ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Διπλωματική Εργασία

Στα πλαίσια του διατμηματικού προγράμματος μεταπτυχιακών σπουδών «Οργάνωση και Διοίκηση για Μηχανικούς»

Με τίτλο:

Ανάλυση σύγχρονης δομής κυβερνοασφάλειας σε επιχειρήσεις

Νικολαΐδης Βασίλειος ΜΤΟ126

Επιβλέπων Καθηγητής: Ρομπογιαννάκης Ιωάννης

Πράγα 2022

ΠΕΡΙΛΗΨΗ

Το θέμα της παρούσας εργασίας είναι η ανάλυση της σύγχρονης δομής της κυβερνοασφάλειας σε επιχειρήσεις και αποτελείται από τρία κεφάλαια. Το πρώτο κεφάλαιο αφορά το διαδίκτυο όπου κάνοντας μια αναδρομή στο παρελθόν βλέπουμε την εξέλιξη στο πέρασμα των χρόνων ενώ στη συνέχεια αναφερόμαστε στο DNS, στη μορφή των διευθύνσεων αλλά και τη δομή του.

Στο δεύτερο κεφάλαιο αναφερόμαστε στο κυβερνοέγκλημα όπου δίνουμε τον ορισμό και τις κατηγορίες του ενώ εξετάζουμε τους ιούς και τα κακόβουλα λογισμικά τα οποία χρησιμοποιούνται ως εργαλεία για την διάπραξη των εγκλημάτων στον κυβερνοχώρο. Στο τρίτο και τελευταίο κεφάλαιο της εργασίας εξετάζουμε την κυβερνοασφάλεια στις επιχειρήσεις. Δίνουμε τον ορισμό της και τονίζουμε την σπουδαιότητα αλλά και την ανάγκη να υπάρχει κυβερνοασφάλεια στις επιχειρήσεις και τους οργανισμούς ενώ δίνουμε ιδιαίτερη βαρύτητα στην διοίκηση και στην οργανωτική δομή της. Επιπλέον παρουσιάζουμε το πλαίσιο της κυβερνοασφάλειας, τα βασικά του στοιχεία και τις λειτουργίες του. Τελειώνοντας γίνεται εκτενής αναφορά στους καίριους δείκτες απόδοσης που χρησιμοποιούνται για την αξιολόγηση των προγραμμάτων και συστημάτων που διαθέτουν οι εταιρείας για την Κυβερνοασφάλεια.

Λέξεις κλειδιά: Διαδίκτυο, κυβερνοέγκλημα, κυβερνοασφάλεια, επιχειρήσεις

ABSTRACT

The topic of the present thesis is the analysis of the contemporary structure of cybersecurity in businesses and it consists of three chapters. The first chapter is about internet where through retrospection in the past, we see its evolution through the years while we also refer to DNS, the form that internet addresses have and its structure.

In the second chapter we refer to cybercrime where we give its definition and divide it into categories whilst we examine viruses and malware that are used as tools by those who commit crimes on cyberspace. In the third and last chapter of our thesis, we examine cybersecurity in businesses. We provide its definition and highlight its importance and the necessity of its existence in businesses and organizations while giving the appropriate amount of attention to its management and infrastructure. Furthermore, we present cybersecurity framework, its basic components and functions. To end with, we refer thoroughly to the Key Performance Indicators which are used for the evaluation of security programs and systems businesses possess.

Key words: Internet, cybercrime, cybersecurity, businesses

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΛΛΗΝΙΚΟ ΜΕΣΟΓΕΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΕΥΧΑΡΙΣΤΙΕΣ

Στο σημείο αυτό θα ήθελα να ευχαριστήσω τον υπεύθυνο καθηγητή κ. Ιωάννη Ρομπογιαννάκη για την βοήθεια και κυρίως την υποστήριξη του καθ' όλη τη διάρκεια της συγγραφής της παρούσας εργασίας.

Θα ήθελα επίσης να ευχαριστήσω την σύζυγο μου Τερέζα για την υπομονή της και τη στήριξη που μου παρείχε από την αρχή της διαδρομής μου.

ΚΕΦΑΛΑΙΟ 1ο

ΔΙΑΔΙΚΤΥΟ

1.1 ΕΙΣΑΓΩΓΗ

Το διαδίκτυο αποτελεί μια από τις σημαντικότερες εφευρέσεις του 21ου αιώνα που έχουν επηρεάσει τη ζωή των ανθρώπων στο μέγιστο βαθμό. Στις μέρες μας το διαδίκτυο έχει υπερβεί κάθε εμπόδιο και έχει αλλάξει το τρόπο που μιλάμε, παίζουμε παιχνίδια, δουλεύουμε, ψωνίζουμε, κάνουμε φίλους, ακούμε μουσική, βλέπουμε ταινίες, παραγγέλνουμε φαγητό, πληρώνουμε λογαριασμούς, στέλνουμε ευχές στους φίλους μας, ενημερωνόμαστε και εκπαιδευόμαστε. Υπάρχει μια εφαρμογή για οτιδήποτε θέλεις να κάνεις. Έχει διευκολύνει τη ζωή μας κάνοντας την πιο άνετη. Οι μέρες που έπρεπε να περιμένουμε σε ατελείωτες ουρές για να πληρώσουμε τους λογαριασμούς μας έχουν ανήκουν πλέον στο παρελθόν καθώς τώρα μπορούμε να κάνουμε τις πληρωμές μας με το πάτημα ενός κουμπιού. Η τεχνολογία έχει προοδεύσει τόσο πολύ που δεν χρειαζόμαστε πλέον υπολογιστή για να χρησιμοποιήσουμε το διαδίκτυο. Τώρα έχουμε τα έξυπνα κινητά που μας δίνουν πρόσβαση στο διαδίκτυο και μας βοηθούν να μένουμε σε επαφή με τους φίλους και την οικογένειά μας 24 ώρες το 24ωρο.

Το διαδίκτυο δεν έχει απλά απλοποιήσει τη ζωή μας αλλά έχει βοηθήσει τη μεσαία τάξη να αποκτήσει πρόσβαση σε πολλά αγαθά κάνοντας τα πιο οικονομικά. Δεν έχει περάσει πολύς καιρός από τότε που τα τηλεφωνήματα κόστιζαν μια περιουσία και χρησιμοποιούνταν μόνο για εξαιρετικές περιπτώσεις ενώ η κύρια επικοινωνία γινόταν μέσω ταχυδρομείου. Πλέον με το διαδίκτυο μπορούμε όχι μόνο να συνομιλήσουμε αλλά μέσω διάφορων εφαρμογών να κάνουμε τηλε-διασκέψεις.

Το διαδίκτυο επίσης έχει αλλάξει το τρόπο χρήσης των συσκευών. Η τηλεόραση δεν χρησιμοποιείται μόνο για παρακολούθηση προγραμμάτων και ταινιών αλλά και για βιντεοκλήσεις με τους φίλους μας. Το κινητό δεν είναι μόνο για τηλεφωνικές κλήσεις αλλά και για την παρακολούθηση βίντεο και ταινιών. Μπορούμε να είμαστε συνδεδεμένοι με τους πάντες ανεξάρτητα από την τοποθεσία μας. Οι γονείς που δουλεύουν μπορούν να προσέχουν τα παιδιά τους στο σπίτι και να τα βοηθούν με τις ασκήσεις τους. Ένας επιχειρηματίας μπορεί να ελέγχει ανά πάσα στιγμή το προσωπικό

του με το πάτημα ενός κουμπιού. Το διαδίκτυο έχει διευκολύνει τη ζωή μας σε περισσότερα επίπεδα από ότι φανταζόμαστε.

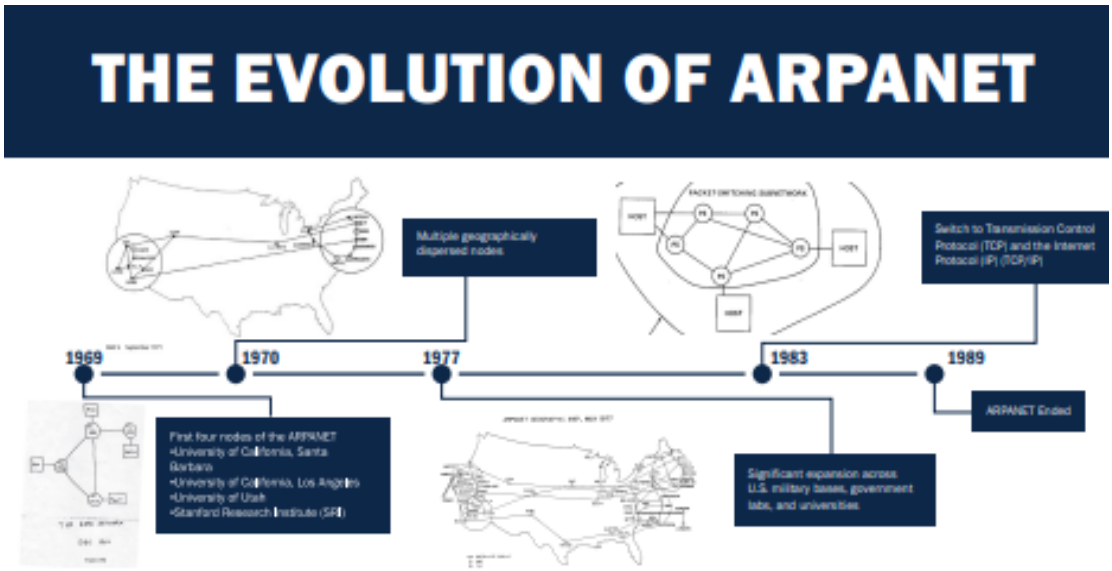
1.2 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Οι βάσεις του διαδικτύου τέθηκαν την περίοδο του ψυχρού πολέμου. Η Ρωσία εκτόξευσε τον πρώτο δορυφόρο στον κόσμο, τον SPUTNIK στις 4 Οκτωβρίου 1957. Αυτό το γεγονός ήταν ξεκάθαρα νίκη της Ρωσίας και ως αντίδραση οι Ηνωμένες Πολιτείες της Αμερικής ανακοίνωσαν τη δημιουργία του ARPANET στις αρχές του 1960. Ήταν ένα πειραματικό δίκτυο που σχεδιάστηκε για να κρατάει συνδεδεμένους όλους τους υπολογιστές ώστε να μπορούν να επικοινωνούν μεταξύ τους ακόμα και σε περίπτωση που κάποιος από τους κόμβους δεν μπορούσε να ανταποκριθεί εξαιτίας των βομβαρδισμών. Το πρώτο μήνυμα που στάλθηκε μέσω του ARPANET ήταν από το εργαστήριο του Leonard Kleinrock στο πανεπιστήμιο της Καλιφόρνιας στο Los Angeles (UCLA) και ήταν “LO”. Στην πραγματικότητα σκόπευαν να στείλουν την λέξη “LOGIN” αλλά μόνο τα δύο πρώτα γράμματα έφτασαν το προορισμό τους, το ινστιτούτο έρευνας του Stanford, καθώς πριν φτάσουν τα άλλα τρία γράμματα έπεσε το δίκτυο. Σύντομα η βλάβη αποκαταστάθηκε και το μήνυμα στάλθηκε ξανά (Jeetendra P.,2017).

Το βασικό μέλημα του ARPANET είναι να διαμορφώσει τους κανόνες της επικοινωνίας , τα πρωτόκολλα δηλαδή της επικοινωνίας μέσω αυτού. Το ARPANET συγκεκριμένα οδήγησε στην ανάπτυξη των πρωτοκόλλων της ενδοδικτύωσης, με την οποία πολλαπλά ξεχωριστά δίκτυα μπορούσαν να ενωθούν σε ένα δίκτυο δικτύων. Αυτό είχε ως αποτέλεσμα την ανάπτυξη της ακολουθίας πρωτοκόλλου TCP/IP που διευκρίνιζε τους κανόνες σύνδεσης και επικοινωνίας μέσω του APRANET. Πολύ σύντομα, το 1986 δημιουργήθηκε το NSF(Nnational Science Foundation) και τα κέντρα υπολογιστών πέντε πανεπιστημίων της Αμερικής ενώθηκαν για να δημιουργήσουν το δίκτυο NSFnet. Τα πέντε πανεπιστήμια που συμμετείχαν ήταν:

- Princeton University -- John von Neumann National Supercomputer Center JvNC
- Cornell University -- Cornell Theory Center, CTC

- University of Illinois at Urbana-Champaign -- National Center for Supercomputing Applications, NCSA
- Carnegie Mellon University -- Pittsburgh Supercomputer Center, PSC
- General Atomics -- San Diego Supercomputer Center, SDSC



Εικόνα 1. Η εξέλιξη του ARPAnet

Το NFSnet, ο διάδοχος του ARPAnet, έγινε δημοφιλές το 1990 και το ARPANET τέθηκε εκτός λειτουργίας. Υπήρχαν πολλά παράλληλα δίκτυα που αναπτύχθηκαν από άλλα πανεπιστήμια και άλλες χώρες όπως το Ηνωμένο Βασίλειο. Το 1965, το National Physical Laboratory(NPL) πρότεινε ένα δίκτυο μεταβίβασης δεδομένων με μεταγωγή κατά πακέτα. Το εκπαιδευτικό ερευνητικό κέντρο του Michigan δημιούργησε το δίκτυο MERIT το 1966 που είχε την υποστήριξη και χρηματοδότηση της πολιτείας του Michigan και του National Science Foundation (NSF). Η Γαλλία ανέπτυξε επίσης ένα δίκτυο μεταβίβασης δεδομένων με μεταγωγή κατά πακέτα, γνωστό ως CYCLADES το 1973. Υπήρχαν πλέον πολλά παράλληλα δίκτυα σε λειτουργία με διαφορετικά πρωτόκολλα και οι επιστήμονες προσπαθούσαν να βρουν κάποια κοινά στοιχεία ώστε να μπορέσουν να ενωθούν. Το 1978 ήταν έτοιμες οι ακολουθίες πρωτοκόλλου TCP/IP και μέχρι το 1983 είχαν υιοθετηθεί από το ARPANET.

Το 1981 έγινε η ενοποίηση δυο μεγάλων δικτύων. Το CSNET ενώθηκε με το ARPANET χρησιμοποιώντας την ακολουθία πρωτοκόλλου TCP/IP. Το δίκτυο δεν ήταν πλέον δημοφιλές μόνο στην επιστημονική κοινότητα αλλά και στους ιδιώτες που

είχαν αρχίσει να ενδιαφέρονται για το δίκτυο. Αρχικά το NFS υποστήριζε ταχύτητα 56 kbit/s αλλά το 1988 αναβαθμίστηκε σε 1.5 Mbit/s για να διευκολύνει την ανάπτυξη του δικτύου περιλαμβάνοντας και άλλα δίκτυα. Όταν οι συμμετέχοντες άρχισαν να καταλαβαίνουν τη δύναμη αυτού του δικτύου συνεργάστηκαν για την περαιτέρω ανάπτυξη του ώστε να δρέψουν τους καρπούς των προσπαθειών τους.

Στα τέλη του 1980 εμφανίστηκαν πολλοί πάροχοι υπηρεσιών διαδικτύου ώστε να παράσχουν τις υπηρεσίες δικτύου και απέκτησαν μεγάλη δημοφιλία. Για να διευκολυνθεί η εμπορική χρήση του διαδικτύου το NFSNET τέθηκε εντός λειτουργίας το 1995 και τώρα το διαδίκτυο μπορούσε να μεταφέρει εμπορική κίνηση ενώ όλο και περισσότερα πανεπιστήμια και ερευνητικά κέντρα ανά τον κόσμο συνδέθηκαν σε αυτό. Πλέον το διαδίκτυο ήταν πολύ δημοφιλές στην ερευνητική κοινότητα και το 1991 ιδρύθηκε το Διεθνές Ερευνητικό και Εκπαιδευτικό Δίκτυο και το World Wide Web ήταν πραγματικότητα (Jeetendra P.,2017).

Αρχικά, ο ρόλος του διαδικτύου περιοριζόταν στην μεταφορά αρχείων. Τα εύσημα για το διαδίκτυο όπως το γνωρίζουμε σήμερα ανήκουν στον Tim Berners-Lee που εισήγαγε το www. Με την έλευση του www, υπήρξε μια μεταμόρφωση στον τρόπο χρήσης του διαδικτύου. Τώρα αυτό το δίκτυο μπορούσε να χρησιμοποιηθεί για να βρεθούν όλες οι πληροφορίες που ήταν διαθέσιμες στο διαδίκτυο.

1.2.1 ΔΙΕΥΘΥΝΣΕΙΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Με τόσες συσκευές συνδεδεμένες στο διαδίκτυο χρειαζόμαστε κάποιου είδους μηχανισμό για να αναγνωρίζουμε κάθε συσκευή που είναι συνδεδεμένη σε αυτό. Επίσης χρειαζόμαστε κάποιο κεντρικό σύστημα που να φροντίζει αυτό τον μηχανισμό τα σήματα που χρησιμοποιούνται για την αναγνώριση αυτών των συσκευών να μην μπορούν να αντιγραφούν. Το σύστημα αυτό είναι γνωστό ως IANA (Internet Assigned Numbers Authority) και είναι υπεύθυνο για την απόδοση ενός μοναδικού αριθμού γνωστού ως διεύθυνση IP (Internet Protocol). Η διεύθυνση IP είναι ένας 32-bit δυαδικός αριθμός ο οποίος χωρίζεται σε 4 οκτάδες και κάθε οκτάδα αποτελείται από οκτώ δυαδικά ψηφία. Αυτές οι οκτάβες χωρίζονται από μια τελεία. Ένα παράδειγμα διεύθυνσης IP είναι η εξής:

11110110.01011010.10011100.1111100

Κάθε ψηφίο σε μια οκτάδα μπορεί να έχει δυαδική αξία για παράδειγμα 0 και 1. Επομένως κάθε οκτάδα μπορεί να έχει ελάχιστη αξία 0 π.χ. 00000000 και μέγιστη αξία 256 π.χ. 11111111 και συνολικά να έχει 2^8 = 256 διαφορετικούς συνδυασμούς (Jeetendra P.,2017).

Το να μπορέσει κάποιος όμως να θυμηθεί αυτόν τον αριθμό με τα 32 ψηφία είναι δύσκολο. Για αυτό το λόγο εκφράζεται σε δεκαδική μορφή. Βέβαια, η δεκαδική μορφή είναι μόνο για την καλύτερη κατανόηση των ανθρώπων καθώς ο υπολογιστής καταλαβαίνει μόνο τη δυαδική μορφή. Στη δεκαδική μορφή, η παραπάνω διεύθυνση IP εκφράζεται ως: 123.45.78.125.

Οι οκτάδες χρησιμοποιούνται για να δημιουργήσουν και να χωρίσουν διαφορετικές τάξεις. Μια διεύθυνση IP αποτελείται από δύο κομμάτια το δίκτυο και τον εξυπηρετητή. Το κομμάτι του δικτύου αναγνωρίζει το εκάστοτε δίκτυο και το κομμάτι του εξυπηρετητή αναγνωρίζει τη συσκευή του συγκεκριμένου δικτύου. Αυτή η διεύθυνση αναγνωρίζει μοναδικά τις συσκευές που είναι συνδεδεμένες στο δίκτυο όπως το ταχυδρομικό σύστημα όπου μπορούμε να αναγνωρίσουμε το κάθε σπίτι ξεκινώντας από τη χώρα, μετά την πολιτεία, την περιφέρεια, το υποκατάστημα του ταχυδρομείου και τέλος τον αριθμό του σπιτιού.

Αυτές οι διευθύνσεις IP χωρίζονται σε πέντε κατηγορίες ανάλογα με τη διαθεσιμότητα εύρους του IP, αν και μονάχα οι τρεις πρώτες κατηγορίες χρησιμοποιούνται. Οι κατηγορίες D,E εξυπηρετούν ερευνητικούς σκοπούς για την ώρα. Αυτές οι κατηγορίες είναι:

Κατηγορίες	**Εύρος διευθύνσεων**	**Υποστήριξη**
Κατηγορία A	1.0.0.1 to 126.255.255.254	Υποστηρίζει 16 εκατομμύρια εξυπηρετητές σε κάθε ένα από τα 127 δίκτυα
Κατηγορία B	128.1.0.1 to 191.255.255.254	Υποστηρίζει 16.000 εξυπηρετητές σε κάθε ένα από τα 16.000 δίκτυα
Κατηγορία C	192.0.1.1 to 223.255.254.254	Υποστηρίζει 254 εξυπηρετητές σε κάθε ένα από τα 2 εκατομμύρια δίκτυα

Κατηγορία D	224.0.0.0 to 239.255.255.255	Κρατούνται για ομάδες πολυεκπομπής
Κατηγορία E	240.0.0.0 to 254.255.255.254	Κρατούνται για μελλοντική χρήση ή για σκοπούς έρευνας και ανάπτυξης.

