη εκπαίδευση οι εργαζόμενοι μπορούν ευκολότερα και πιο αποτελεσματικά να εντοπίζουν και να καταγράφουν ύποπτες δραστηριότητες. Αυτό σημαίνει ότι χρειάζεται λιγότερος χρόνος για την αντιμετώπιση των κινδύνων. Η σύγχυση προκαλεί παράλυση ενώ η εκπαίδευση προκαλεί δράση.

2.Αυτοσυγκράτηση
Έρευνες έχουν δείξει ότι οι περισσότερες απειλές προέρχονται από εσωτερικούς παράγοντες και όχι εξωτερικούς. Όταν γνωρίζουν οι εργαζόμενοι από που πηγάζει ο κίνδυνος είναι σε θέση να βοηθήσει ο ένας τον άλλον ώστε να αποφευχθεί η παραβίαση. Σύμφωνα με την έκθεση της IBM/force threat, ένας πολύ μεγάλος αριθμός περιστατικών προέρχεται από υπαλλήλους που εργάζονται στην επιχείρηση ή άλλους αξιόπιστους. Πιο συγκεκριμένα στο χώρο της υγείας το 75% των επιθέσεων προέρχεται από υπαλλήλους ενώ στον χρηματοπιστωτικό τομέα το ποσοστό ανέρχεται στο 58%. Οι περισσότεροι είναι υπάλληλοι που εξαπατήθηκαν που σημαίνει ότι υπάρχει έλλειψη κατάρτισης. Ακόμα και τα καλύτερα εργαλεία να χρησιμοποιούν για την προστασία των δεδομένων δεν αρκούν για να σταματήσουν την απειλή.

3.Συμμόρφωση
Η εκπαίδευση βοηθά τους υπαλλήλους να συμμορφώνονται σε κανονισμούς χωρίς να χάνουν την προσοχή τους στο μείζον ζήτημα της ασφάλειας. Γενικά οι αυξανόμενες απειλές έχουν οδηγήσει σε μια νέα επιχείρηση ρύθμισης σχετικά με την ασφάλεια και την ιδιωτικότητα και οποιαδήποτε μη συμμόρφωση μπορεί να οδηγήσει σε κανονιστικές και νομικές συνέπειες.

4.Ηθική
Οι απειλές επηρεάζουν τους υπαλλήλους προκαλώντας ανεπιθύμητες αλλαγές στην εργασία τους.

Ένα από τα σοβαρότερα προβλήματα στη λήψη αποφάσεων είναι η αποτυχία επένδυσης στις καλύτερες λύσεις. Αυτό είναι συνέπεια της έλλειψης γνώσης των υπευθύνων που συμμετέχουν στη διαδικασία για αυτό είναι απαραίτητη η εκπαίδευσή τους ώστε να είναι πιο αποτελεσματικοί.

Για να ολοκληρωθεί με επιτυχία η προσπάθεια ευαισθητοποίησης των εργαζομένων θα πρέπει η εκπαίδευση να γίνεται από εμπειρογνώμονες και ειδικούς στην ασφάλεια του κυβερνοχώρου με τρόπο ευχάριστο και δημιουργικό, ικανό να κρατήσει το ενδιαφέρον του κοινού. Το μεγαλύτερο πρόβλημα της μη αποτελεσματικής εκπαίδευσης είναι ότι οι εργαζόμενοι τη θεωρούν βαρετή και μη αποδοτική. Τα αισθήματα που γεννιούνται στους υπαλλήλους κατά την ώρα της εκπαίδευσης συνήθως είναι η ανία, το χάσιμο χρόνου, ότι ήδη τα γνωρίζουν αυτά και ότι ίσως τους περνούν και για όχι τόσο έξυπνους. Για να αποφευχθούν τέτοιες καταστάσεις οι υπεύθυνοι οφείλουν να επενδύσουν χρήματα ακόμα και να αναθέσουν σε εξωτερικούς συνεργάτες την εκπαίδευση. Η εκπαίδευση δεν πρέπει να σταματά αλλά συνεχώς να εξελίσσεται για την αντιμετώπιση νέων απειλών και να πραγματοποιείται όχι μόνο για το τμήμα της πληροφορικής αλλά για όλη την επιχείρηση. Κάθε φορά που ολοκληρώνεται το πρόγραμμα ευαισθητοποίησης, είναι καλό να αξιολογείται. Τα ερωτήματα που πρέπει να τίθενται από τους CISOs είναι:

