



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΜΣ “Ψηφιακές Εφαρμογές και Καινοτομία”

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ & ΕΚΤΙΜΗΣΗ ΡΙΣΚΟΥ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ ΤΟΥΡΙΣΜΟΥ

Κούρκουλου Φανή

ΑΜ:202010

Επιβλέπων Καθηγητής: Νταντογιάν Χριστόφορος

Κέρκυρα, Μάρτιος 2022

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΜΣ “Ψηφιακές Εφαρμογές και Καινοτομία”

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ & ΕΚΤΙΜΗΣΗ ΡΙΣΚΟΥ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ ΤΟΥΡΙΣΜΟΥ

Κούρκουλου Φανή

ΑΜ : 202010

Τριμελής επιτροπή

Νταντογιάν
Χριστόφορος

Τσώχου
Αγγελική

Χριστοπούλου
Ελένη

Κέρκυρα, Μάρτιος 2022

Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ότι είμαι αποκλειστικός συγγραφέας της παρούσας Εργασίας και δηλώνω ότι αυτή προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία με θέμα την «Κυβερνοασφάλεια και εκτίμηση ρίσκου στις υπηρεσίες τουρισμού» αναφέρεται στους κινδύνους του διαδικτύου που έχει να αντιμετωπίσει μια επιχείρηση, στους τρόπους που έχει για να προστατευθεί αλλά και στα μέτρα που μπορεί να λάβει για να μπορέσει να ανταπεξέλθει στους κινδύνους αυτούς. Αρχικά γίνεται αναφορά στη τρέχουσα κατάσταση που επικρατεί τα τελευταία χρόνια στον πλανήτη αλλά και στην Ελλάδα ειδικότερα όπου λόγω Κορωνοϊού οι συνθήκες εργασίας έχουν αλλάξει. Έπειτα και βάσει των συνθηκών γίνεται αναφορά για την τάση των κυβερνοεπιθέσεων και απαριθμούνται τα είδη των απειλών καθώς και παραδείγματα από επιχειρήσεις στο κλάδο του τουρισμού που έχουν δεχθεί αντίστοιχες επιθέσεις. Στη συνέχεια αναφέρονται τα μέτρα πρόληψης που μπορεί να λάβει μια επιχείρηση για την ασφάλεια της αλλά και οι τρόποι αντιμετώπισης. Τέλος ακολουθεί προσέγγιση για τον τρόπο που μπορεί να διεξάγει μια επιχείρηση μια πλήρη εκτίμηση κινδύνου με ανάλυση όλων των βημάτων, των επιπτώσεων και των τρόπων διασφάλισης της συνέχειάς της. Δεδομένου ότι από τις κυβερνοεπιθέσεις δεν είναι ποτέ κανείς 100% ασφαλείς με την παρούσα εργασία δίνεται μια προσέγγιση στο τι μπορούν να κάνουν οι επιχειρήσεις για να διαχειρίζονται αποτελεσματικά το όποιο συμβάν και να διατηρήσουν την καλή φήμη και τη συνέχιση λειτουργίας τους.

SUMMARY

The report on "Cybersecurity and risk assessment in tourism services" refers to the cyber risks that a business has to deal with, to the ways in which it should be protected and to the measures it must take to be able to deal with these risks. Initially, mentioned to the current situation that prevails in recent years on the planet and especially in Greece where due to Covid- 19 working conditions have changed. Then, based on the circumstances, a report is made on the trend of cyber attacks and the types of threats, as well as with examples from companies in the tourism sector that have received similar attacks. After, refers precautionary measures that the company can take for its security and the measures it can take to deal with. Finally, there is an approach to how a business can conduct business a complete risk assessment by analyzing all the steps, the implications and the ways to ensure its continuity. Given that cyber-attacks are never 100% safe, this approach provides an overview of what companies can do to effectively manage any event and maintain a good reputation and continuity.

Περιεχόμενα

1.	Μεθοδολογία Εργασίας.....	4
2.	Εισαγωγή	4
3.	Ανάλυση αγοράς	6
4.	Ανάλυση της Ελληνικής αγοράς.....	8
5.	Κυβερνοεπιθέσεις	10
5.1.	Τα είδη των Κυβερνοεπιθέσεων	10
6.	Κυβερνοασφάλεια.....	27
7.	Πρόληψη.....	28
8.	Αντιμετώπιση	37
9.	Νομοθετικό πλαίσιο	40
10.	Εκτίμηση Ρίσκου.....	44
10.1.	Τι περιλαμβάνει η Εκτίμηση Κινδύνου	46
10.2.	Προσέγγιση εκτίμησης κινδύνου.....	48
11.	Συμπεράσματα	57
12.	Βιβλιογραφία	58

1. Μεθοδολογία Εργασίας

Η παρούσα εργασία αποτελεί μια έκθεση η οποία βασίζεται σε πληροφορίες που είναι διαθέσιμες από ανοιχτές πηγές όπως άρθρα στα μέσα ενημέρωσης, γνωμοδότηση εμπειρογνομόνων, εκθέσεις πληροφοριών, ανάλυση συμβάντων και εκθέσεις έρευνας για την ασφάλεια που διενεργήθηκαν τα τελευταία χρόνια από τον ENISA, καθώς και στις εκτιμήσεις και στο νομοθετικό πλαίσιο του υπουργείου ψηφιακής διακυβέρνησης της Ελλάδας. Αποτελεί βιβλιογραφική αναφορά για τις κυβερνοεπιθέσεις που έπληξαν τα τελευταία χρόνια τις επιχειρήσεις που δραστηριοποιούνται στον τουρισμό και την κυβερνοασφάλεια η οποία αποτελεί τη μόνη λύση στο πρόβλημα αυτό. Η εκτίμηση ρίσκου που αποδίδεται, αφορά την ποσοτική μέθοδο διεξαγωγής η οποία βασίζεται στην αναγνώριση, στον εντοπισμό, την ανάλυση και την αποτίμηση των επιπτώσεων που μπορεί να προκαλέσει μια απειλή και οδηγεί στον καθορισμό ενός σχεδίου προστασίας λαμβάνοντας μέτρα πρόληψης και αντιμετώπισης.

Λέξεις Κλειδιά: Κυβερνοεπίθεση, κυβερνοασφάλεια, απειλές, κακόβουλο, λογισμικό, Ransomware.

2. Εισαγωγή

Τα τελευταία χρόνια αποτέλεσαν σταθμό για τον ψηφιακό μετασχηματισμό των κρατών, των δημόσιων οργανισμών αλλά και των επιχειρήσεων. Η εμφάνιση της πανδημίας του κορωνοϊού (Covid-19) οδήγησε στην ραγδαία ανάπτυξη και εξέλιξη της ψηφιακής τεχνολογίας σε παγκόσμιο επίπεδο. Σε ολόκληρο τον κόσμο δημόσιοι οργανισμοί, αλλά και επιχειρήσεις μικρές και μεγάλες αναγκάστηκαν να υιοθετήσουν ταχύτατα την απομακρυσμένη εργασία με την χρήση της ψηφιακής τεχνολογίας προκειμένου να προστατεύσουν το προσωπικό τους αλλά και τους πελάτες τους και να παραμείνουν σε λειτουργία οι επιχειρήσεις τους κατά τη διάρκεια των υποχρεωτικών μέτρων που έπρεπε να τηρηθούν κατά την εξάπλωση της πανδημίας με στόχο την επιβράδυνση της εξάπλωσης της πανδημίας. Αυτή η αυξανόμενη χρήση και ανάγκη των ψηφιακών τεχνολογιών, οδήγησε αναπόφευκτα και σε αυξανόμενους κινδύνους για την ψηφιακή ασφάλεια λόγω της αύξησης του ηλεκτρονικού εγκλήματος.

Οι διαδικτυακές εφαρμογές αποτελούν τον πυρήνα του σύγχρονου κυβερνοχώρου. Online τραπεζικές εργασίες, ηλεκτρονικό εμπόριο, κοινωνικά δίκτυα και ηλεκτρονική διακυβέρνηση είναι μερικά μόνο από τα παραδείγματα web εφαρμογών, οι οποίες έχουν πλέον αποκτήσει καθολικότητα στην καθημερινή ψηφιακή δραστηριότητα του ιδιώτη, του πολίτη, της επιχείρησης και του κόσμου.

Οι τεχνολογικές εξελίξεις, η ψηφιακή διακυβέρνηση αλλά και η ευημερία των χωρών μελών της Ευρωπαϊκής Ένωσης, έχουν καταστήσει τα κράτη-μέλη στόχους πληθώρας κυβερνοεπιθέσεων. Από απειλές που προέρχονται από μεμονωμένους εγκληματίες, μέχρι επιθέσεις φερόμενες ως απόρροια ενεργειών τρίτων κρατών, το περιβάλλον κυβερνοαπειλών είναι διαρκώς μεταβαλλόμενο, οδηγώντας σε μια εγγενή αδυναμία άμεσης προστασίας του. Η κατάσταση αυτή οδηγεί στην ανάγκη δημιουργίας μιας στρατηγικής προστασίας των ψηφιακών συστημάτων από τις επιχειρήσεις ώστε να αισθάνονται περισσότερο ασφαλείς κατά τη χρήση τους με την εφαρμογή των απαραίτητων μέτρων. Είναι γεγονός, άλλωστε, ότι όσο περισσότερο η κοινωνία και η οικονομία στηρίζονται στην ψηφιοποίηση διαδικασιών και υπηρεσιών για να εκτελούν την καθημερινή λειτουργία τους τόσο θα αυξάνεται και η επιφάνεια επίθεσης, καθώς με την εξ αποστάσεως χρήση διαφόρων υπηρεσιών, παρουσιάζονται και περισσότερες ευπάθειες στα συστήματα, οι οποίες ως αποτέλεσμα τους αποφέρουν μελλοντικά και σοβαρές επιπτώσεις στην επιχειρησιακή λειτουργία, στα πρόσωπα, στις υποδομές αλλά τα σημαντικότερα είναι η οικονομική και ηθική ζημιά που μπορούν να υποστούν όταν οι επιπτώσεις αφορούν παραβίαση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας δεδομένων.

Οι επιχειρήσεις ανεξαρτήτου κλάδου πρέπει να τηρούν τα απαραίτητα μέτρα προστασίας από κυβερνοεπιθέσεις και στη συνέχεια ανάλογα με τις ανάγκες των υπηρεσιών και των συστημάτων τους να εστιάζουν και να τα θωρακίζουν.

Πολλές επιχειρήσεις προβάλλονται αυτή τη στιγμή στο διαδίκτυο μέσα από ένα δικτυακό τόπο (site), μέσα από σελίδες κοινωνικής δικτύωσης (social media) όπως το facebook, instagram, αλλά και μέσα από ενδιάμεσους γεγονόδες που σημαίνει ότι αφήνουν το ψηφιακό τους αποτύπωμα. Στόχος κυβερνοεπιθέσεων όμως γίνονται όταν μέσα σε όλα αυτά έρχεται να προστεθεί η δυνατότητα διεκπεραίωσης διαδικτυακών συναλλαγών με σκοπό την υποκλοπή ή κρυπτογράφηση των δεδομένων (προσωπικά στοιχεία πελατών) καθώς και η υποψία σύνδεσης με άλλες συσκευές της επιχείρησης

(ενδεχομένως ευπαθή) με σκοπό να αποκτήσουν πρόσβαση στα αρχεία δεδομένων. Τέτοιου είδους επιθέσεων πέρα από τις ζημιές που προαναφέρθηκαν μπορούν να βλάψουν και την φήμη της επιχείρησης και κατ'επέκταση την εμπιστοσύνη των πελατών προς αυτήν, γεγονός που μπορεί να επηρεάσει περισσότερο τη λειτουργία τους.

Ένας κλάδος ευάλωτος στο χώρο των επιχειρήσεων είναι αυτός του τουρισμού ο οποίος περιλαμβάνει επιχειρήσεις όπως τουριστικά γραφεία, ξενοδοχειακές μονάδες, αεροπορικές και ακτοπλοϊκές εταιρείες, κρουαζιέρες, ενοικιαστήρια μέσων μεταφοράς, καθώς και όλες τις λοιπές επιχειρήσεις. Ευάλωτος γιατί καλείται να διαχειριστεί μεγάλο όγκο δεδομένων ατόμων όπως προσωπικά στοιχεία και ευαίσθητες πληροφορίες όπως οι αριθμοί πιστωτικών καρτών καθώς για να μπορέσουν να χρησιμοποιήσουν τις παραπάνω παροχές θα πρέπει να τους να παρέχουν. Το γεγονός αυτό οδηγεί αναπόφευκτα στη δημιουργία στρατηγικών ασφαλείας τόσο από το κράτος στο οποίο ανήκουν οι επιχειρήσεις αυτές όσο και από τις ίδιες τις επιχειρήσεις.

3. Ανάλυση αγοράς

Η Check Point Research (CPR) παρουσίασε παγκόσμια στατιστικά στοιχεία για την αύξηση των επιθέσεων στον κυβερνοχώρο όπως παρατηρήθηκαν το 2021 ανά περιοχή, χώρα και κλάδο. Σε αρκετά υψηλά επίπεδα κινήθηκαν οι κυβερνοεπιθέσεις στις ελληνικές επιχειρήσεις το 2021 με το ποσοστό όμως της αύξησης να είναι χαμηλότερο από εκείνο του ευρωπαϊκού μέσου όρου. Αυτό τουλάχιστον προέκυψε από τα στοιχεία που δημοσιοποίησε το τμήμα έρευνας της Check Point Software, όπου σύμφωνα με αυτά στην Ελλάδα κατά μέσο όρο παρατηρήθηκαν 525 επιθέσεις ανά εβδομάδα σε επιχειρήσεις, δηλαδή 32% περισσότερες σε σχέση με το 2020. Η αύξηση όμως των επιθέσεων σε εταιρικά δίκτυα έφθασε στις 925 την εβδομάδα ανά επιχείρηση και είναι πολύ υψηλότερη παγκοσμίως σε σχέση με πέρυσι, φθάνοντας το ποσοστό 50%, με τους χάκερ να εκμεταλλεύονται το απομακρυσμένο περιβάλλον εργασίας λόγω της καθιέρωσης της απασχόλησης από απόσταση. Όπως αναφέρει η πρόσφατη έρευνα της Check Point, παρότι η πλειονότητα των επιχειρήσεων έχει υιοθετήσει πλήρως την απομακρυσμένη εργασία, υπάρχουν ακόμη πολλά κενά ασφαλείας, τα οποία πρέπει να καλυφθούν ώστε οι συσκευές, τα εταιρικά περιουσιακά στοιχεία και η πρόσβαση σε

αυτά να είναι θωρακισμένα από κυβερνοεπιθέσεις (CNN, 2022; Check Point Research CPR).