Λόγω της ευρείας εξάπλωσης του διαδικτύου και της δικτύωσης πολλαπλών συσκευών (Internet of Things) οι ανεπάρκεια των IP διευθύνσεων ήταν αναπόφευκτη. Για το λόγω αυτό αναπτύχθηκαν διάφορες μέθοδοι όπως ο διαχωρισμός μεταξύ δημοσίων και ιδιωτικών διευθύνσεων. Με αυτό τον τρόπο είναι δυνατή η επανάληψη των ίδιων διευθύνσεων από διαφορετικά ιδιωτικά δίκτυα. Η χρήση υποδικτύωσης(subnetting) και υπερδικτύωσης CIDR (Classless Inter-Domain Routing) και η έκδοση IPv6.

Υποδικτύωση είναι ο χωρισμός ενός μεγάλου δικτύου σε υποδίκτυα με μικρότερο εύρος τερματικών το καθένα. Ο λόγος που χρησιμοποιείται είναι για να αποφύγουμε τη σπατάλη διευθύνσεων δεσμεύοντας μία κλάση δικτύου μεγαλύτερη των απαιτήσεων μας. Πρακτικά, μία διεύθυνση IP αποτελείται από 32bit δυαδικά ψηφία. Τα πρώτα 16 αποτελούν την διεύθυνση δικτύου και τα επόμενα 16 τη διεύθυνση host. Όταν λοιπόν δεσμεύσουμε ψηφία από τη διεύθυνση host για τη μάσκα υποδικτύου, τότε δημιουργούμε υποδίκτυα τα οποία έχουν μικρότερο εύρος hosts καθώς τα ψηφία δεσμεύονται από την διεύθυνση host. Η αντίστροφη τεχνική ονομάζεται υπερδικτύωση και μπορεί να δημιουργήσει υπερδίκτυα, ομαδοποιώντας επιμέρους δίκτυα.

Η IANA έχει μοιράσει τις ευθύνες για την απόδοση των διευθύνσεων IP στα πέντε περιφερειακά μητρώα διαδικτύου (Regional Internet Registries (RIRs) που είναι υπεύθυνα για τη διανομή των διευθύνσεων στη ζώνη τους. Τα περιφερειακά μητρώα όπως επίσης η περιοχή της λειτουργίας τους αναφέρονται παρακάτω:

- APNIC- Αυτό το μητρώο είναι υπεύθυνο για την εξυπηρέτηση της περιοχής της Ασίας και του Ειρηνικού.
- AfriNIC- Αυτό το μητρώο είναι υπεύθυνο για την εξυπηρέτηση της περιοχής της Αφρικής
- ARIN- Αυτό το μητρώο είναι υπεύθυνο για την εξυπηρέτηση της Βόρειας Αμερικής και αρκετών νησιών της Καραϊβικής και του Βόρειου Ατλαντικού.
- LACNIC- Αυτό το μητρώο είναι υπεύθυνο για την εξυπηρέτηση της Λατινικής Αμερικής και της Καραϊβικής.

- RIPE NCC- Αυτό το μητρώο είναι υπεύθυνο για την εξυπηρέτηση της Ευρώπης, της Μέσης Ανατολής και τμημάτων της Κεντρικής Ασίας.

Για τη σωστή συνεργασία και το σωστό συντονισμό αυτών των μητρώων υπάρχει ένας οργανισμός που ονομάζεται NRO (Number Resource Organization)

1.2.2 DNS

Κάθε φορά που περιηγούμαστε στο διαδίκτυο, πληκτρολογούμε κάτι όπως https://en.wikipedia.org/ και πολύ σπάνια ασχολούμαστε με την διεύθυνση IP όπως http://208.80.154.224/ αλλά η αλήθεια είναι πως αν πληκτρολογήσουμε http://208.80.154.224/ στο URL θα μας βγάλει στην ίδια ιστοσελίδα. Γεγονός είναι πως νιώθουμε πιο άνετα να χρησιμοποιούμε και να θυμόμαστε ονόματα αντί να θυμόμαστε αριθμούς. Επιπλέον, αυτές οι διευθύνσεις αλλάζουν ανά διαστήματα και κάποιες από τις ιστοσελίδες έχουν πολλαπλές διευθύνσεις IP. Επίσης, η μεταφορά των δεδομένων μέσω διαδικτύου είναι εφικτή μόνο με τη χρήση της διεύθυνσης IP καθώς η δρομολόγηση του πακέτου των δεδομένων γίνεται μόνο μέσω αυτής. Υπάρχει ένας διακομιστής (Server) που ονομάζεται Domain Name Systems (DNS) που φροντίζει να γίνει πιο απλή αυτή η διαδικασία και μας γλυτώνει από το να θυμόμαστε τις διευθύνσεις που αλλάζουν (Αλεξόπουλος, 2010).

Ο υπολογιστής κρατάει αρχείο των ιστοσελίδων που επισκεφτήκαμε πρόσφατα και διατηρεί μια βάση δεδομένων στην κρυφή μνήμη του DNS του υπολογιστή. Σε περίπτωση που η διεύθυνση IP της ιστοσελίδας που ζητήσαμε δεν βρίσκεται στο DNS cache του υπολογιστή, τότε το επόμενο πιθανό μέρος να την βρει είναι στο διακομιστή DNS του παρόχου ίντερνετ (ISP). Αυτοί οι διακομιστές DNS του παρόχου ίντερνετ διατηρούν επίσης τη κρυφή μνήμη των ιστοσελίδων που επισκεφτήκαμε πρόσφατα. Σε περίπτωση που οι πληροφορίες δεν βρίσκονται ούτε εκεί, ο διακομιστής DNS του ISP προωθεί το αίτημα στους ριζικούς διακομιστές. Υπάρχουν 13 ριζικοί διακομιστές:

- VeriSign Global Registry Services
- University of Southern California - Information Sciences Institute
- Cogent Communications
- University of Maryland
- NASA Ames Research Center
- Internet Systems Consortium, Inc.

- U.S. DOD Network Information Center
- U.S. Army Research Lab
- Autonomica/NORDUnet
- VeriSign Global Registry Services
- RIPE NCC
- ICANN
- WIDE Project

1.2.3 Η ΔΟΜΗ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Το διαδίκτυο, όπως λέει το όνομα μου, είναι ένα δίκτυο δικτύων δηλαδή ένα σύνολο αρκετών μικρών, μεσαίων και μεγάλων δικτύων. Αυτό δείχνει ξεκάθαρα πως κανείς δεν μπορεί να είναι ο ένας και μοναδικός ιδιοκτήτης του διαδικτύου και είναι ένα έμπρακτο παράδειγμα το τι μπορεί να επιτύχει η συνεργασία. Ίσως είναι απορίας άξιο πως γίνεται ένα τόσο μεγάλο δίκτυο το οποίο εκτείνεται σε όλες τις ηπείρους να λειτουργεί χωρίς κανένα πρόβλημα. Για να ελεγχθεί λοιπόν ένα τόσο μεγάλο δίκτυο, απαιτείται να υπάρχει ένα διεθνές σώμα που να διαμορφώνει τους κανόνες, τους κανονισμούς λειτουργίας και τα πρωτόκολλα ώστε να είναι δυνατή η χρήση του δικτύου. Επομένως, υπάρχει ένας διεθνής οργανισμός, γνωστός ως «Η κοινωνία του Διαδικτύου», ο οποίος ιδρύθηκε το 1992 για να ρυθμίζει αυτά τα θέματα (https://www.internetsociety.org).

Όταν δουλεύουμε από το σπίτι με τον υπολογιστή μας χωρίς να είμαστε συνδεδεμένοι στο διαδίκτυο, ο υπολογιστής είναι ένα αυτόνομο σύστημα. Όταν όμως συνδεόμαστε στο διαδίκτυο μέσω του μόντεμ τότε γινόμαστε μέρος του δικτύου. Ο πάροχος υπηρεσιών διαδικτύου είναι ο κρίκος που συνδέει το δίκτυο κορμού με τον χρήστη μέσω των σημείων πρόσβασης δικτύου (Network Access Points). Αυτά τα σημεία πρόσβασης παρέχονται από μεγάλες εταιρείες τηλεπικοινωνιών σε διάφορες περιοχές. Είναι αυτές οι εταιρείες οι οποίες ενώνουν τις χώρες και τις ηπείρους με το να κατασκευάζουν και να συντηρούν την μεγάλη κεντρική υποδομή ώστε να γίνεται η μεταφορά των δεδομένων από το ένα σημείο πρόσβασης στο άλλο.

ΚΕΦΑΛΑΙΟ 2ο

ΚΥΒΕΡΝΟ- ΕΓΚΛΗΜΑ

2. ΓΕΝΙΚΑ

Το κυβερνό-έγκλημα δεν είναι τόσο παλιό όσο άλλα είδη εγκλήματος και ορίζεται ως οποιαδήποτε εγκληματική ενέργεια που λαμβάνει χώρα μέσω υπολογιστών, μέσω διαδικτύου ή οποιαδήποτε άλλη τεχνολογία όπως αυτή ορίζεται με τον νόμο τεχνολογίας πληροφοριών. Το κυβερνό-έγκλημα μπορεί όχι μόνο να προκαλέσει μεγάλες απώλειες στη κοινωνία και στην κυβέρνηση αλλά επιτρέπει σε αυτούς που το διαπράττουν να αποκρύπτουν σε μεγάλο βαθμό την ταυτότητά τους.

Υπάρχουν πολλές παράνομες δραστηριότητες οι οποίες διαπράττονται μέσω διαδικτύου από τεχνικά κατηρτισμένους εγκληματίες. Θα μπορούσε λοιπόν να ειπωθεί πως το κυβερνό-έγκλημα περιλαμβάνει κάθε παράνομη δραστηριότητα όπου ο υπολογιστής ή το διαδίκτυο είναι είτε εργαλείο, είτε ο στόχος είτε και τα δυο. Το κυβερνό-έγκλημα έχει γίνει μια ανεξέλεγκτη μάστιγα που βασίζεται στην λανθασμένη χρήση της αυξανόμενης εξάρτησης από τους υπολογιστές.

Η χρήση των υπολογιστών και άλλων συναφών τεχνολογιών στην καθημερινή ζωή αυξάνεται ραγδαία και δημιουργεί την επίσης αυξανόμενη ανάγκη για διευκόλυνση των χρηστών. Το διαδίκτυο είναι ένα μέσο το οποίο δεν μπορεί να μετρηθεί και δεν έχει όρια και παρόλο εξυπηρετεί και διευκολύνει σε μεγάλο βαθμό την ζωή των ανθρώπων, έχει και την σκοτεινή του πλευρά.

Μερικά από νέο-εμφανιζόμενα κυβερνό-εγκλήματα είναι παρακολούθηση μέσω διαδικτύου (cyber-stalking), τρομοκρατία μέσω διαδικτύου (cyber-terrorism), πλαστογράφηση ηλεκτρονικού ταχυδρομείου (email spoofing), διαδικτυακή πορνογραφία (cyber pornography) και άλλα. Κάποια «παραδοσιακά εγκλήματα μπορούν επίσης να ανήκουν στην κατηγορία του κυβερνό-εγκλήματος αν διαπραχθούν μέσω υπολογιστή ή διαδικτύου(Chaubey K.R, 2012).

2.1 ΟΡΙΣΜΟΣ ΤΟΥ ΚΥΒΕΡΝΌ-ΕΓΚΛΉΜΑΤΟΣ

Σύμφωνα με την Britannica «Κυβερνό-έγκλημα είναι η χρήση υπολογιστή ως μέσου για την επίτευξη παράνομων ενεργειών όπως η διάπραξη απάτης, η διακίνηση παιδικής πορνογραφίας και πνευματικής περιουσίας, η κλοπή ταυτότητας ή η παραβίαση της ιδιωτικότητας.» Το κυβερνό-έγκλημα, ειδικά μέσω διαδικτύου, έχει αυξηθεί σημαντικά καθώς οι υπολογιστές παίζουν βασικό ρόλο στο εμπόριο, στην διασκέδαση και στην λειτουργία της εκάστοτε κυβέρνησης.

Εξαιτίας της αρχικής και εκτεταμένης υιοθέτησης των υπολογιστών και του διαδικτύου από τις Ηνωμένες Πολιτείες, πολλά από τα πρώτα θύματα αλλά και πολλοί από τους πρώτους κυβερνό-εγκληματίες ήταν Αμερικάνοι. Αλλά τον 21ο αιώνα δεν έχει μείνει κάποιος σε όλο τον κόσμο που να μην έχει έρθει αντιμέτωπος με το κυβερνό-έγκλημα με τον ένα τρόπο ή τον άλλο.

Οι νέες τεχνολογίες δημιουργούν νέες εγκληματικές ευκαιρίες αλλά λίγους νέους τύπους εγκλήματος. Αυτό που διαχωρίζει το κυβερνό-έγκλημα από την παραδοσιακή εγκληματική δραστηριότητα είναι αρχικά η χρήση του υπολογιστή. Όμως δεν αρκεί μόνο η τεχνολογία για τη διάκριση μεταξύ των διαφορετικών ειδών εγκληματικής δραστηριότητας. Οι εγκληματίες δεν χρειάζονται υπολογιστή για να διαπράξουν απάτη, να διακινήσουν παιδική πορνογραφία, να κλέψουν την ταυτότητα κάποιου ή να εισβάλλουν στην ιδιωτική του ζωή. Όλες αυτές οι δραστηριότητες προϋπήρχαν πολύ πριν προστεθεί η λέξη «κυβερνό» πριν τη λέξη έγκλημα. Το κυβερνό-έγκλημα αντιπροσωπεύει μια επέκταση της υπάρχουσας εγκληματικής συμπεριφοράς μαζί με ορισμένες νέες παράνομες δραστηριότητες.

Τα περισσότερα κυβερνό-εγκλήματα αποτελούν επίθεση σε πληροφορίες που αφορούν άτομα, επιχειρήσεις ή κυβερνήσεις. Παρόλο που οι επιθέσεις δεν γίνονται στο πραγματικό σώμα, γίνονται στο προσωπικό ή επιχειρησιακό ψηφιακό σώμα, που είναι το σύνολο των πληροφοριακών χαρακτηριστικών που ορίζουν τα άτομα και τις επιχειρήσεις στο διαδίκτυο. Με άλλα λόγια, στον ψηφιακό κόσμο, η εικονική μας ταυτότητα αποτελεί ουσιώδες στοιχείο της καθημερινότητας μας καθώς είμαστε ένα σύνολο αριθμών και αναγνωριστικών σε πολλαπλές βάσεις δεδομένων που ανήκουν στις κυβερνήσεις και στις επιχειρήσεις. Το κυβερνό-έγκλημα τονίζει την κεντρική θέση

που έχουν οι υπολογιστές στη ζωή μας όπως επίσης το πόσο εύθραυστα είναι τα φαινομενικά στερεά στοιχεία που απαρτίζουν την εικονική μας ταυτότητα.

Μια σημαντική πλευρά του κυβερνό-εγκλήματος είναι ο μη τοπικός του χαρακτήρας καθώς οι εγκληματικές πράξεις μπορούν να συμβούν σε δικαιοδοσίες που χωρίζονται από μεγάλες αποστάσεις. Αυτό αποτελεί μεγάλο πρόβλημα για την επιβολή του νόμου καθώς τα μέχρι τώρα τοπικά ή ακόμα και εθνικά εγκλήματα τώρα απαιτούν διεθνή συνεργασία.

Το κυβερνό-έγκλημα είναι απλά μια πιο πλούσια εκδοχή του χώρου όπου λαμβάνει χώρα μια τηλεφωνική συζήτηση μεταξύ δυο ανθρώπων. Καθώς το διαδίκτυο αποτελεί ένα αχανές δίκτυο, προσφέρει στους εγκληματίες πολλαπλές κρυψώνες τόσο στον πραγματικό κόσμο όσο και στον ψηφιακό. Ωστόσο, όπως οι άνθρωποι αφήνουν ίχνη πίσω τους όταν περπατούν, έτσι και οι κυβερνό-εγκληματίες αφήνουν στοιχεία για την ταυτότητα και την τοποθεσία τους παρόλες τις προσπάθειες του να καλύψουν τα ίχνη τους. Για να υπάρχει όμως η δυνατότητα να ακολουθήσουν οι αρμόδιες αρχές αυτά τα ίχνη θα πρέπει να επικυρωθούν οι διεθνείς συνθήκες για το κυβερνό-έγκλημα.

Το 1996, το Συμβούλιο της Ευρώπης μαζί με τους κυβερνητικούς αντιπροσώπους των Ηνωμένων Πολιτειών, του Καναδά και της Ιαπωνίας συνέταξαν μια προκαταρτική διεθνή συνθήκη που να περιλαμβάνει το ηλεκτρονικό έγκλημα. Σε όλο τον κόσμο, ομάδες που υπερασπίζονται τις κοινωνικές ελευθερίες αμέσως διαμαρτυρήθηκαν για τους όρους της συνθήκης που απαιτούσαν από τους παρόχους διαδικτύου να αποθηκεύουν πληροφορίες για τις συναλλαγές των πελατών τους και να τις αποκαλύπτουν όταν τους ζητηθεί. Παρόλα αυτά, οι εργασίες για την συνθήκη συνεχίστηκαν και στις 23 Νοεμβρίου 2001 η συνθήκη του Ευρωπαϊκού Συμβουλίου για το κυβερνοέγκλημα υπογράφτηκε από 30 χώρες. Η συνθήκη τέθηκε σε εφαρμογή το 2004. Το 2002 προτάθηκαν και συμπληρωματικά πρωτόκολλα για τις τρομοκρατικές δραστηριότητες και τα κυβερνοεγκλήματα ρατσισμού και ξενοφοβίας, τα οποία τέθηκαν σε εφαρμογή το 2006. Επιπλέον, διάφοροι εθνικοί νόμοι όπως ο πατριωτικός νόμος των Ηνωμένων Πολιτειών του 2001 έχουν επεκτείνει την εξουσία των οργάνων του νόμου ώστε να μπορούν να ελέγχουν και να προστατεύουν τα δίκτυα των υπολογιστών.

2.2 ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΤΟΥ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑΤΟΣ

Το άτομο που διαπράττει το κυβερνο-έγκλημα μπορεί να είναι εντός ή εκτός της επιχείρησης που δέχεται την επίθεση. Λαμβάνοντας αυτό υπόψη μπορούμε να κατηγοριοποιήσουμε το κυβερνοέγκλημα σε δύο τύπους:

Εσωτερική επίθεση: μια επίθεση στο δίκτυο του συστήματος των υπολογιστών από κάποιο άτομο που έχει εξουσιοδοτημένη πρόσβαση στο σύστημα είναι γνωστή ως εσωτερική επίθεση. Συνήθως γίνεται από δυσαρεστημένους υπαλλήλους ή εργολάβους. Το κίνητρο της επίθεσης μπορεί να είναι είτε η εκδίκηση είτε η απληστία. Είναι σχετικά εύκολο για κάποιον που δουλεύει μέσα στην εταιρεία να πραγματοποιήσει μια επίθεση καθώς γνωρίζει τις πολιτικές της εταιρείας, τις διαδικασίες, τη δομή του συστήματος των υπολογιστών και τον τρόπο που δουλεύει το σύστημα ασφαλείας ενώ είναι πολύ εύκολο να αποκτήσει πρόσβαση στο δίκτυο και να κλέψει ευαίσθητες πληροφορίες ή να «ρίξει» το σύστημα. Η εσωτερική επίθεση μπορεί να εμποδιστεί με τον σχεδιασμό και την εγκατάσταση στον οργανισμό ενός εσωτερικού συστήματος ανίχνευσης εισβολών (Jeetendra P.,2017).

Εξωτερική επίθεση: Όταν ο επιτιθέμενος είτε έχει προσληφθεί από κάποιον μέσα στην επιχείρηση ή είναι μια οντότητα εκτός αυτής τότε μιλάμε για εξωτερική επίθεση. Ο οργανισμός ή η επιχείρηση που έχει πέσει θύμα αυτής της επίθεσης μπορεί να έρθει αντιμέτωπη όχι μόνο με την οικονομική απώλεια αλλά και με την απώλεια της φήμης της. Ο επιτιθέμενος για να μπορέσει να πραγματοποιήσει την επίθεση αφού είναι εκτός της επιχείρησης συνήθως ανιχνεύει και συγκεντρώνει πληροφορίες που θα τον βοηθήσουν να επιτύχει τον στόχο του. Για την αποτροπή της επίθεσης θα πρέπει ο υπεύθυνος της ασφάλειας να είναι έμπειρος και κατηρτισμένος και θα πρέπει να ελέγχει και να αναλύει με προσοχή τα αρχεία καταγραφής των προγραμμάτων ασφαλείας τα οποία ανιχνεύουν εξωτερικές επιθέσεις.

