ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Αντιμετώπιση ενός Ransomware σε μικρομεσαία επιχείρηση. Τρόποι αντιμετώπισης, επάνοδος της επιχείρησης και επιπτώσεις στην επιχείρηση.** **Incident response for a ransomware attack on an SME: Mitigation methods, business recovery and impact**
Ονοματεπώνυμο Φοιτητή	**Ιωάννης Γοζαδίνος**
Πατρώνυμο	**Αθανάσιος**
Αριθμός Μητρώου	**ΜΜΠΛ18012**
Επιβλέπων	**Κωνσταντίνος Πατσάκης, Αναπληρωτής Καθηγητής**

Ημερομηνία Παράδοσης **Ιούλιος 2024**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Κωνσταντίνος Πατσάκης Αναπληρωτής Καθηγητής	Ευθύμιος Αλέπης Καθηγητής	Ευάγγελος Σακκόπουλος Αναπληρωτής Καθηγητής

ΠΕΡΙΛΗΨΗ

Η εξάρτηση φυσικών προσώπων αλλά και επιχειρήσεων από το διαδίκτυο στη σύγχρονη εποχή, δημιουργεί προβληματισμό σχετικά με τις αυξανόμενες κυβερνοεπιθέσεις. Το ζήτημα της ασφάλειας του διαδικτύου θέτει σε κίνδυνο προσωπικά δεδομένα και βάσεις δεδομένων επιχειρήσεων. Η εμφάνιση τέτοιου είδους προγραμμάτων με στόχο την υποκλοπή δεδομένων αλλά και στον συνεχή εκβιασμό των θυμάτων για λύτρα έχουν αποτελέσει το εφαλτήριο για τη δημιουργία ενός πλέγματος ασφαλείας.

Είναι πλέον συχνή τακτική η παγίδευση των χρηστών από hackers μέσω κακόβουλων μηνυμάτων. Οι όροι όπως «spam mails», «phishing» έχουν εισχωρήσει στην καθημερινότητά μας και οι κυβερνοεγκληματίες προσπαθούν να επωφεληθούν όσο γίνεται περισσότερο προκειμένου να αποκομίσουν «λύτρα» από τους υποψήφιους στόχους τους.

Οι στρατηγικές των επιχειρήσεων για τη διασφάλιση των προσωπικών τους δεδομένων συνθέτουν ένα πλαίσιο κανόνων και οδηγιών που οφείλουν να ακολουθηθούν προκειμένου να συνεχιστεί η βέλτιστη λειτουργία τους.

Συνεπώς, η εργασία αυτή αποτελεί μελέτη για το ρόλο των ransomware επιθέσεων και του αντικτύπου τους στην εύρωστη λειτουργία μίας μικρομεσαίας επιχείρησης. Γίνεται μία παρουσίαση των σημαντικότερων ζητημάτων και επιπτώσεων που προκαλούν τέτοιου είδους συνθήκες, οι διαδικασίες που πρέπει να ακολουθηθούν από τους εργαζόμενους προκειμένου να μην στοχοποιηθούν αλλά και ενδεχομένως οι επιπτώσεις που θα προκύψουν στην περίπτωση που δεν αποφευχθεί η οικονομική ζημία.

ABSTRACT

The rapid dependence of individuals and businesses on cyberspace in the modern era has raised concerns about the ever-increasing cyber-attacks that are occurring online. The issue of security in the vast world of the internet primarily puts personal data at high risk as the emergence of powerful programs designed to intercept and constantly extort ransom from victims has been the main goal for the creation of a security grid.

It is now a common practice for hackers to trap users through malicious messages. Terms such as "spam mails", "phishing" form a part of our daily vocabulary while cybercriminals try to take advantage of their potential targets' weaknesses to demand "ransoms".

Businesses' strategies for securing their personal data constitute a framework of rules and guidelines that must be followed to continue to operate optimally.

Therefore, this thesis is a study of the role of ransomware attacks and their impact on the robust operation of an SME. A presentation is made of the major issues and impacts caused

by such conditions, the procedures to be followed by employees in order to avoid being targeted and potentially the consequences that will arise if financial loss is not avoided.

ΕΙΣΑΓΩΓΗ

Με την ραγδαία τεχνολογική εξέλιξη και την εξάρτηση από τον κυβερνοχώρο το ζήτημα της ασφάλειας του ψηφιακού κόσμου έχει καταστεί πιο κρίσιμο από ποτέ. Ιδιαίτερα οι μικρομεσαίες επιχειρήσεις αποτελούν στόχο για κυβερνοεπιθέσεις, λόγω των περιορισμένων πόρων τους για την ανάπτυξη ισχυρών συστημάτων ασφαλείας. Μια από τις πιο επικίνδυνες και συχνές απειλές που αντιμετωπίζουν είναι το ransomware, ένα είδος κακόβουλου λογισμικού που κρυπτογραφεί τα δεδομένα της επιχείρησης και απαιτεί λύτρα για την αποκατάστασή τους.

Ο όρος **ransomware** προέρχεται από τη λέξη «λύτρα» (ransom) και «λογισμικό» (software). Σύμφωνα με τον ορισμό του **NIST**, το ransomware είναι είδος κακόβουλου λογισμικού που κρυπτογραφεί τα δεδομένα της επιχείρησης του οποίου οι χειριστές / διαχειριστές απαιτούν λύτρα για την αποκατάστασή τους.

Οι επιθέσεις ransomware ξεκινούν συνήθως με την αποστολή ενός κακόβουλου email, το οποίο περιέχει ένα μολυσμένο συνημμένο αρχείο ή έναν κακόβουλο σύνδεσμο. Μόλις ο χρήστης κάνει κλικ, το ransomware εγκαθίσταται στον υπολογιστή του και αρχίζει να διαδίδεται σε όλο το δίκτυο της επιχείρησης, κρυπτογραφώντας αρχεία με στόχο τις οικονομικές απολαβές σε μορφή κρυπτονομισμάτων για την αποκρυπτογράφησή τους.

Οι επιπτώσεις μιας επίθεσης ransomware μπορούν να αποβούν καταστροφικές για μια μικρομεσααία επιχείρηση αν δεν έχει θωρακιστεί καταλλήλως. Οι οικονομικές ζημίες περιλαμβάνουν το άμεσο κόστος των λύτρων, τις έμμεσες οικονομικές απώλειες από την διακοπή λειτουργίας, καθώς και τις επιπτώσεις στη φήμη της επιχείρησης.

Η αναστολή λειτουργίας μπορεί να οδηγήσει σε απώλεια παραγωγικότητας και υψηλά κόστη ανάκτησης των δεδομένων καθώς και η απώλεια εμπιστοσύνης από τους πελάτες μπορεί να έχει μακροπρόθεσμες επιπτώσεις στην επιχειρηματική στρατηγική και φήμη της εταιρείας.

Για την αποτελεσματική αντιμετώπιση και ανάκαμψη από μια επίθεση ransomware, οι επιχειρήσεις πρέπει να εφαρμόσουν ένα σύνολο στρατηγικών που θα περιλαμβάνουν τόσο προληπτικά όσο και αντιδραστικά μέτρα.

Η εκπαίδευση των εργαζομένων στην αναγνώριση και αποφυγή κακόβουλων μηνυμάτων, η δημιουργία τακτικών αντιγράφων ασφαλείας και η εφαρμογή αυστηρών πολιτικών ασφαλείας πληροφορικών συστημάτων είναι μερικές από τις βασικές προληπτικές στρατηγικές.

Σε περίπτωση επίθεσης, η ύπαρξη ενός σχεδίου αντιμετώπισης συμβάντων και η συνεργασία με ειδικούς στην κυβερνοασφάλεια μπορούν να συμβάλλουν στην ταχεία αποκατάσταση της λειτουργικότητας της επιχείρησης.

Η προστασία από τις επιθέσεις ransomware απαιτεί μια ολιστική προσέγγιση που συνδυάζει την τεχνολογική υποδομή με την εκπαίδευση και ευαισθητοποίηση των εργαζομένων. Για μία μικρομεσαία επιχείρηση, η επένδυση σε μέτρα κυβερνοασφάλειας δεν αποτελεί πλέον επιλογή, αλλά αναγκαιότητα για την επιβίωση και την ανάπτυξή της στον σύγχρονο ψηφιακό κόσμο. Η συνεχής αναβάθμιση των συστημάτων ασφαλείας και η προσαρμογή στις νέες απειλές είναι απαραίτητες για την προστασία των δεδομένων και τη διασφάλιση της επιχειρηματικής συνέχειας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1: RANSOMWARE

1.1 ΟΡΙΣΜΟΣ

Με βάση το NIST ως Ransomware ορίζεται ένας τύπος κακόβουλης επίθεσης όπου οι «εισβολείς» κρυπτογραφούν τα δεδομένα ενός οργανισμού και απαιτούν πληρωμή με στόχο την αποκατάσταση και ανάκτηση της πρόσβασης στα δεδομένα.

Ακολουθεί ένα παράδειγμα για το πώς μπορεί να συμβεί μια επίθεση ransomware:

1. Ένας χρήστης λαμβάνει ένα email και εν αγνοία του κάνει κλικ στον συνημμένο σύνδεσμο που υπάρχει στο μήνυμα και έτσι κατεβάζει ένα αρχείο από έναν εξωτερικό ιστότοπο μόνο που ο σύνδεσμος αυτός είναι κακόβουλος.
2. Ο χρήστης προχωράει κανονικά στην εκτέλεση ή στην χρήση ου αρχείου μη γνωρίζοντας πως το αρχείο αυτό είναι ransomware.
3. Η διαδικασία που ακολουθεί το ransomware είναι να εκμεταλλευτεί τις όποιες ευπάθειες τόσο στον υπολογιστή του χρήστη όσο και στους υπόλοιπους υπολογιστές του οργανισμού ώστα να διαδοθεί.
4. Παράλληλα το ransomware κρυπτογραφεί αρχεία σε όλους τους υπολογιστές και στη συνέχεια, εμφανίζει μηνύματα στις οθόνες των χρηστών απαιτώντας την πληρωμή με αντάλλαγμα – κατά κύριο λόγο σε μορφή κρυπτονομισμάτων- ώστε να προχωρήσει στην αποκρυπτογράφηση των αρχείων που έχουν κλειδωθεί.

Οι πιο συχνοί τρόποι με τους οποίους ένα ransomware μπορεί να χτυπήσει μία επιχείρηση είναι οι κάτωθι:

• **Μέσω Email** : Σε καθημερινή βάση όλοι οι εργαζόμενοι σε μικρομεσαίες επιχειρήσει δέχονται πληθώρα μηνυμάτων, κάποια από τα οποία μπορεί να είναι μηνύματα ηλεκτρονικού ψαρέματος, τόσο καλά φτιαγμένα που μπορούν να σας εξαπατήσουν ώστε να κάνετε κλικ σε ένα συνημμένο («Επείγοντα τιμολόγιο», αλλαγή στοιχείων τραπεζικής κάρτας, κλπ.) και έτσι δίνεται η ανάλογη πρόσβαση στο κακόβουλο πρόγραμμα λογισμικού να μολύνει τον υπολογιστή σας.

• **Μέσω Κακόβουλου λογισμικού**: Εάν το δίκτυο ή κάποιο λογισμικό είναι ευάλωτο, τότε πολύ εύκολα ένας εγκληματίας του κυβερνοχώρου [hacker] μπορεί να εισέλθει κρυφά και να εγκαταστήσει ένα κακόβουλο κώδικα ή αρχείο. Με τον τρόπο αυτό έχει τη δυνατότητα να παραμείνει ανενεργό και απαρατήρητο για κάποιο χρονικό διάστημα είτε μικρό είτε μεγάλο, δίνοντας τον χρόνο να υπάρξει η απαραίτητη πρόσβαση σε αρχεία με σκοπό να κλαπούν δεδομένα, και στη συνέχεια να ολοκληρωθεί με την απελευθέρωση ενός ransomware, με την παραπάνω διαδικασία αυτό είναι μη αντιληπτό από την πλευρά του χρήστη.

Το ransomware αποτελεί πλέον μια κοινή απειλή για κάθε επιχείρηση, μεγάλη ή μικρή. Αυτό μπορεί να προκαλέσει διάφορα θέματα όπως να θέσει μια εταιρεία εκτός λειτουργίας ή να διαταράξει τις λειτουργίες για μεγάλο χρονικό διάστημα. Η πληρωμή των λύτρων μπορεί να είναι πολύ ακριβή και δεν υπάρχει καμία εγγύηση ότι τα δεδομένα θα ανακτηθούν ποτέ. Εάν κλαπούν δεδομένα πελατών, ενδέχεται να ενεργοποιηθούν οι νόμοι για την ειδοποίηση παραβίασης δεδομένων. Επιπλέον έχει τη δυνατότητα να διακόψει τις λειτουργίες ενός οργανισμού και θέτει το εξής δίλημμα στην διοίκηση της επιχείρησης: ο οργανισμός πληρώνει τα λύτρα και ελπίζει ότι οι εισβολείς τηρούν τον λόγο τους σχετικά με την αποκατάσταση της πρόσβασης ή ο οργανισμός δεν προχωράει στην πληρωμή και αποκαθιστά ο ίδιος τις όποιες λειτουργίες έχουν υποστεί ζημιά.

Πλέον δίνεται η δυνατότητα στους οργανισμούς ώστε να μπορούν να λάβουν μέτρα με απώτερο στόχο την προετοιμασία τους σε πιθανές επιθέσεις ransomware. Αυτό περιλαμβάνει την προστασία δεδομένων και συσκευών από ransomware και την ετοιμότητα να ανταποκριθεί σε οποιεσδήποτε επιθέσεις ransomware που πετυχαίνουν.

1.1.1 Ποια περιουσιακά στοιχεία μολύνονται από ransomware.

Μία μικρομεσαία επιχείρηση διαθέτει μία σειρά περιουσιακών στοιχείων εκ των οποίων ορισμένα θεωρούνται ως η κερκόπορτα για ένα Ransomware. Τα παρκάτω περιουσιακά στοιχεία που παρατίθονται θεωρούνται με βάση τον κατάλογο της ENISA τα πιο συχνά περιουσιακά στοιχεία που αποτελούν στόχο ενός ransomware.

- Αρχεία (Files)
- Φάκελοι (Folders)
- Μνήμη (Memory)
- Περιεχόμενο βάσης δεδομένων (Data Base)
- Οθόνη (Screen)
- Πίνακας κύριων αρχείων [master file table – (mft)]
- Master root record [mbr]
- Cloud
- Σύστημα διαχείρισης περιεχομένου [content management system – (cms)

1.1.2 Τι προκαλεί μια μόλυνση ransomware

Οι κύριες αιτίες του ransomware περιλαμβάνουν το phishing, τις κακές πρακτικές των χρηστών και τους αδύναμους κωδικούς πρόσβασης.

Το 41% των επιθέσεων ransomware χρησιμοποιούν το phishing ως μέθοδο παράδοσης. Αυτά τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου περιέχουν έναν σύνδεσμο στον οποίο, όταν γίνει κλικ, θα μπορούσε να κατεβάσει το ransomware ή να μεταφέρει τον στόχο

σε έναν πλαστό ιστότοπο, όπου οι χάκερ μπορούν να δουν τις λεπτομέρειες που εισάγουν. Άλλοτε, περιέχουν κάποιο επισυναπτόμενο αρχείο το οποίο θα δελεάσει τον χρήστη να το ανοίξει, π.χ. έγγραφο του MS Office, PDF κτλ., τα οποία θα κατεβάσουν κακόβουλο κώδικα από κάποια ιστοσελίδα και θα τον εκτελέσουν [11].

Μια μελέτη με περισσότερα από 2000 θύματα επιθέσεων στον κυβερνοχώρο διαπίστωσε ότι το 63% είχαν παραβιαστεί τα διαπιστευτήριά τους, τα οποία θα μπορούσαν να χρησιμοποιηθούν σε περαιτέρω επιθέσεις για να εισέλθουν σε επιχειρηματικά δίκτυα και να εισαγάγουν ransomware.

Αν και οι απλές επιθέσεις τύπου ransomware έχουν την δυνατότητα να κλειδώσουν ένα σύστημα με τέτοιον τρόπο που δεν είναι δύσκολο να ξεκλειδωθεί από ένα έμπειρο άτομο στον τομέα της πληροφορικής και ειδικότερα της κυβερνοασφάλειας, οι πιο εξελιγμένες επιθέσεις αυτού του είδους χρησιμοποιούν τεχνικές που συνδυάζουν την κρυπτογραφία με την κακόβουλη σχεδίαση λογισμικού (cryptoviral extortion), ώστε να πετύχουν την κρυπτογράφηση των αρχείων του θύματος, καθιστώντας τα μη προσβάσιμα και ζητώντας λύτρα για την αποκρυπτογράφησή τους. Μάλιστα, αν και αυτό δεν είναι αρκετό, θα απειλήσουν με την δημοσίευση των αρχείων του θύματος, προκειμένου να το πείσουν να πληρώσει τα λύτρα [12].

1.1.3 Τα Εξι Σταδια Μιας Επιθεσης Ransomware

Η επίθεση ransomware αποτελείται από έξι κύρια στάδια. Οι χάκερ έχουν τη δυνατότητα να επιτύχουν τα επιθυμητά αποτελέσματα ακολουθώντας τα παρακάτω βήματα κατά την εκτέλεση μιας επίθεσης ransomware.

1. Campaign

Είναι η μέθοδος που χρησιμοποιείται από έναν επιτιθέμενο στον κυβερνοχώρο για να πραγματοποιήσει μια επίθεση ransomware. Αυτές οι μέθοδοι περιλαμβάνουν απομακρυσμένες επιθέσεις σε διακομιστές ιστού, κακόβουλα λογισμικά σε ιστοτόπους και παραπλανητικά μηνύματα ηλεκτρονικού ταχυδρομείου. Το κακόβουλο ηλεκτρονικό ταχυδρομείο, το οποίο έχει γίνει μια συστηματική επίθεση κοινωνικής μηχανικής, είναι μία από τις πιο κοινές μεθόδους. Με αυτόν τον τρόπο, ένας εισβολέας αναγκάζει τον χρήστη να κατεβάσει το κακόβουλο λογισμικό ασυνείδητα.

2. Infection

Σε αυτό το στάδιο, ο κακόβουλος κώδικας που προετοιμάζεται από έναν εισβολέα στον κυβερνοχώρο αρχίζει να εξαπλώνεται μέσω ενός δικτύου. Εάν το κακόβουλο λογισμικό εντοπιστεί έγκαιρα και οι απαραίτητες ενέργειες εκτελεστούν άμεσα, μπορείτε να αποτρέψετε την περαιτέρω διάδοση.

3. Staging

Σε αυτό το στάδιο, ο εισβολέας προσπαθεί να ενσωματώσει το ransomware στο συμβιβασμένο σύστημα κάνοντας μικρές αλλαγές στους προετοιμασμένους φορείς επίθεσης

στον κυβερνοχώρο. Σε αντίθεση με το στάδιο της μόλυνσης, υπάρχει επικοινωνία μεταξύ του ransomware και του διακομιστή C2, ο οποίος προστατεύει το κλειδί αποκρυπτογράφησης.

4. Scanning

Το ransomware αρχίζει να σαρώνει το δίκτυο πληροφορικής για να αναγνωρίσει τα αρχεία που πρόκειται να κρυπτογραφηθούν. Αυτό είναι ένα σημαντικό στάδιο για έναν επιτιθέμενο στον κυβερνοχώρο ώστε να επιτύχει τα επιδιωκόμενα αποτελέσματα, καθώς οι εγκεκριμένοι ορισμοί πρόσβασης και τα επίπεδα δικαιωμάτων στο σύστημα καθορίζουν τις διαδρομές που μπορεί να ακολουθήσει ένας εισβολέας μετά τη σάρωση.

5. Encryption

Η διαδικασία κρυπτογράφησης ξεκινά όταν ολοκληρωθεί η σάρωση. Τα τοπικά αρχεία στο δίκτυο πληροφορικής κρυπτογραφούνται σε δευτερόλεπτα και το ransomware μετακινείται στο σύννεφο και μοιράζει τα αρχεία στο δίκτυο και εν συνεχεία αντιγράφονται. Τέλος, τα αντιγραμμένα και κρυπτογραφημένα δεδομένα επαναφορτώνονται για να αντικαταστήσουν τα αρχικά αρχεία στο δίκτυο.

6. Remuneration

Όταν ένας επιτιθέμενος στον κυβερνοχώρο συλλαμβάνει κρίσιμα δεδομένα, στέλνει ένα σημείωμα λύτρων στον λογαριασμό ενός χρήστη του δικτύου αναφέροντας το ποσό και τις λεπτομέρειες της αποπληρωμής. Μερικές φορές οι επιτιθέμενοι θέτουν προθεσμίες και τα λύτρα αυξάνονται με την πάροδο του χρόνου. Σε ορισμένες περιπτώσεις, οι χάκερ προσφέρουν επίσης γραμμές εξυπηρέτησης πελατών στα θύματά τους για να συζητήσουν τους όρους πληρωμής. Η πληρωμή των λύτρων πρέπει να γίνεται χρησιμοποιώντας τον απαιτούμενο τρόπο πληρωμής, ωστόσο, δεν υπάρχει εγγύηση ότι τα δεδομένα σας θα ανακτηθούν.

1.1.4 Τυποι Επιθεσεων Ransomware

Οι επιθέσεις ransomware είναι ποικίλες και εξελίσσονται συνεχώς. Ορισμένοι από τους πιο κοινούς τύπους περιλαμβάνουν:

1. **Crypto Ransomware**: Κρυπτογραφεί τα αρχεία του θύματος και απαιτεί λύτρα για την αποκρυπτογράφηση τους.
2. **Locker Ransomware**: Κλειδώνει το σύστημα του θύματος, εμποδίζοντας την πρόσβαση σε αυτό, και απαιτεί λύτρα για την επαναφορά της πρόσβασης.
3. **Scareware**: Εμφανίζει ψεύτικες ειδοποιήσεις και προειδοποιήσεις ασφαλείας, πείθοντας το θύμα να πληρώσει για την επίλυση ενός ανύπαρκτου προβλήματος.
4. **Doxware (ή Leakware)**: Απειλεί να δημοσιεύσει ευαίσθητα δεδομένα του θύματος αν δεν καταβληθούν τα λύτρα.
5. **Ransomware-as-a-Service (RaaS)**: Μια πλατφόρμα που επιτρέπει σε επίδοξους εγκληματίες να εκτελούν επιθέσεις ransomware χωρίς τεχνική γνώση, έναντι μιας πληρωμής στον δημιουργό του ransomware.

1.1.5 Διαφορα Μεταξυ Ransomware Και Malware

Το **malware** (κακόβουλο λογισμικό) είναι ένας γενικός όρος που αναφέρεται σε οποιοδήποτε κακόβουλο λογισμικό σχεδιασμένο να προκαλέσει βλάβη, να διακόψει ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα υπολογιστή. Περιλαμβάνει διάφορους τύπους κακόβουλου λογισμικού όπως ιούς, trojans, worms, spyware και φυσικά ransomware.

Το **ransomware** είναι ένας ειδικός τύπος malware που κρυπτογραφεί τα δεδομένα του θύματος ή κλειδώνει το σύστημά του και απαιτεί λύτρα για την επαναφορά της πρόσβασης ή την αποκρυπτογράφηση των αρχείων. Αν και το ransomware είναι κακόβουλο λογισμικό, η κύρια διαφορά έγκειται στο γεγονός ότι το ransomware απαιτεί λύτρα, ενώ το malware μπορεί να έχει διάφορους άλλους στόχους, όπως την κλοπή δεδομένων, την καταστροφή συστημάτων ή την κατασκοπεία.

1.1.6 Αυτοματοποιημένη επίθεση ransomware & επίθεση ransomware από ανθρώπινο παράγοντα

1.1.6.1 Αυτοματοποιημένες επιθέσεις ransomware

Οι επιθέσεις ransomware είναι συχνά αυτοματοποιημένες. Αυτές οι επιθέσεις στον κυβερνοχώρο μπορούν να εξαπλωθούν σαν ιός και να μολύνουν συσκευές με τρόπους όπως το ηλεκτρονικό ψάρεμα ή παράδοση κακόβουλου λογισμικού και να απαιτούν την ανάλογη αποκατάσταση.

1.1.6.2 Επιθέσεις ransomware που πραγματοποιούνται από ανθρώπους

Το ransomware που ελέγχεται από ανθρώπους είναι το αποτέλεσμα μιας ενεργής επίθεσης από εγκληματίες του κυβερνοχώρου που διεισδύουν στην τοπική ή cloud υποδομή πληροφορικής ενός οργανισμού, αυξάνουν τα προνόμιά πρόσβασης τους και αναπτύσσουν ransomware σε κρίσιμα δεδομένα.

Ανθρώπινο χειρισμό σημαίνει επίσης ότι υπάρχει ένας ανθρώπινος παρ'αγοντας ενίοτε εκ των έσω που χρησιμοποιεί τις γνώσεις του σχετικά με τις συνήθεις παραμετροποιήσεις του συστήματος και της ασφάλειας. Στόχος τους είναι να διεισδύσουν στον οργανισμό, να περιηγηθούν στο δίκτυο και να προσαρμοστούν στο περιβάλλον και τις αδυναμίες του. Τα χαρακτηριστικά γνωρίσματα αυτών των επιθέσεων ransomware που πραγματοποιούνται από ανθρώπους περιλαμβάνουν συνήθως κλοπή διαπιστευτηρίων και αύξηση των προνομίων σε αυτούς τους λογαριασμούς. Ο στόχος είναι η ανάπτυξη ενός ωφέλιμου φορτίου ransomware σε οποιονδήποτε πόρο υψηλού επιχειρηματικού αντίκτυπου επιλέξουν οι δράστες των απειλών.

1.1.7 Το Πρωτόκολλο Cryptoviral Extortion

Η ιδέα του ransomware με κρυπτογράφηση αρχείων επινοήθηκε και υλοποιήθηκε από τους Young και Yung του Πανεπιστημίου Columbia και παρουσιάστηκε στο συνέδριο IEEE Security & Privacy το 1996. Ονομάζεται Cryptoviral Extortion και είναι εμπνευσμένο από τον χαρακτήρα Facehugger της ταινίας Alien. Το πρωτόκολλο αυτό έχει τρία επίπεδα μεταξύ επιτιθέμενου και θύματος:

- **Επιτιθέμενος προς Θύμα**

Ο επιτιθέμενος δημιουργεί ένα ζεύγος κλειδιών, τοποθετεί το κλειδί στο λογισμικό το οποίο και είναι κακόβουλο και το διανέμει.

- **Θύμα προς Επιτιθέμενο**

Το κακόβουλο λογισμικό δημιουργεί ένα τυχαίο συμμετρικό κλειδί και κρυπτογραφεί τα δεδομένα του θύματος. Στη συνέχεια, το κλειδί του κακόβουλου λογισμικού χρησιμοποιείται για την κρυπτογράφηση του συμμετρικού κλειδιού. Αυτή η μέθοδος, γνωστή ως υβριδική

κρυπτογράφηση, παράγει ένα συμμετρικό κρυπτογραφημένο κείμενο και ένα μικρό ασύμμετρο κρυπτογραφημένο κείμενο. Το συμμετρικό κλειδί και τα αρχικά δεδομένα μηδενίζονται ώστε να μην μπορούν να ανακτηθούν. Το θύμα λαμβάνει ένα μήνυμα με το ασύμμετρο κρυπτογράφημα και οδηγίες πληρωμής λύτρων, και στέλνει το κρυπτογραφημένο κείμενο και τα χρήματα στον επιτιθέμενο.