Σε επίπεδο περιοχών ωστόσο, το ποσοστό αύξησης των κυβερνοεπιθέσεων διακυμάνθηκε ως εξής:

- Ευρώπη (+68%)
- Βόρεια Αμερική (+61%)
- Λατινική Αμερική (+38%)
- Ασία-Ειρηνικός (+25%)
- Αφρική (+13%)

Ενώ οι τομείς που βρέθηκαν στο στόχαστρο των χάκερ το 2021 παγκοσμίως είναι:

- Εκπαίδευση/Ερευνα (1605 επιθέσεις την εβδομάδα ανά οργανισμό με την αύξηση να είναι της τάξεως του +75%)
- Κυβέρνηση/Ενοπλες δυνάμεις (1136 επιθέσεις και +47%)
- Επικοινωνίες (1079 επιθέσεις και +51%)
- Υπηρεσίες ISP/MSP (1068 επιθέσεις και +67%)
- Υγεία (830 επιθέσεις +71%)

Το ετήσιο παγκόσμιο κόστος του εγκλήματος στον κυβερνοχώρο εκτιμάται ότι θα είναι 10.5 τρισεκατομμύρια δολάρια μέχρι το 2025 σύμφωνα με τους αναλυτές της Cybersecurity Ventures οι οποίοι αξιολογώντας τα ιστορικά οικονομικά κυβερνοεπιθέσεων και το μελλοντικό περιβάλλον απειλών, κλοπές πνευματικής ιδιοκτησίας, κλεμμένα χρήματα και καταστροφή δεδομένων καταλήγουν στο παραπάνω συμπέρασμα, και προβλέπουν ότι το κόστος που σχετίζεται με τα κυβερνοεγκλήματα θα αυξάνεται ετησίως κατά 15% την επόμενη πενταετία.

Η πρόβλεψη του παγκόσμιου κόστους ζημίας στον κυβερνοχώρο έχει ως εξής :

- ❖ 6 τρισεκατομμύρια δολάρια ετησίως
- ❖ 500 δισεκατομμύρια δολάρια το μήνα
- ❖ 115.4 δισεκατομμύρια δολάρια την εβδομάδα
- ❖ 16.4 δισεκατομμύρια δολάρια την ημέρα
- ❖ 684.9 εκατομμύρια δολάρια την ώρα
- ❖ 11.4 εκατομμύρια δολάρια το λεπτό

Ενώ αναμένεται το έγκλημα στον κυβερνοχώρο αναμένεται να είναι έως και 5 φορές πιο επικερδές.

4. Ανάλυση της Ελληνικής αγοράς

Τον Νοέμβριο του 2021, η Ελλάδα βρέθηκε σε μια από τις υψηλότερες θέσεις της λίστας ως προς τον αριθμό των επιθέσεων σε βιομηχανικά συστήματα.

Πιο συγκεκριμένα, σύμφωνα με τα τελευταία στοιχεία της εταιρείας κυβερνοασφάλειας Kaspersky, η Ελλάδα κατατάσσεται στην 5η θέση, με το 32% των βιομηχανικών συστημάτων να έχουν υποστεί κάποιου είδους επίθεση. Στην πρώτη θέση βρίσκεται η Σερβία (39,4%), ακολουθούν η Συρία (36,6%), το Μπαγκλαντές (36,6%) και η Παλαιστίνη (33%), ενώ πίσω από τη χώρα μας βρίσκονται η Βοσνία-Ερζεγοβίνη (31,3%), το Πακιστάν (30,6%) και η Λιβύη (30,6%).

Οι κυβερνοεπιθέσεις σε βιομηχανικούς οργανισμούς θεωρούνται εξαιρετικά επικίνδυνη απειλή, καθώς έχουν τη δυνατότητα να προκαλέσουν μεγάλες υλικές απώλειες και να οδηγήσουν σε διακοπή του κύκλου παραγωγής ολόκληρου του συστήματος. Επιπλέον, λόγω των εξαιρετικά ευαίσθητων πληροφοριών που διαθέτουν οι βιομηχανικοί οργανισμοί, αποτελούν συνήθως ελκυστικό στόχο για τους επιτιθέμενους.

Σύμφωνα με τα τελευταία ευρήματα της Kaspersky, ο μεγαλύτερος αριθμός απειλών τον Νοέμβριο προήλθαν από το Διαδίκτυο, το οποίο έχει γίνει η κύρια πηγή μόλυνσης για τα βιομηχανικά συστήματα με την πάροδο των ετών με ποσοστό 6,48%, ακολουθούμενη από το email με 4,66%, τις φορητές συσκευές με 1,68% και τους φακέλους δικτύου με 0,28%.

«Οι επιθέσεις σε βιομηχανικά συστήματα είναι μια πολύ σοβαρή απειλή που επιφέρει επικίνδυνες και εκτεταμένες συνέπειες. Εκτός από την ανάγκη να δοθεί προσοχή στην ασφάλεια του συστήματος από την αρχή της ενσωμάτωσής του, σημαντικό ρόλο διαδραματίζουν και οι ίδιοι οι εργαζόμενοι στην αποτροπή των επιθέσεων. Συγκεκριμένα, μία από τις τακτικές των εγκληματιών του κυβερνοχώρου είναι να επιτίθενται σε βιομηχανικά συστήματα κυρίως μέσω των εργαζομένων, επομένως η επαρκής εκπαίδευση είναι ένας από τους βασικούς αμυντικούς μηχανισμούς», δήλωσε ο Βασίλης Βλάχος, Channel Manager της Kaspersky για Ελλάδα και Κύπρο.

Ένα από τα θέματα που φάνηκε να διαφεύγει της προσοχής πολλών επιχειρήσεων ήταν η εφαρμογή πολιτικών για την ασφάλεια των πληροφοριών (information security policies), για την προστασία των προσωπικών δεδομένων και την αποτροπή κυβερνοεπιθέσεων τη στιγμή που οι κυβερνοαπειλές αποτελούν καθημερινό φαινόμενο.

Στην πρόσφατη έρευνα της Kaspersky φάνηκε πως πολλές ελληνικές επιχειρήσεις αλλά και οι εργαζόμενοι τους αγνοούν βασικά βήματα για την επίτευξη της απόλυτης προστασίας των δεδομένων των επιχειρήσεων τους (Kaspersky, 2021).

Έτσι, οι περισσότεροι από αυτούς (57,9%) χρησιμοποιούν προσωπικά κανάλια κοινωνικής δικτύωσης και εφαρμογές (social media, mail, chat) για εσωτερική επικοινωνία με συναδέλφους και τον διαμοιρασμό επαγγελματικών αρχείων. Ενώ ένα ποσοστό 80% κάνει προσωπική χρήση του εξοπλισμού μέσω του οποίου εργάζεται εξ αποστάσεως, για ψυχαγωγία, social media και streaming ταινιών, μουσικής και video. Τα παραπάνω καθιστούν ευάλωτα τα ευαίσθητα δεδομένα μικρών και μεγάλων επιχειρήσεων, αυξάνοντας σημαντικά τις πιθανότητες να πέσουν θύματα κυβερνοεγκλημάτων.

Παράλληλα ένα σημαντικό ποσοστό δεν έχει εγκατεστημένο στον υπολογιστή του ούτε VPN (26%) ούτε λογισμικό antivirus (14%), αφήνοντας έτσι εκτεθειμένες ευαίσθητες πληροφορίες σε δυνητικά επιβλαβείς ιούς υπολογιστών, κακόβουλο λογισμικό και άλλες κυβερνοαπειλές.

Μεγάλο είναι επίσης το ποσοστό των εργαζομένων (28,4%) που επιτρέπουν σε άλλα μέλη της οικογένειάς τους να αποκτούν πρόσβαση και να χρησιμοποιούν τον επαγγελματικό τους εξοπλισμό. Έτσι, ο υπολογιστής που οι εργαζόμενοι χρησιμοποιούν για πρόσβαση και διαμοιρασμό επαγγελματικών αρχείων καθίσταται επιρρεπής σε διαφόρων ειδών απειλές του κυβερνοχώρου.

Η πλειονότητα των επιχειρήσεων επίσης έχει παραβλέψει τη σημασία της ενημέρωσης και της εκπαίδευσης σχετικά με την τηλεργασία και τους κινδύνους που ενέχει από επιθέσεις στον διαδίκτυο, με το 75% των Ελλήνων εργαζομένων να δηλώνει πως δεν έχει λάβει σχετική εκπαίδευση από την επιχείρηση που εργάζεται αναφορικά με την ασφάλεια και την προστασία από κυβερνοεπιθέσεις κατά τη διάρκεια της τηλεργασίας.

5. Κυβερνοεπιθέσεις

Ένας ορισμός που μπορεί να δοθεί για την έννοια της κυβερνοεπίθεσης είναι ότι είναι οι όποιες παράνομες προσπάθειες πρόσβασης στις πληροφορίες μιας επιχείρησης, ενός οργανισμού αλλά και μεμονωμένων ατόμων με στόχο να διαταράξουν την ομαλή λειτουργία τους. Οι επιθέσεις μπορεί να σχετίζονται με εγκληματική πράξη, κατασκοπία, αντιπάλους ή και με «χάκερ» που δοκιμάζουν τις δυνατότητές τους (ερασιτέχνες). Οι επιχειρήσεις δέχονται καθημερινά εκατομμύρια επιθέσεις, πολλές από τις οποίες καταφέρνουν να σπάσουν την όποια προστασία των συστημάτων τους αν υπάρχει και να προκαλέσουν ζημιές τόσο οικονομικές όσο και λειτουργικές.

5.1. Τα είδη των Κυβερνοεπιθέσεων

Κάθε φορά που μια νέα συσκευή συνδέεται στο διαδίκτυο ή με άλλες συσκευές, η λεγόμενη «επιφάνεια επίθεσης» αυξάνεται. Η εκθετική ανάπτυξη του διαδικτύου των πραγμάτων, του υπολογιστικού νέφους, των μαζικών δεδομένων και η ψηφιοποίηση της τεχνολογίας συνοδεύονται με την αυξημένη έκθεση των ευάλωτων σημείων, που παρέχει σε κακόβουλους παράγοντες τη δυνατότητα να στοχεύουν ολόένα και σε περισσότερα θύματα.

Σύμφωνα με την ετήσια έκθεση (για το χρονικό διάστημα Απριλίου 2020 έως τον Ιούλιο 2021) που εξέδωσε ο ENISA (ENISA Threat Landscape -ETL) (ENISA, 2021), για την κατάσταση του τοπίου απειλών και για την ασφάλεια στον κυβερνοχώρο, προσδιορίζει τις κύριες απειλές, τις τάσεις που παρατηρούνται σε σχέση με τις απειλές, τις απειλές που δρουν άμεσα και τις τεχνικές επίθεσης, και επίσης περιγράφει σχετικά μέτρα περιορισμού.

Κατά την περίοδο αναφοράς, οι κύριες απειλές που εντοπίστηκαν είναι οι εξής:

- Κακόβουλο λογισμικό
- Ransomware
- Cryptojacking
- Απειλές που σχετίζονται με το ηλεκτρονικό ταχυδρομείο
- Απειλές κατά των δεδομένων

- Απειλές κατά της διαθεσιμότητας και της ακεραιότητας
- Παραπληροφόρηση
- Μη κακόβουλες απειλές
- Επιθέσεις εφοδιαστικής αλυσίδας

Η ποικιλία που φαίνεται να υπάρχει στα είδη των επιθέσεων σε συνδυασμό με την πολυπλοκότητά τους δυσχεραίνει εξαιρετικά την παρακολούθηση των εξελίξεων (ENISA, 2021, p. 5).

Το Ransomware έχει αξιολογηθεί ως η κύρια απειλή για το 2020-2021. Οι εγκληματίες του κυβερνοχώρου παρακινούνται όλο και περισσότερο από τη δημιουργία εσόδων από τις δραστηριότητές τους με τη χρήση αυτού.

Ο όγκος των μολύνσεων από κρυπτογράφηση έφθασε σε ιστορικό υψηλό το πρώτο τρίμηνο του 2021, σε σύγκριση με τα τελευταία χρόνια. Το οικονομικό κέρδος που σχετίζεται με το cryptojacking παρότρυνε τους φορείς απειλών στο να πραγματοποιήσουν τέτοιες επιθέσεις και έτσι το κρυπτονομίσματα φαίνεται να παραμένει η πιο κοινή μέθοδος πληρωμής για τους παράγοντες απειλών.

Η μείωση του κακόβουλου λογισμικού που παρατηρήθηκε το 2020 συνεχίζεται και το 2021.

Το 2020 και το 2021, παρατηρήθηκε όμως και μια έξαρση των μη κακόβουλων περιστατικών, καθώς η πανδημία COVID-19 έγινε πολλαπλασιαστής για ανθρώπινα λάθη και εσφαλμένες διαμορφώσεις συστήματος, μέχρι το σημείο που οι περισσότερες από τις παραβιάσεις του 2020 προκλήθηκαν από σφάλματα.

Όπως φαίνεται και στην παρακάτω εικόνα (Εικόνα 1) τα διάφορα είδη απειλών μπορούν να ταξινομηθούν είτε σύμφωνα με το τι προκαλούν στα δεδομένα (κοινοποίηση, τροποποίηση, καταστροφή ή άρνηση πρόσβασης) είτε σύμφωνα με τις βασικές αρχές ασφάλειας των πληροφοριών που παραβιάζουν (Διαθεσιμότητα, Εμπιστευτικότητα, Ακεραιότητα) (Ευρωπαϊκή Ένωση, 2020, σ. 12).