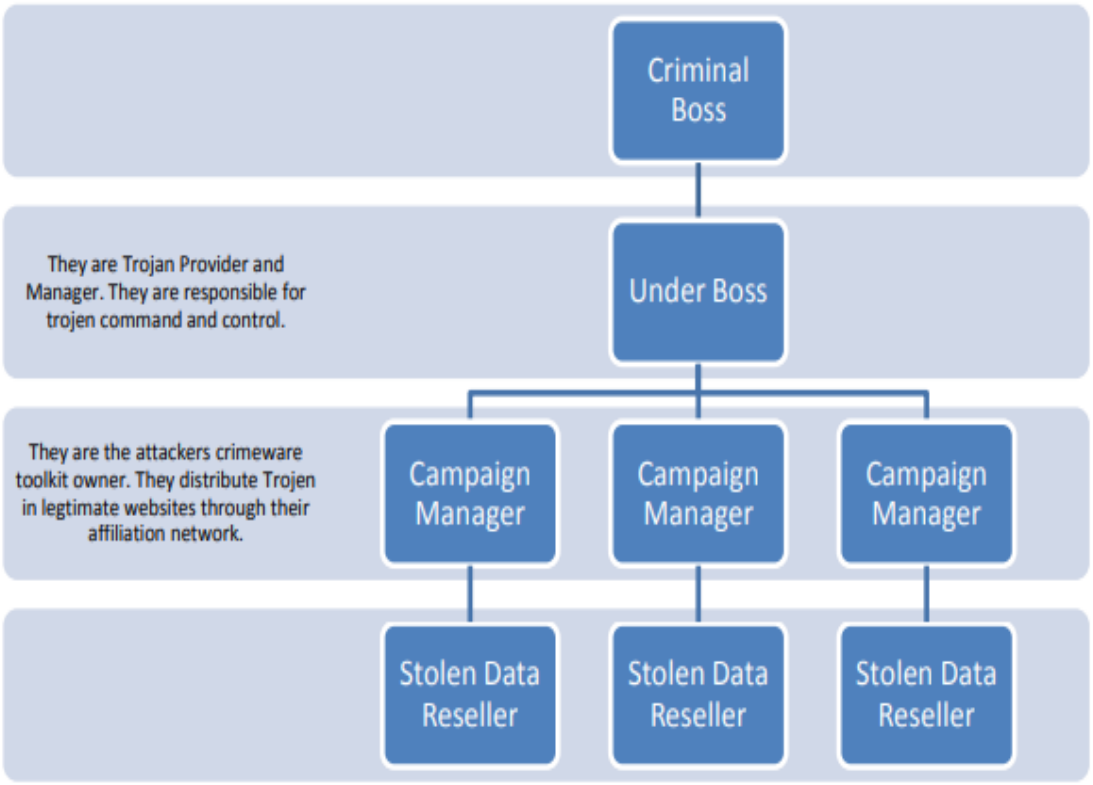
Οι κυβερνοεπιθέσεις μπορούν επίσης να κατηγοριοποιηθούν ως δομημένες και μη δομημένες επιθέσεις με βάση το επίπεδο ωριμότητας του επιτιθέμενου. Κάποιοι συγγραφείς θεωρούν πως αυτές οι επιθέσεις είναι είδος των εξωτερικών επιθέσεων αλλά υπάρχει προηγούμενο όπου μια δομημένη επίθεση έχει πραγματοποιηθεί από υπαλλήλους εντός των επιχειρήσεων. Αυτό μπορεί να συμβεί σε περιπτώσεις όπου μια ανταγωνίστρια επιχείρηση θελήσει να αποκτήσει τον μελλοντικά σχέδια της εταιρείας

και με στρατηγικό τρόπο καταφέρνει να αποκτήσει πρόσβαση στα επιθυμητά στοιχεία με το να τοποθετήσει κάποιον ως υπάλληλο.

Μη δομημένες επιθέσεις: Αυτές οι επιθέσεις γίνονται κυρίως από ερασιτέχνες που δεν έχουν κάποιο συγκεκριμένο κίνητρο και συνήθως θέλουν απλά να δοκιμάσουν κάποιο κακόβουλο λογισμικό που έχουν βρει έτοιμο στο διαδίκτυο στο δίκτυο μιας τυχαίας επιχείρησης.

Δομημένες επιθέσεις: Αυτού του είδους οι επιθέσεις γίνονται από εξαιρετικά έμπειρους και εξειδικευμένους ανθρώπους με ξεκάθαρα κίνητρα στο μυαλό τους. Έχουν πρόσβαση σε προηγμένα εργαλεία και τεχνολογίες που τους επιτρέπουν να αποκτήσουν πρόσβαση σε άλλα δίκτυα χωρίς να γίνουν αντιληπτοί από τα συστήματα ανίχνευσης εισβολών. Επιπλέον, αυτοί οι άνθρωποι έχουν την απαραίτητη εμπειρία για να αναπτύξουν ή να τροποποιήσουν τα υπάρχοντα εργαλεία ώστε να ικανοποιήσουν τον στόχο τους. Αυτές οι επιθέσεις γίνονται συνήθως από επαγγελματίες εγκληματίες, από μια χώρα σε άλλες χώρες, από πολιτικούς που θέλουν να αμαυρώσουν την εικόνα των αντιπάλων τους, από τρομοκράτες, ανταγωνιστικές εταιρείες κ.α.

Τα κυβερνοεγκλήματα έχουν αποδειχτεί μια επιχείρηση με χαμηλό ρίσκο και μικρή επένδυση που έχει όμως μεγάλα κέρδη. Στις μέρες μας, αυτά τα εγκλήματα είναι εξαιρετικά οργανωμένα καθώς υπάρχει μια τέλεια ιεραρχική οργάνωση όμως ακριβώς έχει μια εταιρεία ενώ κάποιες από αυτές τις οργανώσεις έχουν τέτοιο τεχνικό επίπεδο που συγκρίνεται με εκείνο ενός ανεπτυγμένου κράτους. Συνήθως στοχοποιούν μεγάλες οικονομικές επιχειρήσεις, αμυντικές και πυρηνικές εγκαταστάσεις ενώ ασχολούνται και ηλεκτρονικό εμπόριο ναρκωτικών.



Σχήμα 1. Ιεραρχία των εγκληματικών κυβερνό-οργανώσεων

Υπάρχουν κάποιοι κυβερνό-εγκληματίες που προσφέρουν τις υπηρεσίες τους όταν τους ζητηθεί και φυσικά επί πληρωμή. Το άτομο, η εταιρεία ακόμα και μια χώρα μπορεί να έρθει σε επαφή με αυτούς τους εγκληματίες και να τους ζητήσει να αποκτήσουν πρόσβαση σε κάποια ευαίσθητα δεδομένα ή να επιτεθούν στο σύστημα υπολογιστών των ανταγωνιστών τους. ανάλογα με την απαίτηση του πελάτη, οι χάκερς μπορεί να γράψουν τα αντίστοιχα κακόβουλα λογισμικά που ανταποκρίνονται στις ανάγκες τους.

2.3 ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΣΤΟΥΣ ΙΟΥΣ

Ο πρώτος ιός που δημιουργήθηκε ήταν το σκουλήκι creeper το 1971 από τον Robert H. Thomas έναν ερευνητή του Cambridge. Ο ιός αυτός ή για να είμαστε πιο ακριβείς το σκουλήκι, ήταν ένας πειραματικός ιός που είχε δημιουργηθεί για να μετακινείται μεταξύ των υπολογιστών που ήταν συνδεδεμένοι στο ARPANET, τον προκάτοχο του σημερινού διαδικτύου. Ο creeper χρησιμοποιώντας το σύστημα tenax μόλυνε τους

υπολογιστές και τους εκτυπωτές και εμφάνιζε το μήνυμα «I'M THE CREEPER: CATCH ME IF YOU CAN» (Feradhita NKD, 2020).

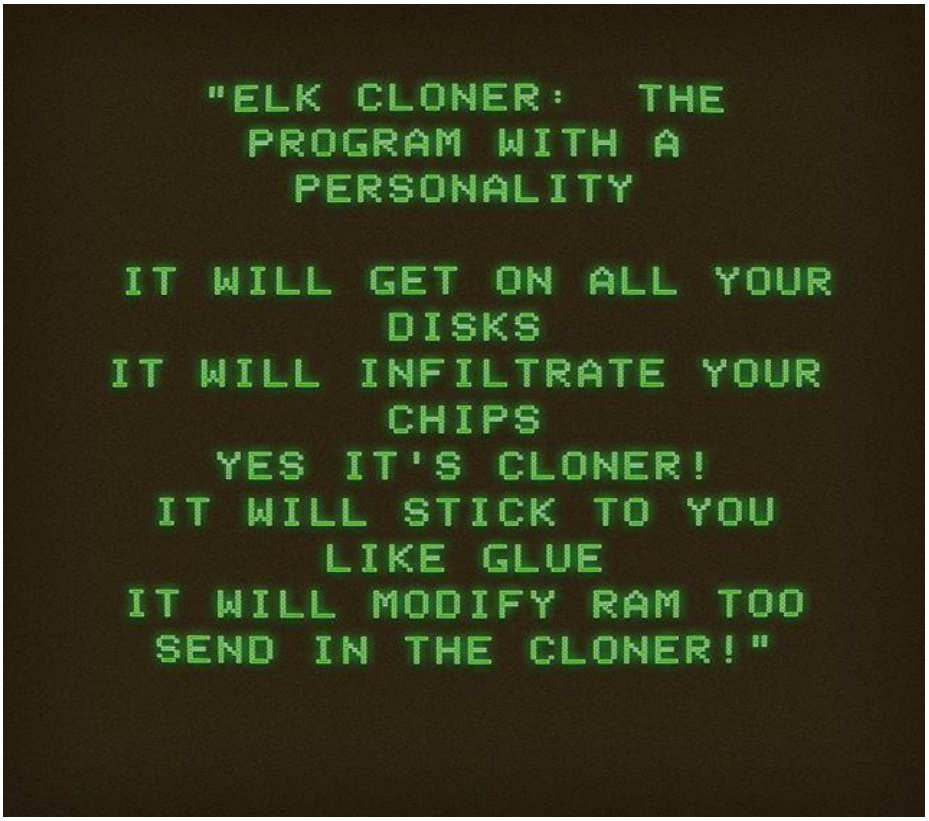
Εικόνα 2. Το μήνυμα το εμφανιζόταν στην οθόνη ενός υπολογιστή που είχε μολυνθεί με τον creeper

Στις 30 Ιανουαρίου 1982, ο δεκαπεντάχρονος Richard Skrenta έγραψε τον πρώτο ιό που μπορούσε να εξαπλωθεί σε μεγάλη κλίμακα. Ο "Elk Cloner" του Skrenta ήταν 400 γραμμές και ήταν μεταμφιεσμένο ως το λειτουργικό πρόγραμμα της Apple. Ο Skrenta είχε προσθέσει τον ιό του στο λειτουργικό σύστημα της Apple DOS 3.3 και αυτός μεταδιδόταν μέσω των δισκετών (Deffree S, 2019).

Εικόνα 3. Richard Skrenta

Ο Skrenta ήταν ήδη γνωστός φαρσέρ καθώς μοιραζόταν το λογισμικό πρόγραμμα των παιχνιδιών που έπαιζε αφού πρώτα τροποποιούσε τις δισκέτες με τέτοιο τρόπο ώστε να διακόπτεται το παιχνίδι με την εμφάνιση περιπαικτικών μηνυμάτων. Για να συνεχίσει τις φάρσες τους, ο Skrenta έπρεπε να βρει έναν τρόπο να τροποποιεί τις δισκέτες χωρίς να τις αγγίζει. Αυτό ήταν που τον οδήγησε στο να δημιουργήσει στον πρώτο ιό γνωστό πλέον ως Elk Cloner.

Ο Skrenta άφησε τον ιό του στο λειτουργικό σύστημα του σχολείου του και όποιος μαθητής δεν έκανε καθαρή εκκίνηση με τη δικιά του δισκέτα τώρα μπορούσε να μολυνθεί από τον κώδικα. Κάθε υπολογιστής που μολυνόταν, εμφάνιζε στην οθόνη ένα μικρό ποίημα.



Εικόνα 4. Το ποίημα που εμφανιζόταν στην οθόνη ενός υπολογιστή μολυσμένου με τον Elk Cloner

Ο Elk Cloner αποδείχτηκε πολύ μολυσματικός καθώς κατάφερε να μολύνει τις δισκέτες των περισσότερων ανθρώπων που γνώριζε ο Skrenta. Βέβαια, αυτό ήταν σχετικά εύκολο να γίνει το 1982 καθώς το να έχει κάποιος προσωπικό υπολογιστή ήταν κάτι νέο και πολλοί δεν είχαν γνώση των ιών και ούτε φυσικά υπήρχαν ειδικά προγράμματα ανίχνευσης ιών. Ο Elk Cloner μπορούσε να αφαιρεθεί αλλά απαιτούσε σημαντική χειρωνακτική προσπάθεια.

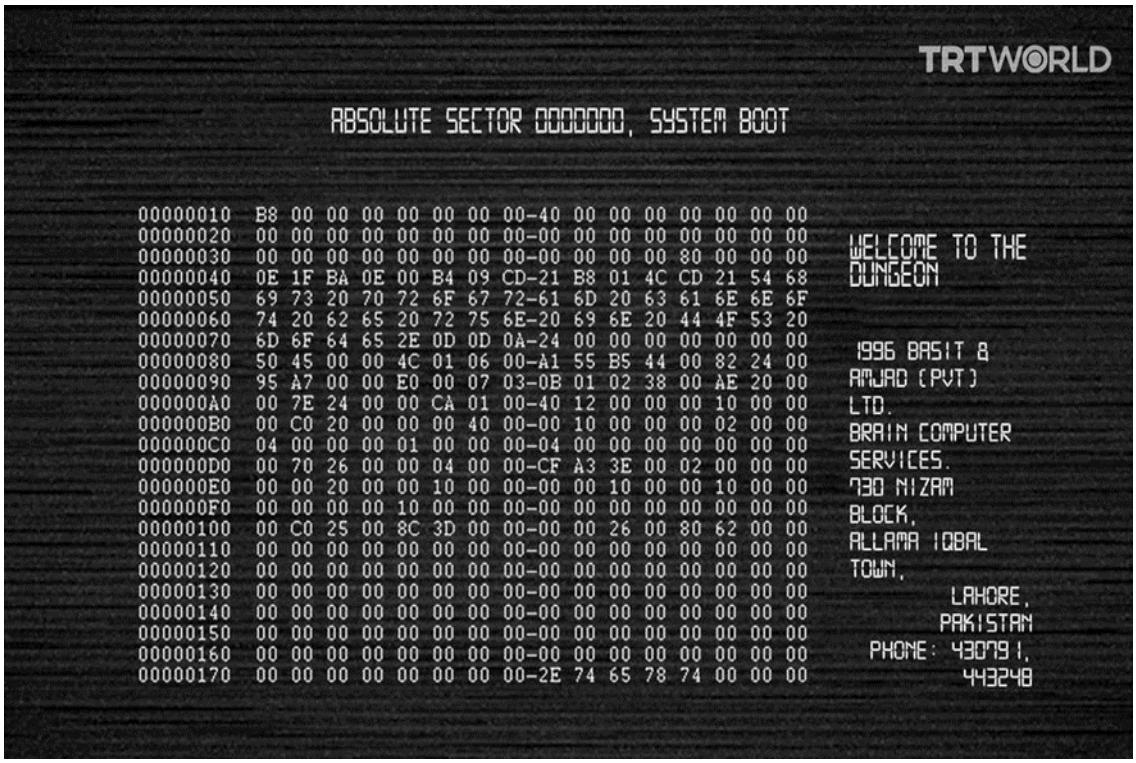
Ο όρος ιός υπολογιστή χρησιμοποιήθηκε το 1983 σε ένα σεμινάριο ασφάλειας(Deffree S,2019). Σε εκείνο το σεμινάριο ένας απόφοιτος του πανεπιστημίου της Νότιας Καλιφόρνια, ο Fred Cohen εισήγαγε μια δισκέτα σε έναν κεντρικό υπολογιστή για να δείξει στους παρευρισκόμενους πως ένας κώδικας που ήταν κρυμμένος σε ένα πρόγραμμα Unix μπόρεσε να εγκατασταθεί και να αναλάβει τον έλεγχο σε λίγα μόλις λεπτά, αναπαραγόμενος και εξαπλωμένος όπως ένας βιολογικός ιός (https://www.bbvaopenmind.com).

Αυτοί οι πρώτοι ιοί ήταν τεχνολογικές επιδείξεις. Το κίνητρο των δημιουργών τους ήταν η έρευνα και οι κώδικες δεν ήταν κακόβουλοι. Όπως τονίζει ο καθηγητής John

Aycock οι ιοί των υπολογιστών γεννήθηκαν ως φυσικό προϊόν της ανθρώπινης περιέργειας και επομένως η εφεύρεσή τους ήταν αναπόφευκτη.

2.3.1 ΟΙ ΠΡΩΤΟΙ ΚΑΚΟΒΟΥΛΟΙ ΚΩΔΙΚΕΣ

Οι πρώτοι κακόβουλοι κώδικες δεν άργησαν να εμφανιστούν. Το 1986, εμφανίστηκε ο Brain, ένας ιός που δημιουργήθηκε από δύο αδέρφια από το Πακιστάν και σκοπός τους ήταν να τιμωρήσουν τους χρήστες των υπολογιστών IBM που είχαν εγκαταστήσει ένα πειρατικό αντίγραφο του λογισμικού που είχαν δημιουργήσει οι ίδιοι. Ωστόσο, οι επιπτώσεις του Brain ήταν ελάχιστες και ο ιός περιείχε τα στοιχεία επικοινωνίας των δημιουργών ώστε αυτοί που είχαν μολυνθεί από τον ιό να μπορούν να επικοινωνήσουν μαζί τους και να ζητήσουν τη λύση.



Εικόνα 5. Ο ιός Brain

Με τη χρήση δισκετών, ο Brain εξαπλώθηκε διεθνώς, προκαλώντας τη δημιουργία των πρώτων εταιριών antivirus.

Στο τέλος του 1980, άρχισαν να αυξάνονται οι κώδικες που διέγραφαν δεδομένα ή κατέστρεφαν συστήματα. Το 1988, το «σκουλήκι» που δημιούργησε ο Robert Morris μόλυνε πολλούς από τους υπολογιστές των ερευνητικών ιδρυμάτων που ήταν

συνδεδεμένοι στο διαδίκτυο προκαλώντας τη παύση λειτουργίας των υπολογιστών. Υπολογίζεται πως 6.000 υπολογιστές από τους 60,000 συνολικά που ήταν συνδεδεμένοι στο ίντερνετ «χτυπήθηκαν» (https://www.fbi.gov).

Οι επιπτώσεις ήταν πιο σοβαρές από ότι περίμενε ο ίδιος ο Morris καθώς έγινε ο πρώτος άνθρωπος που κατηγορήθηκε στις Ηνωμένες Πολιτείες για παραβίαση του νόμου του 1986 για την ηλεκτρονική απάτη.

Εικόνα 6. Robert Morris

2.4 ΕΙΔΗ ΚΑΚΟΒΟΥΛΩΝ ΛΟΓΙΣΜΙΚΏΝ

Κακόβουλο λογισμικό είναι οποιοδήποτε πρόγραμμα ή αρχείο που μπορεί να βλάψει έναν υπολογιστή ή τον χρήστη του. Οι κοινοί τύποι κακόβουλου λογισμικού περιλαμβάνουν ιούς υπολογιστών, ransomware, «σκουλήκια», trojan horses και spyware. Αυτά τα κακόβουλα προγράμματα μπορούν να κλέψουν, να κωδικοποιήσουν ή να διαγράψουν ευαίσθητα δεδομένα, να αλλάξουν ή να υφαρπάξουν τις βασικές λειτουργίες του υπολογιστή και να παρακολουθούν την δραστηριότητα του θύματος στο διαδίκτυο.

Οι κυβερνό-εγκληματίες χρησιμοποιούν μια σειρά από φυσικά και ψηφιακά μέσα για να μολύνουν τις συσκευές και τα δίκτυα με κακόβουλα λογισμικά. Για παράδειγμα το

WannaCry, ένα γνωστό κακόβουλο λογισμικό ransomware κατάφερε να εξαπλωθεί εκμεταλλευόμενο ένα γνωστό τρωτό σημείο του συστήματος.