- **Επιτιθέμενος προς Θύμα**

Ο επιτιθέμενος λαμβάνει την πληρωμή, αποκρυπτογραφεί το κείμενο με το ιδιωτικό κλειδί και στέλνει το συμμετρικό κλειδί στο θύμα, το οποίο αποκρυπτογραφεί τα δεδομένα του.

Το συμμετρικό κλειδί παράγεται τυχαία και δεν βοηθάει άλλα θύματα. Το ιδιωτικό κλειδί του επιτιθέμενου δεν αποκαλύπτεται ποτέ στο θύμα, και το θύμα χρειάζεται να στείλει μόνο ένα μικρό κρυπτογραφημένο κείμενο στον επιτιθέμενο.

Οι επιθέσεις ransomware υλοποιούνται συνήθως με τη χρήση Trojan Horses, οι οποίοι εισάγονται στο σύστημα του θύματος μέσω ευπάθειας σε αρχείο ή υπηρεσία δικτύου. Ένα ωφέλιμο φορτίο Trojan εκτελείται, κλειδώνοντας το σύστημα ή ισχυριζόμενο ότι το κλειδώνει (scareware). Συχνά εμφανίζονται ψευδείς προειδοποιήσεις από την “αστυνομία", ισχυριζόμενες ότι το σύστημα χρησιμοποιήθηκε για παράνομες δραστηριότητες.

Το κύριο ωφέλιμο φορτίο των Trojans κλειδώνει το σύστημα μέχρι την πληρωμή των λύτρων, επιτυγχάνοντας αυτό με διάφορες μεθόδους, όπως η πειρατεία του κελύφους των Windows, η αντικατάσταση του explorer.exe ή η τροποποίηση του master boot record. Οι πιο προηγμένες εφαρμογές κρυπτογραφούν αρχεία με ισχυρές τεχνικές, καθιστώντας τα προσβάσιμα μόνο με τα κλειδιά του επιτιθέμενου.

Το θύμα αναγκάζεται να πληρώσει για να απαλλαγεί από το ransomware, είτε λαμβάνοντας ένα πρόγραμμα που αποκρυπτογραφεί τα αρχεία είτε τον κώδικα που απαιτείται για την επαναφορά των αλλαγών. Ένα σημαντικό στοιχείο στην επιτυχία του ransomware είναι ένα βολικό και δύσκολο να εντοπιστεί σύστημα πληρωμών, όπως οι ηλεκτρονικές μεταφορές κεφαλαίων, τα SMS ειδικής τιμής, οι προπληρωμένες κάρτες όπως η Paysafecard και το ψηφιακό νόμισμα bitcoin. Μια έρευνα του 2016 από τη Citrix ανέφερε ότι μεγάλες εταιρείες κατέχουν bitcoin για να πληρώσουν για πιθανές επιθέσεις ransomware.

1.1.8 Συχνότητα επιθέσεων ransomware

Το πρώτο εξάμηνο του 2022 καταγράφηκαν μόλις 236,1 εκατομμύρια επιθέσεις ransomware παγκοσμίως. Αντιθέτως, έως το 2021, ο αριθμός ήταν πολλαπλάσιος αφού είχαν σημειωθεί 623,3 εκατομμύρια επιθέσεις. Αυτό δεν σημαίνει ότι κάθε επίθεση ήταν επιτυχής, αλλά υπογραμμίζει την επικράτηση αυτής της απειλής στον κυβερνοχώρο.

1.1.9 Ποιοι και πόσοι επηρεάζονται από μία επίθεση τύπου ransomware

Οι παραβιάσεις δεδομένων μέσω ransomware μπορούν να επηρεάσουν οποιονδήποτε. Το 71% των οργανισμών παγκοσμίως φέρεται να επηρεάστηκαν από επιθέσεις ransomware το 2022. Ενώ οι ομάδες ransomware στοχεύουν συνήθως οργανισμούς ως πιο επικερδείς στόχους, περίπου 3700 άτομα ανέφεραν ότι έπεσαν θύματα επιτυχημένων επιθέσεων ransomware το 2021. Ωστόσο, αυτός ο αριθμός είναι πιθανότατα υψηλότερος, καθώς πολλά θύματα δεν θα αναφέρουν απώλειες. Αξίζει να σημειωθεί ότι η ζημιά ανέρχεται στα 49,2 εκατομμύρια δολάρια που κλάπηκαν από χρήστες του Διαδικτύου κατά τη διάρκεια του 2021.

1.2 ΙΣΤΟΡΙΚΑ ΔΕΔΟΜΕΝΑ & ΣΤΑΤΙΣΤΙΚΑ

Οι επιθέσεις τύπου ransomware αποτελούν μια αυξανόμενη απειλή και συνεχόμενα εξελισσόμενη, για την ασφάλεια στον κυβερνοχώρο, επηρεάζοντας επιχειρήσεις και ιδιώτες παγκοσμίως καθώς τα αρχεία τους μπορούν να κρυπτογραφηθούν και να ζητηθούν λύτρα για να απελευθερωθούν.

Από το 2012 οι απάτες με χρήση ransomware άρχισαν να εξαπλώνονται παγκοσμίως. Τον Ιούνιο του 2013, το MC Daddy έβγαλε στη δημοσιότητα δεδομένα τα οποία έδειχναν ότι οι περιπτώσεις επιθέσεων ransomware είχαν διπλασιαστεί εκείνο το τρίμηνο συγκριτικά με το αντίστοιχο τρίμηνο της προηγούμενης χρονιάς.

Το CryptoLocker παρουσίασε ιδιαίτερα μεγάλη επιτυχία, αποσπώντας το εκτιμώμενο ποσό των 3 εκατομμυρίων δολαρίων (USD) προτού οδηγηθεί σε καταστολή από τις αρμόδιες αρχές. Ακόμα, εκτιμάται από το Ομοσπονδιακό Γραφείο Ερευνών (FBI) ότι οι εισπράξεις του CryptoWall ανέρχονταν στα 18 εκατομμύρια δολάρια (USD) μέχρι τον Ιούνιο του 2015.

1.2.1 ΙΣΤΟΡΙΚΗ ΕΞΕΛΙΞΗ ΤΟΥ RANSOMWARE

Η χρονική αλληλουχία που παρατίθεται παρακάτω βασίζεται σε όσα είναι γνωστά για αυτό το ransomware, με τις ημερομηνίες να είναι κατά προσέγγιση.

Είναι απολύτως αποδεκτό ότι λείπουν λεπτομέρειες, καθώς το ransomware αποτελεί είδος παρανομίας. Παρ' όλα αυτά, παρουσιάζεται μία εικόνα για τη γενικότερη εξέλιξη και ανάπτυξη του ransomware. Θα πρέπει επίσης να σημειωθεί ότι παρόλο που τα ονόματα που χρησιμοποιούνται για τις διάφορες εκδόσεις του ransomware είναι γενικά παρόμοια, οι πηγές δεν είναι οι ίδιες.

1989

Ο Joseph L. Popp δημιούργησε τον πρώτο ιό ransomware, με την ονομασία AIDS Trojan (επίσης γνωστός ως PC Cyborg). Ο Popp ήταν εξελικτικός βιολόγος με σπουδές στο Πανεπιστήμιο του Χάρβαρντ. Ο ιός διαδόθηκε με δισκέτες που τις διένειμε στο διεθνές συνέδριο στο διεθνές συνέδριο του Παγκόσμιου Οργανισμού Υγείας για το AIDS. Με τον τρόπο αυτό χρησιμοποίησε έναν απλό κρυπτογράφο ώστε να μπορέσει να υποκλέψει το όνομα του αρχείου ενώ στη συνέχεια τα αποκρυπτογραφούσε με τη βοήθεια ενός εργαλείου. (Sjouwerman, 2015b).

2005

Το πρώτο σύγχρονο ransomware ήταν το Trojan.Gpcoder, επίσης γνωστό ως GP Code ή GPCoder. Κυκλοφόρησε τον Μάιο του 2005 και αρχικά χρησιμοποιούσε μια ιδιόκτητη τεχνική συμμετρικής κρυπτογράφησης που ήταν αδύναμη και εύκολη στο σπάσιμο- το Trojan.Gpcoder διανεμήθηκε μέσω συνημμένων spam που εμφανίζονταν ως αιτήσεις εργασίας (Sjouwerman, 2015b).

Τα περισσότερα από τα πρώιμα ransomware αναπτύχθηκαν στη Ρωσία από ρωσικές ομάδες οργανωμένου εγκλήματος. Στόχευαν κυρίως ρωσικά θύματα και γειτονικές χώρες όπως η Λευκορωσία, η Ουκρανία και το Καζακστάν (Cawley, 2016).

2006

Μέχρι τις αρχές του 2006, το ransomware είχε διαδοθεί και περισσότεροι επιτιθέμενοι άρχισαν να δοκιμάζουν τη δύναμή του. Τον Μάρτιο του 2006 εμφανίστηκε το Trojan.Cryzip. Αντέγραφε αρχεία δεδομένων σε ένα αρχείο προστατευμένο με κωδικό πρόσβασης και διέγραφε τα πρωτότυπα. Ο κώδικας του κακόβουλου λογισμικού περιείχε έναν κωδικό πρόσβασης, καθιστώντας εύκολη την ανάκτησή του.Το Trojan.Archiveus εμφανίστηκε επίσης το 2006. Αυτό το κακόβουλο λογισμικό λειτουργούσε παρόμοια με το Trojan.Cryzip, αλλά αντί να απαιτεί λύτρα, προσέφερε στα θύματα την ευκαιρία να αγοράσουν φάρμακα από ορισμένα διαδικτυακά φαρμακεία και να δώσουν ένα αναγνωριστικό παραγγελίας για να αποκτήσουν έναν κωδικό πρόσβασης (Savage, Coogan , & Lau, 2015).

Το ransomware Locker λειτούργησε για πρώτη φορά το 2007. Η πρώτη έκδοση έπληξε τη Ρωσία: Πορνογραφικές εικόνες εμφανίζονταν στην οθόνη του υπολογιστή και απαιτούνταν πληρωμή μέσω SMS ή κλήσης σε ένα ακριβό αριθμό τηλεφώνου ώστε να αφαιρεθεί. Οι επιθέσεις σύντομα εξαπλώθηκαν στην Ευρώπη και τις ΗΠΑ (Zetter, 2015).

2008

Εμφανίστηκε για πρώτη φορά μια παραλλαγή του Trojan.Gpcoder με την ονομασία GPcode.AK, η οποία χρησιμοποιούσε κλειδί RSA 1024 bit. Αυτός ο δούρειος ίππος χρησιμοποιούσε κλειδί RSA 1024-bit και άφηνε ένα αρχείο κειμένου σε κάθε υποκατάλογο με οδηγίες που κρυπτογράφησαν τα αρχεία. Αυτό το Trojan horse ήταν σε θέση να χρεώνει 100 δολάρια. για να πληρώσει 200 δολάρια σε e-gold ή Liberty Reserve (Tromer, 2008).

2011

Στα μέσα του 2011 σημειώθηκε το πρώτο μεγάλο ξέσπασμα ransomware, σε μεγάλο βαθμό λόγω της εμφάνισης ανώνυμων υπηρεσιών πληρωμών. Περίπου 30.000 νέα δείγματα ransomware δημιουργήθηκαν το πρώτο τρίμηνο, ενώ άλλα 30.000 το δεύτερο τρίμηνο. Μέχρι το τρίτο τρίμηνο, ο αριθμός των νέων δειγμάτων έφτασε τα 60.000 (Sjouwerman, 2015b).

2012

Κυκλοφορεί η εργαλειοθήκη Citadel με κόστος περίπου 3.000 δολάρια (Sjouwerman, 2015b). Το Citadel διευκόλυνε τη δημιουργία και τη διανομή ransomware (Segura, 2016).

Την ίδια χρονιά παρουσιάστηκε μια άλλη εργαλειοθήκη με την ονομασία Lyposit. Πρόκειται για.Lyposit malware | win32/Lyposit.A", n.d.) Η έκδοση που δημιουργήθηκε από το Lyposit ήταν γνωστή ως Reveton. Στην οθόνη εμφανιζόταν ένα αναδυόμενο μήνυμα που ανέφερε ότι ο υπολογιστής εμπλέκεται σε παιδική πορνογραφία, λήψη υλικού που προστατεύεται από πνευματικά δικαιώματα ή άλλη εγκληματική δραστηριότητα και ότι είχε μπλοκαριστεί από το FBI ή το Υπουργείο Δικαιοσύνης (Sjouwerman, 2015b; Savage, 2015), ψεύτικα μηνύματα του Κέντρου Ασφαλείας των Windows που ζητούσαν από τους χρήστες να καλέσουν έναν αριθμό τηλεφώνου υψηλού κινδύνου για να ενεργοποιήσουν εκ νέου την άδεια χρήσης των Windows (Savage, Coogan, & Lau, 2015).

Τα ελαττώματα του ransomware τύπου locker και άλλων παρόμοιων συστημάτων ransomware, τα οποία δεν εξετάζονται εδώ, οδήγησαν σε αναζωπύρωση του κρυπτο-ransomware το 2013. Μια τυπική επίθεση απαιτούσε πληρωμή περίπου 300 δολαρίων ΗΠΑ, ενώ οι ίδιες οι επιθέσεις γίνονταν όλο και πιο εξελιγμένες (Savage, Coogan & Lau, 2015).

Το 2013, ο αριθμός των επιθέσεων που απαιτούσαν πληρωμή περίπου 300 USD αυξήθηκε και οι ίδιες οι επιθέσεις έγιναν πιο εξελιγμένες (Savage, Coogan, & Lau, 2015).

2013

Το πιο γνωστό ransomware, το CyptoLocker, κυκλοφόρησε τον Αύγουστο του 2013 από έναν χάκερ με το όνομα Slavik. Χρησιμοποιούσε δημόσια και ιδιωτικά κλειδιά κρυπτογράφησης των αρχείων των θυμάτων και στη συνέχεια για την αποκρυπτογράφηση τους.

Αρχικά διανεμήθηκε μέσω του botnet ZeuS banking Trojan Gameover ενώ στη συνέχεια μέσω μηνυμάτων, διανεμήθηκε μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου που φαινόταν να προέρχονται από την UPS ή τη FedEx (Zetter, 2015) Οι πρώτες εκδόσεις του CryptoLocker κρυπτογράφησαν περίπου 67 διαφορετικά αρχεία, συμπεριλαμβανομένων όλων των αρχείων δεδομένων του Microsoft Office (Cannell, 2016).

Το CyptoLocker έδινε στα θύματα τρεις ημέρες για να πληρώσουν. Η τιμή τότε ήταν 2 bitcoin ή περίπου 100 δολάρια ΗΠΑ. Άλλες μέθοδοι πληρωμής ήταν οι CashU, Ukash, Paysafecard και MoneyPak. Σε ορισμένες εκδόσεις, τα θύματα μπορούσαν να πληρώσουν πολύ υψηλότερα λύτρα προκειμένου να ανακτήσουν τα αρχεία τους, εάν δεν τηρούνταν η προθεσμία των τριών ημερών. Το ποσό διέφερε ανάλογα με την έκδοση (Sjouwerman, 2015b).

Τον Νοέμβριο, η αξία των λύτρων αυξήθηκε από 2 bitcoins σε περίπου 460 δολάρια ΗΠΑ. Χωρίς αρχική προθεσμία, η τιμή μεταβλήθηκε στα 10 bitcoin- μέχρι τον Δεκέμβριο, 250.000 μηχανήματα μολύνθηκαν- διαπιστώθηκε ότι είχαν καταβληθεί 41.928 λύτρα bitcoin (Sjouwerman, 2015b). Τον Δεκέμβριο εμφανίστηκε ένας αντιγραφέας με την ονομασία Locker. Τα λύτρα ήταν 150 δολάρια και πληρώνονταν με τη χρήση Perfect Money ή αριθμών εικονικών καρτών QIWI Visa.

Αργότερα τον ίδιο μήνα κυκλοφόρησε το CryptoLocker 2.0. Πρόκειται για ένα λογισμικό γραμμένο από το αρχικό CryptoLocker και πιθανότατα δημιουργήθηκε και κυκλοφόρησε από διαφορετικό επιτιθέμενο (Sjouwerman, 2015b). Κατά τη διάρκεια του 2013, η Symantec εκτιμά ότι ο αριθμός των επιθέσεων αυξήθηκε από 100.000 τον Ιανουάριο σε 600 000 τον Δεκέμβριο. Υπολόγισε επίσης ότι το 3% των μολυσμένων χρηστών πλήρωσε τα λύτρα (Rosenberg, 2015).

2014

Εκτιμάται ότι περισσότερα από 500 000 θύματα μολύνθηκαν με το CryptoLocker μεταξύ Σεπτεμβρίου 2013 και Μαΐου 2014 ενώ φαίνεται πως το 1,3% των θυμάτων κατέβαλε λύτρα (Cannell, 2016). Τον Ιούνιο, η Επιχείρηση Tovar, ένας συνασπισμός των αρχών επιβολής του νόμου, προμηθευτών ασφάλειας και ακαδημαϊκών, κατέβασε τους διακομιστές διανομής του CryptoLocker. δύο προμηθευτές, η FireEye και η Fox-IT, μπόρεσαν να βρουν τα κλειδιά αποκρυπτογράφησης όλων των θυμάτων του CryptoLocker σε ένα βάση δεδομένων και κυκλοφόρησαν μια δωρεάν υπηρεσία αποκρυπτογράφησης από όλα τα θύματα (Cawley, 2016).

Τον Φεβρουάριο κυκλοφόρησε η υπηρεσία CryptoDefence. Αυτό ήταν ένα αρκετά αδύναμο ransomware, ωστόσο κατάφερε να αποφέρει 34 000 δολάρια ΗΠΑ τον πρώτο μήνα.

Τον Απρίλιο κυκλοφόρησε μια βελτιωμένη έκδοση με την ονομασία CryptoWall. Αυτή εκμεταλλευόταν μια ευπάθεια στη Java και διανεμήθηκε μέσω κακόβουλης διαφήμισης. Αυτή η έκδοση απέφερε πάνω από 1 εκατομμύριο δολάρια σε λύτρα (Sjouwerman, 2015b).

2015

Μέχρι το τέλος του 2015, το FBI εκτίμησε ότι τα θύματα είχαν καταβάλει 27 εκατομμύρια δολάρια σε λύτρα στους επιτιθέμενους πίσω από το CryptoLocker (Cannell, 2016). το CryptoWall ξεπέρασε το Cryptolocker και κατάφερε να γίνει η κορυφαία έκδοση ransomware (Sjouwerman, 2015b).

Σύμφωνα με έρευνα της Kaspersky, μεταξύ 2014 και 2015, οι επιθέσεις ransomware αυξήθηκαν κατά 17,7%, ενώ οι επιθέσεις crypto-ransomware κατά 448% (Townsend, 2016).

Τον Μάιο εμφανίστηκε το Ransomware-as-a-Service: χρησιμοποιώντας τον ιστότοπο TOR, οι επιτιθέμενοι μπορούσαν να δημιουργήσουν ransomware δωρεάν. Ο ιστότοπος επεξεργάζεται τις πληρωμές και ο επιτιθέμενος λαμβάνει το 20% των λύτρων (Sjouwerman, 2015b).

Τον Σεπτέμβριο κυκλοφόρησε το LockerPin. Μολύνει συστήματα Android, αλλάζει τους κωδικούς PIN και χρεώνει λύτρα 500 δολάρια.

Τον Οκτώβριο, σύμφωνα με νέα έκθεση της Cyber Threat Alliance, η συνολική ζημία που προκλήθηκε από το ransomware έφτασε τα 325 εκατομμύρια δολάρια (Sjouwerman, 2015b).

Τον Νοέμβριο, το Linus.Encoder.1 δημιουργήθηκε από τον Δρ. Web, μια ρωσική εταιρεία ασφάλειας υπολογιστών. Όπως υποδηλώνει το όνομά του, στοχεύει σε συστήματα Linux καθώς κρυπτογραφεί τόσο αρχεία δεδομένων όσο και αρχεία που σχετίζονται με διαδικτυακές εφαρμογές (Cawley, 2016).

Τον Νοέμβριο εμφανίστηκε μια τέταρτη επανάληψη του Cryptowall. το Cryptowall έχει τροποποιήσει τα πρωτόκολλά του για να αποφύγει τον εντοπισμό. Αλλάζει επίσης το όνομα του αρχείου κατά την κρυπτογράφηση των αρχείων, καθιστώντας δύσκολη την αναγνώριση του πραγματικού κρυπτογραφημένου αρχείου (Pauli, 2015).

2016

Τον Ιανουάριο ανακαλύφθηκε ένα ransomware-as-a-service που χρησιμοποιεί μόνο JavaScript- με τη χρήση JavaScript επιτρέπει επιθέσεις σε πολλαπλές πλατφόρμες, συμπεριλαμβανομένων των Linus και macOS X.

Τον Φεβρουάριο, ransomware μόλυνε χιλιάδες ιστότοπους του WordPress- το WordPress είναι μια δημοφιλής πλατφόρμα blogging.

Τον Απρίλιο, ένα ransomware με την ονομασία Petya ήταν κυκλοφόρησε- το Petya απενεργοποιεί την πρόσβαση σε ολόκληρο σκληρό δίσκο μέχρι να καταβληθούν λύτρα (Fitzpatrick & Griffin, 2016). Αυτό το επιτυγχάνει αντικαθιστώντας το Master Boot Record (MBR) του μολυσμένου υπολογιστή- χωρίς το MBR, το λειτουργικό σύστημα δεν μπορεί να ανακατασκευάσει τα μη κρυπτογραφημένα αρχεία (Constantin, 2016). Η Apple αναγκάστηκε να κυκλοφορήσει μια ενημερωμένη έκδοση για να μπλοκάρει το ransomware KeRanger Το KeRanger πιστεύεται ότι αποτελεί την πρώτη επίθεση ransomware που στοχεύει υπολογιστές της Apple. Μόλις εγκατασταθεί, το KeRanger χρειάζεται τρεις ημέρες για να ξεκινήσει και έχει σχεδιαστεί για να κρυπτογραφεί πάνω από 300 διαφορετικά αρχεία (Kirk, 2016a).

Τον Φεβρουάριο, εντοπίστηκε κακόβουλο λογισμικό με την ονομασία Xbot που στόχευε συσκευές Android στην Αυστραλία και τη Ρωσία.

Τον Ιούλιο, ένας μηχανισμός ασφαλείας προστέθηκε στο ransomware Locky, επιτρέποντας στο ransomware να ξεκινήσει την κρυπτογράφηση αρχείων ακόμη και όταν ο υπολογιστής-στόχος είναι εκτός σύνδεσης ή οι επικοινωνίες έχουν μπλοκαριστεί, ώστε το ransomware να μην μπορεί να ζητήσει ένα μοναδικό κλειδί κρυπτογράφησης από τον διακομιστή του δράστη (Constantin, 2016c).

Το FBI εκτιμά ότι το ransomware απέφερε 209.000.000 δολάρια τους πρώτους τρεις μήνες του 2016 και είναι σε καλό δρόμο για να γίνει ένα έγκλημα δισεκατομμυρίων δολαρίων φέτος (Fitzpatrick & Griffin, 2016).

Κατά τη διάρκεια του πρώτου τριμήνου, η McAfee Labs μέτρησε 1,2 εκατομμύρια επιθέσεις ransomware. Πρόκειται για αύξηση 24% σε σύγκριση με το τέταρτο τρίμηνο του 2015 (McAfee Labs Threats Report, 2016).

Οι τρεις κορυφαίες εκδόσεις που επικρατούν σήμερα είναι οι CryptoWall, CTB-Locker και TorrentLocker. το CryptoWall είναι μια βελτιωμένη έκδοση του CryptoDefence. Δεν κρυπτογραφεί μόνο τα αρχεία στους μολυσμένους υπολογιστές, αλλά στοχεύει επίσης στην εξωτερική αποθήκευση και στους κοινόχρηστους δίσκους που είναι συνδεδεμένοι με τον στόχο- το CTB-Locker σημαίνει Curve-Tor-Bitcoin- τόσο το CryptoWall όσο και το CTB-Locker είναι θυγατρικές

Το TorrentLocker συλλέγει διευθύνσεις ηλεκτρονικού ταχυδρομείου όταν ένας υπολογιστής μολύνεται, προκειμένου να στείλει spam σε άλλους χρήστες (Zetter 2015).

1.2.2 ΤΟ RANSOMWARE ΣΗΜΕΡΑ

- Ο όγκος των επιθέσεων ransomware μειώθηκε κατά 23% το 2022 σε σύγκριση με το προηγούμενο έτος.
- Το πρώτο εξάμηνο του 2022, εκτιμάται ότι σημειώθηκαν 236,1 εκατομμύρια επιθέσεις ransomware παγκοσμίως.
- Υπήρξαν 623,3 εκατομμύρια επιθέσεις ransomware παγκοσμίως το 2021.
- Το ransomware αντιπροσώπευε περίπου το 20% όλων των εγκλημάτων στον κυβερνοχώρο το 2022.
- Το 20% του κόστους ransomware αποδίδεται σε βλάβη της φήμης.
- Το 93% του ransomware είναι εκτελέσιμα που βασίζονται σε Windows.
- Το πιο κοινό σημείο εισόδου για ransomware είναι το phishing.
- Οι οργανισμοί στις ΗΠΑ είναι οι επιχειρήσεις που είναι πιο πιθανό να επηρεαστούν από ransomware, αντιπροσωπεύοντας το 47% των επιθέσεων.
- Το ransomware ήταν ο πιο κοινός τύπος επίθεσης για τον κατασκευαστικό κλάδο το 2021.
- Το 90% των επιθέσεων ransomware αποτυγχάνουν ή οδηγούν σε μηδενικές απώλειες για το θύμα.
- Το πρώτο εξάμηνο του 2022, υπήρξαν περίπου 236,1 εκατομμύρια επιθέσεις ransomware παγκοσμίως.
- Κατά τη διάρκεια του 2021, τουλάχιστον το 15,45% των χρηστών του διαδικτύου παγκοσμίως υπέστη τουλάχιστον 1 επίθεση κατηγορίας κακόβουλου λογισμικού, η οποία περιλαμβάνει ransomware.
- Η Kaspersky ανέφερε ότι οι επιθέσεις ransomware ηττήθηκαν σε 366.256 μοναδικούς υπολογιστές χρηστών το 2021.
- Το ransomware αντιπροσώπευε περίπου το 20% των παραβιάσεων στον κυβερνοχώρο το 2022. Για σύγκριση, η χρήση κλεμμένων διαπιστευτηρίων (hacking) αντιπροσώπευε το 40% των παραβιάσεων το 2022 και το phishing περίπου το 20%.
- Το ποσοστό περιστατικών για επιθέσεις ransomware ήταν χαμηλότερο στις ΗΠΑ (7%) σε σύγκριση με τον παγκόσμιο μέσο όρο (37%) το 2022.
- Μόλις το 13% των οργανισμών ανέφερε ότι υπέστη επίθεση ransomware και δεν πλήρωσε τα λύτρα το 2022.
- Το FBI ανέφερε αύξηση του αριθμού των επιθέσεων ransomware κατά τη διάρκεια των διακοπών και τα Σαββατοκύριακα (ημέρες που τα γραφεία του FBI είναι κλειστά).
- Το Κέντρο Καταγγελιών Εγκλημάτων Διαδικτύου (IC3) του FBI ανέφερε ότι έλαβε 2084 καταγγελίες σχετικά με περιστατικά ransomware μεταξύ Ιανουαρίου-Ιουλίου 2021, με απώλειες που ανέρχονται σε 16,8 εκατομμύρια δολάρια.