Εικόνα 1- Αρχές που αντιμετωπίζουν κίνδυνο

Ransomware: ή λυτρισμικό, κρυπτογραφεί δεδομένα, εμποδίζοντας την πρόσβαση των αυθεντικών χρηστών στα αρχεία τους μέχρι να καταβάλουν το χρηματικό ποσό που τους ζητάτε (τα λύτρα δηλαδή), συνήθως σε κρυπτονόμισμα. Σύμφωνα με την Ευρωπαϊκή Επιτροπή, οι επιθέσεις με λυτρισμικό είναι οι συνηθέστερες σε όλους τους τομείς, ενώ τα είδη λυτρισμικού γνώρισαν πρωτοφανή αύξηση τα τελευταία χρόνια.

Malware: ή κακόβουλο λογισμικό, σχεδιάζεται με σκοπό να προκαλέσει βλάβες σε συσκευές ή δίκτυα. Μπορεί να περιλαμβάνει ιούς, λογισμικά σκουλήκια, δούρειους ίππους, λυτρισμικό, προγράμματα διαφημίσεων και κατασκοπευτικό λογισμικό. Μπορεί να είναι λογισμικό ή υλικολογισμικό που προορίζεται να εκτελέσει μια μη εξουσιοδοτημένη διαδικασία που θα έχει αρνητικές επιπτώσεις για την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα ενός συστήματος. Η απειλή από κακόβουλο λογισμικό κατατάσσεται σταθερά σε υψηλή θέση εδώ και πολλά χρόνια, παρά την μείωση που καταγράφηκε κατά την τελευταία χρονιά σύμφωνα με την αναφορά του ETL 2021 και η οποία φαίνεται να οφείλεται στη χρήση νέων τεχνικών αντιμετώπισης και επιβολής νόμων περί των σχετικών απειλών.

Cryptojacking: ή κρυφή cryptomining, η επίθεση αυτού του είδους λειτουργεί όπως το malware, ένας εγκληματίας εγκαθιστά το κακόβουλο λογισμικό στην συσκευή του θύματος και χρησιμοποιεί κρυφά τους πόρους του συστήματος για τη δημιουργία

κρυπτονομισμάτων. Με τον πολλαπλασιασμό των κρυπτονομισμάτων και την ολοένα αυξανόμενη απορρόφησή τους από στο ευρύτερο κοινό, έχει παρατηρηθεί αύξηση των αντίστοιχων περιστατικών κυβερνοασφάλειας. Ενώ είναι μια απειλή η οποία μπορεί να μολύνει όλους τους τύπους συσκευών, διακομιστές δικτύου και προγράμματα περιήγησης ιστού.

Διαρροή δεδομένων: Είναι η απελευθέρωση, ακούσια απώλεια ή έκθεση ευαίσθητων, εμπιστευτικών ή προστατευμένων δεδομένων σε μη αξιόπιστους χρήστες. Οι παραβιάσεις δεδομένων μπορεί να προκύψουν ως αποτέλεσμα κυβερνοεπίθεσης. Η απειλή είναι υψηλή, καθώς η πρόσβαση στα δεδομένα είναι

πρωταρχικός στόχος για τους κυβερνοεγκληματίες για πολλούς λόγους, όπως εκβιασμός, λύτρα, δυσφήμιση, παραπληροφόρηση κλπ.

Απειλές κατά της διαθεσιμότητας και της ακεραιότητας: Η διαθεσιμότητα και η ακεραιότητα είναι στόχος πολλών απειλών και επιθέσεων, μεταξύ των οποίων και οι επιθέσεις άρνησης υπηρεσίας. Οι επιθέσεις κατανεμημένης άρνησης υπηρεσίας (Distributed Denial of Service – DDoS), και οι επιθέσεις Ιστού ξεχωρίζουν καθώς σχετίζονται αυστηρά με επιθέσεις που βασίζονται στον ιστό, το DDoS είναι μία από τις πιο κρίσιμες απειλές για συστήματα πληροφορικής, αφού στοχεύει τη διαθεσιμότητά τους, εξαντλώντας τους πόρους, κατακλύζοντάς τους με περισσότερα αιτήματα από όσα μπορούν να διαχειριστούν προκαλώντας μειώσεις στην απόδοση, απώλεια δεδομένων και διακοπές υπηρεσιών.

Λόγω του COVID-19, οι κακόβουλοι παράγοντες στοχεύουν όλο και περισσότερο τα οικιακά δίκτυα ως αφετηρία για πιο περίπλοκες επιθέσεις, κάνοντας το DNS όχι μόνο φορέα επίθεσης αλλά και στόχο επιθέσεων.

Το λογισμικό τηλεδιάσκεψης και η απομακρυσμένη συνεργασία, όπως το Microsoft Teams, Skype ή Zoom και άλλες πλατφόρμες σύσκεψης γνώρισαν κορύφωση χρήσης. Ωστόσο, η χρήση τους συνοδεύεται από ορισμένες ανησυχίες. Πρώτον, οι πλατφόρμες αυτές συχνά βασίζονται σε αδύναμες επικοινωνίες, ευάλωτες σε πιθανές επιθέσεις και δεύτερον, η υψηλή τους ζήτηση ως προς το εύρος ζώνης μπορεί να επηρεάσει αρνητικά το δίκτυο.

Επιπλέον, η μαζική υιοθέτηση της τηλεργασίας αύξησε τον κίνδυνο για τις επιχειρήσεις να γίνουν στόχος επιθέσεων DDoS. Στο πλαίσιο αυτό, ο αντίκτυπος των επιθέσεων

DDoS εναντίον υπηρεσιών απομακρυσμένης σύνδεσης (πχ VPN, RDP κ.α) αυξήθηκαν με την πανδημία.

Οι επιθέσεις DDoS αυξήθηκαν επίσης σημαντικά το 2020 λόγω του COVID-19 με περισσότερες από 10 εκατομμύρια επιθέσεις (1,6 εκατομμύρια περισσότερο από το 2019) και αύξηση 22% στη συχνότητα επιθέσεων τους τελευταίους 6 μήνες του 2020. Τον Μάρτιο του 2020, καταγράφηκαν περισσότερες από 800.000 επιθέσεις DDoS, κατά μέσο όρο 839.083 επιθέσεις ανά μήνα κατά τη διάρκεια του έτους και περισσότερες από 929.000 επιθέσεις τον Μάιο του 2020. Ενώ οι παγκόσμιες επιθέσεις τύπου DDoS αυξήθηκαν κατά 125%. (ENISA, 2021, p. 69)

Social engineering: Κοινωνική μηχανική ένα σύνολο απειλών όπου άρχισαν να αυξάνονται από το 2017. Οι χρήστες μπορούν να χειραγωγηθούν ώστε να εκτελέσουν εν αγνοία τους μια ενέργεια ή να καταχωρίσουν εμπιστευτικές πληροφορίες όπως αριθμό ταυτότητας, ΑΦΜ, αριθμούς λογαριασμών τραπεζής, και άλλων κωδικών πρόσβασης.

Αυτή η τεχνική μπορεί να χρησιμοποιηθεί για κλοπή δεδομένων ή και χρημάτων και είναι μια από τις δημοφιλέστερες μορφές κυβερνοεπίθεσης όπου μέσω emails, τα οποία πολλές φορές φαίνεται ότι προέρχονται από συνάδελφο ή συνεργάτη ενώ στη πραγματικότητα αποτελούν τον Δούρειο Ίππο μέσω του οποίου οι χάκερς μπορούν και εγκαθιστούν το κακόβουλο λογισμικό. Πρόκειται για ένα λάθος που εύκολα μπορεί να γίνει και να οδηγήσει στο κλείσιμο μιας επιχείρησής και συνεπώς και σε μεγάλες οικονομικές απώλειες με ότι μπορεί αυτό να συνεπάγεται. Μερικές από τις τεχνικές κοινωνικής μηχανικής αναφέρονται παρακάτω:

Phishing: Μια επίθεση ηλεκτρονικού ψαρέματος όπως λέγεται, είναι η επικοινωνία μέσω ηλεκτρονικής αλληλογραφίας (email), η οποία προέρχεται φαινομενικά από μια νόμιμη πηγή και προτρέπει τους χρήστες να αποκαλύψουν προσωπικά ή εταιρικά στοιχεία ή να ακολουθήσουν κάποιο σύνδεσμο σε άλλο ιστότοπο, με απώτερο σκοπό την κλοπή δεδομένων ή την εγκατάσταση κακόβουλου λογισμικού.

Spear phishing: Πρόκειται για μια πιο στοχευμένη έκδοση της απάτης phishing με την οποία ένας εισβολέας επιλέγει συγκεκριμένα άτομα ή επιχειρήσεις. Στη συνέχεια προσαρμόζουν τα μηνύματά τους με βάση τα χαρακτηριστικά, τις θέσεις εργασίας και τις επαφές που ανήκουν στα θύματά τους για να κάνουν την επίθεσή τους λιγότερο εμφανή. Το phishing των Spear απαιτεί πολύ περισσότερη προσπάθεια εκ μέρους του

δράστη και μπορεί να χρειαστούν εβδομάδες και μήνες για να αποσυρθούν. Είναι πολύ πιο δύσκολο να εντοπιστούν και έχουν καλύτερα ποσοστά επιτυχίας αν γίνουν με επιδεξιότητα.

Ένα spear phishing scenario μπορεί να περιλαμβάνει έναν εισβολέα ο οποίος, με τον ίδιο τρόπο που μιμείται έναν σύμβουλο πληροφορικής ενός οργανισμού, στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου σε έναν ή περισσότερους υπαλλήλους. Είναι διατυπωμένο και υπογεγραμμένο ακριβώς όπως θα έκανε ένας σύμβουλος, εξαπατώντας έτσι τους παραλήπτες του, ώστε να πιστεύουν ότι είναι ένα αυθεντικό μήνυμα. Το μήνυμα ζητά από τους παραλήπτες να αλλάξουν τον κωδικό πρόσβασής τους και τους παρέχει έναν σύνδεσμο που τους ανακατευθύνει σε μια κακόβουλη σελίδα όπου ο εισβολέας συλλαμβάνει τώρα τα διαπιστευτήριά τους.

Smising: Είναι μια ακόμα επίθεση ηλεκτρονικού ψαρέματος αυτή τη φορά όμως όχι μέσω email αλλά μέσω SMS (Short message service). Επιτήδειοι, υποδουόμενοι κάποια γνωστή εταιρεία, αποστέλλουν ένα μήνυμα με ψευδή εννοείται περιεχόμενο κειμένου στα υποψήφια θύματα τους παραπέμποντας τους να πατήσουν έναν σύνδεσμο, ο οποίος εάν πατηθεί οδηγεί το θύμα προς έναν ψεύτικο ιστότοπο (ιστότοπος ηλεκτρονικού ψαρέματος) σχεδόν πανομοιότυπο με τη νόμιμη έκδοση του όπου προτρέπουν το ανυποψίαστο θύμα να εισάγει τα τρέχοντα διαπιστευτήρια και τον νέο κωδικό πρόσβασής του. Με την υποβολή της φόρμας, οι πληροφορίες υποκλέπτονται.

Αντίστοιχα μηνύματα χρησιμοποιούνται και στα IM (Instant messages) όλο και περισσότερο τα τελευταία χρόνια όπου εκεί χρησιμοποιούν έντονα το αίσθημα του φόβου παροτρύνοντας πάντα τα θύματα να κάνουν κλικ σε κάποιο σύνδεσμο.

Pharming: είναι είδος επίθεσης που στόχο έχει την ανακατεύθυνση του προγράμματος περιήγησης (browser) σε άλλες ψεύτικες ιστοσελίδες με απώτερο σκοπό την κλοπή δεδομένων ή την εγκατάσταση κακόβουλου λογισμικού. Σε περίπτωση επιτυχημένης επίθεσης Pharming, ακόμη και αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου που θέλει να επισκεφτεί, θεωρώντας πως βρίσκεται σε ασφαλή χώρο, η ανακατεύθυνση θα τον οδηγεί πάντα σε ψεύτικη.

Baiting: Όπως υποδηλώνει και το όνομά του, οι επιθέσεις Baiting χρησιμοποιούν μια ψευδή υπόσχεση για να κινήσουν την περιέργεια του θύματος. Προσελκύουν τους χρήστες σε μια παγίδα που κλέβει τις προσωπικές τους πληροφορίες ή μολύνει τα συστήματά τους με κακόβουλο λογισμικό.

Η πιο επικίνδυνη μορφή Baiting χρησιμοποιεί φυσικά μέσα για την διανομή κακόβουλου λογισμικού. Για παράδειγμα, οι επιτιθέμενοι στέλνουν το δόλωμα (flash drivers με μολυσμένο λογισμικό) σε εμφανείς περιοχές, όπου τα πιθανά θύματα είναι βέβαιο ότι θα το δουν (πχ σε κοινόχρηστους χώρους μιας εταιρείας που έχει στοχοποιηθεί). Το δόλωμα θα έχει κάτι που συνήθως τραβάει την προσοχή των θυμάτων, όπως μια ετικέτα που αναγράφει “λίστα μισθοδοσίας της εταιρείας”. Τα θύματα παίρνουν το δόλωμα από περιέργεια και το εισάγουν σε έναν υπολογιστή εργασίας ή στο σπίτι, με αποτέλεσμα την αυτόματη εγκατάσταση κακόβουλου λογισμικού στο σύστημα.

Βέβαια, μια επίθεση baiting δεν είναι απαραίτητο να πραγματοποιηθεί μόνο σε φυσικό χώρο. Υπάρχουν και τα Online baiting forms που αποτελούνται από δελεαστικές διαφημίσεις που οδηγούν σε κακόβουλους ιστότοπους ή που ενθαρρύνουν τους χρήστες να κατεβάσουν μια εφαρμογή που έχει μολυνθεί από κακόβουλο λογισμικό.

Scareware: Είναι ο βομβαρδισμός των θυμάτων με ψευδείς συναγερμούς και πλασματικές απειλές. Οι χρήστες παραπλανούνται για να σκεφτούν ότι το σύστημά τους είναι μολυσμένο από κακόβουλο λογισμικό, προτρέποντάς τους να εγκαταστήσουν λογισμικό που δεν έχει κανένα πραγματικό όφελος. Το Scareware αναφέρεται επίσης ως λογισμικό εξαπάτησης, rogue scanner software ή fraudware.