Εικόνα 7. Το ransomware WannaCry

Το ηλεκτρονικό ψάρεμα (Phishing) είναι μια ακόμα γνωστή μέθοδος παράδοσης λογισμικού όπου email τα οποία φαίνονται αξιόπιστα περιέχουν κακόβουλους συνδέσμους ή επισυναπτόμενα αρχεία τα οποία εκτελούν κακόβουλα λογισμικά στους ανυποψίαστους χρήστες(https://www.upguard.com).

Οι εξελιγμένες επιθέσεις με κακόβουλο λογισμικό χρησιμοποιούν ένα διακομιστή εντολών και ελέγχου που επιτρέπει στους επιτιθέμενους να επικοινωνούν με το σύστημα υπολογιστών που έχει μολυνθεί, να κλέβουν ευαίσθητες πληροφορίες από τον σκληρό δίσκο ή να αποκτούν απομακρυσμένη πρόσβαση στη συσκευή.

Καινούργια είδη κυβερνό-επίθεσης με τη χρήση κακόβουλων λογισμικών περιλαμβάνουν τεχνικές αποφυγής και σύγχυσης με σκοπό να ξεγελάσουν τους χρήστες, τους υπευθύνους ασφαλείας και τα προϊόντα αντιμετώπισης των κακόβουλων λογισμικών. Οι τεχνικές αποφυγής μπορεί να είναι απλές τακτικές για την απόκρυψη της διεύθυνσης IP και περιλαμβάνουν πολυμορφικό κακόβουλο λογισμικό που μπορεί να αλλάζει τον κώδικα του για να αποφύγει την ανίχνευση του από τα εργαλεία ανίχνευσης. Ένα ακόμα παράδειγμα είναι το κακόβουλο λογισμικό χωρίς αρχείο του βρίσκεται μόνο στη RAM του συστήματος για να αποφύγει την ανίχνευση.

Οι διάφοροι τύποι των κακόβουλων λογισμικών έχουν μοναδικά χαρακτηριστικά:

Ιοί υπολογιστών: ο ιός είναι ένα είδος κακόβουλου λογισμικού που όταν εκτελείται, αυτό- αντιγράφεται με το να τροποποιεί τα προγράμματα των υπολογιστών και εισάγει τον δικό τους κωδικό. Όταν η αντιγραφή είναι επιτυχής, τότε μπορούμε να πούμε πως οι περιοχές που επλήγησαν είναι μολυσμένες.

Οι συγγραφείς των ιών χρησιμοποιούν την κοινωνική μηχανική και εκμεταλλεύονται αδυναμίες για να μολύνουν τα συστήματα και να διαδώσουν τον ιό. Τα λειτουργικά συστήματα των Microsoft Windows και MAC αποτελούν τον στόχο των περισσοτέρων ιών που συχνά χρησιμοποιούν πολύπλοκες στρατηγικές για να αποφύγουν το antivirus λογισμικό.

Οι ιοί δημιουργούνται για τη δημιουργία κέρδους, για την αποστολή μηνύματος, για προσωπική ευχαρίστηση, για την κατάδειξη ύπαρξης αδυναμιών ενός συστήματος, για σαμποτάζ ή απλά για την εξερεύνηση θεμάτων κυβερνό-ασφάλειας, τεχνητής νοημοσύνης και επαναστατικών αλγόριθμων.

Οι ιοί μπορούν προκαλέσουν οικονομική ζημιά δισεκατομμυρίων δολαρίων προκαλώντας την πτώση του συστήματος, την διαφθορά των δεδομένων, την αύξηση κόστους συντήρησης, την κλοπή προσωπικών πληροφοριών όπως ο αριθμός της πιστωτικής κάρτας.

Σκουλήκι υπολογιστή: το σκουλήκι είναι αυτό-αναπαραγόμενο κακόβουλο πρόγραμμα που ο πρωταρχικός του στόχος είναι να μολύνει άλλους υπολογιστές με το να κλωνοποιείται ενώ είναι ενεργό σε μολυσμένα συστήματα. Συχνά, τα σκουλήκια χρησιμοποιούν τα δίκτυα των υπολογιστών για να εξαπλωθούν βασισμένα στις αδυναμίες ή στις ελλείψεις ασφάλειας του συστήματος. Τα σκουλήκια σχεδόν πάντα προκαλούν κάποια ζημιά στο δίκτυο ακόμα και αυτό είναι ευρυζωνικό σε αντίθεση με τους ιούς που πάντα διαβρώνουν ή τροποποιούν αρχεία του υπολογιστή.

Επίσης, ενώ πολλά σκουλήκια είναι σχεδιασμένα μόνο για να εξαπλώνονται χωρίς να αλλάζουν τα συστήματα από τα οποία περνάνε, ωστόσο μπορούν να προκαλέσουν σημαντική αναστάτωση. Το σκουλήκι Morris και το Mydoom προκάλεσαν μεγάλη αναστάτωση καθώς αύξησαν την κίνηση του δικτύου παρά την καλοήθη φύση τους.

Trojan Horse:

Το trojan horse ή απλά trojan είναι οποιοδήποτε κακόβουλο λογισμικό που παραπλανάει τους χρήστες για τις πραγματικές του προθέσεις καθώς εμφανίζεται ως

αξιόπιστο πρόγραμμα. Αυτός ο όρος προέρχεται από την αρχαία ελληνική ιστορία όπου ο παραπλανητικός Δούρειος Ίππος οδήγησε στην πτώση της Τροίας.

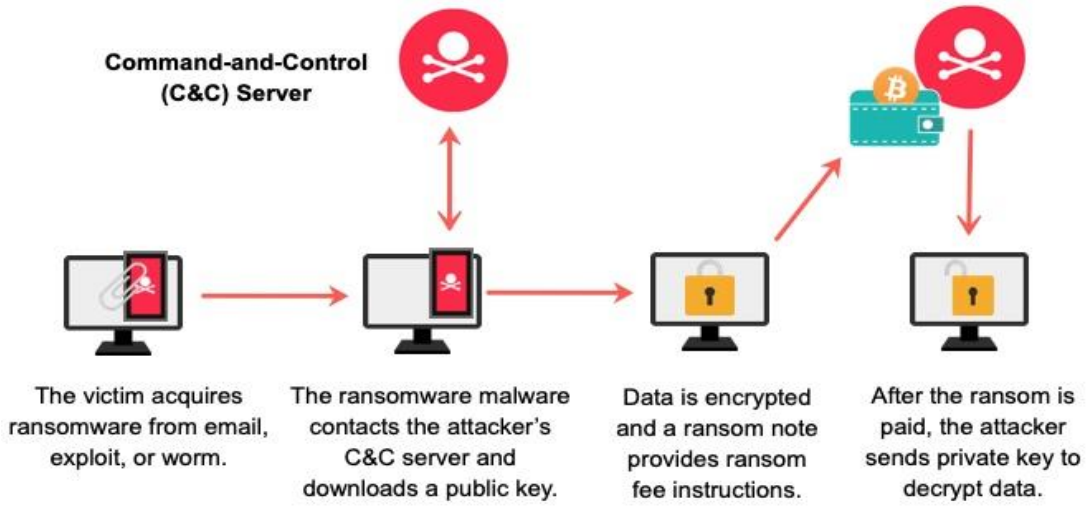
Τα trojans συνήθως εξαπλώνονται με την κοινωνική μηχανική όπως το ηλεκτρονικό ψάρεμα (phishing). Παρόλο που το ωφέλιμο φορτίο ενός trojan μπορεί να είναι οτιδήποτε, συνήθως δρα ως κερκόπορτα που επιτρέπει στον επιτιθέμενο να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στον μολυσμένο υπολογιστή. Τα trojans μπορούν να δώσουν πρόσβαση σε προσωπικές πληροφορίες όπως η διαδικτυακή δραστηριότητα και οι κωδικοί πρόσβασης στην τράπεζα. Τα trojans μπορούν να χρησιμοποιηθούν για επιθέσεις ransomware. Σε αντίθεση με τους ιούς και τα σκουλήκια, τα trojans γενικά δεν προσπαθούν να εισάγουν κακόβουλους κώδικες σε άλλα αρχεία ή να αναπαραχθούν.

Rootkits

Το rootkit είναι ένα σύνολο κακόβουλων προγραμμάτων που είναι σχεδιασμένο να δίνει μη εξουσιοδοτημένη πρόσβαση σε ένα υπολογιστή ή σε ένα τμήμα του λογισμικού και πολύ συχνά καλύπτει την ύπαρξη του ή την ύπαρξη άλλων λογισμικών. Η εγκατάσταση του rootkit μπορεί να γίνει αυτόματα ή από τον ίδιο τον επιτιθέμενο αν έχει πρόσβαση διαχειριστή.

Η ανίχνευση του rootkit είναι δύσκολη καθώς μπορεί να υπονομεύσει το πρόγραμμα antivirus που υπάρχει εγκατεστημένο. Η απομάκρυνση μπορεί να είναι επίσης πολύπλοκη ή πρακτικά αδύνατη, ειδικά όταν τα rootkits βρίσκονται στον πυρήνα.

Ransomware: το ransomware είναι μια μορφή κακόβουλου λογισμικού που έχει σχεδιαστεί να απαγορεύει την πρόσβαση σε ένα σύστημα υπολογιστή ή σε δεδομένα μέχρι να πληρωθούν λύτρα. Το ransomware εξαπλώνεται μέσω ηλεκτρονικού ψαρέματος, κακόβουλης διαφήμισης, μολυσμένων ιστοσελίδων ή εκμετάλλευσης αδυναμιών του συστήματος. Οι επιθέσεις ransomware μπορούν να προκαλέσουν διακοπές, διαρροή πληροφοριών, κλοπή πνευματικής ιδιοκτησίας και παραβίαση δεδομένων. Το ποσό των λύτρων κυμαίνεται από μερικές εκατοντάδες δολάρια σε εκατοντάδες χιλιάδες δολάρια και η πληρωμή γίνεται σε κρυπτονομίσματα όπως το Bitcoin (Kapoor,2022).



Εικόνα 8. Ransomware

Keyloggers: οι keyloggers είναι ένα είδος κακόβουλου λογισμικού που χρησιμοποιείται για την παρακολούθηση και την καταγραφή κάθε πληκτρολόγησης στο πληκτρολόγιο ενός συγκεκριμένου υπολογιστή. Υπάρχουν keyloggers και για τα έξυπνα τηλέφωνα (smartphones). Οι keyloggers αποθηκεύουν τις πληροφορίες που έχουν συγκεντρώσει και τις στέλνουν στον επιτιθέμενο ο οποίος μπορεί να βρει ευαίσθητες πληροφορίες όπως οι κωδικοί πρόσβασης σε τραπεζικούς λογαριασμούς ή τα στοιχεία πιστωτικών καρτών (https://www.getcert.gr).

Grayware: ο όρος grayware επινοήθηκε τον Σεπτέμβριο 2004 και περιγράφει ανεπιθύμητες εφαρμογές και αρχεία που ενώ δεν είναι κακόβουλα, δυσχεραίνουν την απόδοση του υπολογιστή και μπορούν να αποτελέσουν κίνδυνο για την κυβερνό-ασφάλεια. Στην καλύτερη περίπτωση, το grayware συμπεριφέρεται με έναν ενοχλητικό ή ανεπιθύμητο τρόπο ενώ στη χειρότερη περίπτωση παρακολουθεί το σύστημα και συλλέγει πληροφορίες. Το grayware θυμίζει τα adware και spyware αλλά ευτυχώς τα περισσότερα λογισμικά antivirus μπορούν να ανιχνεύσουν πιθανόν ανεπιθύμητα προγράμματα και να τα διαγράψουν. Γενικά τα adware και spyware είναι εύκολο να αφαιρεθούν καθώς δεν είναι τόσο μοχθηρά όσο τα άλλα είδη κακόβουλου λογισμικού. Η μεγαλύτερη ανησυχία είναι ο μηχανισμός που χρησιμοποιεί το grayware για να αποκτήσει πρόσβαση στον υπολογιστή που είναι η κοινωνική μηχανική ή μέσω αδυναμιών του συστήματος, που είναι ένας μηχανισμός ο οποίος χρησιμοποιείται και από άλλα κακόβουλα λογισμικά.

Fileless Malware: το fileless malware είναι ένα είδος λογισμικού που χρησιμοποιεί αξιόπιστα προγράμματα για να μολύνει έναν υπολογιστή. Σε αντίθεση με τις μολύνσεις από άλλα κακόβουλα λογισμικά, δεν εξαρτάται από αρχεία και δεν αφήνει ίχνη, με αποτέλεσμα να είναι εξαιρετικά δύσκολη η ανίχνευση του και κατά συνέπεια η αφαίρεση του. Υπάρχει αποκλειστικά στη μνήμη του υπολογιστή για παράδειγμα στη RAM.

Το Fileless malware εμφανίστηκε το 2017 ως κυρίαρχη κυβερνό-απειλή αλλά υπήρχε για αρκετό καιρό πριν. 'Frodo', 'Number of the Beast' και ο 'Dark Avenger' ήταν από τις πρώτες επιθέσεις fileless malware. Πρόσφατα, η Δημοκρατική Εθνική Επιτροπή έπεσε θύμα επίθεσης αυτού του κακόβουλου λογισμικού.

Το Fileless malware δεν αφήνει ίχνη της δραστηριότητας του στον σκληρό δίσκο του υπολογιστή και έτσι είναι πολύ δύσκολο να ανιχνευτεί. Τα στοιχεία που αφήνει είναι ελάχιστα ως μηδαμινά με αποτέλεσμα να μην μπορούν οι ειδικοί να ανακαλύψουν κάποια παράνομη ενέργεια.

Εικόνα 9. Πως λειτουργεί το Fileless Malware

Adware: το adware ή λογισμικό διαφήμισης είναι ένα είδος grayware που έχει σχεδιαστεί να εμφανίζει διαφημίσεις στην οθόνη του υπολογιστή ή του τηλεφώνου. Τυπικά διαχωρίζεται σε αξιόπιστες διαφημίσεις ή σε διαφημίσεις άλλου προγράμματος που σε ξεγελά ώστε να το εγκαταστήσεις στον υπολογιστή, στο tablet ή στο κινητό σου τηλέφωνο.

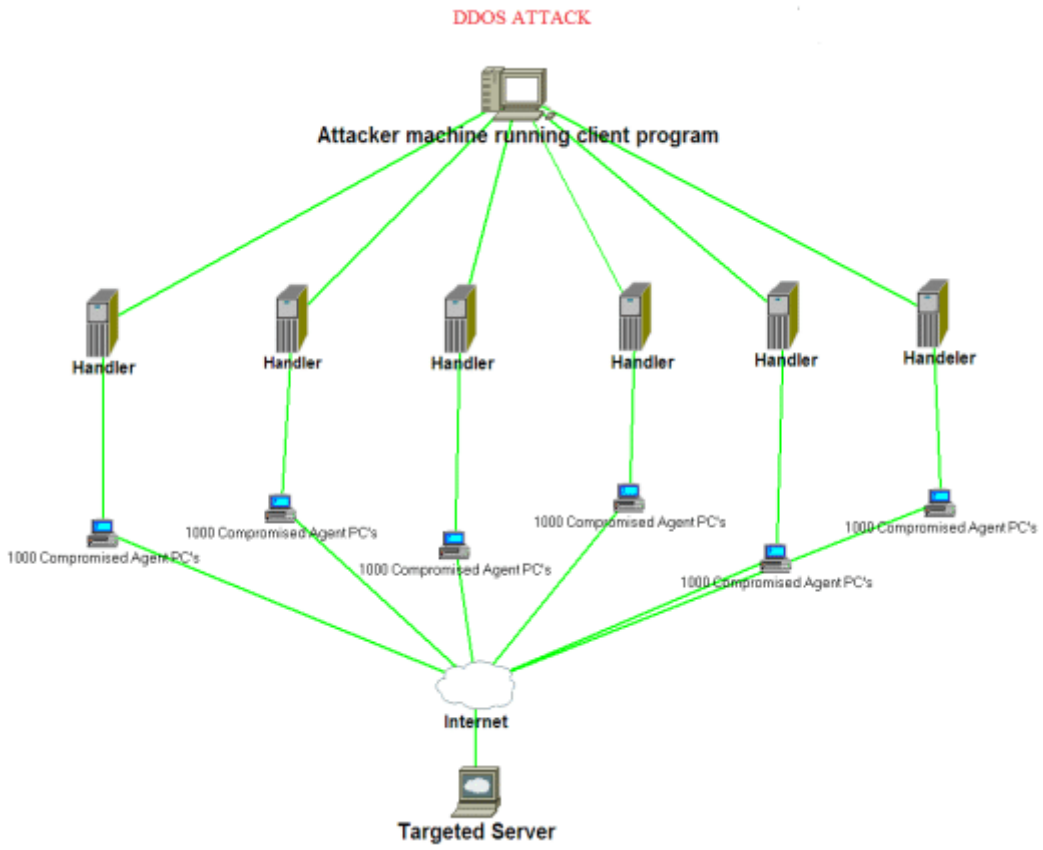
Το adware είναι από τα πιο επικερδή και τα λιγότερο επιβλαβή είδη κακόβουλου λογισμικού και γίνεται όλο και πιο δημοφιλές στις συσκευές κινητών τηλεφώνων. Το adware παράγει κέρδος με την αυτόματη εμφάνιση διαφημίσεων στον χρήστη του λογισμικού.

Malvertising: ο όρος malvertising προέρχεται από τις λέξεις malicious (επιβλαβής) και advertising (διαφήμιση) και είναι η χρήση της διαφήμισης για τη διασπορά κακόβουλου λογισμικού. Συνήθως περιλαμβάνει την εισχώρηση επιβλαβών διαφημίσεων σε αξιόπιστα διαφημιστικά δίκτυα και ιστοσελίδες. Η διαφήμιση είναι ένας καταπληκτικός τρόπος να εξαπλωθεί ένα κακόβουλο λογισμικό καθώς απαιτείται μεγάλη προσπάθεια για να προσελκύσουν οι διαφημίσεις τους χρήστες ώστε να πουλήσουν ή να διαφημίσουν ένα προϊόν. Το malvertising επωφελείται επίσης από τη φήμη των ιστοσελίδων στις οποίες βρίσκεται ειδικά όταν πρόκειται για ευυπόληπτες ιστοσελίδες ειδησεογραφικών πρακτορείων.

Spyware: το spyware είναι ένα κακόβουλο λογισμικό το οποίο συγκεντρώνει πληροφορίες για ένα άτομο ή για έναν οργανισμό, συχνά χωρίς να το γνωρίζουν, και στέλνει τις πληροφορίες αυτές στον επιτιθέμενο χωρίς την συγκατάθεση του θύματος. Το spyware συνήθως έχει ως στόχο την ανίχνευση και την πώληση των δεδομένων χρήση του διαδικτύου, την κλοπή των στοιχείων της πιστωτικής κάρτας ή του τραπεζικού λογαριασμού. Μερικά είδη spyware μπορεί να εγκαταστήσουν επιπλέον λογισμικό και να αλλάξουν τις ρυθμίσεις της συσκευής. Το spyware είναι συνήθως εύκολο να αφαιρεθεί καθώς δεν είναι τόσο κακοήθες όσο τα άλλα είδη κακόβουλου λογισμικού.

Bots and Botnets: Bot είναι ένας υπολογιστής που έχει μολυνθεί από κακόβουλο λογισμικό και έτσι μπορεί ο επιτιθέμενος να τον ελέγχει από απόσταση. Τότε το bot μπορεί να χρησιμοποιηθεί ώστε να εξαπολυθούν και άλλες κυβερνό-επιθέσεις ή μπορεί να γίνει μέρος ενός botnet (δίκτυο bots).

Τα botnets είναι μια δημοφιλής μέθοδος για επιθέσεις άρνησης υπηρεσιών, διασπείροντας ransomware, keyloggers και άλλα είδη κακόβουλου λογισμικού.



Εικόνα 10. Παράδειγμα επίθεσης άρνησης υπηρεσιών

Backdoor: Backdoor είναι μια συγκαλυμμένη μέθοδος παράκαμψης της τυπικής αυθεντικοποίησης ή κωδικοποίησης που υπάρχει σε έναν υπολογιστή, σε ένα προϊόν ή σε κάποιο άλλο μέρος του υπολογιστή. Τα backdoors χρησιμοποιούνται για την απόκτηση απομακρυσμένης πρόσβασης σε ένα υπολογιστή ή σε κρυπτογραφημένα αρχεία. Στη συνέχεια χρησιμοποιούνται για αποκτήσουν πρόσβαση, να διαφθείρουν, να διαγράψουν ή να μεταφέρουν ευαίσθητα δεδομένα.