- Γνωρίζουν οι υπάλληλοι την πολιτική ασφάλειας;
- Γνωρίζουν οι υπάλληλοι τι πρέπει να κάνουν στην περίπτωση που εντοπίσουν μια παραβίαση της ασφάλειας;

- Ποιες πρακτικές και τεχνολογίες χρησιμοποιούν οι υπάλληλοι για να ανιχνεύσουν την απειλή;
- Ασχολούνται τα στελέχη και η ανώτερη διοίκηση με το πρόγραμμα ευαισθητοποίησης;
- Φροντίζει η εταιρική διακυβέρνηση για την εκπαίδευση και ευαισθητοποίηση ολόκληρου του οργανισμού;
- Θέτουν οι πολιτικές ασφάλειας επί τάπητος την ευαισθητοποίηση της ασφάλειας;

Τέλος είναι πολύ σημαντική η συνεργασία και η επικοινωνία των εργαζομένων κατά τη διαδικασία ευασθητοποποίησης καθώς και κίνητρα για συμμετοχή τους ώστε να κατανοήσουν καλύτερα την ανάγκη της ασφάλειας του κυβερνοχώρου και τη δημιουργίας κουλτούρας σύμφωνα με τους στόχους της επιχείρησης. Η εκπαίδευση των εργαζόμενων αποτελεί βασικό μέρος μιας γενικότερης τακτικής που πρέπει να ακολουθούν οι επιχειρήσεις που θέλουν να μειώσουν την πιθανότητα της απειλής.

Άλλωστε η μεγαλύτερη απειλή στην κυβερνοασφάλεια είναι η παρανόηση. Πολλοί θεωρούν ότι η ασφάλεια είναι ένα ζήτημα που πρέπει να διαχειρίζεται ο τομέας της πληροφορικής όποτε και δεν αισθάνονται υπεύθυνοι να προστατέψουν τα αγαθά τους. Η μη ανάληψη ευθύνης, η έλλειψη επικοινωνίας και η μη επαρκής εκπαίδευση είναι παράγοντες που εμποδίζουν την εφαρμογή αποτελεσματικών στρατηγικών. Η ασφάλεια είναι ένα ζήτημα διαχείρισης κινδύνου που πρέπει να αντιμετωπιστεί από μια στρατηγική και οικονομική προοπτική.

6.3 Μελλοντικές προεκτάσεις

Ο κυβερνοχώρος αποτελεί ένα νέο πεδίο μελέτης. Η ταχύτατη εξέλιξη της τεχνολογίας οδηγεί σε ραγδαίες και συνεχείς αλλαγές επομένως οι επιστήμονες δεν θα πάψουν να τον μελετούν. Αν και η απόλυτη ασφάλεια φαίνεται να είναι ουτοπική, πρέπει να συνεχιστεί η προσπάθεια μείωσης των επιθέσεων από τους κακόβουλους χρήστες ώστε να διατηρηθεί το σημαντικότερο χαρακτηριστικό του κυβερνοχώρου, η ασφάλεια. Οι ειδικοί της ασφάλειας πρέπει να εξετάσουν νέους τρόπους αντιμετώπισης των εισβολών που ταυτόχρονα θα είναι αποτελεσματικές αλλά και θα μειώνουν το κόστος επένδυσης των επιχειρήσεων .