Ένα κοινό παράδειγμα scareware είναι τα νόμιμα εμφανιζόμενα αναδυόμενα banners που εμφανίζονται στο πρόγραμμα περιήγησής σας κατά το σερφάρισμα, παρουσιάζοντας ένα τέτοιο κείμενο “Ο υπολογιστής σας μπορεί να μολυνθεί από επιβλαβή προγράμματα spyware.” Προσφέρεται είτε να εγκαταστήσει για εσάς το απαραίτητο εργαλείο (συχνά μολυσμένο με κακόβουλο λογισμικό) είτε θα σας κατευθύνει σε μια κακόβουλη τοποθεσία όπου ο υπολογιστής σας θα μολυνθεί. Το Scareware διανέμεται επίσης μέσω spam email.

Τα πιο ειδικά όμως είδη απειλών είναι οι προηγμένες συνεχείς απειλές (advanced persistent threats, APTs). Πρόκειται για πολύπλοκες επιθέσεις που περιλαμβάνουν μακρόχρονη παρακολούθηση και κλοπή δεδομένων και σε ορισμένες περιπτώσεις έχουν σκοπό και την πρόκληση μεγάλων ζημιών.

Το ζητούμενο στην περίπτωση τους είναι να μην εντοπιστούν για όσο το δυνατόν μεγαλύτερο διάστημα. Οι απειλές αυτές συχνά συνδέονται με δράση κρατικών

υπηρεσιών και οργανισμών και έχουν στόχο ιδιαίτερα ευαίσθητους τομείς όπως η τεχνολογία, η άμυνα και οι υποδομές ζωτικής σημασίας.

Η κυβερνοκατασκοπεία θεωρείται πως αντιπροσωπεύει τουλάχιστον το ένα τέταρτο του συνόλου των κυβερνοπεριστατικών και έχει το μεγαλύτερο κόστος.

Λογισμικά κακόβουλης λειτουργίας:

Καθώς η χρήση της εξ αποστάσεως εργασίας αυξάνεται πως θα μπορούσαν οι συσκευές smartphone να παραμείνουν ασφαλείς. Το 2020, τα ψεύτικα ad block, που αναφέρονται επίσης και ως adware, αυξήθηκαν για τις συσκευές Android. Αυτός ο τύπος κακόβουλης εφαρμογής δελεάζει τον χρήστη με δυνατότητες "προσθήκη αποκλεισμού", και ζητά εκτεταμένες άδειες στο λειτουργικό σύστημα. Έπειτα ξεκινά να χρησιμοποιεί κάθε είδους ειδοποιήσεις και ανακατευθύνσεις του προγράμματος περιήγησης.

Αντίστοιχο κακόβουλο λογισμικού αυτού του είδους είναι και το hiddenAds, κακόβουλο λογισμικό πάλι για συσκευές Android. Το 2020, ο εντοπισμός αυτού του τύπου κακόβουλου λογισμικού αυξήθηκε από 280.000 σε 700.000 σε σύγκριση με 2019. Το μεγάλο ποσοστό adware σε κακόβουλο λογισμικό για κινητά συνεχίζεται καθ' όλη τη διάρκεια του 2021, όπου όπως έδειξε έφτασε στο 45%.

Τα λογισμικά κακόβουλης λειτουργίας για τις συσκευές Android σχεδιάστηκαν με σκοπό να υποκλέβουν προσωπικές πληροφορίες όπως τη λίστα επαφών του χρήστη, τη τοποθεσία του, κωδικούς πρόσβασης καθώς και παρακολουθούν συνομιλίες τους στα social media. Παράλληλα μπορούν να κάνουν τη συσκευή να στέλνει μηνύματα SMS με μεγάλο κόστος καθώς και να οδηγούνται σε λήψη εφαρμογών άθελά τους. Οι ενδείξεις λογισμικού κακόβουλης λειτουργίας είναι οι εξής:

- Αργή λειτουργία του τηλεφώνου – φόρτωση εφαρμογών
- Γρήγορη αποφόρτιση απ' ότι συνήθως
- Εφαρμογές που δεν γνωρίζουμε
- Αυξημένη χρήση δεδομένων
- Υψηλότεροι λογαριασμοί

Το κακόβουλο λογισμικό Mobile banking παρουσίασε επίσης αύξηση το 2020.

Το κακόβουλο λογισμικό προσπαθεί να κλέψει διαπιστευτήρια ηλεκτρονικής τραπεζικής και πληρωμής και πληροφορίες, εμφανίζοντας πλαστές οθόνες σύνδεσης.

Το κακόβουλο λογισμικό είναι τότε ικανό να εκτελεί συναλλαγές σε λογαριασμούς με χρηματοπιστωτικά ιδρύματα. Οι πιο κοινές κακόβουλες τραπεζικές εφαρμογές το 2021 περιλαμβάνουν τα Ghimob, Eventbot και Thiefbot. Άλλα κοινά κακόβουλα προγράμματα είναι τα Blackrock, Wroba και TrickMO. Τον Μάιο του 2021, οι μολύνσεις Flubot αυξήθηκαν χρησιμοποιώντας SMS ως μηχανισμό διάδοσης. Η αύξηση παρατηρήθηκε κυρίως σε Ευρώπη και Ηνωμένο Βασίλειο. Στα περισσότερα μηνύματα παρίσταναν ότι ήταν, είτε κρατικές υπηρεσίες (σχετικές με τον COVID-19), είτε επώνυμες εταιρείες παράδοσης δεμάτων, για να παρασύρουν τα θύματα τους να εγκαταστήσουν μια κακόβουλη εφαρμογή.

Οι διαδικτυακές επιθέσεις αποτελούν πλέον την πιο σύγχρονη μορφή απάτης, με τους διαδικτυακούς απατεώνες να εφευρίσκουν συνεχώς νέες μεθόδους για να προσεγγίζουν όλους τους κλάδους των επιχειρήσεων.

Σύμφωνα με στοιχεία της έρευνας “The Hotel Hijackers” που είχε παρουσιάσει η εταιρεία Panda Security πριν 5 χρόνια στο στόχαστρο των κυβερνοεπιθέσεων είχε τεθεί και ο ξενοδοχειακός κλάδος και κατ’ επέκταση όλες οι εταιρείες που προσφέρουν υπηρεσίες στα ξενοδοχεία.

Οι εταιρείες φιλοξενίας εξαρτώνται σε μεγάλο βαθμό από τις ψηφιακές τεχνολογίες για να χειριστούν κρίσιμες λειτουργίες για τις επιχειρήσεις, συμπεριλαμβανομένων της διεκπεραίωσης πληρωμών, της λογιστικής και της κράτησης τραπεζιών/ δωματίων. Στα ξενοδοχεία, αυτή η χρήση της τεχνολογίας επεκτείνεται ακόμη και στην παροχή πρόσβασης με κάρτα-κλειδί σε δωμάτια που χρησιμοποιούν τεχνολογία ελεγχόμενη από υπολογιστή.

Τα συστήματα υπολογιστών που χρησιμοποιούνται τόσο από ξενοδοχειακές μονάδες όσο και από εστιατόρια, μπαρ και άλλες τουριστικές επιχειρήσεις, όπως τα συστήματα POS, και τα δίκτυα στα οποία είναι συνδεδεμένα φαίνεται να είναι ευάλωτα σε επιθέσεις ransomware με τους φορείς απειλών συχνά να θεωρούν τις παραπάνω επιχειρήσεις ως εύκολη λεία για το κλείδωμα των συστημάτων τους με κακόβουλο λογισμικό οδηγώντας τις σε μεγάλες πληρωμές λύτρων. Όσο αυξάνεται η χρήση των

POS από τους πελάτες στο κλάδο του τουρισμού και όχι μόνο, τόσο αυξάνεται και ο κίνδυνος να παραβιαστούν από κάποιο κακόβουλο λογισμικό τα δεδομένα των πιστωτικών και χρεωστικών καρτών και να περάσουν τα στοιχεία υπό την κατοχή μη εξουσιοδοτημένων χρηστών.

Ο τεράστιος όγκος δεδομένων και τα μεγάλα δίκτυα που έχουν οι ξενοδοχειακές μονάδες φαίνεται να αποτελούν κύρια πηγή εσόδων για τους διαδικτυακούς απατεώνες που έχουν χτυπήσει κορυφαίες μονάδες παγκοσμίως όπως τα Hilton, Marriott, Mandarin Oriental, Hyatt, Sheraton, Westin, κ.α.

Έτσι οι μεγαλύτερες απειλές που έχουν να αντιμετωπίσουν σήμερα οι επιχειρήσεις είναι η παραβίαση και υποκλοπή δεδομένων τόσο των πελατών όσο και των εργαζομένων, πληροφορίες όπως ιδιωτικές δραστηριότητες, χρόνος παραμονής σε ένα κατάλυμα, διαρροή προσωπικών δεδομένων ή και κλοπή υλικού από ψηφιακές κάμερες ασφαλείας.

Εκτός δηλαδή από τα προφανώς ευαίσθητα προσωπικά δεδομένα, υπάρχουν και περαιτέρω πληροφορίες στον τουριστικό κλάδο που πρέπει να αντιμετωπίζονται με προσοχή. Στον κλάδο της φιλοξενίας, συλλέγονται και διατηρούνται δεδομένα που σχετίζονται με ειδικές προτιμήσεις και συμπεριφορές επισκεπτών, προκειμένου να προαχθεί η ικανοποίηση και η αφοσίωση των πελατών μέσω ειδικών υπηρεσιών. Αυτά τα προσωπικά δεδομένα περιλαμβάνουν, για παράδειγμα, εάν ένας επισκέπτης προτιμά μια vegan διατροφή ή απέχει από την κατανάλωση χοιρινού ή βοείου κρέατος για θρησκευτικούς λόγους. Επίσης, η προτίμηση για ένα δωμάτιο καπνιστών θα επιτρέψει αναπόφευκτα συμπεράσματα για την υγεία ενός ατόμου (Thomas, 2021).

Ένας ακόμα μεγάλος κίνδυνος είναι η μερική ή ολική κατάρρευση των συστημάτων διαχείρισης των κρατήσεων όπου ο υπεύθυνος μιας μονάδας δεν θα μπορεί για παράδειγμα να έχει πρόσβαση στα συστήματα του π.χ για τα αναμενόμενα check in, check out, πληρωμές, κρατήσεις κ.α.

Μεταξύ των μεγάλων απειλών που αντιμετωπίζουν οι ξενοδόχοι είναι και η υποβάθμιση συστημάτων υπολογιστών μέσω καταστροφής αρχείων, αλλοίωσης ή και κρυπτογράφησης των αρχείων αυτών, με στόχο να ενδώσουν και να καταθέσουν τα ζητούμενα λύτρα στους κυβερνοεγκληματίες (χάκερ).

Τα παραδείγματα που ακολουθούν είναι από μεγάλες ξενοδοχειακές μονάδες οι οποίες έπεσαν θύματα κυβερνοαπειλών τα τελευταία χρόνια.

Marriott Hotel

Η παραβίαση της αλυσίδας ξενοδοχείων Marriott ήταν τεράστια τόσο λόγω του όγκου των δεδομένων που εκτέθηκαν (στοιχεία 500 εκατομμυρίων πελατών) όσο και λόγω της ευαισθησίας των πληροφοριών αυτών. Οι χάκερς παραβίασαν τα συστήματα κράτησης των ξενοδοχείων Starwood, τα οποία αγοράστηκαν από τη Marriott το 2016. Το σύστημα Starwood περιλαμβάνει τα ξενοδοχεία W Hotels, St. Regis, Sheraton Hotels & Resorts, Westin Hotels & Resorts, Element Hotels, Aloft Hotels, Le Méridien Hotels & Resorts, Four Points by Sheraton και Design Hotels.

Οι εγκληματίες του κυβερνοχώρου είχαν επιτεθεί στο σύστημα Starwood κατά το έτος 2014 στην ουσία 4 χρόνια πριν γίνει αντιληπτή η επίθεση από την επιχείρηση και οι πληροφορίες που διέρρευσαν για 327 εκατ. πελάτες περιλάμβαναν συνδυασμό κάποιου ονόματος, ηλεκτρονικού ταχυδρομείου, τηλεφωνικού αριθμού, αριθμού διαβατηρίου, αριθμού κράτησης, ημερομηνίας γέννησης, φύλου, αλλά και πληροφορίες άφιξης-αναχώρησης, καθώς και λοιπά στοιχεία επικοινωνίας για το διάστημα διαμονής μεταξύ 2014 και 2018. Ενώ κάποια ακόμη από τα δεδομένα που χάθηκαν περιλαμβάνουν στοιχεία πιστωτικών καρτών και ημερομηνίες λήξης αυτών.

Μετά από εκτεταμένη έρευνα, η Αρχή Προστασίας Δεδομένων του Ηνωμένου Βασιλείου (ICO) ανακοίνωσε το πρόστιμο ύψους 99 εκατομμυρίων βρετανικών λιρών (περίπου 117 εκατ. ευρώ) στη Marriott International για παραβάσεις του Κανονισμού Γενικής Προστασίας Δεδομένων (GDPR) καθώς δεν εντόπισε τις ευπάθειες που προϋπήρχαν και εκτέθηκαν προσωπικά στοιχεία εκατομμυρίων ανθρώπων (Brewster, 2018).