Τα backdoors μπορούν να πάρουν τη μορφή του κρυμμένου τμήματος ενός προγράμματος ή ενός ξεχωριστού προγράμματος ή κώδικα στα λειτουργικά συστήματα. Πολλά από τα backdoors χρησιμοποιούνται και για νόμιμους λόγους όπως σε περιπτώσεις που ο κατασκευαστής χρειάζεται ένα τρόπο να ξαναρυθμίσει τους κωδικούς χρήστη.

Browser Hijacker: ο browser hijacker αλλάζει τη συμπεριφορά του προγράμματος περιήγησης στέλνοντας τον χρήστη σε μια καινούργια σελίδα, αλλάζοντας την αρχική σελίδα, εγκαθιστώντας ανεπιθύμητες γραμμές εργαλείων, δείχνοντας ανεπιθύμητες διαφημίσεις ή κατευθύνοντας το χρήστη σε διαφορετική ιστοσελίδα.

Crimeware: το Crimeware είναι ένα είδος κακόβουλου λογισμικού που σχεδιάστηκε για να αυτοματοποιεί το κυβερνό-έγκλημα. Σχεδιάστηκε για τη διάπραξη κλοπής ταυτότητας μέσω της κοινωνικής μηχανικής και για την απόκτηση πρόσβασης σε οικονομικούς λογαριασμούς και σε οικονομικές συναλλαγές για την υπεξαίρεση πόρων ή για την πραγματοποίηση μη εξουσιοδοτημένων συναλλαγών. Εναλλακτικά, μπορεί να κλέψει εμπιστευτικές ή ευαίσθητες πληροφορίες ως τμήμα της βιομηχανικής κατασκοπείας.

RAM Scraper: το RAM scraper είναι ένα είδος κακόβουλου λογισμικού που συλλέγει τα δεδομένα που αποθηκεύονται προσωρινά στη RAM. Αυτού του είδους το λογισμικό συνήθως στοχεύει συστήματα POS καθώς μπορούν να αποθηκεύουν τα νούμερα των πιστωτικών καρτών χωρίς κωδικοποίηση για ένα σύντομο χρονικό διάστημα προτού κωδικοποιηθούν.

Rogue Security Software: το Rogue security software ξεγελάει τον χρήστη και τον κάνει να πιστεύει πως το σύστημά του έχει κάποιο πρόβλημα ασφάλειας όπως έναν ιό και τον πείθει να πληρώσει για να επιδιορθωθεί.

Εικόνα 11. Ψεύτικη προειδοποίηση

Στην πραγματικότητα αυτό που πρέπει να αφαιρεθεί είναι το ψεύτικο λογισμικό ασφάλειας.

Cryptojacking: Cryptojacking είναι ένα είδος κακόβουλου λογισμικού που χρησιμοποιεί τη δύναμη του υπολογιστή του θύματος για να βρει κρυπτονομίσματα.

Hybrid Malware: Τα περισσότερα κακόβουλα λογισμικά που υπάρχουν σήμερα είναι ένας συνδυασμός των υπαρχουσών επιθέσεων, συχνά trojan horses, σκουλήκια, ιοί και ransomware. Για παράδειγμα, ένα κακόβουλο λογισμικό μπορεί να φαίνεται πως είναι trojan αλλά μόλις εκτελεστεί να συμπεριφέρεται ως σκουλήκι και να προσπαθεί να επιτεθεί στα θύματα του μέσω διαδικτύου.

ΚΕΦΑΛΑΙΟ 3ο

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ ΕΠΙΧΕΙΡΗΣΕΙΣ

3. ΕΙΣΑΓΩΓΗ

Καθώς η εξάρτηση των ανθρώπων από τις ψηφιακές τεχνολογίες συνεχίζει να αυξάνεται με γρήγορο ρυθμό, έτσι αυξάνεται και το κυβερνό-έγκλημα. Οι κυβερνό-εγκληματίες αρπάζουν κάθε ευκαιρία για να εκμεταλλευτούν κάθε τρωτό σημείο που ανακαλύπτουν εναντίον των ανθρώπων και των επιχειρήσεων μέσω της τεχνολογίας. Οι εγκληματίες είναι πιο ευέλικτοι από ποτέ, προσαρμόζονται γρήγορα στις καινούργιες τεχνολογίες, τροποποιούν τις επιθέσεις τους χρησιμοποιώντας καινούργιες μεθόδους και συνεργάζονται στενά μεταξύ τους.

Το πιο γνωστό η παραδοσιακό οργανωμένο έγκλημα, όπως η «μαφία», αρχίζει να μεταμορφώνεται ψηφιακά αλλάζοντας τον τρόπο που ενεργούσε μέχρι πρότινος. Πολλές εγκληματικές οργανώσεις όπως η «μαφία» πληρώνουν χάκερς για να υποστηρίξουν τις εγκληματικές τους ενέργειες συμπεριλαμβανομένου του εκβιασμού και της διακίνησης ναρκωτικών (Franceschi-Bicchierai, L., 2021).

Η Europol ανακοίνωσε πρόσφατα πως οργανωμένες εγκληματικές ομάδες προσέλαβαν χάκερς για επιθέσεις κοινωνικής μηχανικής, ανταλλαγής καρτών SIM και αποστολής κακόβουλων λογισμικών στα θύματα ώστε να αποκτήσουν τον έλεγχο των τραπεζικών τους λογαριασμών. Η πρόσληψη κυβερνό-εγκληματιών είναι πλέον μια διαδεδομένη πρακτική. Επιπλέον, αυτές οι οργανώσεις συχνά κρύβουν κυβερνό-εγκληματίες σε νόμιμες επιχειρηματικές δραστηριότητες, κάνοντας ακόμα πιο δύσκολο τον εντοπισμό τους. Αυτοί οι «υπάλληλοι» βρίσκονται σε όλο τον κόσμο προστατεύοντας αυτές τις ομάδες από τον νόμο.

Το dark web είναι τμήμα του διαδικτύου το οποίο δεν είναι ορατό από τις μηχανές αναζήτησης και για είναι προσβάσιμο απαιτεί τη χρήση ενός προγράμματος περιήγησης με το όνομα The Onion Router. Το dark web είναι γεμάτο με υπηρεσίες hacking που προσφέρουν ολοκληρωμένες δεξιότητες, οικονομικές τιμές και γρήγορη παράδοση. Είναι το μέρος όπου μαζεύονται οι κυβερνό-εγκληματίες, ανταλλάσσουν πληροφορίες, πουλάνε και αγοράζουν παράνομε είδη και υπηρεσίες. Οι κυβερνό-

εγκληματίες που είναι επίσης γνωστοί ως Blackhat Hackers, μπορούν να προσληφθούν για να μπουν παράνομα σε λογαριασμούς κοινωνικής δικτύωσης, να διαγράψουν χρέη ακόμα και να αλλάξουν βαθμούς φοιτητών (Bischoff, P., 2021).

Οι τιμές για αυτές τις υπηρεσίες είναι συχνά σχετικά οικονομικές ειδικά αν λάβουμε υπόψη την πιθανότητα της προσωπικής ή της επαγγελματικής ζημιάς. Οι τιμές ποικίλουν ανάλογα με το πόσο περίπλοκες είναι οι υπηρεσίες που απαιτούνται, το επιθυμητό αποτέλεσμα και το προφίλ του θύματος. Οι τυπικές τιμές για παράδειγμα για υπηρεσίες όπως παράνομη πρόσβαση σε λογαριασμό κοινωνικής δικτύωσης κυμαίνονται γύρω στα $230 ενώ η παράνομη πρόσβαση σε δίκτυο και η αλλαγή βαθμών κυμαίνεται από $394 μέχρι $526. Οι τιμές ανεβαίνουν όταν πρόκειται για επίθεση εναντίον του δικτύου μιας επιχείρησης καθώς η πρόκληση της ζημιάς είναι πολύ μεγαλύτερη. Μπορεί λοιπόν κάποιος να αντιληφθεί πόσο ευάλωτες είναι οι επιχειρήσεις σε μια ενδεχόμενη επίθεση και πόσο σημαντική είναι η ύπαρξη κυβερνό-ασφάλειας.

3.1 ΟΡΙΣΜΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Ο όρος κυβερνοασφάλεια έχει αποτελέσει αντικείμενο πολλών μελετητών που έχει δει το θέμα από μια συγκεκριμένη προοπτική. Βασισμένοι στην βιβλιογραφία, βρήκαμε πως ο όρος αυτός χρησιμοποιείται ευρέως, έχει πολλούς ορισμούς που συχνά είναι υποκειμενικοί και μερικές φορές είναι μη ενημερωτικοί. Υπάρχει έλλειψη βιβλιογραφίας στο τι σημαίνει πραγματικά αυτός ο όρος και πως τοποθετείται σε διάφορα πλαίσια. Η απουσία ενός ακριβή και ευρέως αποδεκτού ορισμού που να συλλαμβάνει τις πολλές διαστάσεις που έχει η κυβερνό-ασφάλεια εμποδίζει τις τεχνολογικές και επιστημονικές προόδους με το να ενισχύει την κυρίαρχη τεχνική πλευρά της κυβερνό-ασφάλειας διαχωρίζοντας τις άλλες πλευρές που θα έπρεπε να λειτουργούν ταυτόχρονα για να επιλύσουν τις προκλήσεις με τις οποίες έρχεται αντιμέτωπη η κυβερνό-ασφάλεια (DHS. 2014).

Για παράδειγμα, υπάρχει ένα σύνολο τεχνικών λύσεων που υποστηρίζουν την κυβερνό-ασφάλεια. Ωστόσο, αυτές οι λύσεις δεν μπορούν από μόνες τους να επιλύσουν το πρόβλημα καθώς υπάρχουν κάποιες προκλήσεις που σχετίζονται με τις οργανωτικές, οικονομικές, κοινωνικές, πολιτικές και άλλες διαστάσεις που συνδέονται άρρηκτα με την κυβερνό-ασφάλεια (Goodall, J. R., 2009).

Ο Fredrick Chang (Chang, F. R. 2012) πρώην διευθυντής Έρευνας στην Εθνική Υπηρεσία Ασφάλειας των Ηνωμένων Πολιτειών αναφέρει σχετικά για την πολυδιάστατη φύση της κυβερνό-ασφάλειας:

« Μια επιστήμη της κυβερνό-ασφάλειας προσφέρει πολλές ευκαιρίες για εξελίξεις που βασίζονται σε μια πολυδιάστατη προσέγγιση αφού στην τελική, η κυβερνό-ασφάλεια είναι μια ανταγωνιστική διαδικασία. Οι άνθρωποι πρέπει να υπερασπιστούν μηχανές που δέχονται επίθεση από άλλους ανθρώπους χρησιμοποιώντας μηχανές. Έτσι, εκτός από τα σημαντικά παραδοσιακά πεδία την επιστήμης των υπολογιστών, της ηλεκτρικής μηχανικής και των μαθηματικών, χρειαζόμαστε και την οπτική των άλλων πεδίων.»

Παρακάτω παραθέτουμε τους εννιά ορισμούς της κυβερνό-ασφάλειας που θεωρούμε πως παρουσιάζουν όλες τις πλευρές της κυβερνό-ασφάλειας:

- Η κυβερνό-ασφάλεια αποτελείται κυρίως από αμυντικές μεθόδους που χρησιμοποιούνται για να ανιχνεύσουν και να απωθήσουν επίδοξους εισβολείς(Kemmerer, R. A. 2003).
- Η κυβερνό-ασφάλεια περιλαμβάνει την προστασία των δικτύων των υπολογιστών και των πληροφοριών που περιέχουν από την εισβολή και την κακόβουλη ζημιά(Lewis, J. A. 2006).
- Η κυβερνό-ασφάλεια περιλαμβάνει την ελάττωση του ρίσκου μιας κακόβουλης επίθεσης στο λογισμικό, στους υπολογιστές και στο δίκτυο. Αυτό περιλαμβάνει εργαλεία που χρησιμοποιούνται για την ανίχνευση εισβολών και ιών, την διευκόλυνση κωδικοποιημένων επικοινωνιών και τα λοιπά (Amoroso, E. 2006).
- Η κυβερνό-ασφάλεια είναι η συλλογή των εργαλείων, των πολιτικών, των θεωριών ασφάλειας, των οδηγιών, των προσεγγίσεων, των πράξεων, των καλύτερων τεχνικών και τεχνολογιών που μπορούν να χρησιμοποιηθούν για να προστατεύσουν το κυβερνό-περιβάλλον και τα περιουσιακά στοιχεία των επιχειρήσεων και των χρηστών (ITU. 2009).
- Η ικανότητα να προστατεύει ή να υπερασπίζεται τη χρήση του κυβερνοχώρου από τις κυβερνό-επιθέσεις (CNSS. 2010).
- Το σώμα των τεχνολογιών, των διαδικασιών, των πρακτικών και των μέτρων που έχουν σχεδιαστεί για να προστατεύσουν τα δίκτυα, τους υπολογιστές, τα προγράμματα και τα δεδομένα από επίθεση, καταστροφή ή μη

εξουσιοδοτημένη πρόσβαση ώστε να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα (Public Safety Canada. 2010).

- Η τέχνη της διασφάλισης της ύπαρξης και της συνέχειας της κοινωνίας των πληροφοριών ενός έθνους, της εγγύησης και της προστασίας στο διαδίκτυο των πληροφοριών, των στοιχείων και των δομών (Canongia, C., & Mandarins, R. 2014).
- Η κατάσταση του να είσαι προστατευμένος ενάντια σε κάθε εγκληματική ή μη εξουσιοδοτημένη χρήση των ηλεκτρονικών δεδομένων ή τα μέτρα που λαμβάνονται για να επιτευχθεί αυτό (Oxford University Press. 2022).
- Η πράξη ή η διαδικασία, ικανότητα ή κατάσταση όπου οι πληροφορίες και τα συστήματα επικοινωνιών όπως και οι πληροφορίες που εμπεριέχονται εκεί είναι προστατευμένες ή αμύνονται ενάντια στην καταστροφή, στην μη εξουσιοδοτημένη χρήση ή τροποποίηση ή εκμετάλλευση (DHS. 2014).

3.2 Η ΑΝΑΓΚΗ ΓΙΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Η κυβερνό-ασφάλεια θεωρείται πλέον εξίσου σημαντική τόσο για τα άτομα και τις οικογένειες όσο και για τους οργανισμούς, τις κυβερνήσεις, τα εκπαιδευτικά ιδρύματα και τις επιχειρήσεις. Είναι σημαντική για τις οικογένειες για την προστασία των παιδιών αλλά και όλων των μελών από την απάτη. Σε όρους οικονομικής ασφάλειας, είναι σημαντικό να ασφαλίζουμε τις οικονομικές μας πληροφορίες που μπορεί να επηρεάσουν την προσωπική οικονομική μας κατάσταση. Το διαδίκτυο είναι πολύ σημαντικό και ωφέλιμο για το εκπαιδευτικό προσωπικό, τους μαθητές, τους φοιτητές και τους εκπαιδευτικούς οργανισμούς καθώς μπορεί να παρέχει πολλές εκπαιδευτικές δυνατότητες και ευκαιρίες. Είναι ζωτική ανάγκη να μάθουν οι χρήστες πως να προστατευτούν από την διαδικτυακή απάτη και την κλοπή ταυτότητας (A Report form CISCO).

Οι εταιρείες κάθε μεγέθους επίσης έρχονται αντιμέτωπες με θέματα που αφορούν την κυβερνό-ασφάλεια με αποτέλεσμα να κινδυνεύουν από κάθε είδους διαδικτυακής επίθεσης. Η εξέλιξη των τεχνολογιών παρόλο που έχει βοηθήσει τις επιχειρήσεις να αναπτυχθούν έχουν βοηθήσει και τους εγκληματίες να εξελιχθούν και να επιτίθενται στα λογισμικά και στα δίκτυα των επιχειρήσεων. Το κόστος αυτό των επιθέσεων

μπορεί να είναι υψηλό και σύμφωνα με το Cost of a Data Breach Report (2021) μπορεί κατά μέσο όρο κάθε επίθεση να αγγίξει τα $ 3,6 εκατομμύρια.

Ίσως ακόμα πιο ανησυχητικό είναι το γεγονός πως οι εταιρείες χρειάζονται κατά μέσο όρο 280 μέρες για να αναγνωρίσουν και να ανταποκριθούν σε μια κυβερνό-επίθεση, σύμφωνα με στοιχειά από το IBM Security (2020). Για παράδειγμα, ένα περιστατικό που λαμβάνει χώρα την 1η Ιανουαρίου μπορεί να μην έχει περιοριστεί ολοκληρωτικά μέχρι τις 8 Οκτωβρίου. Ένα άλλο παράδειγμα που δείχνει πόσο χρονικό διάστημα χρειάζεται για να γίνουν γνωστές οι επιθέσεις που γίνονται στο διαδίκτυο είναι το πρόσφατο κακόβουλο λογισμικό Emotet. Παρόλο που η αστυνομία σταμάτησε το Emotet και τη δομή του τον Ιανουάριο του 2021, τα νέα για την επιστροφή του λογισμικού στο προσκήνιο μέσω botnets κυκλοφόρησαν τον Νοέμβριο του 2021. Επομένως, είναι αναμενόμενο πως ο αντίκτυπος του Emotet ή κάποιου παρόμοιου κακόβουλου λογισμικού θα ξανακάνει την εμφάνιση του το 2022.

Επιπλέον, ο αγώνας μεταξύ επιτιθέμενων και αμυνόμενων εντείνεται και από το ρυθμό που ανακαλύπτονται και δημοσιοποιούνται οι αδυναμίες ασφαλείας των πιο γνωστών λογισμικών εργαλείων και συστημάτων. Οι παραβιάσεις επίσης ασκούν πίεση και έχουν αρνητικό αντίκτυπο στην οικονομική επίδοση των επιχειρήσεων και στην τιμή των μετοχών. Σύμφωνα με μια ανάλυση του NASDAQ, φάνηκε πως 14 μέρες αφού γίνει γνωστή μια παραβίαση, η τιμή της μετοχής βυθίζεται στο -3,5% και έξι μήνες μετά η τιμή βρίσκεται στο -3% (Bischoff, P.,2021).

3.3 ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΔΙΚΤΥΩΝ

Το άρθρο 37 του Ν. 4070/2012 αναφέρεται στην ασφάλεια και την ακεραιότητα δικτύων και υπηρεσιών. Σύμφωνα με αυτό το άρθρο:

«1.*Οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό λαμβάνουν πρόσφορα τεχνικά και οργανωτικά μέτρα για την κατάλληλη διαχείριση του κινδύνου όσον αφορά στην ασφάλεια των δικτύων και υπηρεσιών. Τα μέτρα αυτά, λαμβάνοντας υπόψη τις πλέον πρόσφατες τεχνικές δυνατότητες, πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τον υφιστάμενο κίνδυνο. Οι επιχειρήσεις αυτές λαμβάνουν ιδίως μέτρα για την*

αποτροπή και ελαχιστοποίηση των επιπτώσεων από περιστατικά ασφαλείας που επηρεάζουν τους χρήστες και τα διασυνδεμένα δίκτυα.

2. Οι επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών λαμβάνουν όλα τα κατάλληλα μέτρα για την εξασφάλιση της ακεραιότητας των δικτύων τους έτσι ώστε να διασφαλίζεται η συνέχεια της παροχής των υπηρεσιών που διανέμονται μέσω των δικτύων αυτών.

3. Τα μέτρα των παραγράφων 1 και 2 καθορίζονται από την Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) με κανονιστικές πράξεις.

4. Οι επιχειρήσεις που παρέχουν πρόσβαση σε δημόσια δίκτυα επικοινωνιών ή σε υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό κοινοποιούν στην Ε.Ε.Τ.Τ. κάθε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας που είχε σημαντικό αντίκτυπο στη λειτουργία δικτύων ή υπηρεσιών, η οποία με τη σειρά της κοινοποιεί κάθε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας στην Α.Δ.Α.Ε., κατ` εφαρμογή της παραγράφου 8.

5. Κατά περίπτωση, η Α.Δ.Α.Ε. ενημερώνει τις αρμόδιες εθνικές αρχές στα άλλα κράτη - μέλη, καθώς και τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA). Η Ε.Ε.Τ.Τ. μπορεί να ενημερώσει το κοινό ή να απαιτήσει την ενημέρωση αυτή από τις επιχειρήσεις, εφόσον κρίνει ότι η αποκάλυψη της παραβίασης είναι προς το δημόσιο συμφέρον. Η Ε.Ε.Τ.Τ. υποβάλλει κατ` έτος στην Ευρωπαϊκή Επιτροπή και στον ENISA συνοπτική έκθεση σχετικά με τις κοινοποιήσεις που έχει παραλάβει και τη δράση που έχει αναλάβει σύμφωνα με την παρούσα παράγραφο.