- Τουλάχιστον 130 διαφορετικές οικογένειες ransomware έχουν αποκαλυφθεί. Το Gandcrab είναι η πιο δραστήρια οικογένεια, με το 78,5% των αναφερόμενων επιθέσεων να του αποδίδονται.
- Το 93,28% των αρχείων ransomware που εντοπίστηκαν είναι εκτελέσιμα που βασίζονται στα Windows. Ο επόμενος πιο κοινός τύπος αρχείου είναι το Android, στο 2,09%.
- Το ransomware αντιπροσώπευε το 4% των παραβιάσεων στον κυβερνοχώρο σε επιχειρήσεις του Ηνωμένου Βασιλείου το 2022.
- Το πιο κοινό σημείο εισόδου για επιθέσεις ransomware είναι μέσω phishing, με ποσοστό 41%.
- Μεταξύ 2020-2021, σημειώθηκε αύξηση 33% στον αριθμό των επιθέσεων ransomware που προκαλούνται από την εκμετάλλευση ευπάθειας.
- Ο Ιούνιος βίωσε τις περισσότερες επιθέσεις ransomware το 2021, με 33% – πρόκειται για μείωση σε σχέση με τα στοιχεία του 2020, όπου το 50% των επιθέσεων ransomware εκείνο το έτος συνέβη τον Ιούνιο.
- Ο κορυφαίος τύπος επίθεσης εναντίον επιχειρήσεων στον κατασκευαστικό κλάδο ήταν το ransomware το 2021, με τους χάκερ να χρησιμοποιούν αυτόν τον τύπο στο 23% των παρατηρούμενων επιθέσεων. Αυτό ήταν μπροστά από τις επιθέσεις πρόσβασης διακομιστή (12%) και τον συμβιβασμό του επαγγελματικού email (10%).
- Το 2022, το Εθνικό Κέντρο Ασφάλειας Κυβερνοασφάλειας με έδρα το Ηνωμένο Βασίλειο συντόνισε απαντήσεις σε 18 επιθέσεις ransomware υψηλού προφίλ, μεταξύ άλλων κατά του αριθμού μη έκτακτης ανάγκης NHS 111 και του South Staffordshire Water.
- Το 90% των επιθέσεων ransomware είτε αποτυγχάνουν είτε καταλήγουν σε μηδενικές απώλειες για το θύμα.
- Το 65% των καναδικών εταιρειών αναμένει να πληγεί από επίθεση ransomware.
- Το 11% των καναδικών εταιρειών πλήρωσαν τα λύτρα μετά από επίθεση ransomware.
- Το 12% των καναδικών εταιρειών που επλήγησαν από επίθεση ransomware διέρρευσαν τα δεδομένα τους στο διαδίκτυο.
- Υπολογίζεται ότι, μέχρι το 2031, μια επίθεση ransomware θα συμβαίνει κάθε 2 δευτερόλεπτα.
- Το IC3 με έδρα τις ΗΠΑ έλαβε 2385 καταγγελίες από θύματα ransomware, με απώλειες που ξεπερνούν τα 34,3 εκατομμύρια δολάρια.
- Το 2021, οι επιθέσεις ransomware κόστισαν στον τομέα της υγειονομικής περίθαλψης των ΗΠΑ περίπου 7,8 δισεκατομμύρια δολάρια μόνο σε διακοπές λειτουργίας. Πάνω από 19,7 εκατομμύρια αρχεία ασθενών επηρεάστηκαν σε 108 μεμονωμένες επιθέσεις κατά τη διάρκεια του έτους.

- Μια μεμονωμένη επίθεση κόστισε σε έναν πάροχο υγειονομικής περίθαλψης 112 εκατομμύρια δολάρια, συμπεριλαμβανομένου του κόστους αποκατάστασης της παραβίασης, του χρόνου διακοπής λειτουργίας και της διακοπής στους ασθενείς – ορισμένοι κρίσιμοι ασθενείς, όπως τα θύματα εγκεφαλικού και καρδιακής προσβολής, επαναδρομολογήθηκαν λόγω της παραβίασης.
- Οι απαιτήσεις για λύτρα στις επιθέσεις κυμαίνονταν από περίπου 250.000 έως 5 εκατομμύρια δολάρια.
- Στις χειρότερες περιπτώσεις, η διακοπή λόγω επίθεσης χρειάστηκε μήνες για να επιλυθεί. Οι οργανισμοί που ήταν πιο προετοιμασμένοι, με τακτικά αντίγραφα ασφαλείας δεδομένων, αντιμετώπισαν πολύ λιγότερη διακοπή στις υπηρεσίες τους. Ο μέσος χρόνος που χάθηκε ήταν περίπου 6 ημέρες.

Οι χώρες που γίνονται πιο συχνά δέκτες επιθέσεων και επηρεάζονται περισσότερο από επιθέσεις ransomware είναι:

1. Ισραήλ
2. Νότια Κορέα
3. Βιετνάμ
4. Κίνα
5. Σιγκαπούρη
6. Ινδία
7. Καζακστάν
8. Φιλιππίνες
9. Ιράν
10. Ηνωμένο Βασίλειο

Όσον αφορά στους οργανισμούς, οι πέντε χώρες που πλήττονται περισσότερο είναι:

1. ΗΠΑ (47%)
2. Ιταλία (8%)
3. Αυστραλία (8%)
4. Βραζιλία (6%)
5. Γερμανία (6%)

1.3 ΑΞΙΟΣΗΜΕΙΩΤΕΣ ΕΠΙΘΕΣΕΙΣ RANSOMWARE

1.3.1 Επίθεση ransomware WannaCry

Το WannaCry αποτελεί ένα παράδειγμα crypto ransomware, δηλαδή ένα είδος κακόβουλου λογισμικού (malware) που χρησιμοποιείται από εγκληματίες του κυβερνοχώρου με στόχο τα λύτρα. Το εν λόγω Ransomware λειτουργεί είτε κρυπτογραφώντας πολύτιμα αρχεία, ώστε να μην μπορούν να διαβαστούν, είτε κλειδώνοντάς τον υπολογιστή χωρίς να υπάρχει η δυνατότητα πρόσβασης. Το ransomware που χρησιμοποιεί κρυπτογράφηση ονομάζεται crypto ransomware ενώ το κλείδωμα του υπολογιστή ονομάζεται locker ransomware. Όπως και άλλοι τύποι crypto-ransomware, το WannaCry κρατά τα δεδομένα «όμηρο» και υπόσχεται να επιστραφούν εάν πληρωθούν τα λύτρα. Στοχεύει υπολογιστές που χρησιμοποιούν ως λειτουργικό σύστημα τα Microsoft Windows κρυπτογραφεί δεδομένα και απαιτεί πληρωμή λύτρων στο κρυπτονόμισμα Bitcoin για την επιστροφή του.

Τι ήταν η επίθεση ransomware WannaCry;

Η επίθεση ransomware WannaCry ήταν μια παγκόσμια επιδημία που έλαβε χώρα τον Μάιο του 2017. Αυτή η επίθεση ransomware εξαπλώθηκε μέσω υπολογιστών που λειτουργούσαν με Microsoft Windows. Τα αρχεία του χρήστη κρατήθηκαν ως «όμηροι» και ζητήθηκαν λύτρα σε μορφή Bitcoin για την επιστροφή τους. Εάν δεν υπήρχαν τα απαρχαιωμένα συστήματα υπολογιστών και η κακή εκπαίδευση του προσωπικού σχετικά με την διαδικασία ενημέρωσης λογισμικού, η ζημιά που προκλήθηκε από αυτήν την επίθεση θα μπορούσε να είχε αποφευχθεί.

Πώς λειτουργεί μια επίθεση WannaCry;

Οι κυβερνοεγκληματίες που ευθύνονται για την επίθεση εκμεταλλεύτηκαν μια αδυναμία στο λειτουργικό σύστημα Microsoft Windows χρησιμοποιώντας ένα hack που φέρεται να αναπτύχθηκε από την Εθνική Υπηρεσία Ασφαλείας των Ηνωμένων Πολιτειών. Γνωστό ως EternalBlue, αυτό το hack δημοσιοποιήθηκε από μια ομάδα χάκερ που ονομάζεται Shadow Brokers πριν από την επίθεση WannaCry.

Η Microsoft κυκλοφόρησε μια ενημερωμένη έκδοση κώδικα ασφαλείας που προστάτευε τα συστήματα των χρηστών από αυτήν την εκμετάλλευση σχεδόν δύο μήνες πριν από την έναρξη της επίθεσης ransomware WannaCry. Δυστυχώς, πολλά άτομα και οργανισμοί δεν ενημερώνουν τακτικά τα λειτουργικά τους συστήματα και έτσι έμειναν εκτεθειμένα στην επίθεση.

Όσοι δεν είχαν εκτελέσει την ενημέρωση των Microsoft Windows πριν από την επίθεση δεν επωφελήθηκαν από την καινούργια έκδοση κώδικα και η ευπάθεια που εκμεταλλεύτηκε το EternalBlue τους άφησε ανοχύρωτους στις επιθέσεις. Όταν συνέβη για πρώτη φορά, οι χρήστες υπέθεσαν ότι η επίθεση ransomware WannaCry είχε αρχικά εξαπλωθεί μέσω μιας

καμπάνιας phishing (ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου με μολυσμένους συνδέσμους ή συνημμένα που παρασύρουν τους χρήστες να κατεβάσουν κακόβουλο λογισμικό). Ωστόσο, το EternalBlue ήταν η εκμετάλλευση που επέτρεψε στο WannaCry να διαδοθεί και να εξαπλωθεί, με το DoublePulsar να είναι η «πίσω πόρτα» που εγκαθίσταται στους παραβιασμένους υπολογιστές (χρησιμοποιείται για την εκτέλεση του WannaCry).

Τι θα συνέβαινε αν δεν πληρώνονταν τα λύτρα του WannaCry;

Οι χακερς ζήτησαν bitcoin αξίας 300 δολαρίων και στη συνέχεια αύξησαν το ποσό των λύτρων σε bitcoin αξίας 600 δολαρίων. Εάν τα λύτρα δεν πληρώνονταν εντός τριών ημερών, τα θύματα της επίθεσης ransomware WannaCry γνώριζαν πως τα αρχεία τους θα διαγραφούν οριστικά. Η συμβουλή όσον αφορά στις πληρωμές λύτρων είναι να μην υποχωρεί το θύμα σε τέτοιου είδους πιέσεις. Με δεδομένο ότι κανείς δεν εγγυάται ότι τα δεδομένα θα επιστραφούν ακέραια, είναι προτιμότερο να μην γίνεται η καταβολή των λύτρων και αυτό γιατί με κάθε πληρωμή επικυρώνεται και νομιμοποιείται η εγκληματκότητα τέτοιων μοντέλων.

Αυτή η συμβουλή αποδείχθηκε σοφή κατά τη διάρκεια της επίθεσης WannaCry καθώς, σύμφωνα με πληροφορίες, η κωδικοποίηση που χρησιμοποιήθηκε στην επίθεση ήταν ελαττωματική. Όταν τα θύματα κατέβαλαν τα λύτρα τους, οι εισβολείς δεν είχαν τρόπο να συσχετίσουν την πληρωμή με τον υπολογιστή ενός συγκεκριμένου θύματος. Βεβαία το ότι πλήρωσαν δεν απομακρύνει σε κανένα βαθμό την αμφιβολία για το αν κάποιος πήρε πίσω τα αρχεία του ακέραια.

Τι αντίκτυπο είχε η επίθεση WannaCry;

Η επίθεση ransomware WannaCry έπληξε περίπου 230.000 υπολογιστές παγκοσμίως. Μία από τις πρώτες εταιρείες που επηρεάστηκαν ήταν η ισπανική εταιρεία κινητής τηλεφωνίας, Telefónica. Μέχρι τις 12 Μαΐου, χιλιάδες νοσοκομεία και χειρουργεία στο Ηνωμένο Βασίλειο, σχεδόν το 1/3, επλήγησαν από την επίθεση..

Σύμφωνα με πληροφορίες, τα ασθενοφόρα άλλαξαν τη διαδρομή τους, αφήνοντας ανθρώπους που χρειάζονταν επείγουσα περίθαλψη σε ανάγκη. Υπολογίστηκε ότι το συμβάν κόστισε στο Βρετανικό σύστημα υγείας περίπου 92 εκατομμύρια λίρες αφού ακυρώθηκαν 19.000 ραντεβού. Καθώς το ransomware εξαπλώθηκε πέρα από την Ευρώπη, τα συστήματα υπολογιστών σε 150 χώρες υπέστησαν ζημιές.

Η επίθεση ransomware WannaCry είχε σημαντικό οικονομικό αντίκτυπο παγκοσμίως. Υπολογίζεται ότι αυτό το έγκλημα στον κυβερνοχώρο προκάλεσε ζημίες 4 δισεκατομμυρίων δολαρίων σε όλο τον κόσμο.

1.3.2 Επίθεση DarkSide ransomware

Το DarkSide Ransomware είναι ένα RaaS που συχνά χρησιμοποιεί τακτικές διπλού εκβιασμού. Αφού οι χάκερς διεισδύσουν στον οργανισμό του στόχου, τα ευαίσθητα δεδομένα κρυπτογραφούνται και διατηρούνται ως λύτρα. Τα θύματα λαμβάνουν οδηγίες να πληρώσουν λύτρα, συχνά σε Bitcoin, για να ανακτήσουν την πρόσβαση. Επιπλέον, οι κυβερνοεγκληματίες απειλούν να δημοσιοποιήσουν τα δεδομένα είτε πουλώντας τα στη μαύρη αγορά σε άλλους εγκληματίες είτε δημοσιεύοντάς τα στο διαδίκτυο εάν δεν καταβληθούν τα λύτρα.

Μέχρι σήμερα, το DarkSide Ransomware έχει αναπτύξει τέτοιες τακτικές για να κλέψει με επιτυχία περισσότερα από 100 GB εταιρικών δεδομένων και να συγκεντρώσει περισσότερα από 4 εκατομμύρια δολάρια σε λύτρα.

Πώς λειτουργεί το DarkSide ransomware

Σε αντίθεση με άλλα δημοφιλή ransomware που λειτουργούν με επιθέσεις spear-phishing ή εξαπατώντας email με κακόβουλο λογισμικό, το DarkSide Ransomware εκμεταλλεύεται τις αδυναμίες του πρωτοκόλλου απομακρυσμένης επιφάνειας εργασίας (RDP) για να αποκτήσει αρχική πρόσβαση σε έναν υπολογιστή ή ένα δίκτυο. Στη συνέχεια ξεκλειδώνει σιγά σιγά τα δικαιώματα διαχείρισης, έτσι ώστε οι κυβερνοεπιτιθέμενοι να έχουν πλήρη πρόσβαση σε ευαίσθητα δεδομένα ή/και βασικές λειτουργίες.

Μερικές από τις κύριες ευπάθειες που είναι γνωστό ότι το DarkSide θηράμασε περιλαμβάνουν:

- Αδύναμοι κωδικοί πρόσβασης
- Απευθείας σύνδεση με RDP αντί για VPN
- Εσφαλμένα διαμορφωμένα τείχη προστασίας
- Έλλειψη ελέγχου ταυτότητας δύο παραγόντων

Με άλλα λόγια, το DarkSide Ransomware είναι πολύ αποτελεσματικό στην εκμετάλλευση οργανισμών που δεν κρατούν ισχυρές κλειδαριές στις εικονικές τους πόρτες.

1.3.3 Επίθεση REvil

Η ομάδα ransomware REvil αντιπροσώπευε περίπου το 37% όλων των επιθέσεων ransomware που διαπράχθηκαν το 2021. Η συμμορία, που δημιουργήθηκε το 2019, έδρασε για 31 μήνες, λειτουργώντας το REvil ως ransomware-for-service που επέτρεπε στους εγκληματίες να χρησιμοποιούν το λογισμικό με συνδρομή.

Ο ομάδα REvil έκλεισε τον Οκτώβριο του 2021, καθιστώντας τη μια από τις μακροβιότερες συμμορίες ransomware – η μέση συμμορία είτε κλείνει είτε αλλάζει επωνυμία μετά από 17 μήνες.

Κατά τη διάρκεια αυτής της περιόδου, το ransomware REvil χρησιμοποιήθηκε εναντίον χιλιάδων επιχειρήσεων και ατόμων παγκοσμίως. Αυτό περιελάμβανε μια επίθεση το 2020 στον τότε Πρόεδρο Ντόναλντ Τραμπ, απειλώντας τον με δημοσιοποίηση ευαίσθητων εγγράφων εάν δεν καταβάλλονταν λύτρα 42 εκατομμυρίων δολαρίων. Δεν είναι σαφές εάν είχαν όντως παραβιάσει δεδομένα σχετικά με τον Πρόεδρο.

Μια επίθεση υψηλού προφίλ σημειώθηκε το 2021, όταν ο REvil ισχυρίστηκε ότι είχαν κλέψει δεδομένα σχετικά με νέα προϊόντα της Apple, συμπεριλαμβανομένων σχηματικών σχεδίων για ένα επερχόμενο Macbook Pro. Η ομάδα ζήτησε 50 εκατομμύρια δολάρια ως λύτρα.

Το ηλεκτρονικό ψάρεμα φάνηκε να είναι η κύρια μέθοδος παράδοσης για το ransomware REvil. Το X-Force της IBM παρατήρησε ότι τα περιστατικά που αφορούσαν το REvil το 2021 συχνά ξεκίνησαν με ένα email ηλεκτρονικού ψαρέματος «QakBot». Αυτό το μήνυμα ηλεκτρονικού ταχυδρομείου θα έχει ένα μήνυμα που προτρέπει τον στόχο να επιλύσει ένα απλήρωτο τιμολόγιο ή κάτι παρόμοιο. Σε ορισμένες περιπτώσεις, οι χάκερ θα κλέβουν τις συνομιλίες που βρίσκονται σε εξέλιξη για να εισαγάγουν έναν κακόβουλο σύνδεσμο.

Όταν ανοίξει, ο στόχος θα λάβει οδηγίες να επιτρέψει εν αγνοία του το τραπεζικό trojan του QakBot να πέσει σε ένα σύστημα. Οι παράγοντες της απειλής REvil θα μπορούσαν στη συνέχεια να αναλάβουν τη διοίκηση της επιχείρησης, πραγματοποιώντας αναγνώριση πριν επιχειρήσουν να διακυβεύσουν δεδομένα.

1.3.4 Επιθέσεις ransomware στην Κόστα Ρίκα το 2022

Μια σειρά από επιθέσεις ransomware εξαπολύθηκαν κατά της κυβέρνησης της Κόστα Ρίκα το 2022, αναγκάζοντας την ηγεσία, να κηρύξει την χώρα σε κατάσταση έκτακτης ανάγκης καθώς μολύνθηκαν και παραβιάστηκαν κρίσιμα κρατικά συστήματα αφού οι κυβερνοεγκληματίες εξαπέλυσαν δύο επιθέσεις.

Η πρώτη έλαβε χώρα από τα μέσα Απριλίου έως τον Μάιο, με κύριους στόχους την ψηφιακή πλατφόρμα της κρατικής φορολογικής υπηρεσίας και τα συστήματα πληροφορικής που σχετίζονται με τον τελωνειακό έλεγχο. Σύμφωνα με εκτιμήσεις, επηρεάστηκαν επίσης 800 διακομιστές και ένας αξιοσήμειωτος ψηφιακός όγκος πληροφοριών στο υπουργείο Οικονομικών.

Εξαιτίας της κρυπτογράφησης δεδομένων και συστημάτων που σχετίζονται με τον τελωνειακό έλεγχο, το εμπόριο εντός και εκτός της χώρας ήταν εκτός λειτουργίας. Οι απώλειες τόσο σε επίπεδο εισαγωγών όσο και σε επίπεδο εξαγωγών υπολογίζονται ότι κυμάνθηκαν από 38 έως 125 εκατομμύρια δολάρια την ημέρα. Η ομάδα ransomware «Conti» ανέλαβε την ευθύνη για αυτές τις επιθέσεις, ζητώντας λύτρα 10 εκατομμύρια δολάρια για να αποφευχθεί η διαρροή των δεδομένων στο διαδίκτυο.

Η δεύτερη επίθεση είχε στόχο το Ταμείο Κοινωνικής Ασφάλισης της Κόστα Ρίκα, το οποίο διαχειρίζεται τις υπηρεσίες υγείας της χώρας. Περισσότεροι από τους μισούς διακομιστές επηρεάστηκαν, αναγκάζοντας τους γιατρούς να επαναπρογραμματίσουν το 7% των ραντεβού την πρώτη εβδομάδα μετά την επίθεση. Μια ομάδα που χρησιμοποιεί ransomware «HIVE» κατηγορήθηκε για τη δεύτερη επίθεση. Το HIVE έχει κάποιους συνδέσμους με το Conti.

1.3.5 Επίθεση ransomware San Francisco 49ers 2022

Τον Φεβρουάριο του 2022, η ομάδα ποδοσφαίρου των ΗΠΑ, οι San Francisco 49ers, υπέστη επίθεση με ransomware εναντίον του εταιρικού της δικτύου. Η ομάδα ransomware BlackByte κατέγραψε την ομάδα ως ένα από τα θύματά της σε έναν σκοτεινό ιστότοπο διαρροής. Οι 49ers δήλωσαν ότι η επίθεση περιορίστηκε στο εταιρικό δίκτυο πληροφορικής, με συστήματα όπως το γήπεδό τους και τους κατόχους εισιτηρίων να μην επηρεάζονται.

Η ομάδα ransomware BlackByte, η οποία ανέλαβε την ευθύνη για την επίθεση, εμφανίστηκε για πρώτη φορά τον Σεπτέμβριο του 2021. Διαχειρίζεται ένα μοντέλο Ransomware-as-a-Service, νοικιάζοντας το κακόβουλο λογισμικό τους σε άλλους παράγοντες απειλών που στη συνέχεια πραγματοποιούν επιθέσεις. Η πρώτη έκδοση του λογισμικού είχε ένα σφάλμα που έδωσε σε μια εταιρεία ασφάλειας στον κυβερνοχώρο το άνοιγμα να δημιουργήσει έναν αποκρυπτογραφητή για όποιον δεχόταν επίθεση από το κακόβουλο λογισμικό. Σε απάντηση, η BlackByte κυκλοφόρησε μια ενημερωμένη έκδοση που χρησιμοποιήθηκε στην επίθεση των 49ers.

1.3.6 Επίθεση ransomware ION Cleared Derivatives 2023

Στις 31 Ιανουαρίου 2023, η ION Cleared Derivatives, ένα τμήμα της ION Markets, υπέστη επίθεση ransomware που έβγαλε τα συστήματά της εκτός σύνδεσης. Αυτά τα συστήματα βοηθούσαν στην αυτοματοποίηση του κύκλου ζωής των συναλλαγών των χρηματοπιστωτικών εταιρειών.

Ως αποτέλεσμα της επίθεσης, οι εταιρείες χρηματοδότησης που χρησιμοποιούν το ION αναγκάστηκαν να πραγματοποιήσουν όλες τις συναλλαγές τους χειροκίνητα. Τα προβλήματα με την υποβολή δεδομένων σήμαιναν ότι οι μεγάλες εμπορικές εταιρείες έλαβαν συμβουλές να εκτιμήσουν τις τιμές των εμπορευμάτων και να τις αναθεωρήσουν αργότερα, σε μια προσπάθεια να αποφευχθούν μεγάλες καθυστερήσεις στην υποβολή εκθέσεων.

ΚΕΦΑΛΑΙΟ 2: ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΜΙΑΣ ΕΠΙΘΕΣΗΣ RANSOMWARE ΣΤΗΝ ΕΠΙΧΕΙΡΗΣΗ

2.1 ΕΙΣΑΓΩΓΗ

Οι επιθέσεις ransomware έχουν αναδειχθεί ως μία από τις πιο σημαντικές απειλές για τις επιχειρήσεις παγκοσμίως. Αυτές οι επιθέσεις περιλαμβάνουν κακόβουλο λογισμικό που κρυπτογραφεί τα δεδομένα του θύματος, με τον εισβολέα να απαιτεί λύτρα για το κλειδί αποκρυπτογράφησης. Ο αντίκτυπος του ransomware στις επιχειρήσεις μπορεί να είναι βαθύς, επηρεάζοντας διάφορες πτυχές, από οικονομικές απώλειες έως ζημιές στη φήμη. Σε αυτό το κεφάλαιο θα αναδείξουμε τον πολύπλευρο αντίκτυπο που έχει μια επίθεση ransomware σε μια επιχείρηση, εξετάζοντας τις οικονομικές επιπτώσεις, τις λειτουργικές διακοπές, τις νομικές συνέπειες και πολλά άλλα.

2.2 ΟΙΚΟΝΟΜΙΚΟΣ ΑΝΤΙΚΤΥΠΟΣ

2.2.1 Άμεσο οικονομικό κόστος

Οι επιθέσεις ransomware προκαλούν άμεσο οικονομικό κόστος στις επιχειρήσεις, το οποίο μπορεί να είναι αρκετά σημαντικό. Οι ίδιες οι πληρωμές λύτρων μπορεί να κυμαίνονται από χιλιάδες έως εκατομμύρια δολάρια. Ωστόσο, τα λύτρα είναι μόνο ένα κλάσμα της συνολικής οικονομικής ζημιάς. Οι επιχειρήσεις συχνά επιβαρύνονται με πρόσθετο κόστος που σχετίζεται με την επαναφορά δεδομένων από αντίγραφα ασφαλείας, τη διερεύνηση της παραβίασης και τη βελτίωση των μέτρων ασφαλείας για την αποτροπή μελλοντικών επιθέσεων.

2.2.2 Πληρωμές λύτρων

Ενώ οι αρχές συχνά συμβουλεύουν τα θύματα να μην πληρώσουν τα λύτρα, πολλές επιχειρήσεις αισθάνονται υποχρεωμένες να το κάνουν με την ελπίδα να ανακτήσουν γρήγορα την πρόσβαση στα δεδομένα τους. Ωστόσο, η καταβολή του ποσού που ζητάται δεν εγγυάται την ανάκτηση δεδομένων, καθώς οι εισβολείς ενδέχεται να παρέχουν ελαττωματικά κλειδιά αποκρυπτογράφησης ή να απαιτήσουν πρόσθετα χρήματα. Επιπλέον, η πληρωμή των λύτρων μπορεί να ενθαρρύνει περαιτέρω επιθέσεις και να διαιωνίσει τον κύκλο του εγκλήματος στον κυβερνοχώρο.