Mandarin Oriental:

Η πολυτελής ξενοδοχειακή μονάδα Mandarin Oriental δέχθηκε επίθεση τον Μάρτιο 2015 με κακόβουλο λογισμικό το οποίο μόλυνε τα τερματικά POS (Point-of-Sale) σε κάποια από τα ξενοδοχεία του ομίλου σε Ευρώπη και σε Αμερική. Το κακόβουλο λογισμικό είχε σχεδιαστεί ειδικά για να επιτεθεί σε αυτούς τους τύπους συστημάτων, επιτρέποντάς τους να αποσπάσουν στοιχεία από χιλιάδες πιστωτικές κάρτες. Αντίστοιχο περιστατικό

συνέβη και στην ξενοδοχειακή μονάδα Trump Hotels όπου δέχθηκαν επιθέσεις σε επτά από τις εγκαταστάσεις τους από τον Μάη 2014 έως τον Ιούνιο 2015. Όπως παραδέχθηκε η εταιρεία, τα στοιχεία πιστωτικών καρτών των πελατών τους κλάπηκαν από μολυσμένα τερματικά POS και υπολογιστές στα εστιατόρια, τα καταστήματα με είδη δώρων και άλλες επιχειρήσεις που λειτουργούν στις εγκαταστάσεις της. Μόλις ένας χρόνος ήταν αρκετός για τους απατεώνες προκειμένου να αποκτήσουν πρόσβαση σε χιλιάδες δεδομένα πελατών. Όπως επίσης και στις μονάδες Hard Rock Las Vegas, Hilton Worldwide, Rosen Hotels & Resorts και Hyatt με το τελευταίο την αλυσίδα ξενοδοχείων Hyatt να επιβεβαιώνει σε δελτίο τύπου πως η κυβερνοεπίθεση είχε ως αποτέλεσμα τη μόλυνση τερματικών POS σε 249 ξενοδοχεία της σε 54 χώρες και όλες οι πληροφορίες πιστωτικών καρτών των πελατών κλάπηκαν.

Romantic Seehotel Jagerwirt:

Ένα πολυτελές ξενοδοχείο στην Αυστρία έπεσε θύμα χάκερς, οι οποίοι προχώρησαν σε σειρά επιθέσεων. Μια από αυτές ήταν ο έλεγχος των “έξυπνων κλειδιών” με αποτέλεσμα να μην μπορούν οι επισκέπτες να έχουν πρόσβαση στα δωμάτιά τους. Οι ηλεκτρονικοί διαρρήκτες κατάφεραν να κλειδώσουν τις πόρτες του ξενοδοχείου οι οποίες λειτουργούσαν μόνο με κάρτα, τις ταμειακές μηχανές ενώ έριξαν και την ιστοσελίδα της επιχείρησης. Οι υπεύθυνοι του ξενοδοχείου δεν είχαν την δυνατότητα να εκδώσουν νέες κάρτες γεγονός που δείχνει πόσο ευάλωτα είναι τα συστήματα που ανήκουν στο λεγόμενο “internet of things”. Μην έχοντας άλλη επιλογή, το τετράστερο θέρετρο Romanric Seehotel Jagerwirt, αναγκάστηκε να δώσει στους χάκερς λύτρα στην τιμή των 1500 ευρώ σε Bitcoin, προκειμένου να ξανά ενεργοποιηθεί το σύστημα.

Το ξενοδοχείο είχε δεχτεί επιθέσεις και στο παρελθόν, αλλά αυτή τη φορά οι χάκερς μπόρεσαν να ρίξουν ολόκληρο το σύστημα με τα κλειδιά. Επίσης, είχαν πρόσβαση στο γενικό σύστημα υπολογιστών, κλείνοντας όλους τους υπολογιστές, συμπεριλαμβανομένου του συστήματος κρατήσεων και του ταμείου.

Όταν πληρώθηκαν τα λύτρα, το σύστημα επανήλθε, επιτρέποντας στο προσωπικό την πρόσβαση, αλλά και στους πελάτες την είσοδο στα δωμάτιά τους. Το ενδιαφέρον είναι ότι παρά την ικανοποίηση των αιτημάτων τους, οι χάκερς είχαν αφήσει μια “πίσω πόρτα” στο σύστημα του ξενοδοχείου για ενδεχόμενη μελλοντική επίθεση. Και όλα αυτά ενώ η συγκεκριμένη ξενοδοχειακή μονάδα έχει ήδη ξοδέψει περίπου 10.000 ευρώ

για την ψηφιακή της ασφάλεια, προκειμένου να σταματήσει τους επίδοξους χάκερς (Σιούτη, 2017) (WOLFF, 2017).

Πέρα από τις ξενοδοχειακές μονάδες όμως θύμα έπεσε και μια από της δημοφιλέστερες πλατφόρμες κρατήσεων ξενοδοχείων η Booking.com κατά το έτος 2018. Οι απατεώνες μέσω της μεθόδου social engineering απέκτησαν πρόσβαση στο extranet πληροφοριακό σύστημα της Booking μέσω του οποίου τα καταλύματα διαχειρίζονταν τις κρατήσεις τους και στη συνέχεια εξαπατώντας τους υπαλλήλους των ξενοδοχειακών μονάδων (40 ξενοδοχειακές μονάδες στο σύνολο) λάμβαναν τα απαραίτητα στοιχεία σύνδεσης και έτσι μπόρεσαν να υποκλέψουν προσωπικά στοιχεία όπως ονόματα, στοιχεία επικοινωνίας και στοιχεία για τις κρατήσεις τους, για 4109 πελάτες, όπου για τους 283 φαίνεται να εκτέθηκαν και οι αριθμοί πιστωτικών καρτών ενώ σε 97 περιπτώσεις οι πελάτες είχαν δηλώσει και τον κωδικό ασφαλείας των καρτών τους (CVV). Το πρόστιμο που κλήθηκε να πληρώσει η Booking ήταν 475.000 ευρώ καθώς σύμφωνα με το Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) δεν ανέφερε εγκαίρως - στο χρονικό διάστημα που επιβάλλεται - την παραβίαση δεδομένων που δέχτηκε ενώ ήταν ήδη ενήμερη από τα ξενοδοχεία για το περιστατικό.

Πρέπει να γίνει αντιληπτό ότι οι κυβερνοεπιθέσεις είναι πλέον μια απειλή για τα ξενοδοχεία αλλά και για όλη την βιομηχανία της φιλοξενίας και μέχρι σήμερα έχουν πέσει θύματα μικρές αλλά και πολύ μεγάλες μονάδες.

Μία κυβερνοεπίθεση μπορεί να επηρεάσει τα συστήματα πληροφορικής που χρησιμοποιούν τα ξενοδοχεία για την διαχείρισή τους και σε περίπτωση που αυτά ανήκουν σε κάποια αλυσίδα μπορεί και όλα τα ξενοδοχεία της αλυσίδας να χάσουν την πρόσβαση στο δίκτυο και τα σημεία πώλησης των υπηρεσιών τους και να δημιουργηθούν προβλήματα στην διαχείριση των κρατήσεων και την εξυπηρέτηση των πελατών τους.

Αντίστοιχες επιθέσεις όμως δέχονται και μεγάλες αεροπορικές εταιρείες όπως η British Airways η οποία πλήρωσε το πρόστιμο των 28 εκατ. δολαρίων για απώλεια δεδομένων 400.000 επιβατών το 2018, αντίστοιχα η εταιρεία Cathay Pacific επεβλήθη σε πρόστιμο 700.00 δολαρίων για απώλεια δεδομένων 9 εκατ. επιβατών. Ενώ και η εταιρεία Easy Jet πριν ένα χρόνο ανακοίνωσε πως μετά από κυβερνοεπίθεση που δέχθηκε κλάπηκαν διευθύνσεις ηλεκτρονικού ταχυδρομείου από 9 εκατ. επιβάτες της. Τέλος η εταιρεία Air India τον Φεβρουάριο του 2021 ανακοίνωσε την κλοπή δεδομένων 14,5 εκατομμυρίων

επιβατών μετά από επίθεση, στα δεδομένα συμπεριλαμβανόταν στοιχεία όπως ονόματα, αριθμοί τραπεζικών καρτών καθώς και πληροφορίες διαβατηρίων.

Τον Οκτώβριο του 2021 Χάκερ επιτέθηκαν στα κεντρικά γραφεία του ομίλου FTI, στο Μόναχο, με αποτέλεσμα να παραλύσει το σύστημα πληροφορικής (IT) του τρίτου μεγαλύτερου ταξιδιωτικού πράκτορα στην Ευρώπη.

Ως αποτέλεσμα της επίθεσης, οι οργανωτές ταξιδιών δεν μπορούσαν να προβούν σε κράτηση, ενώ διακόπηκαν προσωρινά τα συστήματα πληροφορικής και επικοινωνιών. Την ίδια στιγμή, τα συστήματα κράτησης της εταιρίας εμφάνιζαν την ένδειξη «σε διαδικασία αποκατάστασης». Τα ταξίδια που είχαν ήδη προγραμματιστεί δεν επηρεάστηκαν, ενώ η δυνατότητα κράτησης για νέα ταξίδια αποκαταστάθηκε το ίδιο βράδυ. Σύμφωνα με τον διευθύνοντα σύμβουλο Ralph Schiller του ομίλου FTI, ελήφθησαν όλα τα απαραίτητα μέτρα, ενημερώθηκαν οι αρμόδιες αρχές και τέθηκε σε εφαρμογή σχέδιο έκτακτης ανάγκης. Ενώ, υπήρξε συνεργασία του tour operator με ομάδα ειδικών προκειμένου να αποκατασταθούν όλες οι λειτουργίες το συντομότερο δυνατό.

Η Carnival, μια από τις μεγαλύτερες εταιρείες κρουαζιέρας στον κόσμο έπεσε θύμα επίθεσης λογισμικού ransomware τον περασμένο Αύγουστο με την εταιρεία να κάνει γνωστό το περιστατικό, ενημερώνοντας τους επενδυτές της ότι οι χάκερ μπορεί να είχαν πρόσβαση στα προσωπικά στοιχεία των πελατών και του προσωπικού της καθώς και σε ένα τμήμα ενός συστήματος πληροφορικής που αφορούσε ένα από τα εμπορικά σήματα της Carnival (Cunard, Princess και P&O) (Sean O'Neill, 2020).

Επίθεση από χάκερ δέχθηκε επίσης στις 27 Ιουνίου το 2017 η ιστοσελίδα της Mouzenidis Travel στη Ρωσία με αποτέλεσμα για αρκετές ώρες να μην είναι διαθέσιμη για πλοήγηση. Η λειτουργία της ιστοσελίδας αποκαταστάθηκε μία ημέρα αργότερα χωρίς να έχει επηρεαστεί ο βασικός server της εταιρίας από την κυβερνοεπίθεση και χωρίς να υπάρχει λόγος ανησυχίας για μη εξουσιοδοτημένη χρήση προσωπικών δεδομένων των τουριστών, όπως είχε επισημάνει ο CEO του tour operator, κ. Αλέξανδρος Τσαντεκίδης.

Την ίδια χρονιά η ρωσική αστυνομία συνέλαβε 20 χάκερς, οι οποίοι χρησιμοποιώντας έναν ιό τύπου «δούρειου ίππου», κατάφεραν να κλέψουν από λογαριασμούς καταθέσεων σε ρωσικές τράπεζες ποσά της τάξεως των 50 εκατομμυρίων ρουβλίων (892.000 δολαρίων). Οι Ρώσοι χάκερς κάνοντας χρήση ενός κακόβουλου λογισμικού

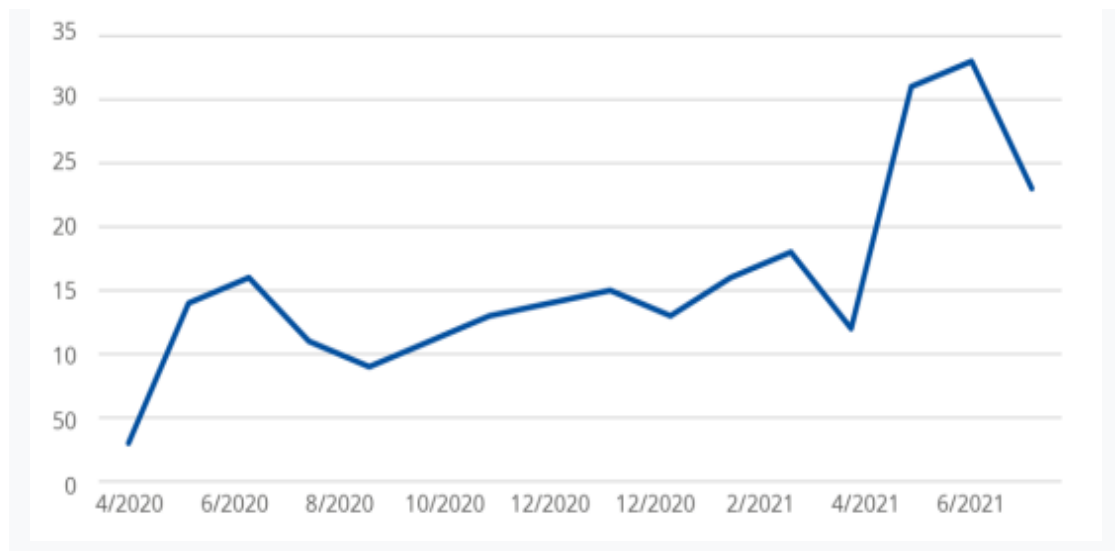
κατάφεραν να μολύνουν περισσότερα από ένα εκατομμύριο smartphones ενώ πριν συλληφθούν σχεδίαζαν να κάνουν το ίδιο σε λογαριασμούς καταθέσεων σε ευρωπαϊκές τράπεζες. Σύμφωνα με την ανάκριση, τα μέλη της ομάδας χρησιμοποιούσαν ένα κακόβουλο λογισμικό που τους επέτρεπε να έχουν πρόσβαση στα smartphones, που είχαν συγκεκριμένο πάροχο, στα οποία έδιναν εντολές με απόκρυψη για μεταφορά χρημάτων σε λογαριασμούς που είχαν δημιουργήσει εκ των προτέρων (Skai.gr, 2017).