Η παρούσα μελέτη έχει ως στόχο να μελετήσει το βασικό ζήτημα της ασφάλειας συνδέοντας τις τεχνικές και οικονομικές της πλευρές. Εφόσον έγινε ανάλυση των υφιστάμενων μέτρων προστασίας και τεχνικών χαρακτηριστικών της διαπιστώνουμε ότι τίποτα δεν είναι αρκετό για του διαπιστώσαμε ότι η επένδυση στον τομέα αυτό δεν επιφέρει επιπλέον κέρδη για την επιχείρηση αλλά ο σκοπός της είναι να περιορίσει τα κόστη και τις αναγκαίο να εφαρμοστούν. Έγιναν προτάσεις εναλλακτικών βασιζόμενες σε προηγμένες τεχνολογίες για την προστασία και αντιμετώπιση των επιθέσεων όπως σύστημα ασφάλειας πληροφοριών, τεχνητή νοημοσύνη και μηχανική μάθησης ωστόσο ο κυβερνοχώρος συνεχώς μεταβάλλεται, η τεχνολογία εξελίσσεται και οι επιτιθέμενοι ανακαλύπτουν νέους τρόπους δράσης με αποτέλεσμα οι λύσεις που προτείνονται να μην επαρκούν πάντα για την πλήρη εξάλειψη των κινδύνων και των απειλών. Θα ήταν χρήσιμο στο μέλλον να γίνει μια μελέτη περίπτωσης στην εφαρμογή των νεών τεχνολογιών στις επιχειρήσεις κα να μελετηθούν τα αποτελέσματά της. Επιπλέον όντας γνωστό ότι η τεχνολογία δεν είναι αρκετή από μόνη της για τη διατήρηση της ασφάλειας και σε συνδυασμό με το γεγονός ότι οι επενδύσεις δεν είναι κερδοφόρες αλλά ο σκοπός του είναι να μειώσουν τα κόστη θα ήταν χρήσιμο οι μελλοντικές μελέτες να εστιάσουν στην καλύτερη διαχείριση των κινδύνων, την ανάλυση και μελέτη των χαρακτηριστικών των πληροφοριακών συστημάτων και των δικτύων, τον εντοπισμό των τρωτών σημείων.

Βιβλιογραφία

[01] 2018 Cost of Insider Threats : Global Sponsored by ObserveIT. (2018), (April).

[02] Afshari, A., Mojahed, M., & Yusuff, R. (2010). Simple additive weighting approach to personnel selection problem. *International Journal of Innovation, Management and Technology*, *1*(5), 511–515. https://doi.org/10.7763/IJIMT.2010.V1.89

[03] Association of British Insurers. (2014). Cyber Insurance, (November), 2–4.

[04] Beissel, S. (n.d.). Progress in IS Cybersecurity Investments Decision Support Under Economic Aspects.

[05] Benefits_of_Cyber_Insurance. (n.d.).

[06] Big Data Security Analytics: A Weapon Against Cyber Security Attacks? [Video]. (n.d.).

[07] Bornman, W. G., & Labuschagne, L. (2004). A comparative framework for evaluating information security risk management methods. *Information Security South Africa Conference*. Retrieved from http://icsa.cs.up.ac.za/issa/2004/Proceedings/Full/015.pdf

[08] Camp, L., & Lewis, S. (2004). *Economics of information security*. Retrieved from http://books.google.com/books?hl=en&lr=&id=PbzP9tgeDcAC&oi=fnd&pg=PR7&dq=Economics+of+Information+Security&ots=8CHswCfdM5&sig=W2ZskFOXJLpmD2E6S8WGkAhNNSc%5Cnhttp://download.springer.com/static/pdf/936/bok%3A978-1-4020-8090-6.pdf?auth66=1406221947_434f6026

[09] Chain, C. K., & Planning, S. A. (2018). Applying Security Awareness to the Cyber Kill Chain | SANS Security Awareness. Retrieved from https://www.sans.org/security-awareness-training/blog/applying-security-awareness-cyber-kill-chain

[10] Dixon, J. (1965). for System Safety.

[11] Does, W. (2009). Chapter 1 . Is There a Security Problem in Computing ?
Down, M. P., & Sands, R. J. (2004). Biometrics: An Overview of the Technology, Challenges and Control Considerations. *Information Systems Control Journal*, *4*, 53–56.

[12] Dynes, S., Goetz, E., & Freeman, M. (n.d.). Chapter 2 CYBER SECURITY : ARE ECONOMIC INCENTIVES ADEQUATE ?, *253*, 15–27.