2.2.3 Έμμεσες οικονομικές ζημιές

Πέρα από το άμεσο κόστος, οι επιθέσεις ransomware οδηγούν σε σημαντικές έμμεσες οικονομικές απώλειες. Αυτά περιλαμβάνουν απώλεια εσόδων λόγω διακοπής λειτουργίας και πιθανής διακοπής της επιχείρησης. Πολλές επιχειρήσεις αντιμετωπίζουν αναστολή λειτουργίας για μέρες ή και εβδομάδες, οδηγώντας σε σημαντικές απώλειες εσόδων. Επιπλέον, υπάρχουν κόστη που σχετίζονται με νομικές αμοιβές, ρυθμιστικά πρόστιμα και πιθανούς διακανονισμούς εάν τεθούν σε κίνδυνο ευαίσθητα δεδομένα πελατών ή πελατών.

2.2.4 Επιπτώσεις στις τιμές των μετοχών

Είναι ενδιαφέρον ότι ο αντίκτυπος των επιθέσεων ransomware στις τιμές των μετοχών μπορεί να είναι ανάμεικτος. Οι αρχικές αντιδράσεις στο χρηματιστήριο βλέπουν συχνά μια απότομη πτώση της αξίας της μετοχής της εταιρείας-θύματος. Για παράδειγμα, μια μελέτη έδειξε ότι οι μετοχές των οργανώσεων των θυμάτων μειώθηκαν κατά μέσο όρο κατά 22,9% μέσα σε 24 ώρες από τη δημόσια αποκάλυψη μιας επίθεσης. Ωστόσο, αυτή η πτώση είναι συχνά προσωρινή, με τις τιμές να ανακάμπτουν τις επόμενες ημέρες ή εβδομάδες. Σε ορισμένες περιπτώσεις, οι μετοχές ενδέχεται να έχουν καλύτερη απόδοση μήνες μετά το συμβάν, υποδηλώνοντας μια περίπλοκη σχέση μεταξύ επιθέσεων ransomware και μακροπρόθεσμης απόδοσης μετοχών.

2.3 ΛΕΙΤΟΥΡΓΙΚΗ ΔΙΑΤΑΡΑΧΗ

2.3.1 Διακοπή λειτουργίας

Η διακοπή λειτουργίας μιας επιχείρησης είναι μία από τις πιο άμεσες και ορατές επιπτώσεις μιας επίθεσης ransomware. Οι επιχειρήσεις ενδέχεται να αναγκαστούν να διακόψουν εντελώς τις λειτουργίες τους καθώς εργάζονται για την αποκρυπτογράφηση των δεδομένων τους και την επαναφορά των συστημάτων. Αυτός ο χρόνος διακοπής λειτουργίας μπορεί να είναι ιδιαίτερα επιζήμιος για βιομηχανίες που βασίζονται στη συνεχή λειτουργία, όπως η μεταποίηση, η υγειονομική περίθαλψη και η χρηματοδότηση.

2.3.2 Απώλεια Παραγωγικότητας

Κατά τη διάρκεια και μετά από μια επίθεση ransomware, η παραγωγικότητα των εργαζομένων επηρεάζεται σημαντικά. Οι εργαζόμενοι ενδέχεται να μην μπορούν να έχουν πρόσβαση σε κρίσιμα συστήματα και δεδομένα, με αποτέλεσμα σημαντική μείωση της παραγωγικότητας. Ακόμη και μετά την αποκατάσταση των συστημάτων, μπορεί να υπάρξουν παρατεταμένα αποτελέσματα καθώς οι επιχειρήσεις εργάζονται για να διασφαλίσουν ότι τα συστήματα είναι ασφαλή και πλήρως λειτουργικά.

σ

2.3.3 Κόστος ανάκτησης

Η ανάκτηση από μια επίθεση ransomware περιλαμβάνει πολλά βήματα, όπως η αναγνώριση και η απομόνωση των επηρεαζόμενων συστημάτων, η επαναφορά δεδομένων από αντίγραφα ασφαλείας και η πιθανή διαπραγμάτευση με τους εισβολείς. Αυτές οι διαδικασίες απαιτούν χρόνο και πόρους και συχνά ζητείται η βοήθεια εξωτερικών ειδικών στον τομέα της κυβερνοασφάλειας. Το κόστος ανάκτησης μπορεί να είναι σημαντικό, ειδικά για επιχειρήσεις που δεν διαθέτουν ισχυρά εφεδρικά συστήματα ή σχέδια αντιμετώπισης περιστατικών.

2.4 ΖΗΜΙΑ ΣΤΗ ΦΗΜΗ

2.4.1 Απώλεια της εμπιστοσύνης

Οι επιθέσεις ransomware μπορούν να βλάψουν σοβαρά τη φήμη μιας επιχείρησης. Οι πελάτες μπορεί να χάσουν την εμπιστοσύνη τους στην ικανότητα της εταιρείας να προστατεύει τις ευαίσθητες πληροφορίες τους, οδηγώντας σε απώλεια της επιχείρησης και πιθανή μακροπρόθεσμη ζημιά στην επωνυμία. Η διάβρωση της εμπιστοσύνης μπορεί να είναι ιδιαίτερα σοβαρή εάν η επίθεση ransomware έχει ως αποτέλεσμα τη δημόσια αποκάλυψη ευαίσθητων δεδομένων πελατών.

2.4.2 Επιπτώσεις στις σχέσεις με τους πελάτες

Η διατήρηση των σχέσεων με τους πελάτες μετά την επίθεση μπορεί να είναι δύσκολη. Οι επιχειρήσεις ενδέχεται να αντιμετωπίσουν απώλεια πελατών καθώς εκείνοι αναζητούν πιο ασφαλείς εναλλακτικές λύσεις. Επιπλέον, οι εταιρείες συχνά χρειάζεται να επενδύσουν πολλά σε προσπάθειες δημοσίων σχέσεων για να ξαναχτίσουν την εικόνα τους και να διαβεβαιώσουν τους ενδιαφερόμενους ότι έχουν λάβει μέτρα για να ενισχύσουν την ασφάλεια τους στον κυβερνοχώρο.

2.4.3 Αρνητική Δημοσιότητα

Τα μέσα ενημέρωσης υπογραμμίζουν συχνά επιθέσεις ransomware, ειδικά όταν επηρεάζουν μεγάλες εταιρείες ή περιλαμβάνουν σημαντικές παραβιάσεις δεδομένων. Αυτή η αρνητική δημοσιότητα μπορεί να διαβρώσει περαιτέρω την εμπιστοσύνη των πελατών και να αμαυρώσει την εικόνα της επιχείρησης. Επιπλέον, οι ανταγωνιστές μπορούν να εκμεταλλευτούν την κατάσταση προς όφελός τους, δίνοντας έμφαση στα μέτρα ασφαλείας και την αξιοπιστία τους.

2.5 ΝΟΜΙΚΕΣ ΚΑΙ ΚΑΝΟΝΙΣΤΙΚΕΣ ΣΥΝΕΠΕΙΕΣ

2.5.1 Κανονιστικά πρόστιμα και κόστος συμμόρφωσης

Οι επιθέσεις ransomware μπορεί να έχουν σημαντικές νομικές και ρυθμιστικές συνέπειες. Οι εταιρείες που δεν προστατεύουν ευαίσθητα δεδομένα ενδέχεται να αντιμετωπίσουν πρόστιμα από ρυθμιστικούς φορείς. Αυτά τα πρόστιμα μπορεί να είναι σημαντικά, ιδιαίτερα σε κλάδους που υπόκεινται σε αυστηρές ρυθμίσεις, όπως η χρηματοδότηση και η υγειονομική περίθαλψη. Επιπλέον, οι επιχειρήσεις μπορεί να χρειαστεί να επενδύσουν σε προσπάθειες συμμόρφωσης για την εκπλήρωση των κανονιστικών απαιτήσεων και την αποφυγή μελλοντικών κυρώσεων.

2.5.2 Νομικές Ενέργειες

Οι οργανισμοί-θύματα ενδέχεται επίσης να αντιμετωπίσουν νομικές ενέργειες από πελάτες ή συνεργάτες των οποίων τα δεδομένα παραβιάστηκαν. Αυτές οι νομικές ενέργειες μπορεί να οδηγήσουν σε δαπανηρούς διακανονισμούς και περαιτέρω βλάβη στη φήμη της εταιρείας. Οι νομικές αμοιβές και το κόστος που σχετίζεται με την υπεράσπιση κατά αγωγών προσθέτουν άλλο ένα επίπεδο οικονομικής επιβάρυνσης μετά από επίθεση ransomware.

2.6 ΜΑΚΡΟΠΡΟΘΕΣΜΟΣ ΣΤΡΑΤΗΓΙΚΟΣ ΑΝΤΙΚΤΥΠΟΣ

2.6.1 Αλλαγές στην επιχειρησιακή στρατηγική

Ο μακροπρόθεσμος στρατηγικός αντίκτυπος των επιθέσεων ransomware στις επιχειρήσεις ενδέχεται να είναι βαθύς. Οι οργανισμοί μπορεί να χρειαστεί να επανεξετάσουν το δικό τους Ολόκληρη η προσέγγιση της κυβερνοασφάλειας, επενδύοντας σε μεγάλο βαθμό σε νέες τεχνολογίες και διαδικασίες για την πρόληψη μελλοντικών επιθέσεων. Αυτή η μετατόπιση απαιτεί συχνά ανακατανομή πόρων και ίσως επηρεάσει άλλους τομείς της επιχείρησης.

2.6.2 Αυξημένο κόστος ασφάλειας

Στον απόηχο μιας επίθεσης ransomware, οι επιχειρήσεις συχνά επενδύουν πολλά στην ενίσχυση των μέτρων ασφάλειας στον κυβερνοχώρο για την πρόληψη μελλοντικών περιστατικών. Αυτή η επένδυση περιλαμβάνει την εφαρμογή προηγμένου λογισμικού ασφαλείας, τη διενέργεια τακτικών ελέγχων ασφαλείας, την εκπαίδευση των εργαζομένων στις βέλτιστες πρακτικές ασφάλειας στον κυβερνοχώρο και την ανάπτυξη ισχυρών σχεδίων αντιμετώπισης συμβάντων. Ενώ αυτά τα μέτρα είναι απαραίτητα, μπορούν να αυξήσουν σημαντικά το λειτουργικό κόστος.

2.6.3 Μακροπρόθεσμη Διαταραχή Επιχειρήσεων

Πέρα από τη φάση άμεσης ανάκτησης, οι επιθέσεις ransomware μπορεί να έχουν μακροπρόθεσμες επιπτώσεις στις επιχειρηματικές δραστηριότητες. Η απώλεια κρίσιμων δεδομένων ενδέχεται να διαταράξει τα στρατηγικά σχέδια, να καθυστερήσει την κυκλοφορία προϊόντων και να εμποδίσει την ανάπτυξη της επιχείρησης. Επιπλέον, ο χρόνος και οι πόροι που δαπανώνται για την ανάκτηση και τη βελτίωση των μέτρων ασφαλείας μπορούν να αποσπάσουν την προσοχή από τις βασικές επιχειρηματικές δραστηριότητες, επηρεάζοντας τη συνολική παραγωγικότητα και ανταγωνιστικότητα.

2.7 ΑΝΤΙΚΤΥΠΟΣ ΣΤΗΝ ΚΑΙΝΟΤΟΜΙΑ

Οι συνέπειες μιας επίθεσης ransomware μπορεί να καταπνίξουν την καινοτομία. Προκειμένου να αποφύγουν μεγαλύτερο κίνδυνο, οι εταιρείες εστιάζουν τους πόρους τους στην ασφάλεια και όχι στην ανάπτυξη νέων προϊόντων ή υπηρεσιών. Αυτή η αλλαγή εστίασης βοηθά να εμποδίσει την ικανότητα μιας εταιρείας να ανταγωνίζεται αποτελεσματικά στην αγορά.

2.8 ΨΥΧΟΛΟΓΙΚΟΣ ΚΑΙ ΠΟΛΙΤΙΣΤΙΚΟΣ ΑΝΤΙΚΤΥΠΟΣ

2.8.1 Το ηθικό των εργαζομένων

Οι επιθέσεις ransomware ενδεχομένως να έχουν σημαντικό ψυχολογικό αντίκτυπο στους εργαζόμενους. Το άγχος και η αβεβαιότητα που συνδέονται με μια επίθεση συχνά μειώνουν το ηθικό και να επηρεάσουν τη συνολική εργασιακή ικανοποίηση. Οι εργαζόμενοι μπορεί να αισθάνονται ανασφαλείς για τη σταθερότητα της εργασίας τους και απογοητευμένοι με τις διακοπές που προκαλούνται από την επίθεση.

2.9 ΟΡΓΑΝΩΤΙΚΗ ΚΟΥΛΤΟΥΡΑ

Ο πολιτιστικός αντίκτυπος του ransomware μπορεί να είναι μακροχρόνιος. Ίσως χρειαστεί οι επιχειρήσεις να καλλιεργήσουν μια κουλτούρα ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο, να εκπαιδεύουν τακτικά τους υπαλλήλους σχετικά με τις βέλτιστες πρακτικές και να διασφαλίζουν ότι όλοι κατανοούν τη σημασία της προστασίας ευαίσθητων δεδομένων. Αυτή η πολιτισμική αλλαγή είναι απαραίτητη για την πρόληψη μελλοντικών επιθέσεων, αλλά μπορεί επίσης να δημιουργήσει ένα περιβάλλον αυξημένης επαγρύπνησης και προσοχής.

2.10 ΥΠΟΘΕΣΗ ΕΡΓΑΣΙΑΣ

Μια μικρή κατασκευαστική επιχείρηση έπεσε θύμα επίθεσης ransomware που κρυπτογραφούσε τα χρονοδιαγράμματα παραγωγής, τα δεδομένα αποθέματος και τα οικονομικά της αρχεία. Χωρίς αυστηρά μέτρα κυβερνοασφάλειας, η επιχείρηση δυσκολεύτηκε να ανακάμψει. Ο χρόνος διακοπής διήρκεσε δύο εβδομάδες, με αποτέλεσμα να υπάρξουν χαμένες παραγγελίες και δυσαρεστημένους πελάτες. Η επιχείρηση τελικά πλήρωσε λύτρα 50.000 $, αλλά η διαδικασία αποκρυπτογράφησης ήταν εν μέρει επιτυχής. Οι οικονομικές επιπτώσεις της επίθεσης, σε συνδυασμό με το κόστος εφαρμογής νέων μέτρων ασφαλείας, απείλησαν τη βιωσιμότητα της επιχείρησης.

Εν κατακλείδι οι επιθέσεις ransomware αποτελούν σημαντική απειλή για τις επιχειρήσεις, επηρεάζοντας τη χρηματοοικονομική σταθερότητα, τη λειτουργική αποτελεσματικότητα, τη φήμη και τους μακροπρόθεσμους στρατηγικούς στόχους. Ο πολύπλευρος αντίκτυπος αυτών των επιθέσεων υπογραμμίζει τη σημασία των ισχυρών μέτρων κυβερνοασφάλειας και του προληπτικού σχεδιασμού. Κατανοώντας το πλήρες εύρος των επιπτώσεων του ransomware, οι επιχειρήσεις μπορούν να προετοιμαστούν καλύτερα για να αμυνθούν έναντι αυτών των απειλών και να ελαχιστοποιήσουν την πιθανή ζημιά τους. Η εφαρμογή ολοκληρωμένων στρατηγικών ασφάλειας και η προώθηση μιας κουλτούρας ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο είναι ουσιαστικά βήματα για την προστασία των επιχειρήσεων από το συνεχώς εξελισσόμενο τοπίο των επιθέσεων ransomware.

ΚΕΦΑΛΑΙΟ 3: ΠΡΟΤΥΠΑ, ΚΑΛΕΣ ΠΡΑΚΤΙΚΕΣ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ & ΕΠΙΘΕΣΕΩΝ ΤΥΠΟΥ RANSOMWARE

3.1 ΠΟΛΙΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ (ISMS Policy)

3.1.1 Τι είναι το σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS)

Ένα σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) αποτελείτε από ένα σύνολο πολιτικών και διαδικασιών για τη συστηματική διαχείριση των ευαίσθητων δεδομένων μίας επιχείρησης. Ένα ISMS στοχεύει στην ελαχιστοποίηση του κινδύνου και την διασφάλιση της επιχειρηματικής συνέχειας περιορίζοντας προληπτικά τον αντίκτυπο μιας κυβερνοεπίθεσης.

Το ISMS συνήθως αντιμετωπίζει τη συμπεριφορά και τις διαδικασίες των εργαζομένων, όπως επίσης τα δεδομένα όσο και τα συστήματα που χρησιμοποιούνται. Ταυτόχρονα μπορεί να στοχεύει σε έναν συγκεκριμένο τύπο δεδομένων, όπως τα δεδομένα πελατών, ή μπορεί να εφαρμοστεί με έναν ολοκληρωμένο τρόπο που γίνεται μέρος της κουλτούρας της εταιρείας.

3.1.2 Πώς λειτουργεί το ISMS;

Ένα ISMS παρέχει μια συστηματική προσέγγιση για τη διαχείριση της ασφάλειας πληροφοριών μίας επιχείρησης. Η ασφάλεια πληροφοριών περιλαμβάνει ορισμένες γενικές πολιτικές που ελέγχουν και διαχειρίζονται τα επίπεδα κινδύνου ασφάλειας σε μία επιχείρηση.

Το ISO/IEC 27001 είναι το διεθνές πρότυπο για την ασφάλεια πληροφοριών και για τη δημιουργία ISMS. Δημοσιεύτηκε από κοινού από τον Διεθνή Οργανισμό Τυποποίησης (International Organization for Standardization) και τη Διεθνή Ηλεκτροτεχνική Επιτροπή (International Electrotechnical Commission), το πρότυπο δεν επιβάλλει συγκεκριμένες ενέργειες αλλά περιλαμβάνει προτάσεις για τεκμηρίωση, εσωτερικούς ελέγχους, συνεχή βελτίωση και διορθωτικές και προληπτικές ενέργειες. Για να αποκτήσει πιστοποίηση ISO 27001, ένας οργανισμός απαιτεί ένα ISMS που προσδιορίζει τα περιουσιακά στοιχεία του οργανισμού και παρέχει την ακόλουθη αξιολόγηση:

- τους κινδύνους που αντιμετωπίζουν τα περιουσιακά στοιχεία ενός οργανισμού.
- τα μέτρα που λαμβάνονται για την προστασία των περιουσιακών στοιχείων.
- ένα σχέδιο δράσης σε περίπτωση που υπάρξει παραβίαση της ασφάλειας και
- ο ορισμός ρόλων των ατόμων που είναι υπεύθυνα για κάθε βήμα της διαδικασίας ασφάλειας πληροφοριών.

Ο στόχος ενός ISMS δεν είναι μόνο η μεγιστοποίηση της ασφάλειας των πληροφοριών, αλλά και η επίτευξη ενός επιθυμητού επιπέδου ασφάλειας πληροφοριών ενός οργανισμού. Ανάλογα με τις ειδικές ανάγκες του κλάδου, αυτά τα επίπεδα ελέγχου μπορεί να διαφέρουν. Για παράδειγμα, δεδομένου ότι η υγειονομική περίθαλψη είναι ένας τομέας υψηλής ρύθμισης, ένας οργανισμός μπορεί να αναπτύξει ένα σύστημα για να διασφαλίσει ότι τα ευαίσθητα δεδομένα ασθενών προστατεύονται πλήρως.

Ένα ISMS παρέχει μια συστηματική προσέγγιση για τη διαχείριση της ασφάλειας πληροφοριών ενός οργανισμού και περιλαμβάνει πολιτικές και διαδικασίες για τη διαχείριση των δεδομένων του.

3.1.3 Οφέλη του ISMS

Το ISMS παρέχει μια συνολική προσέγγιση της διαχείρισης των πληροφοριακών συστημάτων μέσα σε μία επιχείρηση. Αυτό έχει πολλαπλά οφέλη για μία επιχείρηση, μερικά από τα οποία επισημαίνονται παρακάτω.

• **Προστατεύει ευαίσθητα δεδομένα.**

Ένα ISMS μπορεί να προστατεύσει όλους τους τύπους ιδιόκτητων περιουσιακών στοιχείων πληροφοριών είτε βασίζονται σε χαρτί είτε διατηρούνται ψηφιακά είτε βρίσκονται στο cloud. Αυτά τα περιουσιακά στοιχεία μπορεί να περιλαμβάνουν προσωπικά δεδομένα, πνευματικά δικαιώματα, οικονομικά δεδομένα, δεδομένα πελατών και δεδομένα που ανατίθενται σε εταιρείες μέσω τρίτων.

• **Τηρεί την κανονιστική συμμόρφωση.**

Το ISMS βοηθά τους οργανισμούς να ανταποκρίνονται σε όλες τις κανονιστικές και συμβατικές απαιτήσεις συμμόρφωσης και παρέχει καλύτερη κατανόηση των νομικών θεμάτων που αφορούν τα πληροφοριακά συστήματα. Δεδομένου ότι η παραβίαση των νομικών κανονισμών συνοδεύεται από υψηλά πρόστιμα, η ύπαρξη ενός ISMS μπορεί να είναι ιδιαίτερα επωφελής για κλάδους με έντονα ρυθμιζόμενες διαδικασίες και κρίσιμες υποδομές, όπως ο χρηματοπιστωτικός τομέας ή η υγειονομική περίθαλψη.

• **Παρέχει επιχειρηματική συνέχεια.**

Όταν μία επιχείρηση αποφασίσει να επενδύσει σε ένα ISMS πλάνο, τότε αυξάνεται αυτόματα το επίπεδο άμυνάς έναντι πληθώρας απειλών. Επίσης μειώνεται ο αριθμός των περιστατικών ασφαλείας, όπως οι επιθέσεις στον κυβερνοχώρο, με αποτέλεσμα λιγότερες διακοπές και λιγότερο χρόνο διακοπής λειτουργίας, που είναι σημαντικοί παράγοντες για τη διατήρηση της επιχειρηματικής συνέχειας.

• **Μειώνει το κόστος.**

Ένα ISMS προσφέρει εις βάθος αξιολόγηση των κινδύνων για όλα τα περιουσιακά στοιχεία της επιχείρησης. Αυτό δίνει τη δυνατότητα στις επιχειρήσεις να ιεραρχούν τα περιουσιακά στοιχεία με κριτήριο τον υψηλότερο κίνδυνο, ώστε να αποφεύγονται οι αλόγιστες δαπάνες για αχρείαστες άμυνες και να παρέχεται μια εστιασμένη προσέγγιση για

την ασφάλισή τους. Αυτή η προσέγγιση, σε συνδυασμό με τον μικρότερο χρόνο διακοπής λειτουργίας λόγω της μείωσης των περιστατικών ασφαλείας, μειώνει σημαντικά τις συνολικές δαπάνες ενός οργανισμού.

• **Ενισχύει την εταιρική κουλτούρα.**

Το ISMS παρέχει μια ολοκληρωμένη προσέγγιση για την ασφάλεια και τη διαχείριση περιουσιακών στοιχείων σε ολόκληρο τον οργανισμό, η οποία δεν περιορίζεται στην ασφάλεια πληροφορικής. Αυτό ενθαρρύνει όλους τους εργαζόμενους να κατανοήσουν τους κινδύνους που συνδέονται με τα περιουσιακά στοιχεία πληροφοριών και να υιοθετήσουν βέλτιστες πρακτικές ασφάλειας ως μέρος της καθημερινότητάς τους.

• **Προσαρμόζεται στις αναδυόμενες απειλές.**

Οι απειλές για την ασφάλεια εξελίσσονται συνεχώς. Ένα ISMS βοηθά τους οργανισμούς να προετοιμαστούν και να προσαρμοστούν σε νεότερες απειλές και στις συνεχώς μεταβαλλόμενες απαιτήσεις του τοπίου ασφάλειας.

3.1.4 Ποιες οι βέλτιστες πρακτικές ενός ISMS

Το ISO 27001, μαζί με ISO 27002, προσφέρουν εκείνες τις κατευθυντήριες γραμμές βέλτιστων πρακτικών για τη δημιουργία ενός ISMS. Παρακάτω ακολουθεί μία ενδεικτική λίστα ελέγχου των βέλτιστων πρακτικών που πρέπει να λάβει υπόψη μία επιχείρηση πριν επενδύσει στην δημιουργία και υιοθέτηση ενός ISMS:

- **Προσδιορισμός των επιχειρηματικών αναγκών.**

Πριν από την εκτέλεση ενός ISMS, είναι σημαντικό για τους οργανισμούς να έχουν μια συνολική άποψη για τις επιχειρηματικές λειτουργίες, τα εργαλεία και τα συστήματα διαχείρισης ασφάλειας πληροφοριών ώστε να έχουν πλήρη γνώση για το ποιες είναι τόσο οι επιχειρηματικές απαιτήσεις όσο και οι απαιτήσεις ασφάλειας.

- **Καθιερώστε μια πολιτική ασφάλειας πληροφοριών.**

Η ύπαρξη μιας πολιτικής ασφάλειας πληροφοριών πριν από τη δημιουργία ενός ISMS είναι επωφελής, καθώς μπορεί να βοηθήσει έναν οργανισμό να ανακαλύψει τα αδύνατα σημεία του. Η πολιτική ασφαλείας θα πρέπει συνήθως να παρέχει μια γενική επισκόπηση των τρεχόντων ελέγχων ασφαλείας σε έναν οργανισμό.

- **Παρακολούθηση πρόσβασης δεδομένων.**

Οι εταιρείες πρέπει να είναι σε θέση να παρακολουθούν όλες τις πολιτικές ελέγχου πρόσβασης για να διασφαλίζουν ότι μόνο εξουσιοδοτημένα άτομα αποκτούν πρόσβαση σε ευαίσθητες πληροφορίες. Αυτή η διαδικασία θα πρέπει να παρατηρεί ποιος έχει πρόσβαση στα δεδομένα, πότε και από πού. Εκτός από την παρακολούθηση της πρόσβασης στα δεδομένα, οι εταιρείες θα πρέπει επίσης να παρακολουθούν τις συνδέσεις και τους ελέγχους ταυτότητας και να τηρούν αρχείο τους για περαιτέρω διερεύνηση.

- **Διεξαγωγή εκπαίδευσης ευαισθητοποίησης για την ασφάλεια.**

Όλοι οι εργαζόμενοι οφείλουν να λαμβάνουν τακτική εκπαίδευση ευαισθητοποίησης σχετικά με την ασφάλεια. Η εκπαίδευση θα πρέπει να εισάγει τους χρήστες στο εξελισσόμενο τοπίο απειλών, τις κοινές ευπάθειες δεδομένων που περιβάλλουν τα συστήματα πληροφοριών και τις τεχνικές μετριασμού και πρόληψης για την προστασία των δεδομένων από τον κίνδυνο.

- **Ασφαλείς συσκευές.**

Η προστασία όλων των εταιρικών συσκευών τόσο από φυσική ζημιά όσο και από παραβίαση, θα πρέπει να γίνεται με τη λήψη σχετικών μέτρων ασφαλείας λαμβάνοντας μέτρα για την αποτροπή επίθεσης και εισβολής. Εργαλεία όπως το Google Workspace και το Office 365 προσφέρουν ενσωματωμένη ασφάλεια συσκευής, καθώς και λογισμικά τύπου Mobile Device Management (MDM) όπως Scalefusion, Kandji, Hexnode, Citrix Endpoint Management, Miradore, κλπ.