Έχει παρατηρηθεί επίσης ότι οι εγκληματίες του κυβερνοχώρου είναι πιο πιθανό να στοχεύουν σε δεδομένα όπου μια ενδεχόμενη διαρροή τους θα έχει αντίκτυπο στις ίδιες τις επιχειρήσεις παρά σε δεδομένα που σχετίζονται με πληρωμές όπως για παράδειγμα οι πιστωτικές κάρτες των πελατών. Αυτό τουλάχιστον φαίνεται να εφαρμόζουν μέσω του στοχευόμενου ransomware τον τελευταίο χρόνο. Η αύξηση επιθέσεων ransomware ξεπέρασε το 150% το 2020 έχοντας γίνει μια από τις μεγαλύτερες απειλές που αντιμετωπίζουν οι επιχειρήσεις ανεξαρτήτου κλάδου τα τελευταία χρόνια. Χρησιμοποιώντας πολλαπλές μεθόδους εκβίασης ασκούν πίεση τα θύματά τους (επιχειρήσεις) και τους αναγκάζουν να πληρώσουν τα λύτρα. Ένα παράδειγμα αυτής της μεθόδου είναι η διπλή εκβιαστική τακτική που εφαρμόστηκε στα τέλη του 2019 με χρήση Maze ransomware μια παραλλαγή του ransomware όπου:

- A. κρυπτογραφεί τα συστήματα και τα δεδομένα μιας επιχείρησης και ζητούν λύτρα για να τα επαναφέρουν.
- B. και ως μέθοδο εξαναγκασμού τους εκβιάζουν με την δημοσίευση των ευαίσθητων προσωπικών δεδομένων που κρατούν.

Στο παρελθόν ομάδες ransomware στόχευαν περισσότερο σε μικρές και μεσαίες επιχειρήσεις πλέον όμως έχει παρατηρηθεί να εστιάζουν σε μεγαλύτερες επιχειρήσεις οι οποίες θα μπορούσαν να πληρώσουν υψηλότερα ποσά για τα λύτρα που τους ζητούν.

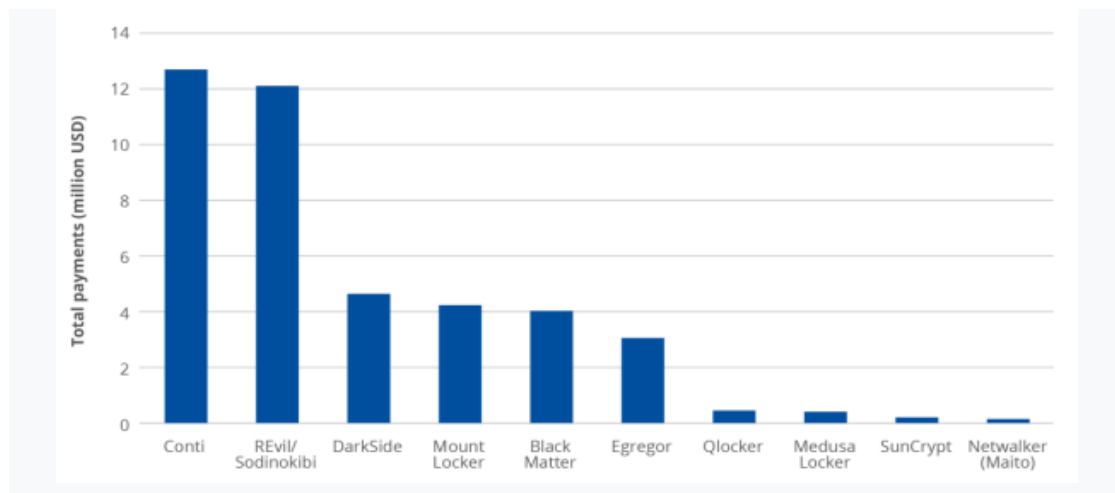
Αρκετές επιθέσεις ransomware αναφέρθηκαν κατά την περίοδο αναφοράς ETL. Το παρακάτω σχήμα - Εικόνα 2 - δείχνει την αύξηση των περιστατικών ransomware που αναφέρθηκαν από το 2020 και μια απότομη αύξηση τον Μάιο και τον Ιούνιο του 2021. Τα περιστατικά παρατηρήθηκαν με βάση το OSINT (Open Source Intelligence) που συλλέχθηκαν από τον ENISA με το εύρος της συλλογής να είναι παγκόσμιο.



Εικόνα 2- Περιστατικά Ransomware

Οι παραλλαγές ransomware όπως φαίνεται και στο παρακάτω γράφημα - Εικόνα 3 - που χρησιμοποιήθηκαν για τις επιθέσεις αυτές ήταν αρκετές, εκείνες όμως που κατάφεραν και απέσπασαν τα περισσότερα κέρδη είναι οι εξής:

- Conti (12,7 εκατομμύρια δολάρια): Σε επιθέσεις τύπου ransomware Conti, οι εγκληματίες, κλέβουν αρχεία, κρυπτογραφούν server και σταθμούς εργασίας και απαιτούν πληρωμή λύτρων (CISA, 2021).
- REvil/Sodinokibi (12 εκατομμύρια δολάρια): Μετά από μια επίθεση, ο REvil θα απειλούσε να δημοσιεύσει τις πληροφορίες σε γνωστά Blog, εκτός εάν λάμβανε τα ζητούμενα λύτρα.
- DarkSide (4,6 εκατομμύρια δολάρια) Αντίστοιχο με το REvil.
- MountLocker (4,2 εκατομμύρια δολάρια) Σε μια επίθεση MountLocker οι κυβερνοεγκληματίες μπορούν να υποκλέψουν και να κρυπτογραφήσουν δεδομένα ως και 400GB. Το γεγονός αυτό κάνει τους κυβερνοεγκληματίες να ζητούν μεγάλα ποσά λύτρων. Παράλληλα έχει τη δυνατότητα να αφαιρέσει το δικαίωμα πρόσβασης από τους εξουσιοδοτημένους χρήστες. Αυτό σημαίνει ότι το θύμα δεν μπορεί να έχει πρόσβαση σε οποιαδήποτε συσκευή όπως στον υπολογιστή του ή στην κινητή συσκευή του αλλά ούτε και στο λειτουργικό σύστημα ή σε άλλες υπηρεσίες δικτύου.
- Blackmatter (4,0 εκατομμύρια δολάρια)
- Egregor (3,1 εκατομμύρια δολάρια).



Εικόνα 3 Παραλλαγές του Ransomware

Η ταχεία ανάπτυξη υποδομών και υπηρεσιών cloud λόγω των τρεχουσών και επειγουσών αναγκών της τηλεργασίας, το εργατικό δυναμικό κατά τη διάρκεια της πανδημίας, καθώς και οι ελλιπείς γνώσεις που αφορούν την τεχνογνωσία που σχετίζεται με το cloud, οδήγησε σε κακή ασφάλεια και διαχείριση, δίνοντας έτσι ευκαιρίες σε εγκληματίες του κυβερνοχώρου να επιτεθούν, φτάνοντας σε σημείο να είναι και η κύρια αιτία παραβιάσεων.

Οι κυβερνοεγκληματίες έχουν ήδη εντοπίσει αυτές τις ευκαιρίες και έχουν αναπτύξει ικανότητες παραβίασης υποδομών και υπηρεσιών cloud. Κατά την περίοδο Απρίλιος 2020 ως Ιούλιος 2021, παρατηρήθηκαν κυβερνοεπιθέσεις σε cloud περιβάλλοντα, κάνοντας ανάπτυξη λογισμικού worm cryptomining για κλοπή διαπιστευτηρίων, cryptomining σε διακομιστές Linux και στόχευση των περιβαλλόντων Docker και Kubernetes.

Επιπλέον, υπάρχει μια αυξητική τάση στους παρόχους cloud όπως BlackBaud, Swiss Cloud, Equinix, και Cloudstar που παραβιάζονται από ομάδες ransomware. Τέλος οι επιθέσεις που φαίνεται να πολλαπλασιάζονται είναι εκείνες που βασίζονται σε αδύναμη ταυτοποίηση υπηρεσιών cloud (αδύναμα password ή χρήση προεπιλεγμένων) ή δεν έχουν ενεργοποιημένο τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA).

Καθώς λοιπόν η πανδημία επιτάχυνε την υιοθέτηση υποδομών και υπηρεσιών cloud παγκοσμίως και η τάση αναμένεται να συνεχιστεί και στο άμεσο μέλλον θα πρέπει να ληφθούν υπόψη και οι ανάλογοι κίνδυνοι που προκύπτουν από την μετάβαση στην

διαδικτυακή εργασία. Γι' αυτό είναι απαραίτητο τα λαμβάνονται και τα αντίστοιχα μέτρα πρόληψης και αντιμετώπισης.

6. Κυβερνοασφάλεια

Καθώς η κοινωνία μας εξαρτάται όλο και περισσότερο από τα συστήματα επικοινωνιών και πληροφορικής, η ασφάλειά τους αποτελεί πλέον μείζον θέμα εθνικού ενδιαφέροντος, ενώ ταυτόχρονα παρατηρείται και μία συνεχώς αυξανόμενη ανάγκη για προστασία των επιχειρήσεων, των χρηστών και των ψηφιακών υπηρεσιών.

Ο όρος «κυβερνοασφάλεια» αναφέρεται σε μια σειρά από ενέργειες και δράσεις που πρέπει να εφαρμόζονται προκειμένου να διασφαλιστεί η προστασία του κυβερνοχώρου από εκείνες τις απειλές και τους κινδύνους που είναι άμεσα συνυφασμένοι με αυτόν και που μπορούν να βλάψουν τα αλληλοεξαρτώμενα συστήματα Τεχνολογιών Πληροφορικής και Επικοινωνιών ΤΠΕ.

Η ανάπτυξη και θωράκιση των τουριστικών επιχειρήσεων αλλά και γενικότερα των ψηφιακών υπηρεσιών και αγορών αποτελεί βασικό άξονα στήριξης της εθνικής οικονομίας και προσφέρει ανταγωνιστικό πλεονέκτημα τόσο σε εθνικό όσο και σε Ευρωπαϊκό επίπεδο.

Καθώς η χώρα μας συνεχίζει να αναπτύσσεται και να επενδύει στους τομείς των ψηφιακών αγορών, δικτύων και υπηρεσιών τόσο του ιδιωτικού όσο και του δημόσιου τομέα καθίσταται απαραίτητη η δημιουργία και τήρηση στρατηγικής πρόληψης και αντιμετώπισης από τις ίδιες τις επιχειρήσεις. Κάθε επιχείρηση θα πρέπει να ορίζει, υλοποιεί και να διατηρεί επίκαιρη και καταγεγραμμένη Πολιτική Ασφαλείας σχετική με την ασφάλεια των συστημάτων δικτύου και πληροφοριών που διαθέτει η οποία φυσικά θα πρέπει να συνάδει με τους στόχους της εθνικής αρχής και της πολιτικής κυβερνοασφάλειας.

Βασικοί στόχοι της Πολιτικής Ασφαλείας είναι:

- Διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των δεδομένων, συστημάτων και υπηρεσιών έναντι εκούσιων ή ακούσιων απειλών.
- Ικανοποίηση των νομικών και κανονιστικών απαιτήσεων σχετικών με την ασφάλεια και προστασία δεδομένων.

- Επιχειρησιακή συνέχεια των βασικών υπηρεσιών μιας επιχείρησης έναντι περιστατικών κυβερνοεπιθέσεων.
- Ενημέρωση και εκπαίδευση όλων των υπαλλήλων και λοιπών εμπλεκομένων τρίτων σχετικά με την παροχή των βασικών υπηρεσιών της επιχείρησης.
- Άμεση κοινοποίηση και διαχείριση περιστατικών ή αδυναμιών ασφαλείας.

Οι παραπάνω στόχοι μπορούν να χωριστούν σε μέτρα πρόληψης και αντιμετώπισης ούτε ώστε να περιορίζονται και να προλαμβάνονται τα όποια περιστατικά.

7. Πρόληψη

Τα μέτρα πρόληψης που οφείλουν να τηρούν όλες οι επιχειρήσεις προκειμένου να προστατευτούν επαρκώς είναι:

- Εκπαίδευση προσωπικού:
- Προστασία από κακόβουλο λογισμικό
- Αυθεντικοποίηση χρηστών
- Έλεγχος πρόσβασης
- Έλεγχος δικτύου
- Ασφάλιση

Εκπαίδευση προσωπικού:

Οι επιχειρήσεις οφείλουν να ενημερώνουν ή και να εκπαιδεύουν κατάλληλα το προσωπικό και τους συνεργάτες τους σχετικά με τα τηρούμενα μέτρα για την Ασφάλεια Συστημάτων Δικτύου και Πληροφοριών, λαμβάνοντας υπόψη τη φύση της παρεχόμενης εργασίας, και να απαιτούν την αποδοχή εκ μέρους τους, και την τήρηση τους ώστε να διατηρούν και να προάγουν την ασφάλεια των συστημάτων αυτών. Η εκπαίδευση αφορά το προσωπικό ολόκληρης της εταιρίας για το πώς θα συμπεριφέρονται απέναντι σε διαφορετικά είδη κινδύνων στο διαδίκτυο. Θα πρέπει να γνωρίζουν πώς να λειτουργούν σε περιπτώσεις για τις οποίες υπάρχει ακόμα και η υποψία ότι μπορεί να έχουν δεχθεί επίθεση και να δρουν άμεσα.

Η ευαισθητοποίηση σχετικά με τις απειλές και τις ευπάθειες που σχετίζονται με την Κυβερνοασφάλεια, καθώς και τις επιπτώσεις αυτών τόσο στις ίδιες τις επιχειρήσεις όσο και στην κοινωνία γενικότερα, είναι ζωτικής σημασίας.

Μέσω κατάλληλων και στοχευμένων εκστρατειών ενημέρωσης και εκπαίδευσης τόσο για τους χρήστες των επιχειρήσεων όσο και για τους πολίτες γενικότερα, ενισχύεται η γνώση σχετικά με τους κινδύνους του διαδικτύου αλλά και η προστασία από συνήθεις απειλές, κάτι που εκτιμάται ότι μελλοντικά θα αυξήσει σημαντικά το επίπεδο κυβερνοασφάλειας της χώρας.