6. Η Ε.Ε.Τ.Τ. μπορεί να εκδίδει δεσμευτικές υποδείξεις, στο πλαίσιο εφαρμογής των κανονιστικών πράξεων των παραγράφων 1 και 2 του παρόντος, όσον αφορά στην ασφάλεια των δικτύων και υπηρεσιών και στην εξασφάλιση της ακεραιότητας των δικτύων τους, συμπεριλαμβανομένων εκείνων που αφορούν τις προθεσμίες εφαρμογής, προς τις επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών διαθέσιμες στο κοινό.

7. Η Ε.Ε.Τ.Τ. μπορεί να απαιτεί από τις επιχειρήσεις που παρέχουν δημόσια δίκτυα επικοινωνιών ή υπηρεσίες ηλεκτρονικών επικοινωνιών που διατίθενται στο κοινό να παρέχουν πληροφορίες απαραίτητες για την εκτίμηση της ασφάλειας και της ακεραιότητας των υπηρεσιών και δικτύων τους, περιλαμβανομένων τεκμηριωμένων

πολιτικών ασφαλείας, κατ` εφαρμογήν των κανονιστικών πράξεων που εκδίδονται σύμφωνα με την παράγραφο 3 του παρόντος.

8. Ο έλεγχος ασφάλειας διενεργείται από την Α.Δ.Α.Ε., η οποία θέτει τα σχετικά πορίσματα της στη διάθεση της Ε.Ε.Τ.Τ.. Το κόστος του ελέγχου επιβαρύνει την ελεγχόμενη επιχείρηση.

9. Η Α.Δ.Α.Ε., κατά την άσκηση του ελέγχου της, έχει την εξουσία και τις αρμοδιότητες που προβλέπονται από το ν. 3115/2003 (Α 47), το ν. 703/1977 (Α 278) και το ν. 3674/2008 (Α` 136), όπως ισχύουν».

Με τον Ν. 4577/2018 (ΦΕΚ 199/Α'/03-12-2018) έγινε η ενσωμάτωση στην Ελληνική νομοθεσία της οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου αναφορικά με τα μέτρα για υψηλό κοινό επίπεδο ασφαλείας συστημάτων δικτύων και πληροφοριών σε όλη την Ευρώπη.

Άρθρο 7:

«Εθνική Αρχή Κυβερνοασφάλειας

(Άρθρο 8 της Οδηγίας 2016/1148/ΕΕ)

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

2.Η Εθνική Αρχή Κυβερνοασφάλειας:

α) παρακολουθεί την εφαρμογή του παρόντος,

β) ορίζεται ως το εθνικό ενιαίο κέντρο επαφής, εφεξής «Ενιαίο Κέντρο Επαφής», για την ασφάλεια των συστημάτων δικτύου και πληροφοριών, ασκώντας καθήκοντα συνδέσμου για τη διασφάλιση της διασυνοριακής συνεργασίας των αρχών των κρατών

μελών, καθώς και με τις Αρμόδιες Αρχές άλλων κρατών μελών στο πλαίσιο των μηχανισμών συνεργασίας, όπως αυτοί προσδιορίζονται στα άρθρα 11 και 12 της Οδηγίας που ενσωματώνεται με τον παρόντα,

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

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

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

στ) συνεργάζεται με τις Αρμόδιες Αρχές των λοιπών κρατών

μελών, στο πλαίσιο των μηχανισμών συνεργασίας, όπως αυτοί προσδιορίζονται στα άρθρα 11 και 12 της Οδηγίας που ενσωματώνεται με τον παρόντα νόμο, ζ) συμμετέχει στην ομάδα συνεργασίας του άρθρου 11 της ως άνω Οδηγίας, ορίζει τους εθνικούς αντιπροσώπους της χώρας σ' αυτήν και ενημερώνει τους λοιπούς εμπλεκόμενους εθνικούς φορείς αναφορικά με τις εργασίες και τις αποφάσεις που λαμβάνονται στο πλαίσιο αυτής,

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

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

Άρθρο 8:

Ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT)

(Άρθρο 9 της Οδηγίας 2016/1148/ΕΕ)

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

2.Η αρμόδια CSIRT:

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

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

γ) αναφορικά με τη συνέχεια της επιχειρησιακής δραστηριότητάς της, η αρμόδια CSIRT:
αα) είναι εφοδιασμένη με κατάλληλο σύστημα διαχείρισης και δρομολόγησης αιτημάτων, προκειμένου να διευκολύνεται η παράδοση καθηκόντων,

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

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

δ) συμμετέχει σε διεθνή δίκτυα συνεργασίας.

3.Οι αρμοδιότητες της αρμόδιας CSIRT είναι οι εξής:

α) η παρακολούθηση συμβάντων σε εθνικό επίπεδο,

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

γ) η παρέμβαση σε περίπτωση συμβάντος,

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

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

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

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

η) η εγκαθίδρυση σχέσεων συνεργασίας με τον ιδιωτικό τομέα,

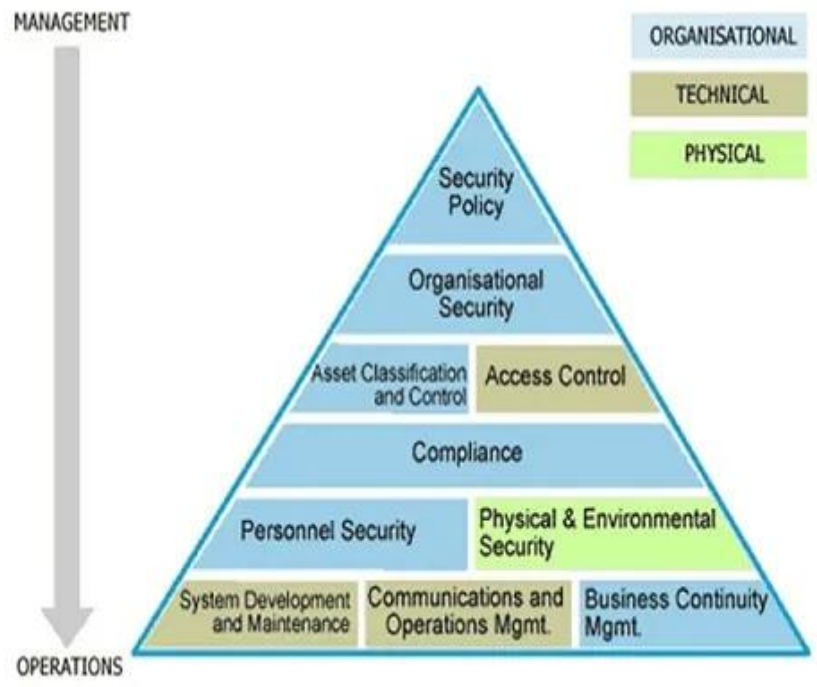
θ) η προώθηση, η υιοθέτηση και η χρήση κοινών ή τυποποιημένων πρακτικών για:

αα) τις διαδικασίες χειρισμού συμβάντων και κινδύνων,

ββ) τα συστήματα ταξινόμησης συμβάντων, κινδύνων και πληροφοριών.

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

3.4 ΔΙΟΙΚΗΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ



Εικόνα 12. Δομή διοίκησης κυβερνό-ασφάλειας.

Διοίκηση κυβερνό-ασφάλειας είναι το σύστημα διαχείρισης με το οποίο οι εταιρείες ρυθμίζουν και ελέγχουν την κυβερνό-ασφάλεια. Το διοικητικό πλαίσιο καθορίζει ποιος είναι αυτός που αποφασίζει για τη λήψη των αποφάσεων και ποιος αναλαμβάνει την ευθύνη των αποτελεσμάτων κάθε απόφασης. Οι διοικητικές διαδικασίες παρέχουν την κατάλληλη επίβλεψη ώστε να διασφαλιστεί πως υπάρχει επαρκή αντιμετώπιση των απειλών (https://cyberrisk-countermeasures.info).

Το πρόγραμμα διοίκησης της κυβερνό-ασφάλειας επικεντρώνεται στην δημιουργία και διατήρηση ενός πλαισίου, το οποίο θα μπορεί να παράσχει την επιβεβαίωση πως οι στρατηγικές ασφαλείας υποστηρίζουν και συμβαδίζουν με τους στόχους που έχει θέσει η επιχείρηση, συνάδουν με τους νόμους και τους κανονισμούς και παρέχουν σωστό επιμερισμό ευθυνών. Όλα αυτά έχουν ως στόχο την διαχείριση του κινδύνου.

Οι στόχοι μιας επιχείρησης μπορεί να διαφέρουν ανάλογα με το είδος της, αλλά οι στόχοι του προγράμματος διοίκησης της κυβερνό-ασφάλειας είναι ίδιοι ανεξάρτητα από το είδος της επιχείρησης. Οι στόχοι είναι οι εξής:

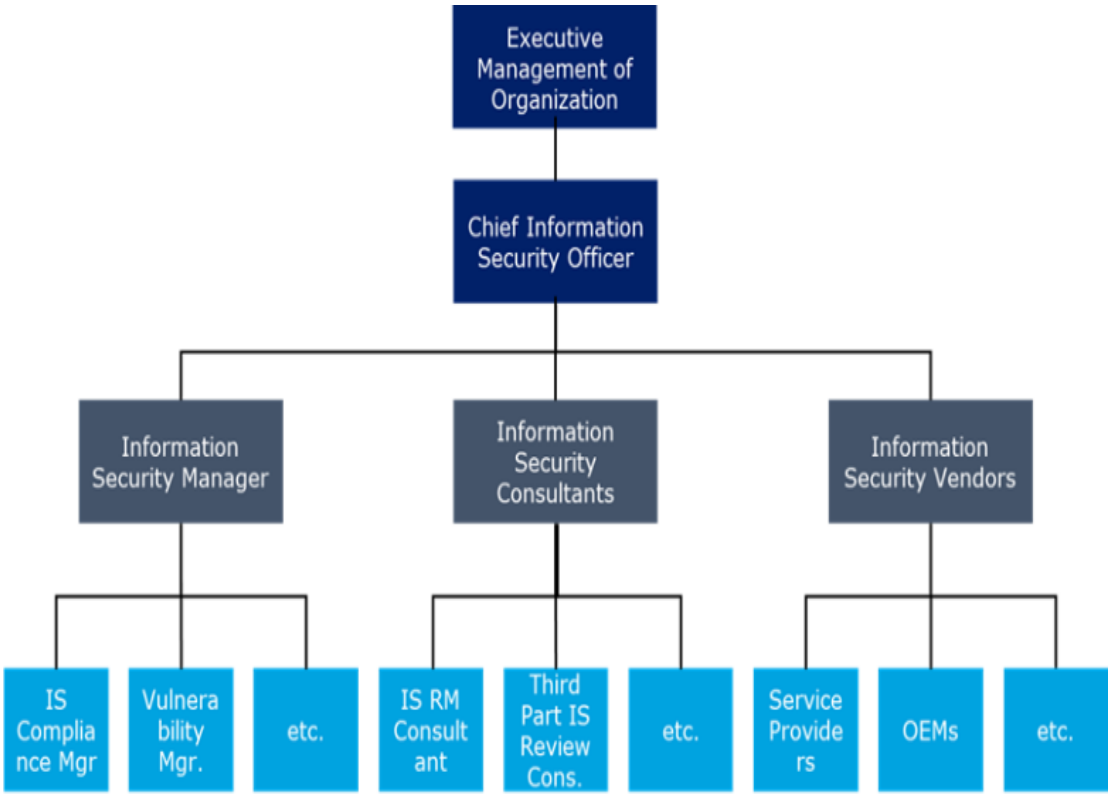
- Η προστασία της φήμης της επιχείρησης και των μετόχων της με τη διατήρηση ενός ασφαλούς κυβερνό-περιβάλλοντος.

- Η προστασία του μεριδίου αγοράς της επιχείρησης και της τιμής της μετοχής της.
- Η διασφάλιση μιας αποδοτικής οργανωτικής δομής ασφάλειας χωρίς συγκρούσεις συμφερόντων και με επαρκή εξουσία και πόρους.
- Η διασφάλιση πως οι πολιτικές της διοίκησης της ασφάλειας καλύπτουν κάθε πλευρά της στρατηγικής, του ελέγχου και του κανονισμού.
- Η διασφάλιση ενός ολοκληρωμένου συνόλου προδιαγραφών για κάθε πολιτική ώστε να διασφαλίζεται πως όλες οι διαδικασίες συνάδουν με την εκάστοτε πολιτική.
- Η διασφάλιση πως υπάρχουν, διατηρούνται και ελέγχονται όλες οι διαδικασίες διαχείρισης κινδύνου.
- Η διοίκηση της εφαρμογής και της λειτουργίας της τεχνολογίας πληροφοριών της επιχείρησης και η προστασία των ευαίσθητων δεδομένων της.
- Η επιτυχία ή η αποτυχία του προγράμματος ασφάλειας μιας επιχείρησης ελέγχεται από θεσπισμένες μετρήσεις και διαδικασίες ελέγχου ώστε να διασφαλίζεται η συμβατότητα, η παροχή πληροφοριών για την αποδοτικότητα και την λήψη των κατάλληλων διοικητικών αποφάσεων.
- Η διοίκηση της συμπεριφοράς των χρηστών και η διασφάλιση πως γίνεται υπεύθυνη χρήση των τεχνολογικών πόρων.
- Η διασφάλιση πως καλύπτονται οι απαιτήσεις συμμόρφωσης με τον νόμο

3.4.1 Η ΟΡΓΑΝΩΤΙΚΗ ΔΟΜΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Η οργάνωση της κυβερνό-ασφάλειας είναι ένα δομημένο διοικητικό πλαίσιο το οποίο διευθύνει, ελέγχει και διαχειρίζεται την εφαρμογή και λειτουργία της κυβερνό-ασφάλειας μέσα σε μια επιχείρηση. Η οργάνωση της κυβερνό-ασφάλειας είναι η δομή που δημιουργείται από τον ηγέτη της επιχείρησης και περιλαμβάνει επίσημα οργανωτικά διαγράμματα, τεκμηριωμένες πολιτικές και οδηγίες. Σε περιπτώσεις που η συνολική οργανωτική στρατηγική αναγνωρίζει την κυβερνό-ασφάλεια ως σημαντικό στόχο, τότε αυτό θα αντανακλάται στον σχεδιασμό και στους ανθρώπους. Αυτή η δομή καθορίζει με σαφήνεια τους ρόλους και τις ευθύνες της κυβερνό-ασφάλειας μέσα στην

επιχείρηση και ακολουθεί διάφορα μοντέλα αναφοράς τα οποία βασίζονται στην ευαισθησία και την σπουδαιότητα των πληροφοριών που χειρίζεται.



Εικόνα 13. Οργανωτική δομή κυβερνό-ασφάλειας

Παρακάτω παραθέτουμε κάποιες καλές πρακτικές που συνδέονται με την εδραίωση της οργανωτικής δομής της κυβερνό-ασφάλειας:

- Ο επικεφαλής της ασφάλειας πληροφοριών θα πρέπει να δίνει αναφορά σε άτομο το οποίο να βρίσκεται πολύ ψηλά στην ιεραρχία της επιχείρησης. Θα πρέπει επίσης να έχει την απαραίτητη στήριξη και χρηματοδότηση για να μπορεί να είναι αποδοτικός στην εργασία που του έχει ανατεθεί.
- Όλες οι ευθύνες της ασφάλειας πληροφοριών θα πρέπει να έχουν οριστεί με σαφήνεια και να έχουν διαμοιραστεί.
- Οι συμμέτοχοι θα πρέπει να έχουν επαρκή εξουσία ώστε να μπορούν να ανταπεξέλθουν αποδοτικά στους ρόλους που τους έχουν αποδοθεί στην ασφάλεια πληροφοριών.

- Θα πρέπει να υπάρχει ξεκάθαρος διαχωρισμός των υποχρεώσεων ώστε να μην ολοκληρώνεται μια διαδικασία μόνο από ένα άτομο.

3.4.1.1 ΕΠΙΚΕΦΑΛΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Ο επικεφαλής κυβερνό-ασφάλειας είναι ένα υψηλόβαθμο στέλεχος το οποίο είναι υπεύθυνο για την ανάπτυξη και εφαρμογή ενός προγράμματος κυβερνό-ασφάλειας το οποίο περιλαμβάνει διαδικασίες και πολιτικές σχεδιασμένες να προστατέψουν τις εταιρικές επικοινωνίες, τα συστήματα και περιουσιακά στοιχεία από εσωτερικές και εξωτερικές απειλές.

Τα καθήκοντα του επικεφαλής της κυβερνό-ασφάλειας μπορεί να περιλαμβάνουν:

- Τη διενέργεια εκπαιδευτικών προγραμμάτων για την επιμόρφωση των υπαλλήλων σχετικά με την κυβερνό-ασφάλεια.
- Την ανάπτυξη ασφαλών επαγγελματικών πρακτικών και πρακτικών επικοινωνίας.
- Τον προσδιορισμών των στόχων ασφάλειας και των μετρήσεων.
- Την επιλογή και αγορά προϊόντων ασφάλειας από πωλητές.
- Την διασφάλιση πως η εταιρεία λειτουργεί με βάση τους νόμους όπως αυτοί ορίζονται από τα ρυθμιστικά σώματα.
- Την επιβολή τήρησης των πρακτικών ασφάλειας.

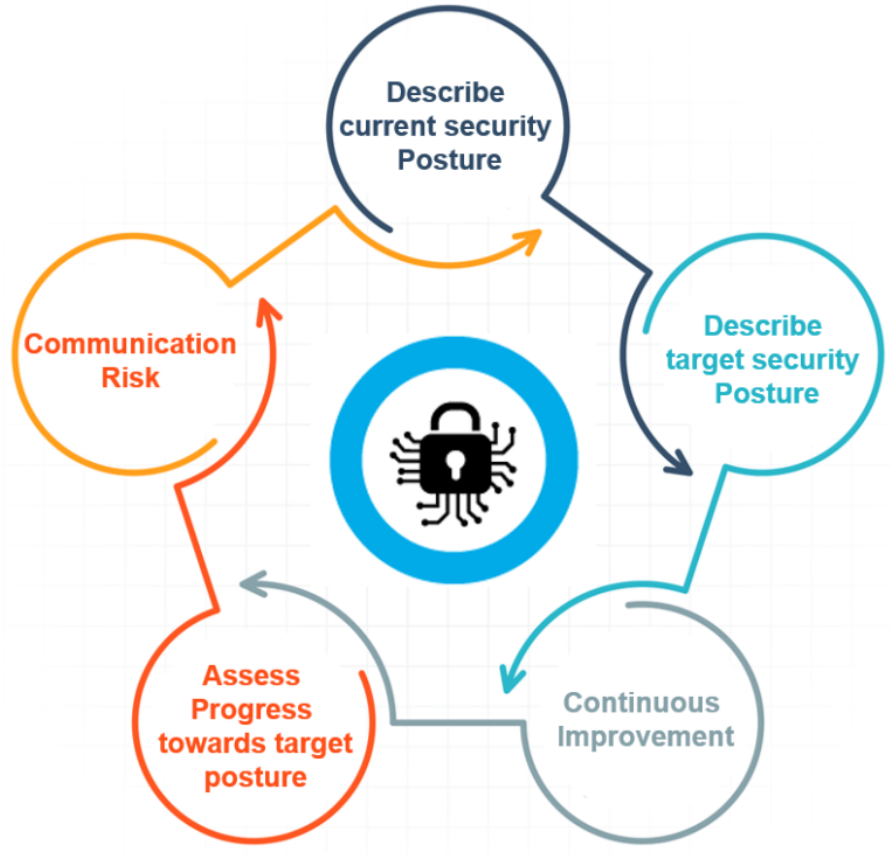
3.5 ΠΛΑΙΣΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ (Cybersecurity Framework)

Το πλαίσιο είναι εθελοντική καθοδήγηση που βασίζεται σε υπάρχουσες κατευθυντήριες γραμμές και πρακτικές και προορίζεται για επιχειρήσεις που επιθυμούν να διαχειριστούν καλύτερα και να μειώσουν την απειλή κυβερνό-επίθεσης. Ανεπτυγμένο μέσω συντονισμένης προσπάθειας μεταξύ επιχειρήσεων και κυβερνήσεων, το πλαίσιο αποτελείται από μέτρα, κανόνες και πρακτικές ώστε να διαφυλάξει την ασφάλεια των επιχειρήσεων. Η οργανωμένη, προσαρμοστική, επαναλαμβανόμενη και αποτελεσματική προσέγγιση του πλαισίου βοηθάει τους ιδιοκτήτες επιχειρήσεων και τους υπεύθυνους ασφαλείας να επιβλέπουν τα ζητήματα που αφορούν τους κινδύνους της κυβερνό-ασφάλειας (Shashank, 2022).