- **Κρυπτογράφηση δεδομένων.**

Η κρυπτογράφηση αποτρέπει τη μη εξουσιοδοτημένη πρόσβαση και είναι η καλύτερη μορφή άμυνας έναντι απειλών ασφαλείας. Όλα τα δεδομένα του οργανισμού θα πρέπει να είναι κρυπτογραφημένα πριν από τη δημιουργία ενός ISMS, καθώς θα αποτρέψει τυχόν μη εξουσιοδοτημένες προσπάθειες υπονόμευσης κρίσιμων δεδομένων.

- **Αντίγραφα ασφαλείας δεδομένων.**

Τα αντίγραφα ασφαλείας διαδραματίζουν βασικό ρόλο στην πρόληψη της απώλειας δεδομένων και θα πρέπει να αποτελούν μέρος της πολιτικής ασφάλειας μιας εταιρείας πριν από τη δημιουργία ενός ISMS. Εκτός από τα τακτικά αντίγραφα ασφαλείας, θα πρέπει να προγραμματιστεί η τοποθεσία και η συχνότητα των αντιγράφων ασφαλείας. Οι οργανισμοί θα πρέπει επίσης να δημιουργήσουν ένα σχέδιο για να διατηρούν τα αντίγραφα ασφαλείας προστατευμένα, το οποίο θα πρέπει να ισχύει τόσο εντός των εγκαταστάσεων όσο και για τα αντίγραφα ασφαλείας στο cloud.

- **Διεξαγωγή εσωτερικού ελέγχου ασφάλειας.**

Θα πρέπει να διενεργείται εσωτερικός έλεγχος ασφάλειας πριν από την εκτέλεση ενός ISMS. Οι εσωτερικοί έλεγχοι είναι ένας πολύ καλός τρόπος για τους οργανισμούς να αποκτήσουν ορατότητα σχετικά με τα συστήματα ασφαλείας, το λογισμικό και τις συσκευές τους, καθώς μπορούν να εντοπίσουν και να διορθώσουν τα κενά ασφαλείας πριν από την εκτέλεση ενός ISMS.

3.1.5 Εφαρμογή ISMS

Υπάρχουν διάφοροι τρόποι για να ρυθμίσετε ένα ISMS. Οι περισσότεροι οργανισμοί είτε ακολουθούν μια διαδικασία plan-do-check-act είτε μελετούν το διεθνές πρότυπο ασφάλειας ISO 27001 το οποίο ουσιαστικά περιγράφει λεπτομερώς τις απαιτήσεις για ένα ISMS.

Τα ακόλουθα βήματα δείχνουν πώς πρέπει να εφαρμοστεί ένα ISMS:

1. **Καθορισμός πεδίου εφαρμογής και στόχων**.

Θα πρέπει να γίνει σωστός καθορισμός των περιουσιακών στοιχειών που χρειάζονται προστασία καθώς και τους λόγους για την προστασία τους. Η διοίκηση της εταιρείας θα πρέπει επίσης να καθορίσει σαφείς στόχους για τους τομείς εφαρμογής και τους περιορισμούς του ISMS.

2. **Προσδιορισμός περιουσιακών στοιχείων**.

Προσδιορισμός των περιουσιακών στοιχειών που πρόκειται να προστατευθούν. Αυτό μπορεί να επιτευχθεί με τη δημιουργία ενός καταλόγου κρίσιμων για τις επιχειρήσεις περιουσιακών στοιχείων, συμπεριλαμβανομένων υλικού, λογισμικού, υπηρεσιών, πληροφοριών, βάσεων δεδομένων και φυσικών τοποθεσιών.

3. **Αναγνώριση των κινδύνων**.

Μόλις εντοπιστούν τα περιουσιακά στοιχεία, ο βαθμός επικινδυνότητας θα πρέπει να αναλυθεί και να βαθμολογηθεί αξιολογώντας τις νομικές απαιτήσεις ή τις κατευθυντήριες γραμμές συμμόρφωσης. Επίσης η επιχείρηση θα πρέπει να σταθμίσουν τις επιπτώσεις των εντοπισμένων κινδύνων. Για παράδειγμα, θα μπορούσαν να αμφισβητήσουν το μέγεθος του αντίκτυπου που θα προκαλούσε εάν παραβιαστεί η εμπιστευτικότητα, η διαθεσιμότητα ή η ακεραιότητα των στοιχείων ενεργητικού ή η πιθανότητα εμφάνισης αυτής της παραβίασης. Ο τελικός στόχος θα πρέπει να καταλήγει σε συμπέρασμα που θα περιγράφει ποιοι κίνδυνοι είναι αποδεκτοί και ποιοι πρέπει να αντιμετωπιστούν πάση θυσία λόγω της πιθανής ζημίας.

4. **Προσδιορισμός των μέτρων μετριασμού**.

Ένα αποτελεσματικό ISMS όχι μόνο προσδιορίζει τους παράγοντες κινδύνου αλλά παρέχει επίσης ικανοποιητικά μέτρα για τον αποτελεσματικό μετριασμό και την καταπολέμησή τους. Τα μέτρα μετριασμού θα πρέπει να καθορίζουν ένα σαφές σχέδιο πρόληψης για την πλήρη αποφυγή του κινδύνου. Για παράδειγμα, μια εταιρεία που προσπαθεί να αποφύγει τον κίνδυνο απώλειας ενός φορητού υπολογιστή με ευαίσθητα δεδομένα πελατών θα πρέπει να αποτρέψει εξαρχής την αποθήκευση αυτών των δεδομένων σε αυτόν τον φορητό υπολογιστή. Ένα αποτελεσματικό μέτρο θα ήταν η θέσπιση μιας πολιτικής ή ενός κανόνα που δεν επιτρέπει στους υπαλλήλους να αποθηκεύουν δεδομένα πελατών στους φορητούς υπολογιστές τους.

5. **Βελτιώσεις**.

Όλα τα προηγούμενα μέτρα θα πρέπει να παρακολουθούνται και να ελέγχονται επανειλημμένα ως προς την αποτελεσματικότητά τους. Εάν η παρακολούθηση αποκαλύψει τυχόν ελλείψεις ή νέους ενδείξεις κινδύνου, τότε η διαδικασία ISMS επαναλαμβάνεται από

την αρχή. Αυτό επιτρέπει στο ISMS να προσαρμόζεται γρήγορα στις μεταβαλλόμενες συνθήκες και να προσφέρει επί του συνόλου μια αποτελεσματική προσέγγιση για τον μετριασμό των κινδύνων ασφάλειας πληροφοριών για μία επιχείρηση.

Τα σχέδια αντιμετώπισης τέτοιων γεγονότων παρέχουν στις ομάδες ασφαλείας ένα τυποποιημένο σύνολο διαδικασιών για τον μετριασμό των κινδύνων που σχετίζονται με συμβάντα ασφαλείας. Κάνουν τις επιθέσεις στον κυβερνοχώρο λιγότερο ενοχλητικές, μειώνουν το χρόνο διακοπής λειτουργίας και περιέχουν παραβιάσεις δεδομένων.

Δεδομένου ότι κάθε οργανισμός είναι μοναδικός, χρειάζεται να δημιουργήσει ένα σύνολο βιβλίων απόκρισης συμβάντων που έχουν σχεδιαστεί για να ταιριάζουν με το προφίλ κινδύνου ασφαλείας του. Πρέπει επίσης να διασφαλίσει ότι οι εργαζόμενοι, οι χρήστες και οι βασικοί ενδιαφερόμενοι μπορούν να επικοινωνούν αποτελεσματικά σχετικά με συμβάντα ασφαλείας καθώς συμβαίνουν.

3.2 ΠΡΟΤΥΠΟ ISO 27001

Το πρότυπο ISO/IEC 27001:2022 «Ασφάλεια πληροφοριών, κυβερνοασφάλεια και προστασία της ιδιωτικότητας -Συστήματα διαχείρισης ασφάλειας πληροφοριών-Απαιτήσεις» εκδόθηκε το 2022 και αντικατέστησε το ISO/IEC 27001:2013.

Το ISO 27001:2022 αποτελεί ένα πρότυπο για τη διαχείριση ασφάλειας πληροφοριών που καλύπτει τρία κύρια θέματα: πληροφοριακή ασφάλεια, κυβερνοασφάλεια και προστασία της ιδιωτικότητας. Το πρότυπο θεσπίζει απαιτήσεις και οδηγίες για την υλοποίηση, λειτουργία, διατήρηση και βελτίωση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS). Ο στόχος του ISO 27001:2022 είναι να βοηθήσει τις εταιρείες/οργανισμούς να διαχειρίζονται τους κινδύνους που σχετίζονται με τις πληροφορίες τους, προστατεύοντάς τις από απειλές όπως η κακόβουλη πρόσβαση, η διαρροή, η καταστροφή και η απώλεια.

Το ISO 27001:2022 απευθύνεται σε επιχειρήσεις όλων των μεγεθών και τομέων δραστηριότητας, καθώς και σε δημόσιους και ιδιωτικούς οργανισμούς, που επιδιώκουν την ενίσχυση της πληροφοριακής τους ασφάλειας και την προστασία των δεδομένων τους, με έμφαση στην κυβερνοασφάλεια, προκειμένου να αντιμετωπίσουν τους αυξανόμενους κινδύνους που σχετίζονται με την ψηφιακή ασφάλεια και τις κυβερνοεπιθέσεις.

Η εφαρμογή του ISO 27001:2022 πλέον θεωρείται σημαντική και απαραίτητη αρχικά για την **προστασία των δεδομένων** καθότι βοηθάει τις επιχειρήσεις και τους οργανισμούς να προστατεύσουν τις πληροφορίες και τα δεδομένα τους από απειλές όπως η κακόβουλη πρόσβαση, η διαρροή, και η απώλεια. Έπειτα θα πρέπει να υπάρχει **συμμόρφωση με την ισχύουσα νομοθεσία** αφού πολλές χώρες αλλά και κυβερνητικοί φορείς έχουν ως προαπαιτούμενο τη σχετική συμμόρφωση με πρότυπα ασφάλειας όπως είναι το ISO 27001, κυρίως σε επιχειρήσεις που διαχειρίζονται ευαίσθητα δεδομένα(προσωπικά, πελατών, οικονομικά, κλπ.). Επιπλέον με την εφαρμογή του προτύπου επιτυγχάνεται **η ενίσχυση της εμπιστοσύνης** και αυτό γιατί η πιστοποίηση στο ISO 27001 δείχνει στους πελάτες, τους

εταίρους και τους ενδιαφερόμενους ότι η επιχείρηση έχει λάβει σοβαρά μέτρα για την προστασία των δεδομένων τους. Επίσης, η υιοθέτηση και συμμόρφωση ενός προτύπου οδηγεί στην **μείωση των κινδύνων** αφού με την εφαρμογή του ISO 27001, οι οργανισμοί μπορούν να αναγνωρίσουν, να αξιολογήσουν και να μειώσουν τους κινδύνους που αντιμετωπίζουν σχετικά με την ασφάλεια των πληροφοριών. Τέλος, με την εφαρμογή του ISO 27001 επιτυγχάνεται η **βελτίωση των διαδικασιών** καθώς η επιτυχής υλοποίηση του ISO 27001 προάγει τη βελτίωση των διαδικασιών και των πρακτικών διαχείρισης ασφαλείας των πληροφοριών μέσα στην επιχείρηση.

3.2.1 Πλεονεκτήματα από την εφαρμογή του ISO 27001:2022

Η εφαρμογή του ISO 27001:2022 προσφέρει πολλά πλεονεκτήματα για μια επιχείρηση ή οργανισμό. Ανάμεσα στα κύρια πλεονεκτήματα περιλαμβάνονται:

Βελτίωση της Ασφάλειας Πληροφοριών: Το ISO 27001:2022 παρέχει ένα ολοκληρωμένο πλαίσιο για την ανάπτυξη, εφαρμογή και διατήρηση ενός συστήματος διαχείρισης ασφάλειας πληροφοριών (ISMS), το οποίο ενισχύει την αντίληψη και τη διαχείριση τους σε μια επιχείρηση.

Προστασία των Δεδομένων: Μέσω του ISO 27001:2022, οι επιχειρήσεις μπορούν να ενισχύσουν την προστασία των δεδομένων τους, συμπεριλαμβανομένων των προσωπικών και να μειώσουν τους κινδύνους διαρροής ή απώλειας αυτών.

Συμμόρφωση με Νομικές Απαιτήσεις: Η υλοποίηση του ISO 27001:2022 βοηθά τις επιχειρήσεις να επιτύχουν συμμόρφωση με τις νομικές απαιτήσεις περί ασφάλειας πληροφοριών και προστασίας δεδομένων, όπως το GDPR.

Ενίσχυση Εμπιστοσύνης: Η πιστοποίηση στο ISO 27001:2022 δείχνει στους πελάτες, τους εταίρους και τους ενδιαφερόμενους ότι η επιχείρηση λαμβάνει σοβαρά μέτρα για την προστασία των πληροφοριών τους.

Βελτίωση Διαδικασιών: Η υλοποίηση του ISO 27001:2022 προωθεί τη βελτίωση των διαδικασιών και των πρακτικών διαχείρισης ασφάλειας πληροφοριών μέσα στην επιχείρηση, βοηθώντας την να λειτουργεί αποτελεσματικότερα και σε ένα πιο ασφαλές πλαίσιο.

Μείωση Κινδύνων: Με την αναγνώριση και τη διαχείριση των κινδύνων ασφάλειας πληροφοριών, οι επιχειρήσεις μειώνουν τον κίνδυνο παραβιάσεων και πιθανών αρνητικών επιπτώσεων.

Οι τροποποιήσεις που έχει φέρει το ISO 27001:2022 σε σχέση με το ISO 27001:2013 περιλαμβάνουν την αναθεώρηση των απαιτήσεων με βάση τις σύγχρονες απειλές κυβερνοεπιθέσεων, την ενίσχυση της διαχείρισης κινδύνων σε όλα τα επίπεδα, την αύξηση της παρακολούθησης και της βελτίωσης του ISMS, την ενσωμάτωση της προστασίας της ιδιωτικότητας και την ενίσχυση της διαφάνειας και της ευθύνης σε όλα τα επίπεδα. Συγκεκριμένα οι αλλαγές που επιφέρει το νέο πρότυπο είναι οι εξής:

Η κυριότερη αλλαγή που εντοπίζεται μετά την αναθεώρηση είναι στο όνομα του προτύπου, όπου η έκδοση του 2022 έχει τίτλο “Information security, cybersecurity and privacy protection – Information security management systems – Requirements” σε αντίθεση με την έκδοση 2013 που είχε τίτλο “Information technology – Security techniques – Information security management systems – Requirements”.

Επιπλέον αλλαγές υπάρχουν και στα Security Controls που πλέον αριθμούν 93, σε σχέση με τα 114 της προηγούμενης έκδοσης, ενώ τα Sections των Security Controls, του Annex A, είναι πλέον 4, σε σχέση με τα 14 της προηγούμενης έκδοσης:

- People (8 controls)
- Organizational (37 controls)
- Technological (34 controls)
- Physical (14 controls)

Τα Security Controls έχουν πλέον 5 τύπους χαρακτηριστικών “attributes” για να είναι πιο εύκολη η κατηγοριοποίησή τους:

- Control type (preventive, detective, corrective)
- Information security properties (confidentiality, integrity, availability)
- Cybersecurity concepts (identify, protect, detect, respond, recover)
- Operational capabilities (governance, asset management, etc.)
- Security domains (governance and ecosystem, protection, defence, resilience).

3.3 ΠΡΟΤΥΠΟ NIST

3.3.1 Τι ορίζει το NIST

Το Πλαίσιο Κυβερνοασφάλειας με βάση το NIST (CSF) είναι ένα σύνολο κατευθυντήριων γραμμών για τον μετριασμό των οργανωτικών κινδύνων κυβερνοασφάλειας, που δημοσιεύθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των ΗΠΑ (NIST) με βάση τα υφιστάμενα πρότυπα, τις κατευθυντήριες γραμμές και τις πρακτικές.

Το συγκεκριμένο πλαίσιο «παρέχει μια υψηλού επιπέδου ταξινόμηση των αποτελεσμάτων της ασφάλειας στον κυβερνοχώρο και μια μεθοδολογία για την αξιολόγηση και τη διαχείριση αυτών των αποτελεσμάτων», καθώς και οδηγίες για την προστασία της ιδιωτικής ζωής και των πολιτικών ελευθεριών στο πλαίσιο της ασφάλειας στον κυβερνοχώρο. Έχει μεταφραστεί σε πολλές γλώσσες και χρησιμοποιείται από αρκετές κυβερνήσεις και ένα ευρύ φάσμα επιχειρήσεων και οργανισμών.

Μελέτη που εκπονήθηκε το 2016 διαπίστωσε ότι το 70% των οργανισμών που συμμετείχαν στην έρευνα θεωρούν το Πλαίσιο Κυβερνοασφάλειας NIST ως μια από τις πιο βέλτιστες πρακτικές για την ασφάλεια των υπολογιστών.

Σύμφωνα με τον NIST [National Institute of Standards and Technology] διακρίνει πέντε βασικές

λειτουργίες του πλαισίου της Κυβερνοασφάλειας, οι οποίες βοηθούν τους οργανισμούς να διαχειριστούν τους κινδύνους κυβερνοασφάλειας σε υψηλό επίπεδο. Οι πέντε βασικές λειτουργίες είναι οι παρακάτω:

1. **Identify** [*Προσδιορισμός*]: Η λειτουργία του προσδιορισμού εξυπηρετεί στην ανάπτυξη οργανωτικής κατανόησης της διαχείρισης των κινδύνων κυβερνοασφάλειας για τα συστήματα, τους υπαλλήλους, τα περιουσιακά στοιχεία, τα δεδομένα και τις ικανότητες.
2. **Protect** [*Προστασία*]: Η λειτουργία της Προστασίας υποστηρίζει την ικανότητα περιορισμού ή ανάσχεσης των επιπτώσεων πιθανών συμβάντων κυβερνοασφάλειας και περιγράφει τις διασφαλίσεις για την παροχή κρίσιμων υπηρεσιών.
3. **Detect** {*Ανίχνευση*]: Η λειτουργία της Ανίχνευσης καθορίζει τις κατάλληλες δραστηριότητες για τον έγκαιρο εντοπισμό ενός συμβάντος κυβερνοασφάλειας.
4. **Respond** [*Ανταπόκριση*]: Η λειτουργία της Απόκρισης περιλαμβάνει τις κατάλληλες δραστηριότητες για την ανάληψη δράσης σχετικά με ένα εντοπισμένο συμβάν κυβερνοασφάλειας για την ελαχιστοποίηση των επιπτώσεων.
5. **Recover** [*Ανάκτηση*]: Η λειτουργία της Ανάκαμψης προσδιορίζει τις κατάλληλες δραστηριότητες για τη διατήρηση των σχεδίων ανθεκτικότητας και την αποκατάσταση των υπηρεσιών που έχουν υποστεί βλάβη κατά τη διάρκεια περιστατικών κυβερνοασφάλειας.

3.4 ΠΡΟΤΥΠΟ SANS

3.4.1 Τι είναι το Πλαίσιο απόκρισης συμβάντων SANS;

Το SANS Institute είναι ο μεγαλύτερος και πιο αξιόπιστος οργανισμός έρευνας και εκπαίδευσης στον τομέα της κυβερνοασφάλειας. Το όνομά του σημαίνει "SysAdmin, Audit, Network, and Security" και το πλαίσιο απόκρισης συμβάντων είναι μια από τις πιο αξιόπιστες επιλογές στον κλάδο.

Το 2012, το Ινστιτούτο SANS δημοσίευσε το Εγχειρίδιο χειριστή συμβάντων, το οποίο καθορίζει την προσέγγισή του για την αντιμετώπιση περιστατικών ασφαλείας σε πραγματικό χρόνο. Η προσέγγιση SANS δίνει τη δυνατότητα στους αναλυτές να αξιολογούν μεθοδικά τη ζημιά από κυβερνοεπιθέσεις, να λαμβάνουν μέτρα για τον περιορισμό των απειλών και να βοηθούν τον οργανισμό να ανακάμψει.

Ακολουθεί μια σύντομη περίληψη της προσέγγισης των έξι βημάτων που περιγράφεται στο Πλαίσιο Αντίδρασης Συμβάντος SANS:

• **Προετοιμασία [Preparation]**. Καθιέρωση πολιτικών ασφαλείας σε ολόκληρο τον οργανισμό, πραγματοποίηση αξιολογήσεις κινδύνου και σαφής ορισμός των κινδύνων ασφαλείας. Επίσης, προτείνεται η δημιουργία μιας Ομάδας Αντιμετώπισης Συμβάντων Ασφάλειας Υπολογιστών (CSIRT) με καλά καθορισμένους ρόλους.

• **Ταυτοποίηση [Identification]**. Θα πρέπει να γίνεται παρακολούθηση των συστημάτων για τυχόν ασυνήθιστη συμπεριφορά καθώς και ενδείξεων παραβίασης. Να γίνεται η απαραίτητη διερεύνηση των συμβάντων ασφαλείας και η απομόνωση αυτών που υποδηλώνουν πιθανή παραβίαση της ασφάλειας. Κρίνεται αναγκαία η συλλογή στοιχείων, η κατηγοριοποίηση των απειλών και η τεκμηρίωση αυτών.

• **Περιορισμός [Containment]**. Θα πρέπει να δρομολογηθεί αποφασιστική, βραχυπρόθεσμη δράση για την απομόνωση πιθανών απειλών και την προστασία του δικτύου από επιθέσεις. Στη συνέχεια, θα πρέπει να εκτελεστούν μακροπρόθεσμες εργασίες περιορισμού και ανασυγκρότηση των επηρεασμένων συστημάτων.

• **Εξάλειψη [Eradication]**. Κατάργηση του κακόβουλο λογισμικό από τα επηρεαζόμενα συστήματα, ανάλυση της βασικής αιτίας επίθεσης και την εφαρμογή λύσεων για την αποτροπή παρόμοιων επιθέσεων στο μέλλον.

• **Ανάκτηση [Recovery]**. Επαναφορά σε λειτουργία των επηρεαζόμενων συστημάτων παραγωγής, προβλέποντας τον μετριασμό του κινδύνου για πρόσθετες επιθέσεις. Σκόπιμο κρίνεται η δοκιμή και επαλήθευση των πρόσφατα ανακτημένων συστημάτων για να διασφαλιστεί η σωστή λειτουργία.

• **Διδάγματα [Lessons Learned]**. Σύνταξη αναδρομικής αναφοράς που θα περιγράφει λεπτομερώς το περιστατικό ασφαλείας όχι περισσότερο από δύο εβδομάδες μετά την πραγματοποίησή του. Η αναφορά θα πρέπει να τεκμηριωθεί πλήρως καθώς και ο εντοπισμός των όποιων ευκαιριών για την βελτίωση της επιχειρησιακής ασφάλειας.

3.5 Η ΔΙΑΦΟΡΑ ΜΕΤΑΞΥ ΤΟΥ SANS ΚΑΙ ΤΟΥ NIST

Το Πλαίσιο αντιμετώπισης περιστατικών SANS Incident Response Framework συγκρίνεται συχνά με το άλλο κορυφαίο πλαίσιο για την αντιμετώπιση των κινδύνων περιστατικών ασφαλείας - το Πλαίσιο Κυβερνοασφάλειας NIST.

Τα δύο αυτά πλαίσια έχουν πολλά κοινά σημεία, αλλά και βασικές διαφορές. Σε γενικές γραμμές, το Πλαίσιο αντιμετώπισης περιστατικών SANS είναι πιο τεχνικά προσανατολισμένο, με αυστηρή εστίαση στον εντοπισμό και την αντιμετώπιση ύποπτης συμπεριφοράς σε προστατευόμενα δίκτυα.

Το Πλαίσιο Κυβερνοασφάλειας NIST παρέχει μια εμπεριστατωμένη εξήγηση των δομών επικοινωνίας που πρέπει να διαθέτουν οι οργανισμοί κατά τον χειρισμό περιστατικών ασφαλείας. Από την άλλη το πλαίσιο SANS παρέχει μια ευρύτερη επισκόπηση αυτής της πτυχής της αντιμετώπισης περιστατικών, όπως επίσης και βαθύτερη καθοδήγηση σχετικά με τον τρόπο με τον οποίο τα μέλη της ομάδας ασφαλείας θα πρέπει να περιορίζουν και να εξαλείφουν τις απειλές.

Αυτό δεν σημαίνει ότι το ένα πλαίσιο είναι «καλύτερο» από το άλλο. Απλώς αντικατοπτρίζει το πεδίο εφαρμογής για το οποίο σχεδιάστηκε το κάθε πλαίσιο. Οι υπεύθυνοι ασφαλείας πρέπει να επιλέξουν το πλαίσιο που ταιριάζει καλύτερα στις συγκεκριμένες ανάγκες μιας επιχείρησης καθώς και στις δυνατότητες ασφαλείας της.

Δεδομένου ότι το πλαίσιο SANS προσφέρει μία πιο συνοπτική επιχειρησιακή καθοδήγηση για την αντιμετώπιση περιστατικών ασφάλειας, θα λέγαμε πως είναι καταλληλότερο για οργανισμούς με καλά αναπτυγμένες δυνατότητες ασφάλειας.

Επίσης είναι ιδιαίτερα κατάλληλο για μικρότερους, πιο ευέλικτους οργανισμούς με εξειδικευμένες ομάδες ασφάλειας. Αυτό οφείλεται στο γεγονός ότι το πλαίσιο που ορίζει το NIST περιλαμβάνει μια πιο γενική προσέγγιση για τη διασφάλιση των δεδομένων έναντι ενός ευρύτερου φάσματος περιστατικών, όπως φυσικές καταστροφές και παραβιάσεις της φυσικής ασφάλειας. Έτσι, ενώ το Πλαίσιο NIST παρέχει ευρεία καθοδήγηση κατάλληλη για μεγάλους, πολύπλοκους οργανισμούς, το Πλαίσιο αντιμετώπισης περιστατικών της SANS επικεντρώνεται στη βελτίωση των δυνατοτήτων των μεμονωμένων επαγγελματιών ασφαλείας και των ομάδων τους.

Πέρα όμως από τα δύο αυτά πλαίσια αντιμετώπισης υπάρχουν και οι κανονιστικές αρχές που θέτουν συγκεκριμένες οδηγίες για το πως πρέπει μία επίχειρηση να αντιμετώπιση ένα συμβάν κυβερνοεπίθεσης, όπως είναι το NIS2 καθώς και οι οδηγίες που απορρέουν από τον ευρωπαϊκό οργανισμό για την κυβερνοασφάλεια, ENISA.

Τα τελευταία χρόνια η Ευρωπαϊκή Ένωση βρίσκεται σε μια συνεχιζόμενη διαδικασία και έχοντας ως γνώμονα την επίτευξη της ανθεκτικότητας ενάντια σε ολοένα και μεγαλύτερες κυβερνοαπειλές, καθώς και τη διατήρηση της ασφάλειας και της προστασίας της ψηφιακής κοινωνίας και οικονομίας λαμβάνει συνεχώς νέες πρωτοβουλίες.