[13] Ed Gelbstein, P. D. (n.d.). Return on Security Investment—15 Things to Consider. Retrieved from https://www.isaca.org/Journal/archives/2015/Volume-1/Pages/Return-on-Security-Investment-15-Things-to-Consider.aspx

[14] Entre, I. C., Niversity, A. D. A. J. U., Koko, A. K., Tate, O. N. D. O. S., & Omputer, D. E. O. F. C. (2017). a Review of Game Theory Approach To Cyber Security Risk Management, *36*(4), 1271–1285.

[15] Fearn, N. (2018). How AI will underpin cyber security in the next few years. *Computerweekly.Com*. Retrieved from http://www.computerweekly.com/feature/How-AI-will-underpin-cyber-security-in-the-next-few-years

[16] Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision Support Systems*, *86*, 13–23. https://doi.org/10.1016/j.dss.2016.02.012

[17] Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment, *5*(4), 438–457.

[18]Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in Cybersecurity : Insights from the Gordon-Loeb Model, *2013*(March), 49–59.

[19] Highland, H. J. (1997). *Security in computing*. *Computers & Security* (Vol. 16). https://doi.org/10.1016/S0167-4048(97)90261-3

[20] Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). *An Introduction to Cryptography*. *Springer* (Vol. XVI). https://doi.org/10.1007/978-0-387-77994-2

[21] Institute, P. (2017). 2017 Cost of Cyber Crime Study. Retrieved from https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-

61/Accenture-2017-CostCyberCrimeStudy.pdf
[22] ISO/IEC. (2016). ISO/IEC 27000:2016(E) Information technology — Security techniques — Information security management systems — Overview and vocabulary. *ISO.Org [Online]*, *4th Editio*, 42. Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip
[23] Joglekar, P., Computer, N. P.-I. J. of, & 2016, undefined. (2016). Solving Cyber Security Challenges using Big Data. *Pdfs.Semanticscholar.Org*, *154*(4), 9–12. Retrieved from https://pdfs.semanticscholar.org/b9aa/3fe200c8e6087e13181969b03c4a6d7ae570.pdf
[24] Johnson, C., Feldman, L., & Witte, G. (2017). Itl Bulletin for May 2017 Cyber-Threat Intelligence and Information Sharing, (May), 1–5. Retrieved from http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=923332
[25] Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing. https://doi.org/10.6028/NIST.SP.800-150
[26] Lewis, J. a, & Zheng, D. E. (2015). Cyber Threat Information Sharing, (March), 11. Retrieved from www.csis.org
[27] Mark, R.-O. (2013). Information Security The Complete Reference, Second Edition. *Wdwqds*, *ww*(wwww), 896. Retrieved from www.it-ebooks.info/book/3340

[28] M. Eric Johnson , “Managing Information Risk and the Economics of Security”, Springer.
[29] Martin C. Libicki, Cyberdeterrence and Cyberwar. USA: RAND Corporation, 2009.
[30] Morgan, S. (2017). 2017 CyberVentures Cybercrime Report, 14. Retrieved from [28] https://www.pwc.com/gx/en/forensics/global-economic-crime-and-fraud-survey-2018-summary-infographic.pdf
[31]N. Sklavos, P. Souras, "Economic Models and Approaches in Information Security for Computer Networks", International Journal of Network Security (IJNS), Science Publications, Vol. 2, No 1, Issue: January 2006, pp. 14-20, 2006.
[32]Sklavos, N. (2011). Cryptographic algorithms-on-a-chip: Architectures, designs & implementation platforms. *6th International Conference on Design and Technology of Integrated Systems in Nanoscale Era, DTIS’11 - Technical Program*, 6. https://doi.org/10.1109/DTIS.2011.5941405
[33]Sklavos, N., Zaharakis, I. D., Kameas, A., & Kalapodi, A. (2017). Security & Trusted Devices in the Context of Internet of Things (IoT). *Proceedings - 20th Euromicro Conference on Digital System Design, DSD 2017*, 502–509. https://doi.org/10.1109/DSD.2017.81
[34] Oltsik, J. (2018). Artificial intelligence and cybersecurity: The real deal. *CSO Online*. Retrieved from https://www.csoonline.com/article/3250850/security/artificial-intelligence-and-cybersecurity-the-real-deal.html
[35]Onwubiko, C., & Lenaghan, A. P. (2007). Managing Security Threats and Vulnerabilities for Small to Medium Enterprises. *2007 IEEE Intelligence and Security Informatics*, 244–249. https://doi.org/10.1109/ISI.2007.379479
[36] Page, A., Page, B., Page, C., & Page, D. (2013). The abc.
[37] Paar, C., & Pelzl, J. (2010). *Understanding Cryptography*. https://doi.org/10.1007/978-3-642-04101-3
38] Ponemon Institute. (2013). Big Data Analytics in Cyber Defense, (February), 32. Retrieved from https://www.ponemon.org/local/upload/file/Big_Data_Analytics_in_Cyber_Defense_V12.pdf%0Ahttp://www.ponemon.org/library/big-data-analytics-in-cyber-defense
[39] Samarati, P., & Capitani, S. De. (2001). Access Control : Policies , Models , and Mechanisms. *Foundations of Security Analysis and Design*, *2171*, 137–196. https://doi.org/10.1007/3-540-45608-2_3