Εκτός από το να βοηθήσει τις επιχειρήσεις να επιβλέπουν και να μειώσουν τους πιθανούς κινδύνους, το πλαίσιο στοχεύει και στο να καλλιεργήσει σωστή επικοινωνία όσον αφορά την κυβερνό-ασφάλεια μεταξύ των εσωτερικών και εξωτερικών συνεργατών.

Οι στόχοι του πλαισίου κυβερνό-ασφάλειας είναι:

- ✓ Περιγραφή της τωρινής κατάστασης της κυβερνό-ασφάλειας
- ✓ Περιγραφή της κατάστασης της κυβερνό-ασφάλειας στην οποία στοχεύει η επιχείρηση
- ✓ Συνεχής βελτίωση
- ✓ Αξιολόγηση της προόδου προς τον επιθυμητό στόχο
- ✓ Βελτίωση της επικοινωνίας για τους κινδύνους



Εικόνα 14. Στόχοι του πλαισίου κυβερνό-ασφάλειας

3.5.1 ΕΙΔΗ ΠΛΑΙΣΙΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Τα πλαίσια που υιοθετούνται πιο συχνά από τις επιχειρήσεις είναι τα εξής:

PCI DSS (Payment Card Industry Data Security Standard): Το PCI DSS είναι ένα σύνολο ελέγχων ασφαλείας που απαιτείται για την ασφάλεια των πληρωμών που πραγματοποιούνται με κάρτα. Έχει σχεδιαστεί για να προστατεύει συν αλλαγές με πιστωτικές κάρτες, χρεωστικές κάρτες και κάρτες ανάληψης μετρητών.

ISO 27001/27002 (International Organization for Standardization): συστήνεται για την προστασία προγραμμάτων διαχείρισης και ασφάλειας.

CIS Critical Security Controls: μια καθορισμένη σύνθεση δραστηριοτήτων για την κυβερνό-προστασία που παρέχει συγκεκριμένες και αξιοσημείωτες προσεγγίσεις για την παύση των πιο επικίνδυνων τωρινών επιθέσεων. Ένα βασικό πλεονέκτημα των Critical Security Controls είναι ότι οργανώνουν και συγκεντρώνουν λιγότερες δραστηριότητες με καλύτερα αποτελέσματα.

NIST Framework: ένα πλαίσιο για την αναβάθμιση της υποδομής της κυβερνό-ασφάλειας με στόχο τη βελτίωση της ετοιμότητας της επιχείρησης στην αντιμετώπιση της απειλής της κυβερνό-ασφάλειας με την αξιοποίηση των τυπικών μεθοδολογιών και διαδικασιών.

3.5.2 ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΤΟΥ ΠΛΑΙΣΙΟΥ ΚΥΒΕΡΝΟ-ΑΣΦΑΛΕΙΑΣ

Υπάρχουν τρία βασικά στοιχεία: Ο πυρήνας του πλαισίου, οι βαθμίδες υλοποίησης και τα προφίλ.

Εικόνα 15. Βασικά στοιχεία του πλαισίου.

Πυρήνας του πλαισίου: παρέχει ένα σύνολο απαιτούμενων ασκήσεων κυβερνό-ασφάλειας και αποτελεσμάτων με τη χρήση κατανοητής γλώσσας. Ο πυρήνας οδηγεί τις επιχειρήσεις στην επίβλεψη και στη βελτίωση της κυβερνό-ασφάλειας με τέτοιο τρόπο ώστε να συμπληρώνει τις υπάρχουσες διαδικασίες διαχείρισης της κυβερνό-ασφάλειας και των απειλών.

Βαθμίδες υλοποίησης: Αυτό το στοιχείο βοηθάει τις επιχειρήσεις δίνοντας τους τη δυνατότητα να αντιληφθούν πως πραγματικά βλέπουν την διαχείριση της κυβερνό-ασφάλειας. Οι βαθμίδες βοηθούν τις επιχειρήσεις να σκεφτούν ποιος είναι ο βαθμός αρτιότητας που επιθυμούν για το πρόγραμμα κυβερνό-ασφάλειας τους και συχνά χρησιμοποιούνται ως εξειδικευμένο μέσο για να μιλήσουν για τους κινδύνους, την ανάγκη ύπαρξης αποστολής και του πλάνου εξόδων.

Προφίλ: τα προφίλ είναι η ρύθμιση των οργανωτικών προαπαιτούμενων, των στόχων και των περιουσιακών στοιχείων μιας επιχείρησης σε σχέση με τα επιθυμητά αποτελέσματα του πυρήνα του πλαισίου. Τα προφίλ χρησιμοποιούνται κυρίως για την αναγνώριση και την οργάνωση «ανοιχτών θυρών» για την ενίσχυση της κυβερνό-ασφάλειας μιας επιχείρησης.

3.5.3 ΟΙ ΠΕΝΤΕ ΛΕΙΤΟΥΡΓΙΕΣ ΤΟΥ ΠΛΑΙΣΙΟΥ ΚΥΒΕΡΝΟ-ΑΣΦΑΛΕΙΑΣ

Οι λειτουργίες αποτελούν τη βάση του πυρήνα του πλαισίου κυβερνό-ασφάλειας και είναι οι εξής:

Αναγνωρίζω (*Identify*): Η λειτουργία αυτή βοηθάει ώστε να χτιστεί μια ιεραρχική κατανόηση της επίβλεψης της κυβερνό-ασφάλειας μέσω πλαισίων, ατόμων, πόρων, πληροφοριών και δυνατοτήτων.

Προστατεύω (*Protect*): Η συγκεκριμένη λειτουργία παρέχει τις κατάλληλες «ασπίδες» για να διασφαλιστεί η μεταβίβαση των βασικών αρχών ενώ ενισχύει την ικανότητα περιορισμού των συνεπειών μιας κυβερνό-επίθεσης.

Ανιχνεύω (*Detect*): Η λειτουργία αυτή χαρακτηρίζεται από τις κατάλληλες ασκήσεις για την αναγνώριση μια κυβερνό-επίθεσης και ενδυναμώνει τις δυνατότητες αποκάλυψης περιστατικών επιθέσεων.

Ανταποκρίνομαι(*Respond*): Η λειτουργία αυτή ενσωματώνει τις κατάλληλες ενέργειες για να αντιμετωπιστεί μια επίθεση ενώ ταυτόχρονα παρέχει τη δυνατότητα περιορισμού των συνεπειών μιας επίθεσης.

Ανακτώ (*Recover*): Η συγκεκριμένη λειτουργία ξεχωρίζει τις κατάλληλες ενέργειες που πρέπει να γίνουν ώστε να διατηρηθούν τα σχέδια για ευελιξία και να επανέρθουν όσα στοιχεία και δυνατότητες επλήγησαν λόγω κυβερνό-επίθεσης.

Εικόνα 16. Οι πέντε λειτουργίες του πλαισίου κυβερνό-ασφάλειας

3.5.4 ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΟ ΠΛΑΙΣΙΟ ΚΥΒΕΡΝΌ-ΑΣΦΑΛΕΙΑΣ

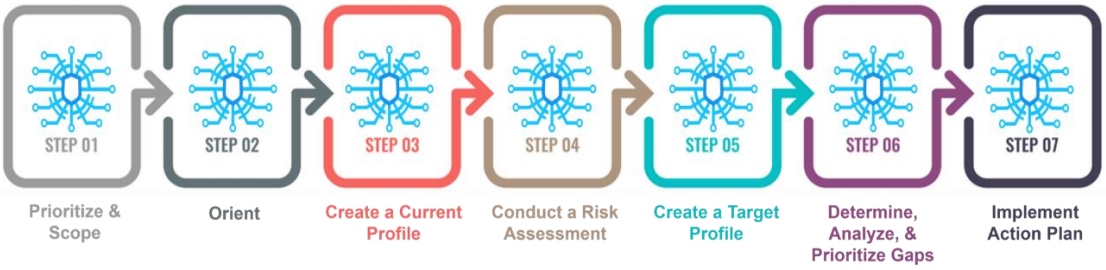
Η χρήση του πλαισίου μπορεί να βελτιώσει την κριτικής σημασίας υποδομή μιας επιχείρησης. Το πλαίσιο μπορεί να εφαρμοστεί σε στάδια και επομένως μπορεί να διαμορφωθεί έτσι ώστε να καλύπτει τις ανάγκες κάθε επιχείρησης. Το πλαίσιο έχει ως στόχο να συμπληρώσει και όχι και αντικαταστήσει το πρόγραμμα κυβερνό-ασφάλειας της επιχείρησης.

Τα τελευταία χρόνια ένας σημαντικός αριθμός επιχειρήσεων έχει υιοθετήσει το πλαίσιο και ως αποτέλεσμα:

- Οι ιθύνοντες έχουν υιοθετήσει το λεξιλόγιο του πλαισίου και μπορούν πλέον να κάνουν εμπεριστατωμένες συζητήσεις για την κυβερνό-ασφάλεια.
- Οι επιχειρήσεις έχουν χρησιμοποιήσει τα στάδια υλοποίησης για να αποφασίσουν τα ιδανικά επίπεδα αντιμετώπισης των κινδύνων.
- Οι επιχειρήσεις έχουν βρει τον τρόπο να δημιουργούν ισχυρά προφίλ ώστε να κατανοούν σε μεγαλύτερο βαθμό την τωρινή κατάσταση της κυβερνό-ασφάλειας που διαθέτουν.
- Τα προφίλ και τα εκτελεστικά σχέδια χρησιμοποιούνται για την οργάνωση και τον σχεδιασμό ενεργειών κυβερνό-ασφάλειας.

Το πλαίσιο κυβερνό-ασφάλειας ορίζει επτά βήματα για τον καθορισμό ενός προγράμματος κυβερνό-ασφάλειας:

- Ορισμός προτεραιοτήτων και αρμοδιοτήτων
- Προσανατολισμός
- Δημιουργία τρέχοντος προφίλ
- Διενέργεια εκτίμησης κινδύνου
- Δημιουργία προφίλ του επιθυμητού στόχου
- Καθορισμός, ανάλυση και προτεραιότητα των κενών
- Εφαρμογή του σχεδίου δράσης.



Εικόνα 17. Τα επτά βήματα για τον καθορισμό του προγράμματος κυβερνό-ασφάλειας.

3.5.5 ΤΑ ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΠΛΑΙΣΙΟΥ

Το πλαίσιο μπορεί να προσαρμοστεί ώστε να χρησιμοποιηθεί και από επιχειρήσεις με αναπτυσσόμενη ψηφιακή ασφάλεια και προγράμματα αντιμετώπισης κινδύνων και από επιχειρήσεις με λιγότερο σύγχρονα προγράμματα. Η εφαρμογή του πλαισίου δίνει στις επιχειρήσεις ένα εργαλείο για να:

- Αξιολογήσουν και να απεικονίσουν την τωρινή τους κατάσταση όσον αφορά την κυβερνό-ασφάλεια.
- Να αναγνωρίσουν κενά στις παρούσες δραστηριότητες, διαδικασίες και ανθρώπινο δυναμικό.
- Να αναγνωρίσουν και να οργανώσουν ανοιχτές πόρτες για ανάπτυξη με τη χρήση μιας συνεχούς και επαναλαμβανόμενης διαδικασίας.
- Να αξιολογήσουν την εξέλιξη όσον αφορά την επίτευξη του στόχου που έχουν θέσει για την κυβερνό-ασφάλεια
- Να υιοθετήσουν τις ευρέως αποδεκτές διαδικασίες πλαισίου και να τις ενσωματώσουν στις ήδη υπάρχουσες.

3.6 ΚΑΙΡΙΟΙ ΔΕΙΚΤΕΣ ΑΠΟΔΟΣΗΣ (Key Performance Indicators)

Στον πυρήνα του, ένας καίριος δείκτης απόδοσης είναι ένας τρόπος να μετρήσουμε την επιτυχία ή την αποτυχία ενός επιχειρησιακού στόχου, μιας λειτουργίας ή ενός σκοπού και ένα μέσο παροχής ενεργών πληροφοριών πάνω στις οποίες θα βασιστεί η λήψη αποφάσεων. Οι στόχοι σε κάποια τμήματα των επιχειρήσεων ορίζονται ξεκάθαρα όπως για παράδειγμα στο μάρκετινγκ. Ωστόσο, ενώ οι λειτουργίες ασφάλειας μπορεί να παρόμοιους στόχους, οι περισσότεροι από αυτούς τους στόχους είναι λιγότερο πεπερασμένοι. Οι περισσότερες λειτουργίες ασφάλειας επικεντρώνονται περισσότερο στις θετικές ή αρνητικές τάσεις παρά το να επιτύχουν ένα συγκεκριμένο στόχο. Για αυτό ακριβώς είναι σημαντικοί οι καίριοι δείκτες απόδοσης των συστημάτων κυβερνό-ασφάλειας μιας επιχείρησης.

Σημαντικό κομμάτι της διαδικασίας των λειτουργιών ασφαλείας επικεντρώνεται στην ανάλυση των δεδομένων και της αναγνώρισης των μοτίβων και των τάσεων. Αυτό ισχύει και για τις τακτικές λειτουργίες των λειτουργιών ασφαλείας- αναζήτηση μοτίβων επιθέσεων και τάσεων κακόβουλης δραστηριότητας όπως επίσης και τις στρατηγικές λειτουργίες των λειτουργιών ασφαλείας- αναγνώριση κενών στα προγράμματα και η λήψη μακροπρόθεσμων αποφάσεων. Η μέτρηση και η ανάλυση των καίριων δεικτών απόδοσης μπορούν να έχουν πολύ μεγάλο θετικό αντίκτυπο τόσο στις τακτικές όσο και στις στρατηγικές λειτουργίες ενός προγράμματος ασφαλείας.

Οι ποιοτικοί καίριοι δείκτες απόδοσης διευκολύνουν ένα πρόγραμμα ασφάλειας και δίνουν την απαραίτητη ώθηση για διαρκή βελτίωση. Το τοπίο των απειλών είναι ένα δυναμικό περιβάλλον το οποίο αλλάζει συνεχώς και τα αποδοτικά προγράμματα ασφάλειας απαιτούν ενεργές πληροφορίες πάνω στις οποίες μπορεί να βασιστεί η λήψη καθοριστικών αποφάσεων. Οι καίριοι δείκτες απόδοσης βοηθούν στο να διασφαλιστεί πως ένα πρόγραμμα ασφάλειας θα συνεχίσει να είναι αποδοτικό και πως οποιαδήποτε κενά υπάρχουν στις διαδικασίες ή στα προγράμματα θα αντιμετωπίζονται όπως πρέπει.

Ο καθορισμός για το ποιοι δείκτες απόδοσης πρέπει να μετρηθούν δεν ξεκινάει από τους ίδιους τους δείκτες αλλά από την αναγνώριση των στόχων των λειτουργιών ασφάλειας που είναι πιο σημαντικοί για το πρόγραμμα ασφάλειας. Ο καθορισμός των καίριων δεικτών απόδοσης μοιάζει με την αξιολόγηση κινδύνου- πριν δοθεί οποιαδήποτε λύση πρέπει πρώτα να αναγνωριστεί ο κίνδυνος. Το να βρεις τη λύση και

μετά να βρεις το πρόβλημα στο οποίο ανταποκρίνεται η λύση θα οδηγήσει σε ένα αναποτελεσματικό πρόγραμμα αντιμετώπισης κινδύνων που φυσικά δεν θα αντιμετωπίζει τις πραγματικές απειλές. Ο καθορισμός πρώτα των δεικτών και μετά η αναζήτηση των πλευρών του προγράμματος ασφαλείας όπου μπορούν οι δείκτες να δώσουν αποτελέσματα είναι σίγουρο πως θα οδηγήσει σε αποτυχία.

Οι καίριοι δείκτες απόδοσης που δεν προσφέρουν τίποτα στη διαδικασία λήψης αποφάσεων θα πρέπει να αποφεύγονται καθώς δεν εξυπηρετούν ουσιαστικά κάποιο στόχο. Επιπλέον, οι περισσότεροι καίριοι δείκτες απόδοσης κοστίζουν είτε σε χρόνο είτε σε χρήμα. Μπορεί να είναι χρόνος ή χρήμα που θα ξοδευτεί για την αλλαγή μιας διαδικασίας για να διευκολυνθεί η μέτρηση ενός δείκτη, μπορεί να είναι χρόνος που θα ξοδέψει ο αναλυτής για να καταγράψει τον δείκτη ή ο χρόνος που θα ξοδέψει η διοίκηση για να υπολογίσει ή να αξιολογήσει τον δείκτη. Φυσικά, θα υπάρξει κόστος όταν θα γίνει η ανάλυση των δεικτών αλλά θα πρέπει να γίνει μόνο όταν κριθεί πως οι δείκτες που επιλέχθηκαν είναι οι κατάλληλοι.

Όταν γίνεται η επιλογή των καίριων δεικτών απόδοσης που θα μετρηθούν η ποιότητα θα πρέπει να προηγείται της ποσότητας. Κάθε καίριος δείκτης απόδοσης θα πρέπει να έχει σημασία για την επιχείρηση και να προσδίδει αξία στο πρόγραμμα ασφάλειας. Υπάρχουν πολλοί τρόποι για να αξιολογηθεί η αποδοτικότητα ενός δείκτη. Κάθε δείκτης πρέπει να είναι:

Απλός: οι καίριοι δείκτες απόδοσης δεν πρέπει να είναι υπερβολικά περίπλοκοι στη μέτρησή τους. Θα πρέπει να είναι ξεκάθαρο ποιος είναι ο σκοπός κάθε δείκτη και ποιος είναι ο αντίκτυπός του στο πρόγραμμα ασφάλειας.

Μετρήσιμος: ένας δείκτης πρέπει να μπορεί να μετρηθεί με κάποιο τρόπο είτε ποσοτικά είτε ποιοτικά. Η μέθοδος με την οποία μετριέται κάθε δείκτης πρέπει να καθορίζεται με σαφήνεια και συνέπεια.

Ενεργός: οι καίριοι δείκτες απόδοσης θα πρέπει να χρησιμοποιούνται ως οδηγοί για τη λήψη αποφάσεων. Ο σκοπός ενός δείκτη είναι να μετρήσει την επίδοση και αν κριθεί απαραίτητο να αναλάβει δράση με βάση τα αποτελέσματα. Ένας δείκτης που δεν είναι ενεργός δεν επιτελεί κανέναν σκοπό.

Σχετικός: κάθε καίριος δείκτης απόδοσης πρέπει να είναι μέτρηση της λειτουργίας που αξιολογείται και στη συγκεκριμένη περίπτωση του προγράμματος ασφάλειας. Οι

καίριοι δείκτες απόδοσης που είναι απλοί, μετρήσιμοί και ενεργοί αλλά δεν είναι σχετικοί με την λειτουργία που αξιολογείται έχουν μικρή αξία.

Χρονικά προσδιορισμένος: οι καίριοι δείκτες απόδοσης μπορούν και πρέπει να χρησιμοποιούνται για να δείχνουν τις αλλαγές που συμβαίνουν στο πέρασμα του χρόνου. Ένας αποδοτικός δείκτης θα πρέπει να μπορεί να συλλέγεται και να ομαδοποιείται σε διάφορα χρονικά διαστήματα ώστε να φαίνονται οι παραλλαγές και τα μοτίβα.

Οι καίριοι δείκτες απόδοσης σίγουρα θα είναι διαφορετικοί ανάλογα με την επιχείρηση. Ωστόσο υπάρχουν κάποια στοιχεία ενός επιτυχημένου προγράμματος ασφάλειας που θα έπρεπε να μετρηθούν με την χρήση των καίριων δεικτών απόδοσης. Οι περισσότεροι δείκτες των λειτουργιών ασφάλειας θα έπρεπε να στοχεύουν στην αξιολόγηση τουλάχιστον ενός από τα κοινά στοιχεία που παρουσιάζουμε παρακάτω.

Ικανότητες αναλυτών: είναι σημαντικό οι ικανότητες των αναλυτών να ανταποκρίνονται στις ανάγκες της επιχείρησης. Κενά στις ικανότητες τους μπορεί να οδηγήσουν σε ανεπάρκειες στην διαδικασία διαχείρισης περιστατικών και να αυξήσει τον βαθμό κινδύνου για την εταιρεία. Η χρήση των καίριων δεικτών απόδοσης για να μετρηθούν οι ικανότητες των αναλυτών και στη συνέχεια να συγκριθούν με τις ανάγκες της επιχείρησης μπορεί να αποκαλύψει κενά στην εκπαίδευση και το προσωπικό, τα οποία μπορούν να αντιμετωπιστούν και να βελτιωθεί έτσι η συνολική ετοιμότητα της επιχείρησης.