Μία από τις πρωτοβουλίες αυτές είναι η ίδρυση και η θέσπιση του ENISA, που ιδρύθηκε το 2004. Συμβάλλει στη χάραξη της πολιτικής της ΕΕ στον τομέα του κυβερνοχώρου, ενισχύει την αξιοπιστία των προϊόντων, υπηρεσιών και διαδικασιών με συστήματα πιστοποίησης της κυβερνοασφάλειας, συνεργάζεται με κράτη μέλη και φορείς της ΕΕ και βοηθά την Ευρώπη να προετοιμαστεί για τις μελλοντικές προκλήσεις στον κυβερνοχώρο. Μέσω της ανταλλαγής γνώσεων, της ανάπτυξης ικανοτήτων και της αύξησης της εγρήγορσης, ο Οργανισμός συνεργάζεται με τους βασικούς συμφεροντούχους για να αυξήσει την εμπιστοσύνη στη συνδεδεμένη οικονομία, να ενισχύσει την ανθεκτικότητα των υποδομών της Ένωσης και, να διατηρήσει, τελικά, την ψηφιακή ασφάλεια για την κοινωνία και τους πολίτες της Ευρώπης.

Για τους παραπάνω λόγους παρουσιάζεται κάθε χρόνο η έκθεση ENISA Threat Landscape (ETL) που βρίσκεται τώρα στην ενδέκατη έκδοσή της και διαδραματίζει κρίσιμο ρόλο στην κατανόηση της τρέχουσας κατάστασης της κυβερνοασφάλειας κυρίως εντός της Ευρωπαϊκής Ένωσης (ΕΕ). Στην έκθεση παρέχονται πολύτιμες πληροφορίες για τις αναδυόμενες τάσεις όσον αφορά τις απειλές για την ασφάλεια στον κυβερνοχώρο, τις δραστηριότητες των παραγόντων απειλών, καθώς και τις ευπάθειες και τα συμβάντα στον κυβερνοχώρο.

Παράλληλα, η έκθεση στοχεύει στην ενημέρωση αποφάσεων, προτεραιοτήτων και συστάσεων στον τομέα της κυβερνοασφάλειας. Προσδιορίζει τις κορυφαίες απειλές και τις ιδιαιτερότητές τους, τα κίνητρα των παραγόντων απειλών και τις τεχνικές επίθεσης, καθώς και παρέχει μια βαθιά εικόνα για συγκεκριμένους τομείς μαζί με μια σχετική ανάλυση επιπτώσεων. Η εργασία υποστηρίχθηκε από την ad hoc ομάδα εργασίας του ENISA για τα τοπία απειλών στον κυβερνοχώρο (CTL).

Στο δεύτερο μέρος του 2022 και το πρώτο εξάμηνο του 2023, το τοπίο της κυβερνοασφάλειας σημείωσε σημαντική αύξηση τόσο στην ποικιλία όσο και στην ποσότητα των κυβερνοεπιθέσεων και στις συνέπειές τους. Ο συνεχιζόμενος επιθετικός πόλεμος κατά της Ουκρανίας συνέχισε να επηρεάζει το τοπίο. Ο χακτιβισμός επεκτάθηκε με την εμφάνιση νέων ομάδων, ενώ

Τα περιστατικά ransomware αυξήθηκαν το πρώτο εξάμηνο του 2023 και δεν έδειξαν σημάδια επιβράδυνσης. Οι κύριες απειλές που εντοπίστηκαν και αναλύθηκαν περιλαμβάνουν:

- Ransomware
- Malware
- Social engineering
- Threats against data
- Threats against availability: Denial of Service
- Threat against availability: Internet threats
- Information manipulation and interference

- Supply chain attacks

Μέσα σε αυτήν την έκθεση η ENISA προχωράει και στην κατηγοριοποίηση των παραγόντων απειλής για την ασφάλεια στον κυβερνοχώρο, οι οποίες είναι οι ακόλουθε:

1. State-nexus threat groups,
2. Cybercriminals,
3. Hackers-for-hire,
4. Hacktivists.

Επιπλέον πρωτοβουλία της Ευρωπαϊκής Ένωσης, έχοντας και μεγαλύτερη βαρύτητα καθώς από οδηγία που είναι μέχρι τώρα, το 2025 θα γίνει κανόνας για κάθε μέλος είναι το NIS2.

Η οδηγία NIS2 θέτει τις βάσεις για τον πλήρη καθορισμό όλων εκείνων των μέτρων διαχείρισης κινδύνων κυβερνοασφάλειας και υποχρεώσεων αναφοράς περιστατικών σε όλους τους τομείς τους οποίους καλύπτει, όπως η ενέργεια, οι μεταφορές, η υγεία και οι ψηφιακές υποδομές, που αποτελούν τους κύριους πυλώνες μιας χώρας.

Η αναθεωρημένη οδηγία αποσκοπεί στην εξάλειψη των αποκλίσεων στις απαιτήσεις κυβερνοασφάλειας και στην εφαρμογή μέτρων κυβερνοασφάλειας στα διάφορα κράτη μέλη. Με βάση την παραπάνω παραδοχή, θέτει και καθορίζει ελάχιστους κανόνες με στόχο ένα κανονιστικό πλαίσιο και τους μηχανισμούς εκείνους που θα επιτρέψουν την αποτελεσματική συνεργασία μεταξύ των αρμόδιων αρχών σε κάθε κράτος μέλος. Επικαιροποιεί τον κατάλογο τομέων και δραστηριοτήτων που υπόκεινται σε υποχρεώσεις στον τομέα της κυβερνοασφάλειας, ενώ παράλληλα προβλέπει λύσεις και κυρώσεις για να διασφαλίζεται η τήρησή τους.

Με βάσει την οδηγία αυτή θεσπίζεται επίσημα το ευρωπαϊκό δίκτυο οργανισμών διασύνδεσης για τις κρίσεις στον κυβερνοχώρο, το EU-CyCLONe, το οποίο θα στηρίζει τη συντονισμένη διαχείριση περιστατικών κυβερνοασφάλειας μεγάλης κλίμακας.

Ενώ, σύμφωνα με την παλιά οδηγία NIS, τα κράτη μέλη ήταν υπεύθυνα για τον προσδιορισμό των οντοτήτων που πληρούν τα κριτήρια για να χαρακτηριστούν φορείς εκμετάλλευσης βασικών υπηρεσιών, με τη νέα οδηγία εισάγεται κανόνας ορίου μεγέθους. Αυτό σημαίνει ότι όλες οι μεσαίες και μεγάλες οντότητες που δραστηριοποιούνται σε τομείς ή παρέχουν υπηρεσίες που καλύπτονται από την οδηγία θα εμπίπτουν στο πεδίο εφαρμογής της.

Στο NIS2 διευκρινίζεται επίσης ότι δεν θα ισχύει για οντότητες που ασκούν δραστηριότητες σε τομείς όπως η άμυνα ή η εθνική ασφάλεια, η δημόσια ασφάλεια, η επιβολή του νόμου και η δικαιοσύνη, όπως επιπλέον τόσο τα κοινοβούλια όσο και οι κεντρικές τράπεζες εξαιρούνται από το πεδίο εφαρμογής.

Τέλος, βελτιστοποίησε επίσης τις υποχρεώσεις αναφοράς περιστατικών προκειμένου να αποφεύγεται η υπερβολική αναφορά και επιβάρυνση των οντοτήτων που καλύπτονται από την οδηγία.

ΚΕΦΑΛΑΙΟ 4: ΤΡΟΠΟΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΜΙΑΣ ΕΠΙΘΕΣΗΣ RANSOMWARE

Οι επιθέσεις τύπου ransomware μπορούν να να μειώσουν ή να σταματήσουν εντελώς τις λειτουργίες μιας επιχείρησης, οδηγώντας σε σημαντικές οικονομικές απώλειες και ζημιά στη φήμη. Η πρόληψη και η αποτελεσματική απόκριση σε επιθέσεις τύπου ransomware απαιτεί μια πολύπλευρη προσέγγιση που περιλαμβάνει προληπτικά μέτρα, εκπαίδευση εργαζομένων και ισχυρές στρατηγικές αντιμετώπισης περιστατικών. Παρακάτω αποτυπώνεται ως ενα βαθμό μια ολοκληρωμένης διαδικασίας που εμβαθύνει στις βέλτιστες πρακτικές για την πρόληψη επιθέσεων ransomware.

4.1 ΣΤΡΑΤΗΓΙΚΕΣ ΠΡΟΛΗΨΗΣ

4.1.1 Τακτικά αντίγραφα ασφάλειας δεδομένων και η σημασία τους

Η συχνή δημιουργία αντιγράφων ασφαλείας δεδομένων αποτελεί πιθανότατα έναν από τους πιο αποτελεσματικούς τρόπους ώστε να μετριαστεί ο αντίκτυπος μιας επίθεσης ransomware. Εάν τα δεδομένα μιας επιχείρησης δημιουργηθούν με ασφάλεια, μπορεί να επαναφέρει τα επηρεαζόμενα συστήματα χωρίς να υποχρεώνει την επιχείρηση να πληρώσει τα λύτρα.

4.1.2 Βέλτιστες πρακτικές για αντίγραφα ασφαλείας

- **Αυτοματοποιημένα αντίγραφα ασφαλείας**: Ο προγραμματισμός για αυτοματοποιημένα αντίγραφα ασφαλείας έχεις ως άμεσο στόχο την διασφάλιση ότι τα δεδομένα αποθηκεύονται με συνέπεια, με τον σωστό τρόπο και στον κατάλληλο χρόνο χωρίς να διακινδυνεύεται η αποθήκευση των αρχείων αν οι διαδικασίες ήταν με μη αυτόματες διαδικασίες.
- **Αποθήκευση εκτός τοποθεσίας**: Αποθήκευση αντιγράφων ασφαλείας σε ξεχωριστή τοποθεσία, κατά προτίμηση εκτός σύνδεσης ή σε ασφαλές περιβάλλον cloud, για την επαρκή προστασία τους από ransomware που μπορεί να εξαπλωθεί μέσω των συνδέσεων δικτύου.
- **Δοκιμαστικές αποκαταστάσεις**: Απαιτείται συχνός έλεγχος όλων των διαδικασιών και βημάτων για την αποκατάσταση των αντιγράφων ασφαλείας για την διασφάλιση της ακεραιότητας των δεδομένων και την αξιοπιστία των συστημάτων δημιουργίας αντιγράφων ασφαλείας.

4.2 ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΕΡΓΑΖΟΜΕΝΩΝ

4.2.1 Phishing και Social Engineering

Οι εργαζόμενοι αποτελούν συχνά την πρώτη γραμμή άμυνας ενάντια σε μία ενδεχόμενη επίθεση ransomware. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν τα μηνύματα ηλεκτρονικού ψαρέματος και τακτικές social engineering για να εξαπατήσουν τους υπαλλήλους να κατεβάσουν κακόβουλα συνημμένα ή να κάνουν κλικ σε επιβλαβείς συνδέσμους.

4.2.2 Προγράμματα εκπαίδευσης

- **Τακτικές εκπαιδευτικές συνεδρίες:** Διενέργεια τακτικών εκπαιδεύσεων στον κυβερνοχώρο με στόχο την ενημέρωση και παράλληλα την εκπαίδευση των υπαλλήλων σχετικά με τις πιο πρόσφατες τακτικές phishing και πώς να αναγνωρίζουν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου και συνδέσμους.
- **Προσομοίωση επιθέσεων ηλεκτρονικού "ψαρέματος"**: Να πραγματοποιούνται σε τακτικό χρονικό διάστημα ασκήσεις προσομοίωσης ηλεκτρονικού "ψαρέματος" για να ελεγχθεί ο βαθμός ευαισθητοποίησης και απόκρισης των εργαζομένων σε πιθανές απειλές.
- **Εκκαθάριση καναλιών αναφοράς**: Να υιοθετηθούν σαφείς διαδικασίες για τους υπαλλήλους ώστε να είναι σε θέση να αναφέρουν έγκαιρα ύποπτες δραστηριότητες.

4.3 ΠΡΟΣΤΑΣΙΑ ΤΕΛΙΚΟΥ ΣΗΜΕΙΟΥ [ENDPOINT DETECTION & RESPONSE]

4.3.1 Λογισμικό προστασίας από ιούς και κακόβουλο λογισμικό

Είναι προς όφελος της εταιρείας η ανάπτυξη ολοκληρωμένων λύσεων προστασίας από ιούς και κακόβουλο λογισμικό τόσο για τον εντοπισμό όσο και για τον αποκλεισμό κακόβουλου λογισμικού προτού μολύνει και κατά συνέπεια επεκταθεί στο σύστημα της επιχείρησης.

4.3.2 Εντοπισμός και απόκριση τελικού σημείου (EDR)

Προτείνεται η εφαρμογή λύσεων EDR για να έχει η επιχείρηση την δυνατότητα πλήρους και συνεχούς παρακολούθησης και απόκρισης για συσκευές τελικού σημείου(υπολογιστές, σέρβερς,κλπ) επιτρέποντας τον γρήγορο εντοπισμό και την αποκατάσταση των απειλών.

4.4 ΤΜΗΜΑΤΟΠΟΙΗΣΗ ΔΙΚΤΥΟΥ

4.4.1 Περιορισμός της εξάπλωσης του Ransomware

Η τμηματοποίηση ενός δικτύου μιας επιχείρησης είναι η διαδικασία της διαίρεσης ενός δικτύου σε μικρότερα τμήματα, το καθένα με τα δικά του στοιχεία ελέγχου ασφαλείας. Αυτή η πρακτική περιορίζει σε ένα μεγάλο ποσοστό την εξάπλωση μιας επίθεσης τύπου ransomware, καθώς οι εισβολείς δυσκολεύονται να μετακινηθούν πλευρικά μέσα σε ένα πιο πολύπλοκο δίκτυο.

4.4.2 Βέλτιστες πρακτικές για τμηματοποίηση δικτύου

- **Διαχωρισμός κρίσιμων συστημάτων:** Κρίνεται αναγκαίο και ήσσονος σημασίας ο διαχωρισμός των πιο κρίσιμων συστημάτων καθώς και των ευαίσθητων δεδομένων από λιγότερο ασφαλή μέρη του δικτύου.
- **Στοιχεία ελέγχου πρόσβασης**: Εφαρμογή αυστηρών ελέγχων πρόσβασης με στόχο την διασφάλιση ότι μόνο εξουσιοδοτημένο προσωπικό μπορεί να έχει πρόσβαση σε συγκεκριμένα τμήματα του δικτύου.
- **Τακτικοί έλεγχοι**: Θα πρέπει να διενεργούνται τακτικοί έλεγχοι του δικτύου ώστε να διασφαλιστεί ότι οι πολιτικές τμηματοποίησης του δικτύου εφαρμόζονται στο ακέραιο και παραμένουν αποτελεσματικές.

4.5 ΕΠΙΔΙΟΡΘΩΣΕΙΣ ΚΑΙ ΕΝΗΜΕΡΩΣΕΙΣ

4.5.1 Τρωτά σημεία λογισμικού

Μια επίθεση τύπου Ransomware εκμεταλλεύεται ως επί των πλείστων γνωστές ευπάθειες τόσο σε λογισμικό όσο και σε λειτουργικά συστήματα. Για το λόγο αυτό η ενημέρωση του λογισμικού θεωρείται ζωτικής σημασίας για την πρόληψη τέτοιων επιθέσεων.

4.5.2 Διαχείριση ενημερώσεων κώδικα

- **Αυτόματη ανάπτυξη ενημερωμένης έκδοσης κώδικα**: Είναι σκόπιμο να χρησιμοποιείτε αυτοματοποιημένα εργαλεία για την άμεση ενημέρωση κώδικα και όλων εκείνων των ενημερώσεων που απαιτούνται σε όλα τα συστήματα.
- **Δώστε προτεραιότητα στις κρίσιμες ενημερώσεις**: Να δίνεται η πρέπουσα σημασία στην επιδιόρθωση των κρίσιμων τρωτών σημείων που ενέχουν τον υψηλότερο κίνδυνο μόλυνσης από μία επίθεση.
- **Ειδοποιήσεις προμηθευτών**: Ενεργοποίηση όλων των σχετικών ειδοποιήσεων από τους προμηθευτές του λογισμικού, ώστε αυτό να ενημερώνετε με τις πιο πρόσφατες ενημερώσεις κώδικα και λειτουργικότητας.

4.6 ΣΤΟΙΧΕΙΑ ΕΛΕΓΧΟΥ ΠΡΟΣΒΑΣΗΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΝΟΜΙΩΝ

4.6.1 Περιορισμός πρόσβασης

Ο περιορισμός της πρόσβασης σε ευαίσθητα δεδομένα και συστήματα είναι ζωτικής σημασίας για την ελαχιστοποίηση μιας πιθανής ζημιάς από μια επίθεση ransomware.

4.6.2 Αρχή του ελάχιστου προνομίου (PoLP)

- **Ορισμός ρόλου χρήστη**: Θα πρέπει να υπάρχει ξεκάθαρος καθορισμός των ρόλων των χρηστών και να υπάρχει η βεβαιότητα ότι τα άτομα έχουν το ελάχιστο επίπεδο πρόσβασης που απαιτείται στις σχετικές λειτουργίες για την εκπλήρωση της εργασίας τους.
- **Αξιολογήσεις Τακτικής Πρόσβασης**: Προς όφελος της επιχείρησης είναι και οι τακτικές αναθεωρήσεις/αλλαγές των επιπέδων πρόσβασης των χρηστών καθώς και η ανάλογη προσαρμογή των δικαιωμάτων όπου αυτή απαιτείται.
- **Επαλήθευση πολλαπλών παραγόντων (MFA):** Επιβάλλεται η υιοθέτηση και εφαρμογή MFA(multi factor authenticator) ώστε να υπάρχει ένα επιπλέον επίπεδο ασφάλειας της επιχείρησης σε πρόσβαση κρίσιμων συστημάτων της.

4.7 ΑΣΦΑΛΕΙΑ EMAIL

4.7.1 Φιλτράρισμα κακόβουλου περιεχομένου

Το email αποτελεί πιθανότοτα το ιδανικότερο περιβάλλον για μια ransomware επίθεση. Για το λόγο αυτό κρίνεται αναγκαίο η σχετική ενίσχυση της ασφάλειας email όπου μπορεί να μειώσει σημαντικά τον κίνδυνο.

4.7.2 Μέτρα ασφαλείας email

- **Φίλτρα ανεπιθύμητων μηνυμάτων**: Εφαρμογή σχετικών φίλτρων ανεπιθύμητης αλληλογραφίας για τον εντοπισμό και τον αποκλεισμό είτε μηνυμάτων ηλεκτρονικού ψαρέματος και είτε μηνυμάτων με συνημμένα κακόβουλα αρχεία, έγγραφα ή εικόνες.
- **Σάρωση συνημμένων**: Θα πρέπει να σαρώνονται συνημμένα email για κακόβουλο λογισμικό πριν φτάσουν στα εισερχόμενα.
- **Φιλτράρισμα URL**: Εφαρμογή σχετικού φίλτρου διευθύνσεων URL για τον αποκλεισμό πρόσβασης σε γνωστούς κακόβουλους ιστότοπους που συνδέονται σε μηνύματα ηλεκτρονικού ταχυδρομείου.

ΚΕΦΑΛΑΙΟ 5: ΕΠΑΝΟΔΟΣ & ΕΠΑΝΑΦΟΡΑ ΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑΣ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ

Η μακροπρόθεσμη βιωσιμότητα μίας επιχείρησης εξαρτάται από τον τρόπο με τον οποίο θα ανακάμψει μετά από μία επίθεση ransomware. Εάν έχει υιοθετήσει ένα σχέδιο ανάκτησης τότε είναι πολύ πιθανόν να συνεχίσει γρήγορα την λειτουργία της.

Στο σχέδιο ανάκτησης θα πρέπει να ορίζονται τα όποια τεχνολογικά εργαλεία που προσφέρουν την απαραίτητη ασφάλεια, όπως είναι η ασφάλεια τελικού σημείου, η ασφάλεια email, τα τείχη προστασίας καθώς και η εκπαίδευση των χρηστών με θέματα που αφορούν την κυβεροασφάλεια τότε έχει κάνει ένα σημαντικό βήμα να μειώσει τον κίνδυνο ενός ransomware. Ωστόσο, εάν το ransomware μολύνει το σύστημα ενός οργανισμού, η ομάδα ασφαλείας θα πρέπει να αναπτύξει αμέσως ένα σχέδιο ανάκτησης ransomware.

Το σχέδιο ανάκτησης ransomware θα πρέπει να περιλαμβάνει τον τρόπο με τον οποίο ο οργανισμός προετοιμάζεται για επιθέσεις, πώς να χειριστεί μια επίθεση σε εξέλιξη και τι πρέπει να κάνει στη συνέχεια. Αυτά είναι τα βασικά βήματα προς αυτήν την κατεύθυνση και τα οποία αναλύονται παρακάτω: **i**. *δημιουργία αντιγράφων ασφαλείας δεδομένων σε τακτά χρονικά διαστήματα,* **ii**. *η προετοιμασία και η ανάπτυξη ενός σχεδίου απόκρισης συμβάντων ransomware,* **iii**. *η χρήση και η εγκατάσταση συστημάτων (π.χ firewall) ώστε να αποτραπεί μία επίθεση,* **iv**. *η το δυνατόν ταχύτερη επαναφορά των επηρεαζόμενων συστημάτων σε κανονική λειτουργία,* **v**. *η άμεση επικοινωνία με τα ενδιαφερόμενα μέρη(φορείς, συνεργάτες, ρυθμιστικές αρχές, προμηθευτές, κλπ)* και **vi**. *συνεχής βελτίωση του εν λόγω σχεδίου ανάκτησης που έχει υιοθέτηση η επιχείρηση*.

5.1 ΔΗΜΙΟΥΡΓΙΑ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ

Η επιχείρηση θα πρέπει να δημιουργεί αντίγραφα ασφαλείας όλων των κρίσιμων για την επιχείρηση δεδομένων όσο το δυνατόν συχνότερα για να μειώσει την όποια μικρή ή μεγάλη απώλεια δεδομένων της. Τα αντίγραφα ασφαλείας δεδομένων θεωρούνται αναγκαία για να ανακτήσει η επιχείρηση τα δεδομένα της μετά από επίθεση ransomware. Επιπλέον, χρήσιμο για τη σωστή διαδικασία δημιουργίας αντιγράφων ασφαλείας αποτελούν οι τακτικές δοκιμές ότι τα αντίγραφα ασφαλείας δημιουργούνται και αποθηκεύονται με τον σωστό τρόπο και ότι η επαναφορά από τα αντίγραφα αυτά λειτουργεί απρόσκοπτα. Για να διασφαλιστεί ότι τα αντίγραφα ασφαλείας δεδομένων παραμένουν ασφαλή, η επιχείρηση θα πρέπει να έχει μεριμνήσει ότι υπάρχουν οι σχετικές δυνατότητες για την προστασία των δεδομένων.

Προς τη σωστή κατεύθυνση θα ήταν το ενδεχόμενο η επιχείρηση να αποθηκεύει τουλάχιστον ένα αντίγραφο ασφαλείας δεδομένων σε μέρος που δεν συνδέεται με το διαδίκτυο όπως ένας εξωτερικός σκληρός δίσκος ο οποίος θα φυλάσσεται σε θυρίδα.

Όπως αναφέρθηκε, η ανάκτηση δεδομένων πραγματοποιείται καλύτερα μέσω αντιγράφων ασφαλείας. Ωστόσο, υπάρχουν και άλλοι τρόποι για να επαναφέρετε τα κρυπτογραφημένα δεδομένα σας:

- Εργαλεία λειτουργικού συστήματος [Operating system tools]:

Ορισμένα λειτουργικά συστήματα, όπως τα Windows 10, διαθέτουν ενσωματωμένα εργαλεία ανάκτησης δεδομένων. Το βοηθητικό πρόγραμμα επαναφοράς συστήματος των Windows μπορεί μερικές φορές να επαναφέρει τις ρυθμίσεις σε ένα σημείο ανάκτησης που έχει δημιουργηθεί προηγουμένως. Ωστόσο, ένα ransomware έχει τη δυνατότητα να τα θέσει εκτός λειτουργίας καθώς και να καταστρέψει τέτοιες εφαρμογές.

- Λογισμικό ανάκτησης δεδομένων[Data recovery software]:

Υπάρχουν διάφορα εργαλεία τόσο για την εξαγωγή κατεστραμμένων δεδομένων από συσκευές αποθήκευσης όσο και για την αποκατάσταση των επηρεαζόμενων αρχείων. Η αποτελεσματικότητα του λογισμικού εξαρτάται από τον τύπο του ransomware που επηρεάζει το σύστημά το οποίο δέχθηκε την επίθεση. Εάν πρόκειται για ένα νέο ransomware, είναι πολύ πιθανό το λογισμικό να μην είναι αποτελεσματικό.

- Εργαλεία αποκρυπτογράφησης [Decryption tools]:

Ανάλογα με την παραλλαγή του ransomware, οι χάκερς ενδέχεται να έχουν ήδη σπάσει τον αλγόριθμο κρυπτογράφησης. Τα εργαλεία αποκρυπτογράφησης χρησιμοποιούν αλγόριθμους για να λύσουν την κρυπτογράφηση και να ξεκλειδώσουν τα δεδομένα που έχουν κλαπεί.

5.2 ΠΡΟΕΤΟΙΜΑΣΙΑ ΚΑΙ Η ΑΝΑΠΤΥΞΗ ΕΝΟΣ ΣΧΕΔΙΟΥ ΑΠΟΚΡΙΣΗΣ ΣΥΜΒΑΝΤΩΝ RANSOMWARE

Η επιχείρηση θα πρέπει να έχει ένα σχέδιο αντιμετώπισης περιστατικών (IRP-Incident Response Plan) για να γνωρίζει πως πρέπει να αντιδράσει σε περίπτωση περιστατικού ασφάλειας στον κυβερνοχώρο. Ορισμένες επιχειρήσεις αναπτύσσουν ένα σχέδιο απόκρισης συμβάντων το οποίο προορίζεται αποκλειστικά για την αντιμετώπιση ενός ransomware.

Το σχέδιο αντιμετώπισης περιστατικών είναι ένα σύνολο γραπτών οδηγιών που περιγράφουν την αντίδραση του οργανισμού σας σε παραβιάσεις δεδομένων, διαρροές δεδομένων, επιθέσεις στον κυβερνοχώρο και περιστατικά ασφαλείας.

Ο σχεδιασμός αντιμετώπισης περιστατικών περιέχει συγκεκριμένες οδηγίες για συγκεκριμένα σενάρια επιθέσεων, αποφυγή περαιτέρω ζημιών, μείωση του χρόνου αποκατάστασης και μετριασμό του κινδύνου κυβερνοασφάλειας.

Οι διαδικασίες αντιμετώπισης περιστατικών επικεντρώνονται στο σχεδιασμό για παραβιάσεις της ασφάλειας και στον τρόπο με τον οποίο ο οργανισμός θα ανακάμψει από αυτές.

Χωρίς ένα επίσημο σχέδιο αντιμετώπισης περιστατικού σε ισχύ, η επιχείρηση ενδέχεται να μην εντοπίζει τις επιθέσεις ή να μην γνωρίζει τι πρέπει να γίνει για να περιορίσει και να αποτρέψει τις επιθέσεις όταν εντοπιστούν.

Μία επιχείρηση θα πρέπει να δημιουργήσει ή να έχει εξωτερική συνεργασία με μια ομάδα αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT), η οποία είναι υπεύθυνη για την ανάλυση, την κατηγοριοποίηση και την αντιμετώπιση περιστατικών ασφάλειας.