Προστασία από κακόβουλο λογισμικό:

Το κακόβουλο λογισμικό είναι από τις σημαντικότερες απειλές των πληροφοριακών συστημάτων των επιχειρήσεων καθώς μπορεί να τα μολύνει με διάφορους τρόπους (e-mail, site, φορητά μέσα αποθήκευσης) και να τους προκαλέσει πολυποίκιλες ζημιές όπως:

- κλοπή δεδομένων και κωδικών πρόσβασης
- διαγραφή ή αλλοίωση δεδομένων
- κρυπτογράφηση δεδομένων

Η μόλυνση των συστημάτων συνήθως οφείλεται σε απρόσεκτη συμπεριφορά των χρηστών όπως με το άνοιγμα συνημμένων αρχείων και συνδέσμων, με την εγκατάσταση προγραμμάτων ή και με την εισαγωγή μολυσμένου USB. Προκειμένου να ανιχνευθεί και να αφαιρεθεί το κακόβουλο λογισμικό, οι μηχανισμοί προστασίας θα πρέπει να εφαρμοστούν σε όλα τα σημεία εισόδου και εξόδου των συστημάτων (σταθμοί εργασίας, web servers, mail servers, proxy servers, remote access servers, firewalls).

Γι' αυτό τα μέτρα που πρέπει να ληφθούν είναι τα εξής:

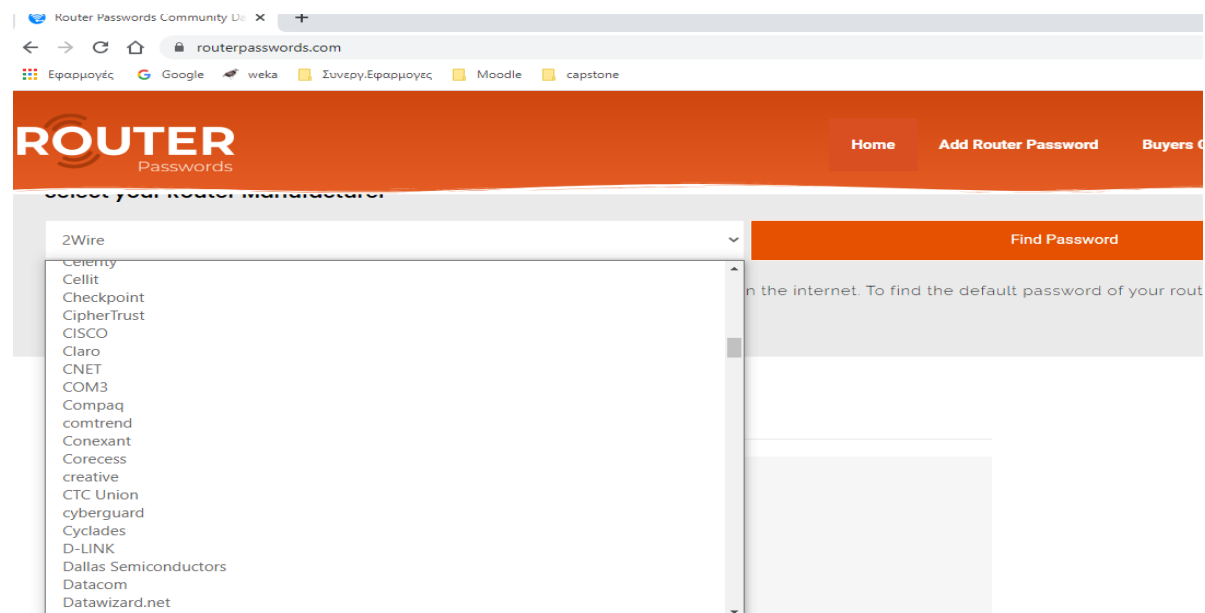
- Εγκατάσταση αντιϊικού προγράμματος (antivirus, anti-malware).
- Καθημερινή ενημέρωση του.
- Σάρωση σε όλα τα φορητά μέσα αποθήκευσης, πριν την χρήση τους (cd, usb, σκληρούς δίσκους) καθώς και σε αρχεία που κατεβάζουμε.
- Χρήση DNS filtering για την παρεμπόδιση πρόσβασης σε γνωστά κακόβουλα domains.
- Ενεργοποίηση φίλτρων σπαμ για τον περιορισμό των εισερχόμενων μολυσμένων email

Παράλληλα και ανάλογα το μέγεθος της επιχείρησης αλλά και των εργασιακών της δραστηριοτήτων θα πρέπει να λαμβάνονται πλήρη αντίγραφα ασφαλείας ανά τακτά διαστήματα.

Αυθεντικοποίηση χρηστών:

Ένα από τα βασικότερα μέτρα προστασίας που πρέπει να λαμβάνονται είναι η τροποποίηση των συνθηματικών σε κάθε νέα συσκευή ή προϊόν κατά την πρώτη εγκατάστασή του, καθώς τα προεπιλεγμένα μπορούν να γίνουν εύκολα γνωστά και έτσι να αποτελέσουν στόχο και να δώσουν πρόσβαση σε μη εξουσιοδοτημένους χρήστες.

Στις εικόνες που ακολουθούν -Εικόνα 4 & Εικόνα 5- απεικονίζεται μία από τις δεκάδες πηγές στο διαδίκτυο όπου είναι δημοσίως διαθέσιμα τα προεπιλεγμένα ζεύγη username και password για τα routers όλων των κατασκευαστών ανά μοντέλο. Το γεγονός αυτό κάνει εύλογα αντιληπτό τον κίνδυνο που αντιμετωπίζουν οι επιχειρήσεις εφόσον δεν τροποποιήσουν τα προεπιλεγμένα συνθηματικά με την πρώτη εγκατάσταση κάθε router και γενικότερα κάθε αντίστοιχου προϊόντος που περιέχει αντίστοιχα προεπιλεγμένα ζεύγη.



Εικόνα 4 Router Password

Cisco Router Default Passwords

Here is the list of all the verified router passwords for **Cisco routers**. Router Passwords keeps a database of all the latest passwords submitted for Cisco routers:

Manufacturer	Model	Protocol	Username	Password
CISCO	CACHE ENGINE	CONSOLE	admin	diamond
CISCO	CONFIGMAKER		cmaker	cmaker
CISCO	CNR	CNR GUI	admin	changeme
CISCO	NETRANGER/SECURE IDS	MULTI	netrangr	attack
CISCO	BBSM	TELNET OR NAMED PIPES	bbsd-client	changeme2
CISCO	BBSD MSDE CLIENT	TELNET OR NAMED PIPES	bbsd-client	NULL

Εικόνα 5 Router Default Passwords

Ταυτόχρονα θα πρέπει να γίνονται αλλαγές σε όλα τα συνηματικά ανά τακτά χρονικά διαστήματα με ισχυρούς πάντα κωδικούς πρόσβασης, αυτό σημαίνει:

- Αποφυγή χρήσης ημερομηνίας γέννησης του ίδιου του χρήστη ή συγγενή του.
- Αποφυγή χρήσης αριθμού τηλεφώνου.
- Αποφυγή χρήσης άλλων προσωπικών ή συγγενικών στοιχείων που μπορούν να εντοπιστούν εύκολα.
- Αποφυγή χρήσης «εύκολων» κωδικών όπως αλφαβητική ή αριθμητική σειρά χαρακτήρων, λέξεων όπως password, qwerty ή παραλλαγές αυτών.
- Αποφυγή χρήσης του ίδιου κωδικού σε πολλές εφαρμογές, κάθε εφαρμογή θα πρέπει να έχει ξεχωριστό κωδικό.
- Ο κωδικός θα πρέπει να αποτελείται τουλάχιστον από 8 ψηφία, στα οποία θα συμπεριλαμβάνονται αριθμοί, σύμβολα και κεφαλαία και πεζά γράμματα.

Οι κωδικοί αυτοί δεν θα πρέπει να δημοσιεύονται, ούτε να βρίσκονται σε κοινή θέα. Θα πρέπει να αποθηκεύονται και να αποστέλλονται αν χρειαστεί μόνο σε κρυπτογραφημένη μορφή όπου η κρυπτογράφηση θα γίνεται με τη χρήση one-way hash αλγορίθμων με την επιπλέον προσθήκη στον υπολογισμό μίας ακολουθίας τυχαίων δεδομένων (salt).

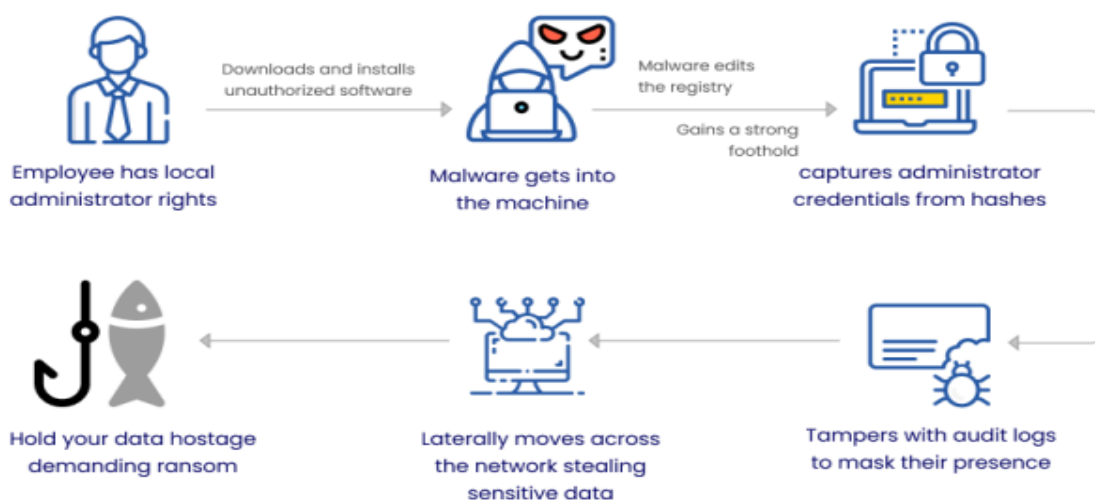
Η κρυπτογράφηση αφορά όλα τα ευαίσθητα δεδομένα τα οποία συλλέγει, αποθηκεύει και ταξινομεί η επιχείρηση. Ενώ θα πρέπει να γίνει συνήθεια των εργαζομένων ότι εφόσον χρειαστεί να απομακρυνθούν από τον υπολογιστή τους ή δεν χρησιμοποιούν

κάποια επιχειρησιακή λειτουργία θα πρέπει να αποσυνδέονται από τις εφαρμογές ώστε να μην γίνουν στόχος μη εξουσιοδοτημένων χρηστών.

Όσον αφορά επίσης τις εφαρμογές που εκτελούνται στο σύστημα χρειάζεται να εφαρμόζεται η αρχή της ελάχιστης λειτουργικότητας που σημαίνει ότι μόνο οι εφαρμογές και λειτουργίες που είναι απαραίτητες για τις επιχειρηματικές λειτουργίες θα πρέπει να εκτελούνται από τα συστήματα αλλιώς κινδυνεύουν από τη λεγόμενη «επιφάνεια επίθεσης» λόγω των πολλών σημείων εισόδου που είναι εκτεθειμένα σε έναν επιτιθέμενο για να αποκτήσει πρόσβαση στο σύστημα.

Επιπρόσθετα το προσωπικό της επιχείρησης θα πρέπει να έχει πρόσβαση στις εφαρμογές ανάλογα με τη θέση εργασίας του. Να υπάρχει δηλαδή περιορισμός στη χορήγηση προνομίων και στα δικαιώματα πρόσβασης ώστε εάν ένας λογαριασμός παραβιαστεί να μην τεθούν σε κίνδυνο συστήματα από διαφορετικά τμήματα μιας επιχείρησης. Αντίστοιχα λογαριασμό χρήστη θα πρέπει να έχουν και οι εξωτερικοί συνεργάτες ώστε να αναγνωρίζονται με τρόπο ώστε να διασφαλίζεται η λογοδοσία.

Στην παρακάτω εικόνα - Εικόνα 6- φαίνεται μια περίπτωση επίθεσης ύστερα από λάθος εκχώρηση δικαιωμάτων. Ένας χρήστης ο οποίος εκτελεί εργασίες ρουτίνας φαίνεται να έχει και δικαιώματα διαχειριστή, από λάθος εγκαθιστά malware στον Η/Υ του. Με τα δικαιώματα που διαθέτει, ο επιτιθέμενος μπορεί να δημιουργήσει νέους admin λογαριασμούς, να τροποποιήσει την registry, να εγκαταστήσει άλλα εργαλεία ή και να σβήσει εγγραφές από τα logs προκειμένου να κρύψει την παρουσία του. Στη συνέχεια, αφού συλλέξει πληροφορίες για το εσωτερικό δίκτυο της επιχείρησης, μετακινείται και μολύνει άλλα συστήματα αποσπώντας ευαίσθητα δεδομένα, ενώ σαν τελικό του στόχο κρυπτογραφεί όλα τα αρχεία απαιτώντας λύτρα (ransomware).



Εικόνα 6 Attack case

Έλεγχος πρόσβασης:

Τα υποστηρικτικά συστήματα πληροφοριών θα πρέπει να βρίσκονται σε ασφαλείς χώρους όπου δεν μπορεί να έχει πρόσβαση ο καθένας.

Επίσης καλό είναι να τηρούνται στοιχεία που να αποδεικνύουν την ουσιαστική εφαρμογή πολιτικών ασφάλειας και να αξιολογούνται ανά διαστήματα.

Για να είναι επιτυχημένη η στρατηγική μέτρων πρόληψης θα πρέπει να γίνει πλήρη καταγραφή από την επιχείρηση του συνόλου των αγαθών Πληροφορικής (συσκευών και λογισμικού) που φιλοξενούνται στη φυσική υποδομή της, καθώς και σε cloud περιβάλλοντα, με σκοπό τη διαμόρφωση πλήρους αντίληψης για το εύρος των αγαθών και τα αναγκαία μέτρα προστασίας και συντήρησής τους.

Όσο μεγαλύτερη σε μέγεθος είναι μια επιχείρηση, τόσο σημαντικότερη είναι η συνολική διαχείριση του εξοπλισμού της (υλικού και λογισμικού), που μπορεί να βρίσκεται σε περισσότερα από ένα κτήρια αλλά και στο cloud, από το οποίο πλέον προωθείτε και πραγματοποιείται η εξ αποστάσεως εργασία με χρήση laptops, tablets, smartphones.