Επιτυχία ανίχνευσης: οι τεχνολογίες πρόληψης και ανίχνευσης θα πρέπει να ενδυναμώνουν και να συμπληρώνουν την ομάδα ασφάλειας. Μη αποδοτικές τεχνολογίες πρόληψης και ανίχνευσης σημαίνει πως είναι πολύ πιθανό να μην γίνουν αντιληπτά διάφορα περιστατικά ασφάλειας και πως οι αναλυτές θα αναγκαστούν να ξοδέψουν περισσότερο χρόνο κάνοντας χειροκίνητη ανάλυση. Η χρήση των καίριων δεικτών για να μετρηθεί η απόδοση των τεχνολογιών πρόληψης και ανίχνευσης μπορεί να αποκαλύψει κενά όπου η επιπλέον τεχνολογία θα μπορούσε να ωφελήσει την εταιρεία όπως επίσης να βρεθούν τρόποι με τους οποίους οι τωρινές τεχνολογίες πρόληψης και ανίχνευσης θα μπορούσαν να γίνουν πιο αποδοτικές.

Βασικοί κίνδυνοι: οι επιχειρήσεις έρχονται αντιμέτωπες με μυριάδες κινδύνους και περιορισμένο προϋπολογισμό για να τους αντιμετωπίσουν. Οι περισσότερες επιχειρήσεις μπαίνουν στην κουραστική διαδικασία να αποφασίσουν ποιους κινδύνους

θα πρέπει να αντιμετωπίσουν και ποιους να αποδεχτούν. Η χρήση των δεικτών μπορεί να βοηθήσει στην αναγνώριση των κινδύνων εκείνων που αποτελούν μεγαλύτερη απειλή για την εταιρεία επιτρέποντας στην ομάδα ασφάλειας να προσφέρει ενεργές πληροφορίες στην συνολική διαδικασία αξιολόγησης κινδύνου, μεγιστοποιώντας την αποτελεσματικότητα του περιορισμένου χρόνου αλλά και των περιορισμένων πόρων της επιχείρησης.

Επιτυχία άμβλυνσης: μόλις αναγνωριστεί το περιστατικό ασφάλειας θα πρέπει να αμβλυνθεί. Όπως στην πρόληψη και την ανίχνευση, η τεχνολογία χρησιμοποιείται συχνά για να αυξήσει την αποτελεσματικότητα και την επιτυχία της διαδικασίας άμβλυνσης. Ωστόσο, η αποτελεσματικότητα και η επιτυχία είναι εφικτές μόνο αν οι τεχνολογίες είναι αποτελεσματικές. Αναποτελεσματικές τεχνολογίες άμβλυνσης μπορεί να οδηγήσουν σε λιγότερη αποτελεσματικότητα και επιτυχία από το αν η ολόκληρη η διαδικασία άμβλυνσης γινόταν χειροκίνητα με αποτέλεσμα ο αντίκτυπος του συμβάντος να είναι μεγαλύτερος. Η χρήση των δεικτών για τη μέτρηση της επίδοσης των τεχνολογιών άμβλυνσης μπορεί να αναγνωρίσει κενά όπου η επιπλέον τεχνολογία μπορεί να ωφελήσει την επιχείρηση όπως επίσης τρόπους με τους οποίους μπορεί να τροποποιηθεί η χρήση των υπαρχόντων τεχνολογιών άμβλυνσης ώστε να αυξηθεί η αποδοτικότητά τους.

Επιτυχία διαδικασίας: οι διαδικασίες αποτελούν καίριο στοιχείο της επιτυχίας οποιασδήποτε ομάδας ασφάλειας. Ωστόσο, για να είναι επιτυχημένες οι διαδικασίες δεν θα πρέπει να μένουν στατικές. Θα πρέπει να αξιολογούνται συνεχώς και να προσαρμόζονται για να διασφαλιστεί πως επιτρέπουν στην ομάδα ασφάλειας να αντιμετωπίσει τα ζητήματα ασφάλειας με τον πιο αποδοτικό και αποτελεσματικό τρόπο. Διαδικασίες που δεν έχουν σχεδιαστεί σωστά μπορεί να οδηγήσουν σε σύγχυση και εκνευρισμό με τους αναλυτές να αυτοσχεδιάζουν και τον αντίκτυπο του συμβάντος να μεγαλώνει. Η χρήση των καίριων δεικτών απόδοσης για την μέτρηση των διαδικασιών επιτρέπει στην επιχείρηση να διασφαλίσει πως οι διαδικασίες βελτιώνονται και μπορούν να αντιμετωπίσουν αποτελεσματικά ένα ευρύ φάσμα περιστατικών ασφάλειας.

Φόρτος εργασίας: οι αναλυτές που έχουν μεγάλο φόρτο εργασίας είναι πολύ πιθανό να διαλέγουν τον σύντομο δρόμο για να ολοκληρώσουν τη δουλειά τους ή να μην αντιληφθούν βασικές ενδείξεις περιστατικών ασφαλείας. Αναλυτές με μεγάλο φόρτο

εργασίας είναι επίσης πιθανό να αναζητήσουν καινούργιες ευκαιρίες σε άλλη επιχείρηση παίρνοντας μαζί τους την πολύτιμη εκπαίδευση και εμπειρία. Η χρήση των καίριων δεικτών για τη μέτρηση του φόρτου εργασίας των αναλυτών μπορεί να εντοπίσει αδυναμίες στο προσωπικό που μπορεί να αποτελέσουν σοβαρό κίνδυνο για την εταιρεία.

Οι καίριοι δείκτες απόδοσης παρέχουν κρίσιμες πληροφορίες που απαιτούνται για τη λήψη αποφάσεων. Παρόλα αυτά, η παρακολούθηση πάρα πολλών δεικτών μπορεί να γίνει εμπόδιο για τους αναλυτές από τους οποίους προέρχονται οι πληροφορίες και για αυτούς που λαμβάνουν τις αποφάσεις οι οποίοι θα πρέπει να λάβουν υπόψη τους υπερβολικά πολλές πληροφορίες. Δεν υπάρχει κάποιος συγκεκριμένος αριθμός δεικτών που θα πρέπει να παρακολουθεί μια επιχείρηση. Κάποιοι ισχυρίζονται πως πρέπει να είναι τρείς ανά στόχο ενώ άλλοι προτείνουν πέντε με εννιά δείκτες συνολικά. Στην πραγματικότητα, ένα νούμερο μεταξύ αυτών που αναφέρθηκαν είναι πιθανώς κατάλληλο για τα προγράμματα ασφάλειας των επιχειρήσεων. Όπως συμβαίνει και με τους ίδιους τους δείκτες, αυτό που χρειάζεται το κάθε πρόγραμμα και η κάθε επιχείρηση είναι πολύ πιο σημαντικό από οποιοδήποτε αριθμό. Παρακάτω παραθέτουμε τους πιο βασικούς καίριους δείκτες απόδοσης που χρησιμοποιούν οι περισσότερες μεγάλες επιχειρήσεις.

Καίριοι δείκτες απόδοσης	**Πιθανές μετρήσεις**	**Αξιολόγηση**
Αριθμός συσκευών που παρακολουθούνται	Αριθμός συσκευών	Φόρτου εργασίας
Συνολικός αριθμός συμβάντων	Αριθμός συμβάντων ανά ώρα, μέρα, μήνα, χρόνο, είδος	Κόστος αξιολόγησης Βασικοί κίνδυνοι Φόρτος εργασίας
Αριθμός συμβάντων ανά συσκευή	Αριθμός συμβάντων ανά συσκευή ανά ώρα, μέρα, μήνα, χρόνο, είδος λειτουργικού συστήματος	Επιτυχία ανίχνευσης Βασικοί κίνδυνοι
Αριθμός συμβάντων ανά υπηρεσία ή εφαρμογή	Αριθμός συμβάντων ανά υπηρεσία	Επιτυχία ανίχνευσης Βασικοί κίνδυνοι

	Αριθμός συμβάντων ανά εφαρμογή	
Αριθμός συμβάντων ανά λογαριασμό	Αριθμός συμβάντων ανά λογαριασμό Αριθμός συμβάντων ανά χρήστη	Επιτυχία ανίχνευσης Βασικοί κίνδυνοι
Αριθμός συμβάντων ανά τοποθεσία	Αριθμός συμβάντων ανά τμήμα Αριθμός συμβάντων ανά γραφείο Αριθμός συμβάντων ανά περιοχή	Βασικοί κίνδυνοι
Αριθμός εσφαλμένων συναγερμών	Αριθμός εσφαλμένων συναγερμών ανά ώρα, μέρα, μήνα, χρόνο	Επιτυχία ανίχνευσης
Χρόνος ανίχνευσης	Μέτρηση σε λεπτά, ώρες ή μέρες Μέσος όρος χρόνου ανίχνευσης	Επιτυχία ανίχνευσης Επιτυχία διαδικασίας
Χρόνος επίλυσης	Μέτρηση σε λεπτά, ώρες ή μέρες Μέσος όρος χρόνου επίλυσης	Επιτυχία άμβλυνσης Επιτυχία διαδικασίας
Χρόνος αναγνώρισης συμβάντος ως εσφαλμένου συναγερμού	Μέτρηση σε λεπτά, ώρες ή μέρες Μέσος όρος χρόνου αναγνώρισης	Ικανότητες αναλυτών Επιτυχία διαδικασίας
Αριθμός αναλυτών που ανέλαβαν τα περιστατικά	Μέσος όρος αριθμού αναλυτών ανά περιστατικό	Ικανότητες αναλυτών Κόστος αξιολόγησης Επιτυχία διαδικασίας
Επίπεδο κλιμάκωσης	Μέσος όρος περιστατικών Επίπεδο κλιμάκωσης ανά περιστατικό	Ικανότητες αναλυτών Κόστος αξιολόγησης Επιτυχία διαδικασίας

	Επίπεδο κλιμάκωσης ανά τεχνολογία Μέσος όρος χρόνου κλιμάκωσης	
Πηγή περιστατικού	Συνολικός αριθμός περιστατικών ανά τεχνολογία Συνολικός αριθμός εσφαλμένου συναγερμού ανά τεχνολογία	Επιτυχία ανίχνευσης Βασικοί κίνδυνοι

ΚΕΦΑΛΑΙΟ 4Ο

ΣΥΜΠΕΡΑΣΜΑΤΑ

Στην παρούσα εργασία αναλύσαμε μία σύγχρονη δομή κυβερνοασφάλειας για επιχειρήσεις και δώσαμε έμφαση στους κύριους δείκτες απόδοσης (KPI) περιγράφοντας κάποιους βασικούς δείκτες που πιστεύουμε ότι πρέπει να αποτελούν προσχέδιο για την ανάπτυξη συγκεκριμένων δεικτών προσαρμοσμένους στις ανάγκες της εκάστοτε επιχείρησης. Παρουσιάσαμε κακόβουλες μεθόδους που χρησιμοποιούνται από κυβερνοεκγληματίες, οι οποίες σύμφωνα με το Official Cybercrime Report (Cybersecurity Ventures, 2021) κόστισαν παγκοσμίως 6 δισεκατομμύρια δολάρια το έτος 2021.

Προσπαθήσαμε να περιγράψουμε τις προκλήσεις που θα αντιμετωπίσει ο υπεύθυνος ασφάλειας (CISO) ο οποίος θα πρέπει να οργανώσει το πλαίσιο κυβερνοασφάλειας. Ο ρόλος του Θα είναι ουσιαστικός καθώς Θα πρέπει αρχικά να περιγράψει την τρέχουσα κατάσταση κυβερνοασφάλειας της επιχείρησης. Για να το πετύχει αυτό θα πρέπει να συλλέξει τα δεδομένα με τη βοήθεια συγκεκριμένων εργαλείων. Έπειτα θα πρέπει να σχεδιάσει την κατάσταση τις κυβερνοασφάλειας για τους επόμενους έξι μήνες, ένα χρόνο και δύο χρόνια στο μέλλον, ώστε να θέσει τους στόχους για την κατάσταση στην οποία η επιχείρηση θα πρέπει να βρίσκεται στο μεσοπρόθεσμα και μακροπρόθεσμα. Με τη χρήση εργαλείων λογισμικού της το τμήμα της κυβερνοασφάλειας θα έχει τη δυνατότητα να καταγράφει με ακριβή τρόπο τα βήματα που ακολουθεί, για να πετύχουν τους στόχους του. Οι υπεύθυνοι των επιμέρους τμημάτων του τομέα κυβερνοασφάλειας θα είναι πρέπει να καταγράφουν την αξιολόγηση της προόδου. Μία πρόκληση για τον υπεύθυνο ασφαλείας θα είναι να πείσει το διοικητικό συμβούλιο της επιχείρησης να αφιερώσει τους κατάλληλους πόρους στο τμήμα της κυβερνοασφάλειας, κάτι που δεν είναι εύκολο για ένα τμήμα όπου δεν μπορεί να παρουσιαστεί σαν κερδοφόρο. Αυτό όμως σε καμία περίπτωση δεν μπορεί να αμφισβητήσει τη σημαντικότητα της καθώς μία επίθεση θα μπορούσε να αποφέρει τεράστια ζημιά οικονομική αλλά και επικοινωνιακή για την εταιρεία. \Ένα πολύ σημαντικό εργαλείο στη διάθεσή του υπεύθυνου ασφαλείας είναι η χρήση καίριων δεικτών απόδοσης μέσω των οποίων μπορεί να μετρηθεί μία πληθώρα δεικτών και να

παρουσιαστεί με αυτό τον τρόπο η πραγματική συνεισφορά του τμήματος κυβερνοασφάλειας.

Σύμφωνα με τον Παγκόσμιο Οργανισμό δεδομένων IDC, το κόστος της επένδυσης σε κυβερνοασφάλεια θα φτάσει στα 175 δισεκατομμύρια δολάρια παγκοσμίως, μόλις του 2024 με τις υπηρεσίες της κυβερνοασφάλειας να αναπτύσσονται ραγδαία. Ταυτόχρονα παρατηρείται έλλειψη εξιδεικευμένου προσωπικού με το 65% των επιχειρήσεων να αναφέρουν πως είναι υποστελεχωμένες (ISC, 2019). Καθώς τα δεδομένα έχουν γίνει πια το πολυτιμότερο αγαθό, όλο και περισσότεροι κακόβολοι παράγοντες θα προσπαθούν να κερδοφορήσουν παράνομα. Η Αυτοματοποίηση διεργασιών καθώς και η συνεχής απλοποίηση των πρακτικών είναι αναγκαίες για να μπορέσουν οι επιχειρήσεις να παραμείνουν ασφαλείς υπό αυτές τις συνθήκες. Αυτές οι τεχνικές μαζί με τις βέλτιστες πρακτικές, την εσωτερική αυτορρύθμιση και τον ολιστικό σχεδιασμό της ασφάλειας, μπορούν να μειώσουν το ρίσκο αποθαρρύνοντας πιθανές απειλές.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Amoroso, E. 2006. *Cyber Security*. New Jersey: Silicon Press

Bischoff, P., 2021, The cost of hiring a hacker on the dark web: report. Comparitech. https://www.comparitech.com/ blog/information-security/hiring-hacker-dark-web-report/

Canongia, C., & Mandarino, R. 2014. Cybersecurity: The New Challengeof the Information Society. In Crisis Management: Concepts, Methodologies, Tools and Applications: 60-80. Hershey, PA: IGIGlobal. Http://dx.doi.org/10.4018/978-1-4666-4707-7.ch003

Chang, F. R. 2012. Guest Editor's Column. The Next Wave, 19(4): 1–2.

Chaubey K.R, 2012, An Introduction to Cyber Crime and Cyber law. Kolkata: Kamal Law House.

CNSS. 2010. National Information Assurance Glossary. Committee on National Security Systems (CNSS) Instruction No. 4009: http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf

DHS. 2014. A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and studies: Department of Homeland Security. October 1, 2014: http://niccs.us-cert.gov/glossary#letter_c

Deffree S,2019, 1st computer virus is written, January 30, 1982, https://www.edn.com/1st-computer-virus-is-written-january-30-1982/

Feradhita NKD, 2020, A Brief Introduction to Ancient Malware: The Creeper Virus. https://www.logique.co.id/blog/en/2020/02/27/brief-introduction-ancient-malware-creeper-virus/

Franceschi-Bicchierai, L., 2021. How the Mafia Is Pivoting to Cybercrime. Vice. https://www.vice.com/en/article/ epne4j/how-the-mafia-is-pivoting-to-cybercrime

Goodall, J. R., Lutters, W. G., & Komlodi, A. 2009. Developing Expertise for Network Intrusion Detection. Information Technology & People, 22(2): 92-108.http://dx.doi.org/10.1108/09593840910962186

IBM Security. 2020. Cost of a Data Breach Report 2020. IBM Corporation. p.5. https://www.ibm.com/security/digitalassets/cost-data-breach-report/1Cost%20of%20a%20Data%20Breach%20Report%202020.pdf

ITU. 2009. Overview of Cybersecurity. Recommendation ITU-T X.1205.Geneva: International Telecommunication Union (ITU).http://www.itu.int/rec/T-REC-X.1205-200804-I/en

Jeetendra P.,2017, Introduction to Cyber Security. Haldwani: Uttarakhand Open University

Kapoor, A. Gupta, R. Tanwar, S. Sharma, G., Davidson, I.E.,2022, Ransomware Detection, Avoidance, and Mitigation Scheme: A Review and Future Directions. Sustainability 2022, 14, 8. https://doi.org/10.3390/su14010008

Kemmerer, R. A. 2003. Cybersecurity. Proceedings of the 25th IEEE International Conference on Software Engineering: 705-715.http://dx.doi.org/10.1109/ICSE.2003.1201257

Lewis, J. A. 2006. Cybersecurity and Critical Infrastructure Protection. Washington, DC: Center for Strategic and International Studies http://csis.org/publication/cybersecurity-and-critical-infrastructure-protection

Matrosov A, Rodionov E, Bratus S,2019, Rootkits and bootkits Reversing Modern Malware and Next Generation Threats. San Francisco: No Starch Press, Inc

Άρης Αλεξόπουλος, Γιώργος Λαγογιάννης, 2010, *Τηλεπικοινωνίες και Δίκτυα Υπολογιστών*, 7η έκδοση, Αθήνα

Oxford University Press. 2022, Oxford Online Dictionary. Oxford: Oxford University Press https://www.lexico.com/definition/cybersecurity

Max Roser, Hannah Richie, 2020, "Technological Progress", OurWorldInData.org. https://ourworldindata.org/technological-progress.

Public Safety Canada. 2010. Canada's Cyber Security Strategy. Ottawa: Public Safety Canada, Government of Canada. http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-eng.aspx

Shashank, 2022, A Beginner's Guide To Cybersecurity Framework, https://www.edureka.co/blog/cybersecurity-framework/

A Report form CISCO,2010, Cybersecurity: Everyone's Responsibility, 2010.

Cost of a Data Breach Report 2021. 2021. IBM. https://www.ibm.com/security/data-breach

Cyber Security Governance, https://cyberrisk-countermeasures.info/cyber-security-governance/

How it Works https://www.internetsociety.org/internet/how-it-works/

Key Performance Indicators (KPIs) for Security Operations and Incident Response. Identifying Which KPIs Should Be Set, Monitored and Measured. https://www.acadiatech.com/wp-content/uploads/2020/11/SOAR-KPIs.pdf

The History of Computer Viruses, https://www.bbvaopenmind.com/en/technology/digital-world/the-history-of-computer-viruses/

The Morris Worm, 30 Years Since First Major Attack on the Internet, https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

22 Types of Malware and How to Recognize Them in 2022 https://www.upguard.com/blog/types-of-malware

https://www.britannica.com/topic/cybercrime

Τι είναι το keylogger; https://www.getcert.gr/ti-einai-to-keylogger/

Τι είναι Root Nameserver ή DNS Root Servers σε DNS Servers, https://www.informatique-mania.com/el/linternet/que-sont-le-serveur-de-noms-racine-ou-les-serveurs-racine-dns-dans-les-serveurs-dnsslug/

N. 4070/2012, https://www.kodiko.gr/nomothesia/document/117878/nomos-4070-2012

N. 4577/2018 (ΦΕΚ 199/Α'/03-12-2018), https://www.e-nomothesia.gr/kat-nomothesia-genikou-endiapherontos/nomos-4577-2018-phek-199a-3-12-2018.html