Τα βήματα σε ένα πλάνο αντιμετώπισης περιστατικού περιλαμβάνουν τα ακόλουθα:

- Θα πρέπει να υπάρξει η επιβεβαίωση ότι πρόκειται για επίθεση ransomware.
- Θα πρέπει να κληθεί η ομάδα αντιμετώπισης περιστατικών που έχει οριστεί από την διοίκηση.
- Θα πρέπει να γίνει αξιολόγηση του περιστατικό.
- Θα πρέπει να περιοριστεί το ransomware.
- Θα πρέπει να απομονωθεί το ransomware.
- Θα πρέπει να γίνει μια αναλυτική ψηφιακή εγκληματολογική έρευνα.

Ένα σχέδιο αντιμετώπισης περιστατικού είναι χρήσιμο μόνο εάν έχει αναπτυχθεί. Πολύ συχνά, τα σχέδια αντιμετώπισης περιστατικού παραμένουν σε αχρηστία κατά τη διάρκεια περιστατικών. Η ομάδα αντιμετώπισης περιστατικών θα πρέπει επίσης να αξιολογεί περιοδικά την προσαρμογή του σχέδιο αντιμετώπισης περιστατικού στις τρέχουσες υποδομές, το προσωπικό και τις διαδικασίες.

Παράλληλα με την αναθεώρηση του σχέδιο αντιμετώπισης περιστατικού, η ομάδα απόκρισης συμβάντων θα πρέπει να διεξάγει τακτικές ασκήσεις για να διασφαλίσει ότι όλοι οι εμπλεκόμενοι κατανοούν το σχέδιο, το ακολουθούν και μπορούν να βελτιώσουν το σχέδιο αφού προσπαθήσουν να το εκτελέσουν.

5.3 ΧΡΗΣΗ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΗ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΤΡΟΠΗΣ ΜΙΑΣ ΕΠΙΘΕΣΗΣ

Οι ενέργειες μετριασμού ενός ransomware θα πρέπει να ενεργοποιούνται μόλις το SOC ειδοποιηθεί για την επίθεση ransomware. Αν και αποτελεί μέρος του σχεδίου αντιμετώπισης περιστατικού, αυτό το βήμα είναι αρκετά σημαντικό ώστε να είναι και η δική του ξεχωριστή δράση στο σχέδιο ανάκτησης ransomware.

Τα συστήματα κυβερνοασφάλειας θα πρέπει να εργάζονται για τον περιορισμό του ransomware και τον μετριασμό της ζημιάς από αυτό. Η πρώτη κίνηση θα πρέπει να είναι η ενίσχυση της ασφάλειας στον κυβερνοχώρο όπου αυτό κρίνεται απαραίτητο. Η ομάδα ασφαλείας θα πρέπει να διασφαλίζει ότι το δίκτυο θέτει αυτόματα σε καραντίνα τα τελικά σημεία που συμπεριφέρονται ύποπτα, κλειδώνει τμήματα δικτύου και αποκλείει τις συνδέσεις εντολών και ελέγχου. Ο αυτοματισμός όσο το δυνατόν περισσότερο των μεθόδων

μετριασμού της ασφάλειας και αποκατάστασης, με στόχο η ομάδα ασφαλείας να μην χρειάζεται να σταματήσει το ransomware εντελώς χειροκίνητα.

Επιπλέον μέτρο είναι η ενεργοποίηση του ελέγχο ταυτότητας δύο παραγόντων (ή αλλιώς έλεγχο ταυτότητας πολλαπλών παραγόντων ή MFA). Αν οι υπάλληλοι μιας επιχειρήσεις πραγματοποιούν απομακρυσμένη πρόσβαση στο δίκτυό τότε θα πρέπει πάντα να απαιτεί MFA. Οι μέθοδοι ελέγχου ταυτότητας εκτός ζώνης, όπως τα SMS και τα soft tokens, είναι κοινές, ευρέως αποδεκτές από τους χρήστες και σχετικά εύκολα εφαρμόσιμες με την επικράτηση των smartphones.

Προς την σωστή κατεύθυνση είναι η αλλαγή στους προεπιλεγμένους κωδικούς πρόσβασης. Μία από τις απλούστερες επιθέσεις είναι η χρήση ενός προεπιλεγμένου κωδικού πρόσβασης που παραδίδεται out-of-the-box από έναν προμηθευτή. Οι συσκευές του Διαδικτύου των Πραγμάτων (IoT) επισημαίνονται συνήθως για αυτή την ευπάθεια, αλλά το πεδίο εφαρμογής της επίθεσης είναι πολύ ευρύτερο. Οι προεπιλεγμένοι κωδικοί πρόσβασης, ειδικά για συσκευές υλικού (π.χ. δρομολογητές Wi-Fi), μπορούν να επιτρέψουν την άμεση πρόσβαση σε κρίσιμα δεδομένα. Θα πρέπει να δίνεται ιδιαίτερη προσοχή στην απαίτηση ισχυρών κωδικών πρόσβασης για όλους τους χρήστες.

Θα πρέπει να εφαρμοστεί κεντρική καταγραφή. Η ισχυρή συγκέντρωση και διατήρηση αρχείων καταγραφής μπορεί να υποστηρίξει μια έρευνα παραβίασης δεδομένων, με στόχο η διοίκηση να συσχετίσει ορισμένα γεγονότα και να αναπτύξει ένα χρονοδιάγραμμα συμβάντος.

Τέλος κρίνεται απαραίτητο να γίνεται η αποθήκευση των δεδομένων καταγραφής σε ένα προστατευμένο σύστημα που είναι συγχρονισμένο με τον χρόνο και μπορεί εύκολα να αναζητηθεί η όποια πληροφορία. Η διάθεση πόρων θεωρείται αναγκαία τόσο για την τακτική ανάλυση των αρχείων καταγραφής όσο και δοκιμές στην διαδικασία καταγραφής μέσω ασκήσεων εισβολής.

5.4 ΕΠΑΝΑΦΟΡΑ ΤΩΝ ΕΠΗΡΕΑΖΟΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ

Μόλις σταματήσει η επίθεση ransomware και πραγματοποιηθεί η αξιολόγηση της ασφάλειας των συστημάτων παραγωγής, τότε θα πρέπει να επανέλθουν και να λειτουργήσουν ξανά. Ορισμένα βήματα για την επανέναρξη των επιχειρηματικών λειτουργιών περιλαμβάνουν τα ακόλουθα:

i. Ανάπτυξη δεδομένων αντιγράφων ασφαλείας.
ii. Διαγραφή και επαναφορά των τελικών σημείων.
iii. Διαγραφή και αντικατάσταση των κεντρικών συστημάτων που έχουν επηρεαστεί.
iv. Προσπάθεια ανάκτησης των δεδομένων, εφόσον είναι απαραίτητο.
v. Σάρωση των αποκατεστημένων δεδομένων για μολύνσεις.

5.5 ΕΠΙΚΟΙΝΩΝΙΑ ΜΕ ΕΜΠΛΕΚΟΜΕΝΟΥΣ ΦΟΡΕΙΣ

Ενώ τα δεδομένα αποκαθίστανται και επανέρχονται στις κανονικές επιχειρηματικές λειτουργίες, η επιχείρηση θα πρέπει να επικοινωνεί εσωτερικά και, ενδεχομένως, εξωτερικά. Το σχέδιο αποκατάστασης από το ransomware θα πρέπει να περιλαμβάνει πότε και πώς θα γίνει η ενημέρωση στους υπεύθυνους λήψης αποφάσεων και στα δυνητικά επηρεαζόμενα μέρη, στα οποία περιλαμβάνονται οι εργαζόμενοι, η διοίκηση, οι προμηθευτές και οι πελάτες.

Το σχέδιο θα πρέπει να ορίζει σημεία λήψης αποφάσεων, ώστε οι ομάδες ασφαλείας να γνωρίζουν με ποιον πρέπει να επικοινωνήσουν ανάλογα με το εύρος και την ταχύτητα της μόλυνσης. Θα πρέπει να προσδιορίζει ποιος λαμβάνει τις αποφάσεις, πώς γίνεται η επικοινωνία με τα άτομα αυτά καθώς και ποιοι είναι οι αναπληρωτές τους, στην περίπτωση που χρειαστεί. Περιλαμβάνει επίσης ποιος, πώς και πότε πρέπει να ενημερωθεί για κάθε απόφαση, καθώς και τις αναμενόμενες επιχειρηματικές επιπτώσεις των αποφάσεων. Η εξωτερική επικοινωνία περιλαμβάνει την αναφορά της επίθεσης στους κρατικούς φορείς με τους οποίους εμπλέκεται η επιχείρηση.

5.6 ΣΥΝΕΧΗΣ ΒΕΛΤΙΩΣΗ ΤΟΥ ΣΧΕΔΙΟΥ ΑΝΑΚΤΗΣΗΣ RANSOMWARE

Η επιχείρηση θα πρέπει να συντάσσει μία έκθεση μετά τη δράση για να ολοκληρωθεί η διαδικασία αποκατάστασης από την καταστροφή. Η έκθεση αυτή θα πρέπει να είναι μια πλήρης και χωρίς των επιμερισμό ευθυνών, ανασκόπηση όλων όσων έγιναν και όσων δεν έγιναν για την αντιμετώπιση το περιστατικού ransomware.

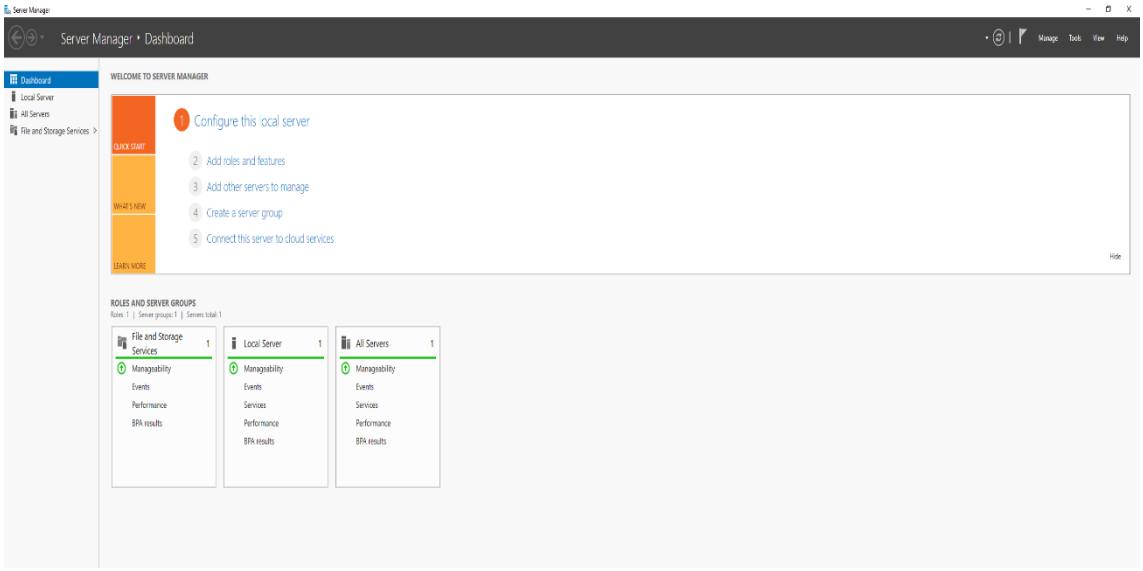
Θα ήταν προς όφελος της εταιρείας να επανεξετάσει τι λειτούργησε και τι όχι στο σχέδιο αποκατάστασης από το ransomware. Η επιχείρηση οφείλει να προσθέσει επιπλέον ό,τι λείπει και να μετριάσει τις περιττές διαδικασίες που επιβράδυναν τις προσπάθειες αντιμετώπισης.

Δεν είναι σίγουρο ότι κάθε επιχείρηση θα βιώσει μια επιτυχημένη επίθεση ransomware. Είναι όμως σίγουρο ότι όσοι δεν σχεδιάζουν μια τέτοια επίθεση θα βρεθούν σε σοβαρό μειονέκτημα όταν αντιμετωπίσουν τους εγκληματίες του κυβερνοχώρου.

ΚΕΦΑΛΑΙΟ 6: ΤΕΧΝΙΚΟ ΜΕΡΟΣ

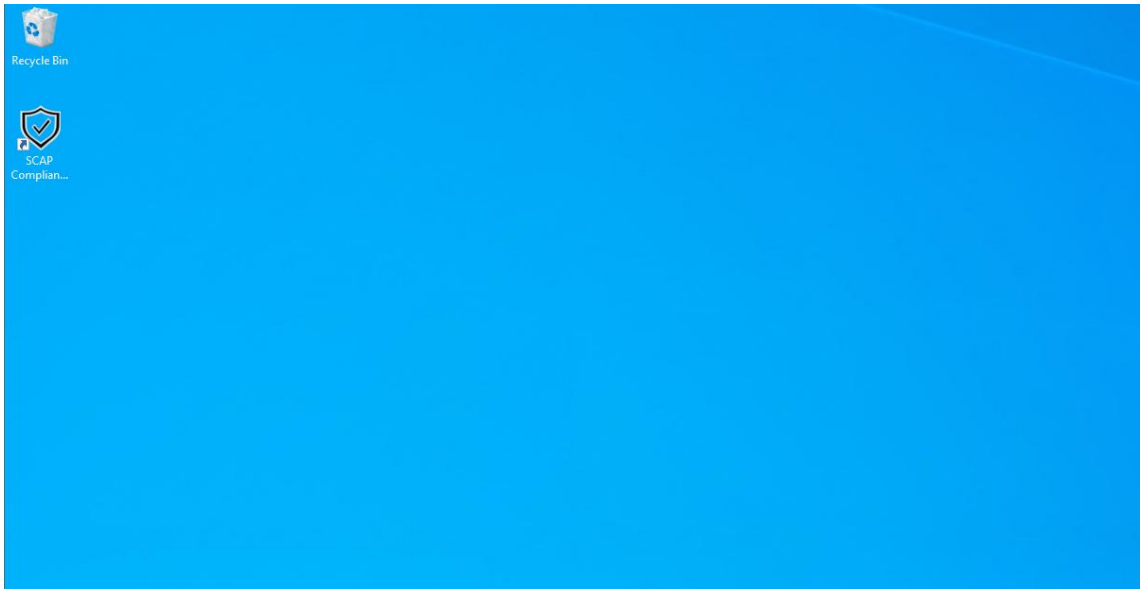
Στο κεφάλαιο αυτό παρουσιάζεται μία υπόθεση εργασίας όπου μία επιχείρηση μπορεί να εντοπίσει σε τι ποσοστό είναι ανοχύρωτα τα συστήματα της και με συγκεκριμένη διαδικασία, η οποία εξηγείται παρακάτω να αυξήσει το ποσοστό ασφαλείας των συστημάτων της.

Η επιχείρηση έχει εγκαταστήσει εναν Windows Server 2022 σε περιβάλλον Virtual Machine χρησιμοποιώντας το VMware Workstation.



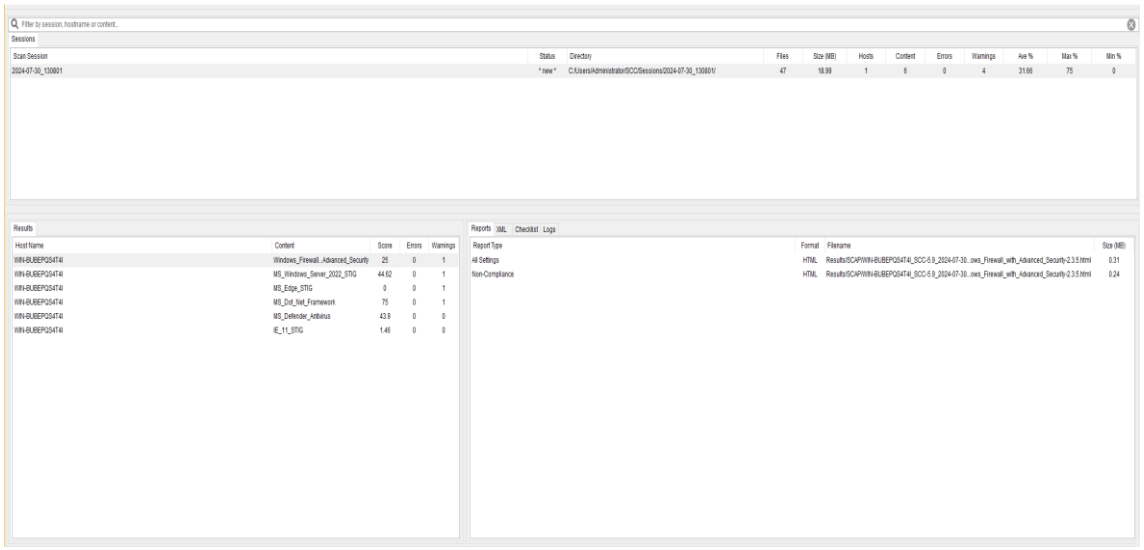
Εικόνα 1: Windows Server 2022

Στη συνέχεια έγινε η εγκατάσταση του προγράμματος SCAP Compliance Checker το οποίο αποτελεί ένα αυτοματοποιημένο εργαλείο σάρωσης που αξιοποιεί τις συγκεκριμένες βασικές κατευθυντήριες γραμμές DISA Security Technical Implementation Guidelines (STIGs) και το λειτουργικό σύστημα (OS), στην προκειμένη περίπτωση το λειτουργικό που χρησιμοποιείται είναι Windows, για την ανάλυση και την αναφορά σχετικά με τη διαμόρφωση ασφαλείας ενός συστήματος πληροφοριών.

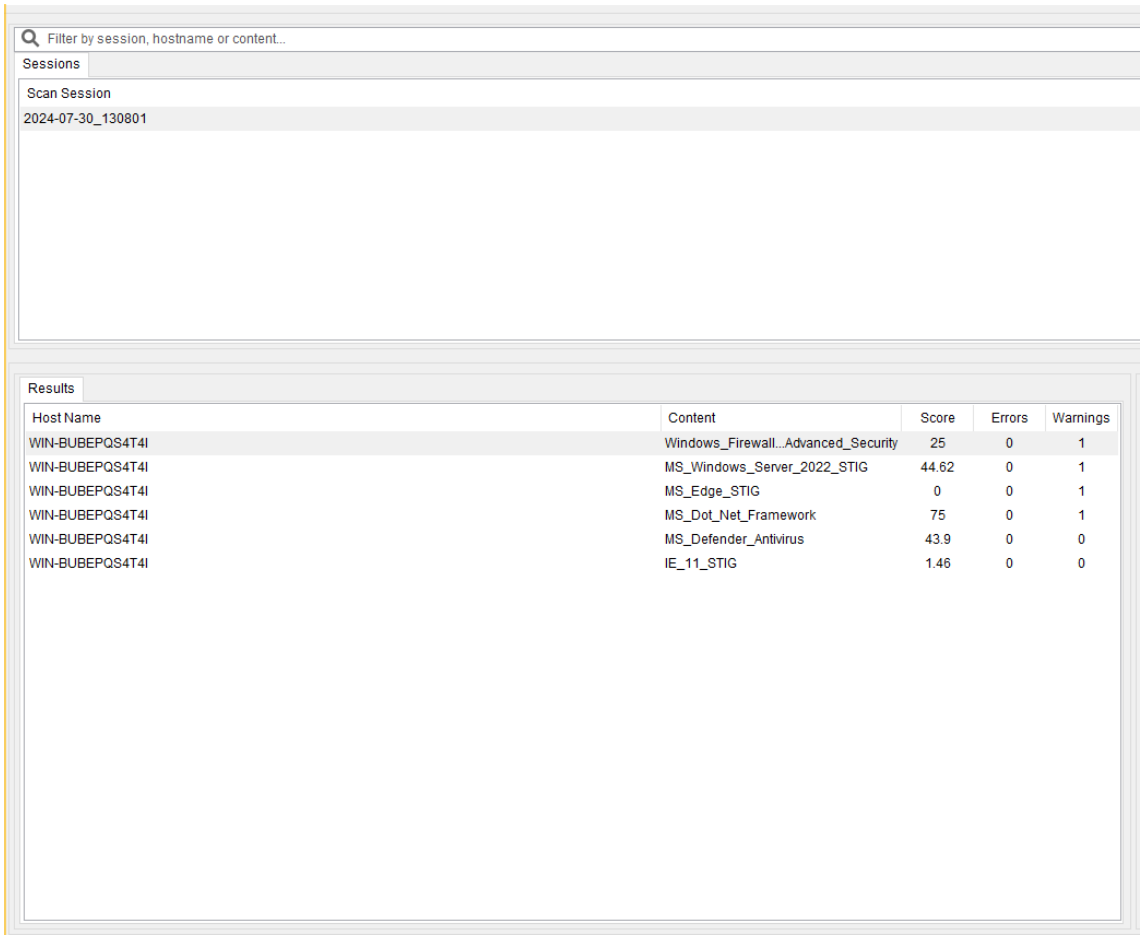


Εικόνα 2: Scap

Αφού έγινε η εγκατάσταση, τρέχουμε το πρόγραμμα ώστε να έχουμε εικόνα σε τι επίπεδο ασφαλείας (Average Score) βρίσκεται το λειτουργικό μας σύστημα. Το αποτέλεσμα που βγήκε είναι 25% όπως φαίνεται και στις εικόνες που ακολουθούν.

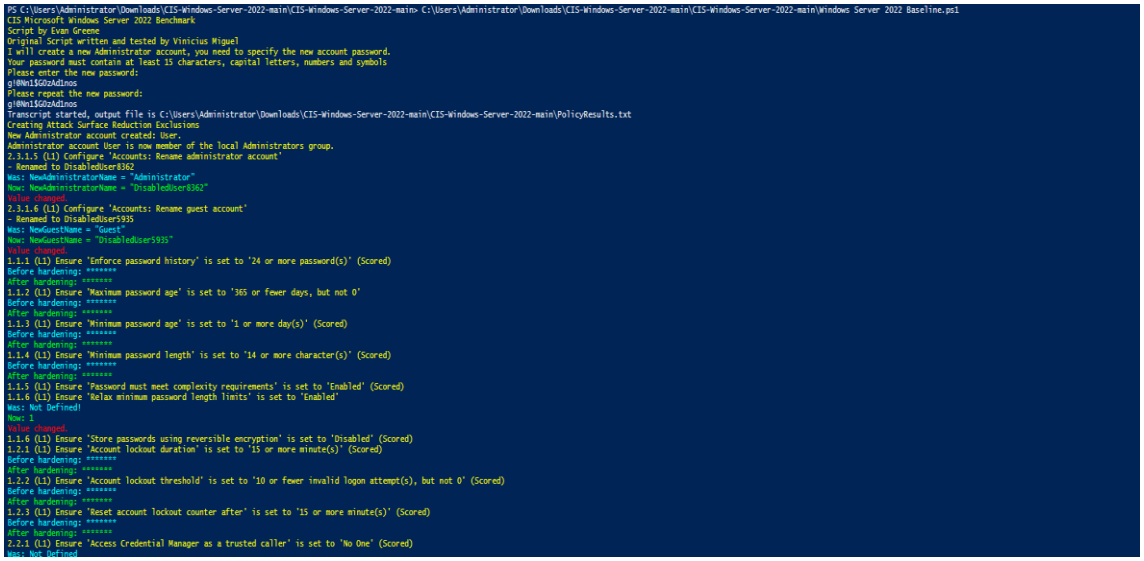


Εικόνα 3a: Αρχικό Αποτέλεσμα

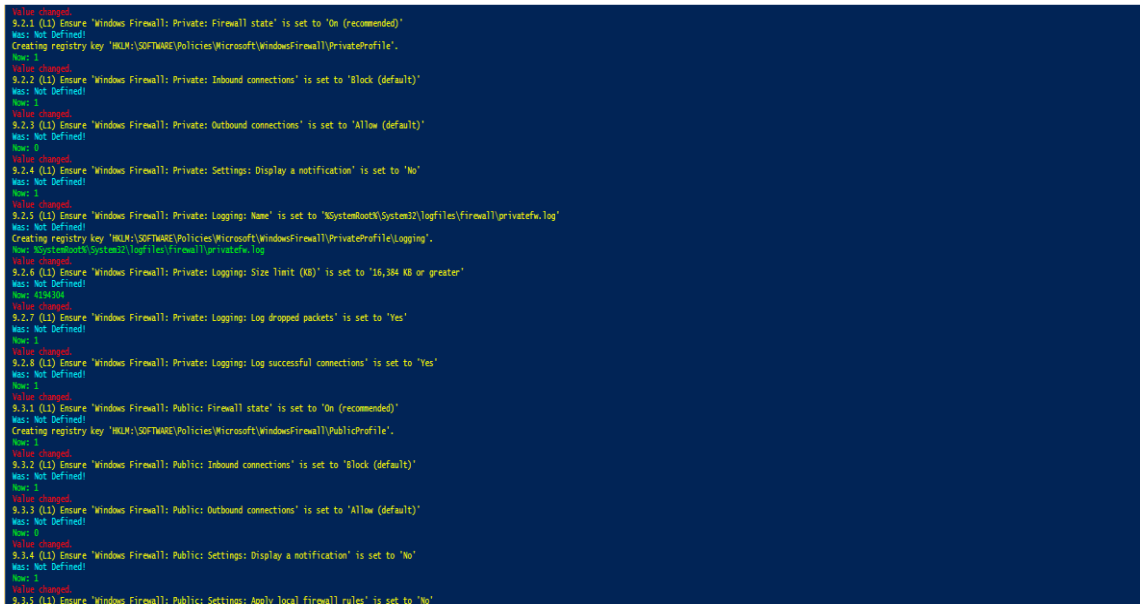


Εικόνα 3b: Αρχικό Αποτέλεσμα

Έχοντας ως οδηγό το παραπάνω ποσοστό, θα προβούμε σε hardening του συστήματος μας. Το hardening ενός συστήματος είναι μια συλλογή εργαλείων, τεχνικών και βέλτιστων πρακτικών για τη μείωση της ευπάθειας σε τεχνολογικές εφαρμογές, συστήματα, υποδομές, υλικολογισμικό και άλλους τομείς. Στόχος του hardening είναι η μείωση του κινδύνου ασφάλειας με την εξάλειψη των πιθανών φορέων επίθεσης.