[40] Security-Intelligence Systems and the Future of Tech - The Data Center Journal. (n.d.).
Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (rosi)-a practical quantitative model. *Journal of Research and …*, *38*(1), 45–56. https://doi.org/10.1145/581271.581274
[41] Sponsored by Palo Alto Networks Flipping the Economics of Attacks. (2016).
[42] Tuchinda, R. (2002). Access control mechanism for intelligent environments. *Bitstream, the MIT Journal of EECS Student Research*, 27–30. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Access+Control+Mechanism+for+Intelligent+Environments#0
[43] Why to Use Artificial Intelligence in Your Cybersecurity Strategy. (n.d.).
[44] Writer, P., Gilligan, J., & Corporation, S. (2014). THE ECONOMICS OF CYBERSECURITY PART II :, (April).

[45] Ι. Μαυρίδης «Ασφάλεια Πληροφοριών στο Διαδίκτυο», Ελληνικά Ακαδημαϊκά Συγγράμματα και Βοηθήματα, 201
[46] Σ. Κ. Κάτσικας, «Διαχείριση της Ασφάλειας Πληροφοριών», Πεδίο, 2014.
[47] Σ. Κάτσικας, Δ. Γκρίτζαλης, Σ. Γκρίτζαλης, «Ασφάλεια Πληροφοριακών Συστημάτων», Εκδόσεις Νέων Τεχνολογιών, 2003.
[48]www.cyberinsurance.com

Παράρτημα Α

Αρκτικόλεξα

AHP	Analytic Hierarchy process
AI	Artificial Intelligence
ALE	Annual Expected Loss
ARO	Annual Rate of Occurrence
CIA	Confidential Integrity Availability
CD	Compact Disk
CISO	Chief Information Security Officer
COBBIT	Control Objective for Information and Related Technology
CRAMM	CCTA risk Analysis Management Method
DAC	Discretionary Access Control
DMZ	Demiliarized Zone
DOS	Denial Of Service
DSA	Digital Signature Algorithm
DVD	Digital Video Disc
EAA	Equivalent Annual Annuity
FAR	Factor Analysis Information Risk
FRAA	Facilitated Risk Analysis and Assessment Process
FTA	Fault Tree Analysis
GSM	Global System for Mobile Communication
HIPS	Host Intrusion Prevention System
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
IOT	Internet of Things
IP	Internet Protocol
IRR	Internet Rate of Return
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
NAT	Network Address Translation
NFV	Net Future Value
NIPS	Network-based Intrusion Prevention System
NPV	Net Present Value
OCTAVE	Operationally Critical Threat Asset Vulnerability Evaluation
OSI	Open System Interconnection
P2P	Peer to Peer
PGP	Pretty Good Privacy
RAM	Random Access Memory
RBAC	Role Based Access Control
ROI	Return on Investment

ROSI	Return on Security Investment
RSA	Rivest Shamir Aldaman
SAW	Simple Addictive Weighting
SLE	Single Loss Expected
SPKI	Single Public Key Infrastracture
SPP	Static Payback Period
SSH	Secure Shell
TCP	Transmission Control Protocol
TTP	Techniques Tactics Procedures
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VOFI	Visualization of Financial Implications
VPN	Virtual Private Network
WIPS	Wireless Intrusion Prevention System