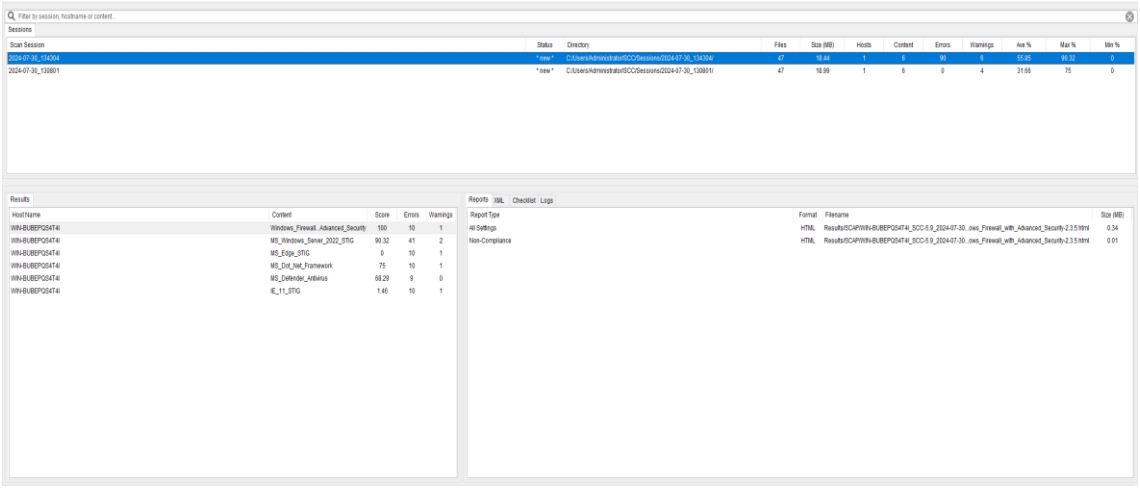
Εικόνα 5: Διαδικασία Hardening



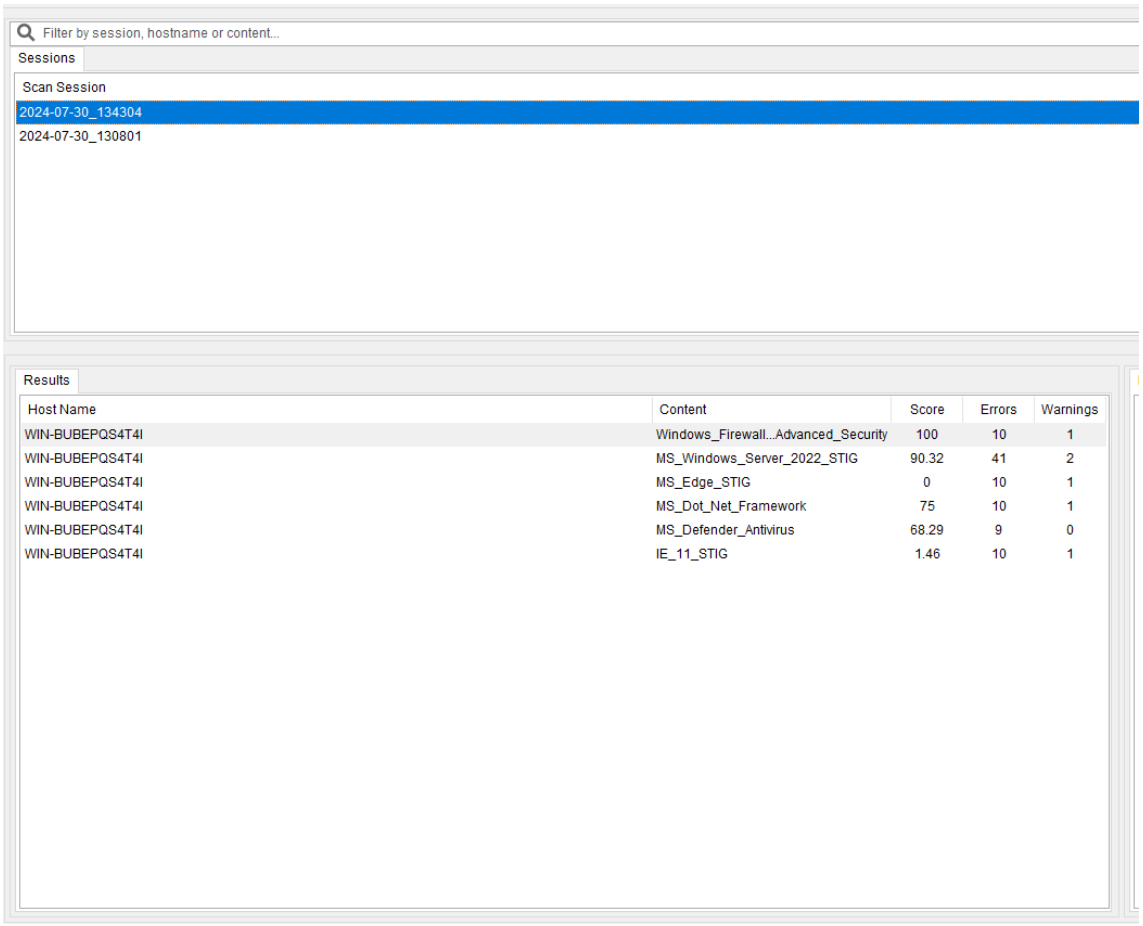
Εικόνα 6: Διαδικασία Hardening

Με την ολοκλήρωση της διαδικασίας του Hardening πραγματοποιούμε εκ νέου τη διαδικασία ώστε να ελέγξουμε σε τι βαθμό έχει μεταβληθεί ή όχι το ποσοστό ασφαλείας του

συστήματος. Όπως φαίνεται και στις εικόνες που ακολουθούν το ποσοστό έχει ανέλθει στο 100%.



Εικόνα 7a: Ποσοστό Ελέγχου μετά το Hardening



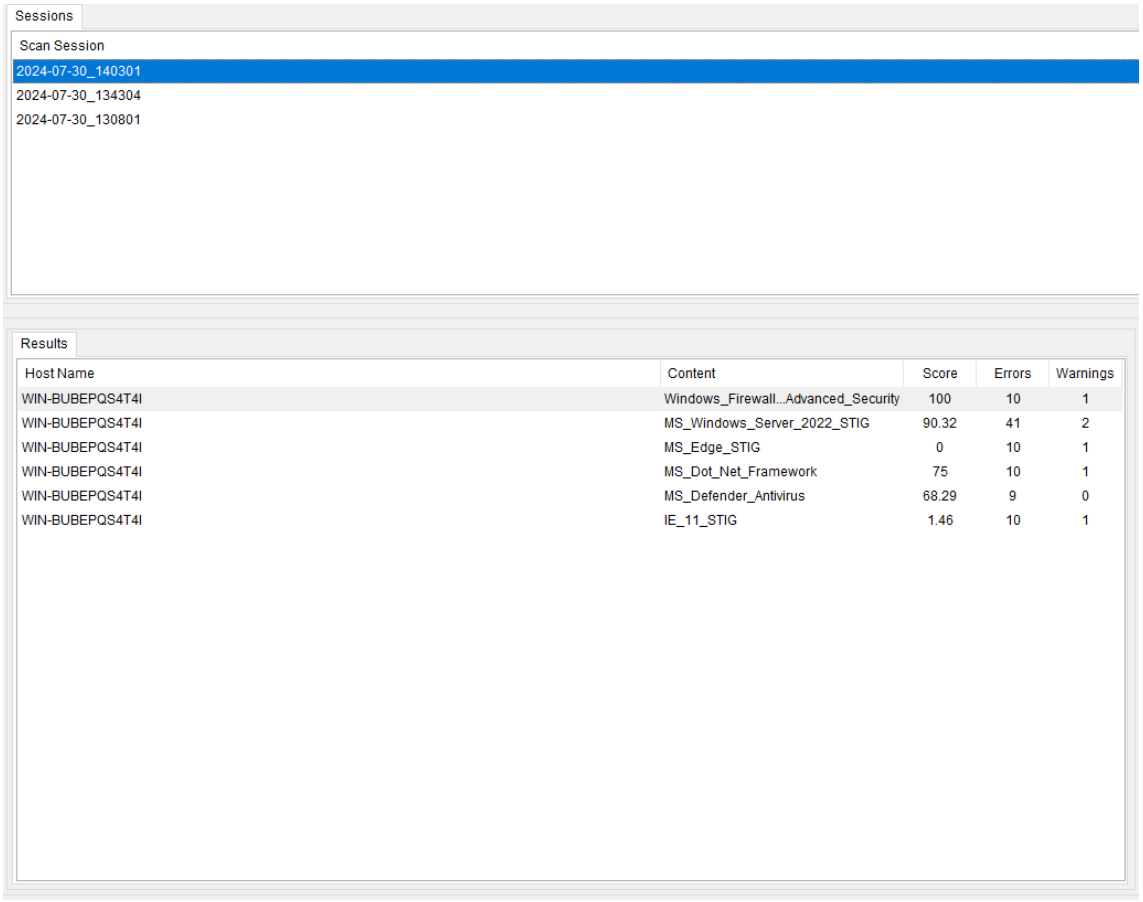
Εικόνα 7b: Ποσοστό Ελέγχου μετά το Hardening

Ολοκληρώνοντας τον έλεγχο του συστήματος μετά το Hardening, «τρέχουμε» το Raccine το οποίο εμποδίζει το ransomware να κάνει κατάχρηση του vssadmin.exe, ενός βοηθητικού προγράμματος των Windows που διαχειρίζεται σκιώδη αντίγραφα των δεδομένων ενός συστήματος Windows.

Εικόνα 8: Raccine

Εικόνα 9: Raccine

Εφόσον ολοκληρωθεί και το «τρέξιμο» του Raccine, πραγματοποιούμαι επανέλεγχο στο σύστημα μας και βλέπουμε πως το ποσοστό παραμένει στο 100%.



Εικόνα 10: Τελικό σκορ επανελέγχου

ΠΑΡΑΡΤΗΜΑ

ΕΠΙΘΕΣΕΙΣ RANSOMWARE

Παρακάτω παρατίθενται συνοπτικά σε μορφή πίνακα οι πιο σημαντικές επιθέσεις ransomware που σημειώθηκαν και κατεγράφησαν τους μήνες Απρίλιο, Μάιο και Ιουνίου της τρέχουσας χρονιάς.

Απρίλιος 2024

Ημερομηνία	Θύμα	Threat Actor	Πηγή
01 Απριλίου 2024	Omni Hotels	Daixin Ransomware	Daixin ransomware attack on Omni Hotels
03 Απριλίου 2024	IxMetro Powerhost	SEXi Ransomware	Ransomware attack on Chile's hosting provider, IxMetro
04 Απριλίου 2024	Panera Bread	Unknown	Panera Bread ransomware attack
04 και 11 Απριλίου 2024	Hoya Corporation	Hunters International ransomware	Hoya Corporation ransomware attack
08 Απριλίου 2024	The government of Palau	DragonForce Ransomware	Ransomware attack on the government of Palau
08 Απριλίου 2024	The Tarrant County Appraisal District	Medusa Ransomware	Ransomware attack on the Tarrant County Appraisal District
08 Απριλίου 2024	German database company Genios	Unknown	Ransomware attack on GBI Genios
09 Απριλίου 2024	Non-profit healthcare service provider Group Health Cooperative of South Central Wisconsin (GHC-SCW)	BlackSuit Ransomware	Group Health Cooperative of South Central Wisconsin (GHC-SCW) ransomware attack
09 Απριλίου 2024	New Mexico Highlands University (NMHU) and East Central University in Ada, Oklahoma	BlackSuit Ransomware	Ransomware attack on the universities in New Mexico
15 Απριλίου 2024	Chipmaker Nexperia	Dunghill Leak	Nexperia ransomware attack

15 Απριλίου 2024	Change Healthcare	RansomHub Extortion Gang	Change ransomware attack update
17 Απριλίου 2024	Cherry Street Services	Unknown	Ransomware attack on Cherry Street Services
18 Απριλίου 2024	D.C. Department of Insurance, Securities and Banking (DISB)	LockBit Ransomware	D.C. Department of Insurance, Securities and Banking (DISB) ransomware attack
19 Απριλίου 2024	The United Nations Development Programme (UNDP)	8Base ransomware	The United Nations Development Programme (UNDP) ransomware attack
21 Απριλίου 2024	Synlab Italia	Unknown	Synlab Italia ransomware attack
22 Απριλίου 2024	UnitedHealth	BlackCat/ALPHV ransomware	UnitedHealth ransomware attack update
23 Απριλίου 2024	Plasma donation company Octapharma	BlackSuit Ransomware	Ransomware attack on a plasma donation company Octapharma
23 Απριλίου 2024	Skanlog, a critical distributor for Systembolaget	Unknown	Ransomware attack on Swedish logistics company

Μάϊος 2024

Ημερομηνία	Θύμα	Threat Actor	Πηγή
01 Μαΐου 2024	Simone Veil hospital in Cannes, France	LockBit Ransomware	Simone Veil hospital Cannes ransomware attack
05 Μαΐου 2024	Wichita government	LockBit Ransomware	Wichita ransomware attack update
08, 09, 29 Μαΐου 2024	Catholic health system Ascension	BlackBasta Group	Ascension hospital ransomware attack update
09 Μαΐου 2024	Ohio Lottery	DragonForce	Ohio Lottery ransomware attack update
12 Μαΐου 2024	British auction house Christie's	RansomHub	Christie’s ransomware attack and RansomHub
14 Μαΐου 2024	Singing River Health System	Rhysida Ransomware	Singing River Health System ransomware attack update
20 Μαΐου 2024	OmniVision	Cactus ransomware	OmniVision ransomware attack update
21 Μαΐου 2024	London Drugs	LockBit	London Drugs ransomware attack update with LockBit
26 Μαΐου 2024	MediSecure	Threat actor, Ansgar	MediSecure ransomware attack
29 Μαΐου 2024	ABN AMRO	Unknown	ABN AMRO ransomware attack
29 Μαΐου 2024	Ticketmaster/Live Nation	ShinyHunters	Ticketmaster/Live Nation ransomware attack
29 Μαΐου 2024	Seattle Public Library	Unknown	Seattle Public Library ransomware attack

Ιούνιος 2024

Ημερομηνία	Θύμα	Threat Actor	Πηγή
02 Ιουνίου 2024	Telecom giant Frontier Communication	RansomHub	Frontier Communications ransomware attack
05 Ιουνίου 2024	PandaBuy	Sanggiero (BreachForum name)	PandaBuy ransomware attack update
06 Ιουνίου 2024	Christie's	RansomHub	Christie's ransomware attack
11 Ιουνίου 2024	Cleveland City	Unknown	Cleveland City ransomware attack update
13, 17 Ιουνίου 2024	Panera Bread	Unknown	Panera Bread ransomware attack update
13 Ιουνίου 2024	Ascension Healthcare	BlackBasta Ransomware	Ascension Healthcare ransomware attack
19 Ιουνίου 2024	CDK Global	BlackSuit Ransomware	CDK ransomware attack update
20 Ιουνίου 2024	Change Healthcare	BlackCat (aka ALPHV) Ransomware	Change Healthcare ransomware attack update
26 Ιουνίου 2024	South Africa’s National Health Laboratory Service (NHLS)	Unknown	South Africa’s National Health Laboratory Service (NHLS) ransomware attack
28 Ιουνίου 2024	Infosys McCamish	LockBit Ransomware	Infosys McCamish Ransomware Attack Impact

ΣΥΜΠΕΡΑΣΜΑΤΑ

Κλείνοντας την εργασία αυτό που πρέπει να σημειωθεί είναι πως οι εποχές έχουν αλλάξει και θα πρέπει η εξέλιξη να αντικατοπτρίζει όχι μόνο σε ατομικό επίπεδο αλλά και στο εργασιακό περιβάλλον αφού μια επιχείρηση πρέπει να κάνει αρκετά βήματα μπροστά εγκαταλείποντας παραδοσιακές πρακτικές, συνθήκες και νοοτροπίες αν θέλει να αντιμετωπίσει τις νέες προκλήσεις και απειλές.

Οι απειλές εξελίσσονται και ολοένα γίνονται πιο πολύπλοκες και σύνθετες καθώς και πιο δαπανηρές. Για να μπορεί μία επιχείρηση ανεξαρτήτως μεγέθους να ανταπεξέλθει σε αυτό το απειλούμενο περιβάλλον, το βασικότερο μέτρο προστασίας παραμένει η πρόληψη.

Πλέον μία επιχείρηση πρέπει να αντιληφθεί ότι η θωράκιση του συνόλου των περιουσιακών της στοιχείων είναι η μόνη λύση για να έχει μελλοντικά τη βιωσιμότητα που απαιτείται ώστε να μπορεί να λειτουργεί αδιάκοπα ή με το μικρότερο κόστος είτε οικονομικό είτε επιχειρησιακό σε μία ενδεχόμενη κυβερνοεπίθεση. Άλλωστε μία επίθεση τύπου ransomware, αφορά περισσότερο τον χειρισμό των τρωτών σημείων της ανθρώπινης ψυχολογίας παρά την τεχνολογική πολυπλοκότητα του αντιπάλου

Θα πρέπει να δοθεί η απαραίτητη βαρύτητα στα πιο ευάλωτα, ευαίσθητα και σημαντικά δεδομένα της επιχείρησης με στόχο την προστασία τους από κακόβουλες ενέργειες, είτε πρόκειται για αντίγραφα ασφαλείας, περιορισμός πρόσβασης, μεγαλύτερη ασφάλεια στην εταιρική ηλεκτρονική αλληλογραφία καθώς και στοχευμένη εκπαίδευση των υπάλληλων της, αφού κατά γενική ομολογία και παραδοχή, ο πιο αδύναμος κρίκος στην ασφάλεια μιας εταιρείας αποτελούν οι άνθρωποι.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Βιβλία & Αρθρογραφία

1. Gibson M.G., 2021. Ransomware Recovery for Dummies. Rubrik
2. Vanover R., Weijdema E., 2021. 5 Ransomware Protection Best Practices. Veeam
3. Liska A., 2021. Ransomware Understand, Prevent, Recover. ActualTech Media
4. Miller L., 2021. Ransomware Defense for dummies. Cisco
5. Richardson R., North M., 2017. Ransomware: Evolution, Mitigation and Prevention. Kennesaw State University, Faculty Publications
6. O'Kane p., Sezer S., Carlin D., 2018. Evolution of ransomware. IET Networks
7. Mohurle S., Patil M., 2017. A brief study of Wannacry Threat: Ransomware Attack 2017. IJARCS.
8. Kok SH., Abdullah A., Jhanjhi NZ., Supramaniam M., 2019. Ransomware, Threat and Detection Techniques: A Review. International Journal of Computer Science and Network Security.
9. Huang D., Aliapoulios M., Li V., Invernizzi L., McRoberts K., Bursztein E., Levin J., Levchenko K., Snoeren A., McCoy D., 2018. Tracking Ransomware End-to-end. IEEE Computer Society.
10. The Evolution of Ransomware and How to Protect Yourself. Dropsuite, 2022.
11. Koutsokostas, Vasilios, et al. "Invoice# 31415 attached: Automated analysis of malicious Microsoft Office documents." Computers & Security 114 (2022): 102582.
12. Patsakis, Constantinos, David Arroyo, and Fran Casino. "The Malware as a Service ecosystem." arXiv preprint arXiv:2405.04109 (2024).
13. Kolodenker, Eugene, et al. "Paybreak: Defense against cryptographic ransomware." Proceedings of the 2017 ACM on Asia conference on computer and communications security. 2017.
14. Genç, Ziya Alper, Gabriele Lenzini, and Peter YA Ryan. "No random, no ransom: a key to stop cryptographic ransomware." Detection of Intrusions and Malware, and Vulnerability Assessment: 15th International Conference, DIMVA 2018, Saclay, France, June 28–29, 2018, Proceedings 15. Springer International Publishing, 2018.
15. Gilbert, Stephen, et al. "Can we learn from an imagined ransomware attack on a hospital at home platform?." NPJ Digital Medicine 7.1 (2024): 65.
16. Patsakis, Constantinos, et al. "Cashing out crypto: state of practice in ransom payments." International Journal of Information Security 23.2 (2024): 699-712.

17. Cannell, J. (2016). Cryptolocker Ransomware: What you need to know. Retrieved from Malwarebytes, https://blog.malwarebytes.com/101/2013/10/cryptolocker-ransomware-what-you-need-to-know/
18. Cawley, C. (2016, August 30). A history of Ransomware: Where it started & where it's going. Retrieved from http://www.makeuseof.com/tag/history-ransomware-russia-reveton/
19. Constantin, L. (2015, September 24). Ransomware pushers up their game against small businesses. PC World. Retrieved from http://www.pcworld.com/article/2985826/security/ransomware-pushers-up-their-game-against-small-businesses.html
20. Constantin, L. (2016c, July 14). New Locky ransomware version can operate in offline mode. Retrieved from PC World, http://www.pcworld.com/article/3095865/security/new-locky-ransomware-version-can-operate-in-offline-mode.html
21. Fitzpatrick, D., & Griffin, D. (2016, April 15). Cyber-extortion losses skyrocket says FBI. CNN.Retrieved August 27, 2016, from http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security
22. Kirk, J. (2016a, March 6). Apple shuts down first-ever ransomware attack against Mac users. Retrieved
23. March 7, 2016, from PC World, http://www.pcworld.com/article/3040987/security/apple-shuts-down-first-ever-ransomware-attack-against-mac-users.html
24. McAfee Labs Threats Report, June 2016.
25. Pauli, D. (2015, November 9). Cryptowall 4.0: Update makes world's worst ransomware worse still. Retrieved November 9, 2015, from http://www.theregister.co.uk/2015/11/09/cryptowall_40/
26. Rosenberg, J. M. (2015, April 8). A Q&A about the malicious software known as ransomware. Retrieved April 8, 2015, from http://www.salon.com/2015/04/08/a_qa_about_the_malicious_software_known_as_ransomware/
27. Savage, K., Coogan, P., & Lau, H. (2015). The Evolution of Ransomware.
28. Segura, J. (2016). Citadel: A cyber-criminal's ultimate weapon? Retrieved August 28, 2016, from https://blog.malwarebytes.com/threat-analysis/2012/11/citadel-a-cyber-criminals-ultimate-weapon/
29. Sjouwerman, S. (2015b). A short history & evolution of Ransomware. Retrieved August 28, 2016, from https://blog.knowbe4.com/a-short-history-evolution-of-ransomware

30. Tromer, E. (2008). Cryptanalysis of the Gpcode.Ak ransomware virus. Retrieved from rump2008.cy.yp.to/6b53f0dad2c752ac2fd7cb80e8714a90.pdf
31. Zetter, K. (2015, September 17). Hacker lexicon: A guide to Ransomware, the scary hack that's on the rise. Retrieved from Security, https://www.wired.com/2015/09/hacker-lexicon-guide-ransomware-scary-hack-thats-rise/

Σύνδεσμοι (Links):

1. https://atos.net/en/lp/turning-tables-on-ransomware/the-impact-of-ransomware-attacks-on-business
2. https://www.a-lign.com/articles/blog-whats-the-difference-between-iso-27001-2013-and-iso-27001-2022
3. https://www.ascenditsolutions.com/blog/executive-summary/65-the-impact-of-ransomware
4. https://www.b4restore.com/financial-impact-of-a-ransomware-attack
5. https://www.backblaze.com/blog/complete-guide-ransomware
6. https://blogs.microsoft.com/on-the-issues/2023/04/06/stopping-cybercriminals-from-abusing-security-tools/
7. https://ccoe.dsci.in/blog/the-rise-of-ransomware-attacks-and-how-to-protect-against-them
8. https://csrc.nist.gov/pubs/ir/8374/final
9. https://cyberreadinessinstitute.org/resource/ransomware-playbook/
10. https://cybriant.com/the-cios-guide-to-preventing-ransomware-attacks/
11. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-131a
12. https://www.cisa.gov/sites/default/files/2023-06/stopransomware_guide_508c_1.pdf
13. https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware
14. https://www.cisa.gov/stopransomware/ive-been-hit-ransomware
15. https://www.cisecurity.org/insights/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware
16. https://www.clearskysec.com/wp-content/uploads/2021/02/Conti-Ransomware.pdf

17. https://www.cloudflare.com/learning/security/ransomware/how-to-prevent-ransomware
18. https://www.crowdstrike.com/cybersecurity-101/ransomware/how-to-protect-against-ransomware/
19. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-examples/
20. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-recovery/
21. https://www.cybereason.com/blog/how-do-ransomware-attacks-impact-victim-organizations-stock
22. https://www.cybereason.com/ransomware-the-true-cost-to-business-2024
23. https://www.cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099
24. https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099
25. https://www.cyberx.gr/diacheirisi-amp-diapragmateysi-ransomware/
26. https://egs.eccouncil.org/what-do-you-know-about-iso-27001/
27. https://en.wikipedia.org/wiki/DarkSide
28. https://en.wikipedia.org/wiki/ISO/IEC_27001
29. https://www.enisa.europa.eu/about-enisa/about/el
30. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
31. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
32. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends
33. https://www.enisa.europa.eu/topics/incident-response/glossary/ransomware
34. https://www.eset.com/blog/company/what-does-nis2-mean-to-you/
35. https://www.eset.com/gr/ransomware-business/
36. https://europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/tips-advice-to-prevent-ransomware-infecting-your-electronic-devices
37. https://github.com/BUseclab/paybreak
38. https://github.com/counteractive/incident-response-plan template/blob/master/playbooks/playbook-ransomware.md

39. https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained
40. https://www.itsecuritypro.gr/oi-epitheseis-ransomware-apoteloyn-sovari-apeili-me-pano-apo-to-60-ton-epitheseon-na-stocheyoyn-tis-mikromesaies-epicheiriseis/
41. https://kirbtech.com/business-ransomware-facts/
42. https://learn.microsoft.com/en-gb/security/ransomware/human-operated-ransomware
43. https://www.lawspot.gr/nomika-nea/kyvernoasfaleia-dimosieythike-i-odigia-nis-2-tis-eyropaikis-enosis
44. https://www.lawspot.gr/nomika-nea/odigia-nis-2-enishysi-tis-kyvernoasfaleias-kai-tis-anthektikotitas-se-epipedo-ee
45. https://www.lumificyber.com/blog/the-sans-incident-response-framework/
46. https://www.mimecast.com/content/darkside-ransomware/
47. https://www.moneyreview.gr/opinion/67638/i-dioikisi-tis-epicheirisis-apenanti-sto-ransomware/
48. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
49. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware
50. https://orbilu.uni.lu/bitstream/10993/40578/1/etaa2019GLR.pdf
51. https://www.pandasecurity.com/en/mediacenter/darkside-ransomware/
52. https://perception-point.io/guides/ransomware/how-to-prevent-ransomware-attacks/
53. https://www.rubrik.com/insights/how-to-recover-from-ransomware
54. https://secureframe.com/hub/iso-27001/clauses
55. https://secureslate.medium.com/iso-domains-demystified-everything-you-need-to-know-67332d8b51d7
56. https://security.berkeley.edu/faq/ransomware/what-possible-impact-ransomware
57. https://www.sealpath.com/blog/ransomware-impact-businesses/
58. https://www.sepe.gr/tehnologia-pliroforiki/kuvernoasfaleia/22434967/oi-misesetaireies-stin-europi-den-vriskoun-eidikous-kuvernoasfaleia/
59. https://staysafeonline.org/resources/how-to-prevent-and-recover-from-ransomware/
60. https://www.sophos.com/en-us/content/state-of-ransomware

61. https://www.sophos.com/en-us/search-results#q=Ransomware%20&firstQueryCause=searchFromLink
62. https://www.techtarget.com/searchsecurity/feature/5-critical-steps-to-creating-an-effective-incident-response-plan
63. https://www.techtarget.com/searchsecurity/tip/How-to-recover-from-a-ransomware-attack
64. https://www.techtarget.com/whatis/definition/information-security-management-system-ISMS
65. https://www.titanfile.com/blog/phases-of-incident-response/
66. https://www.tripwire.com/state-of-security/22-ransomware-prevention-tips
67. https://www.upguard.com/blog/best-practices-to-prevent-ransomware-attacks
68. https://www.upguard.com/blog/incident-response-plan
69. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
70. https://www.cisa.gov/sites/default/files/publications/Incident-Response-Plan-Basics_508c.pdf
71. https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-ransomware