Αφού καταγραφούν υλικό και λογισμικό θα πρέπει να παρθούν τα ακόλουθα μέτρα

(Υπουργείο Ψηφιακής Διακυβέρνησης, 2021, σ. 18):

- Οι προσωπικές συσκευές των εργαζομένων δεν θα πρέπει να έχουν πρόσβαση σε κρίσιμα ή ευαίσθητα συστήματα της επιχείρησης.

- Οι προσωπικές συσκευές των εργαζομένων εφόσον της φέρουν στο χώρο εργασίας τους θα πρέπει να χρησιμοποιούν διαφορετικό δίκτυο για την πρόσβασή τους στο internet.
- Επίσης θα πρέπει να εφαρμόζουν ισχυρή ταυτοποίηση, αυτό σημαίνει, αυθεντικοποίηση 2 παραγόντων (2-factor authentication) για την πρόσβαση στο διαχειριστικό περιβάλλον όλων των κρίσιμων δικτυακών συσκευών καθώς και χρήση δακτυλικού αποτυπώματος και χρήση κωδικών μιας χρήσης όπου κριθεί απαραίτητο.

Έλεγχος δικτύου:

Καθώς τα τελευταία 2 χρόνια λόγω της πανδημίας πολλές επιχειρήσεις καθιέρωσαν την εξ αποστάσεως εργασία εκτός από όλα τα παραπάνω μέτρα θα πρέπει να ελέγχονται και να λαμβάνονται και τα επιπλέον εξής μέτρα:

- Χρήση VPN (το οποίο διατηρείται ενημερωμένο)
- Είσοδος σε αυτό με τα αντίστοιχα μέτρα περί πρόσβασης (ισχυρούς κωδικούς, ταυτοποίηση 2 παραγόντων κτλ) τόσο για τις VPN συνδέσεις με το δίκτυο της επιχείρησης όσο και για την σύνδεση με το οικιακό router.
- Χρήση WPA2 ή WPA3
- Επιλογή μόνο επίσημων site και έλεγχος παροχής ασφαλείας, να διαθέτουν δηλαδή το πρωτόκολλο https και το λουκέτο αλλά και το ισχύον πιστοποιητικό.
- Στην περίπτωση που δεν έχουμε να συνδεθούμε σε οικιακό δίκτυο, είναι προτιμότερο να γίνει χρήση των δεδομένων κινητής τηλεφωνίας μέσω hot spot αντί δημοσίου δικτύου και αν αυτό δεν γίνεται προτιμήστε το VPN.
- Για πληρωμές και άλλες συναλλαγές θα πρέπει επίσης να έχουν απενεργοποιημένη τη λειτουργία «Αυτόματης Καταχώρησης» του browser. Η λειτουργία αυτή αποθηκεύει τους κωδικούς στον υπολογιστή, γεγονός που τους καθιστά έκθετους.

Παράλληλα για τις τουριστικές επιχειρήσεις οι οποίες διαχειρίζονται κρατήσεις σε πραγματικό χρόνο και πρέπει να συνδέονται άμεσα και να μεταφέρουν δεδομένα σε τρίτους είναι απαραίτητη η χρήση ενός παγκόσμιου συστήματος διανομής GDS (Global distribution system) όπως το Amadeus, Sabre και το Travelport. Το σύστημα αυτό παρέχει υπηρεσίες που σχετίζονται με κρατήσεις όπως αεροπορικές θέσεις, κράτηση σε ξενοδοχεία, κρουαζιέρες, ενοικιάσεις αυτοκινήτων κ.α προς τον πελάτη. Όταν για παράδειγμα ένα ταξιδιωτικό γραφείο ζητά να κάνει κράτηση σε μια αεροπορική, το

σύστημα GDS συνδέεται σε πραγματικό χρόνο με τη βάση δεδομένων του προμηθευτή, της αεροπορικής δηλαδή.

Σύμφωνα με τον Paige Schaffer, πρόεδρο της παγκόσμιας μονάδας υπηρεσιών ψηφιακής προστασίας (Generali Global Assistance), τα τουριστικά γραφεία που δεν χρησιμοποιούν παγκόσμιο σύστημα διανομής (GDS) και κάνουν κράτηση απευθείας μέσω των ιστοσελίδων παρόχων, ενέχει τον κίνδυνο να πέσουν θύμα phishing και να γνωστοποιήσουν, χωρίς να το γνωρίζουν, ευαίσθητα δεδομένα σε μη εξουσιοδοτημένους χρήστες.

Ασφάλιση:

Οι κίνδυνοι στο διαδίκτυο είναι γνωστοί στις μεγάλες ασφαλιστικές εταιρείες, ωστόσο η σύναψη ασφάλισης θα μπορούσαμε να πούμε ότι αποτελεί μια στρατηγική και όχι μέτρο πρόληψης, μιας και ο κίνδυνος ασφαλείας δεν περιορίζεται αλλά μεταφέρετε σε κάποιον τρίτο. Ουσιαστικά οι επιχειρήσεις οι οποίες ασφαλίζονται αντιμετωπίζουν τα περιστατικά κυβερνοεπιθέσεων με μεγαλύτερη ευκολία καθώς σε περίπτωση κυβερνοεπίθεσης οι δαπάνες που θα χρειαστεί να καταβάλουν είναι μειωμένες.

Το γεγονός αυτό αφενός είναι πολύ ενθαρρυντικό προς τις επιχειρήσεις αφού ουσιαστικά βοηθούνται στο να αντιμετωπίσουν την καταβολή των λύτρων και να καλύψουν τις ζημιές που ενδεχόμενος θα τους προκληθούν αφετέρου όμως είναι ενθαρρυντικό και για τους επιτιθέμενους καθώς με τον τρόπο αυτό αυξάνονται οι πιθανότητες να τους καταβληθούν τα ποσά που ζητούν και κατά συνέπεια τους δίνεται η ώθηση να συνεχίσουν να διαπράττουν αντίστοιχες επιθέσεις.

Η ασφαλιστική κάλυψη για επιθέσεις ransomware φαίνεται να γίνεται μη βιώσιμη, καθώς τα λύτρα αυξήθηκαν συγκριτικά με την προηγούμενη χρονιά. Έρευνα έδειξε ότι το 2020, το 26% των θυμάτων πλήρωσαν τα λύτρα για να πάρουν πίσω τα δεδομένα τους, το αντίστοιχο ποσοστό όμως για το 2021 έφτασε στο 32%.

Μια ασφαλιστική εταιρεία με 25.000 μικρούς και μεσαίους πελάτες στη Βόρεια Αμερική ανέφερε ότι το 2020, το 41% των πελατών της δέχθηκαν επιθέσεις ransomware.

Στην φάση της πρόληψης οι ασφαλιστικές εταιρείες αυτό που μπορούν να κάνουν είναι να συνδράμουν απαιτώντας από τους πελάτες τους να βελτιώσουν την ασφάλεια των

πληροφοριακών τους συστημάτων. Οι προτεινόμενες συστάσεις που μπορούν να κάνουν είναι:

- Η ταυτοποίηση και τα διαπιστευτήρια θα πρέπει να εκδίδονται, να διαχειρίζονται, να επαληθεύονται, να ανακαλούνται και να ελέγχονται για κάθε εξουσιοδοτημένη συσκευή, χρήστη και διαδικασία.
- Τα δικαιώματα πρόσβασης και οι εξουσιοδοτήσεις θα πρέπει να τυγχάνουν διαχείρισης, ενσωματώνοντας τις αρχές του ελάχιστου προνομίου και διαχωρισμός των καθηκόντων.
- Παρακολούθηση των πρόσφατων τάσεων, εξελίξεων σχετικά με κακόβουλα λογισμικά που κυκλοφορούν αλλά και μεθόδων πρόληψης.
- Παρακολούθηση συστημάτων (ενημέρωση και σάρωση).
- Χρήση εργαλείων αυτοαξιολόγησης ασφαλείας όπως το Ransomware Readiness Assessment (RRA), ένα εργαλείο που αναπτύχθηκε από την CISA – Αμερικανική Υπηρεσία Ασφαλείας στο Κυβερνοχώρο, για την αξιολόγηση πρακτικών ασφάλειας έναντι των διαφορετικών επιπέδων ransomware.

Παράλληλα καθώς στις επιθέσεις φάνηκε σε αρκετές περιπτώσεις η κλοπή και των αριθμών πιστωτικών καρτών, θα πρέπει οι επιχειρήσεις και ειδικά εκείνες που δραστηριοποιούνται στον τουρισμό που συχνά χρειάζεται να κρατούν, να επεξεργάζονται, να αποθηκεύουν ή να μεταφέρουν πληροφορίες καρτών να λειτουργούν σε ασφαλές περιβάλλον. Αυτό προϋποθέτει την ύπαρξη του προτύπου ασφάλειας δεδομένων βιομηχανίας καρτών πληρωμής (PCI DSS), ένα πρότυπο το οποίο βελτιώνει και διαχειρίζεται όλη τη διαδικασία μιας συναλλαγής για κάρτες τραπεζών που συμμετέχουν στο σύστημα Visa, Mastercard, American Express, Discover και JCB. Οι επιχειρήσεις θα πρέπει να λαμβάνουν την πιστοποίηση PCI DSS η οποία θα ισχύει για συγκεκριμένο χρονικό διάστημα.

Συνοπτικά λοιπόν για να μπορέσει να προστατευθεί μια τουριστική επιχείρηση από μελλοντικές απειλές και να ελαχιστοποιήσει τον κίνδυνο από αυτές, θα πρέπει να δημιουργήσουν μια πιο ισχυρή κουλτούρα ασφαλείας στο διαδίκτυο, με βάση την οποία το προσωπικό της θα είναι εκπαιδευμένο για να προστατεύεται από τυχόν επιθέσεις αλλά και να δρα αντίστοιχα στη περίπτωση που συμβεί κάποια επίθεση, το υλικό και λογισμικό της επιχείρησης θα είναι καταγεγραμμένο μαζί με τα μέτρα που

χρειάζονται για την προστασία τους, η παραχώρηση των δικαιωμάτων που θα δίνει η επιχείρηση στο προσωπικό θα πρέπει να είναι μελετημένη βάση των αρμοδιοτήτων του ενώ σε καμία περίπτωση οι επιχειρήσεις δεν θα πρέπει να επαναπαύονται στην ύπαρξη της ασφάλισης.

8. Αντιμετώπιση

Τα νομικά και οικονομικά κίνητρα που παρέχονται στις επιχειρήσεις προκειμένου να γνωστοποιούν τα συμβάντα που αντιμετώπισαν και να μοιράζονται πληροφορίες σχετικά με αυτά εξακολουθούν να είναι υπερβολικά περιορισμένα.

Φοβούμενοι την ενδεχόμενη προσβολή της φήμης τους, πολλές επιχειρήσεις και ειδικά εκείνες που δραστηριοποιούνται στον τουρισμό προτιμούν ακόμη να χειρίζονται τις κυβερνοεπιθέσεις που υφίστανται με διακριτικότητα ή να καταβάλλουν στους δράστες τα ποσά που ζητούν.

Εφαρμόζοντας τα μέτρα προστασίας γίνεται δυνατή η αντιμετώπιση της πλειοψηφίας των επιθέσεων σε καθημερινή βάση. Παρόλα αυτά όμως λόγω της βελτίωσης και της πολυπλοκότητας των ψηφιακών συστημάτων η χρήση όλων αυτών των εργαλείων (των μέτρων) δεν μας εγγυάται ότι είμαστε απόλυτα ασφαλείς από όλα τα είδη επιθέσεων.

Ο βαθμός πολυπλοκότητάς των ψηφιακών συστημάτων σημαίνει ότι συχνά μπορεί να περάσει σημαντικό χρονικό διάστημα μέχρι να αποκαλυφθεί μια επίθεση που δέχτηκε. Γι' αυτό ιδιαίτερη έμφαση πρέπει να δίνετε στην ταχεία ανίχνευση και την άμυνα.

Ωστόσο, ορισμένα εργαλεία ανίχνευσης, όπως η μηχανική μάθηση και η συμπεριφορική ανάλυση, που χρησιμοποιούν τα αντικά προγράμματα (antivirus) και επιδιώκουν τη μείωση των κινδύνων και την ανάλυση και άντληση δεδομένων από τη συμπεριφορά του συστήματος, εμφανίζουν χαμηλά ποσοστά υιοθέτησης από τις επιχειρήσεις. Αυτό οφείλεται εν μέρει στην παραγωγή ψευδώς θετικών αποτελεσμάτων, βάσει των οποίων μη απειλητικές δραστηριότητες παρουσιάζονται εσφαλμένα ως κακόβουλες.

Η απουσία μέχρι πρόσφατα κοινών απαιτήσεων σε επίπεδο Ευρωπαϊκής Ένωσης σχετικά με τη γνωστοποίηση περιστατικών εμπεριείχε τον κίνδυνο της καθυστέρησης κοινοποίησης των επιθέσεων και της παρεμπόδισης της αντίδρασης, πρόβλημα το

οποίο επιδιώχθηκε να αντιμετωπιστεί με τη θέσπιση της οδηγίας για την ασφάλεια δικτύων και πληροφοριών. Έτσι μετά την ανίχνευση και την ανάλυση μιας παραβίασης, πλέον είναι απαραίτητη η ταχεία γνωστοποίηση και αναφορά της, ούτως ώστε άλλοι δημόσιοι και ιδιωτικοί φορείς να λάβουν προληπτικά μέτρα, και οι αρμόδιες αρχές να παράσχουν στήριξη σε εκείνους που επλήγησαν.

Σε περιπτώσεις εκδήλωσης περιστατικού ασφάλειας, κάθε επιχείρηση προκειμένου να μπορέσει να ανταπεξέλθει στο περιστατικό και να προστατευθεί τόσο αυτή όσο και τα πρόσωπα και τα δεδομένα όπου προσβλήθηκαν οφείλει να ενημερώνει και να συνεργάζεται κατά τις διατάξεις του νόμου 4577/2018 (Α' 199), με τις αρμόδιες ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (Computer Security Incident Response Teams — CSIRT), γνωστές επίσης ως «ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική» (Computer Emergency Response Teams — CERT), την Εθνική Αρχή Κυβερνοασφάλειας και τους λοιπούς εμπλεκόμενους φορείς ώστε να διευκολύνεται η συνεργασία και η παροχή πληροφοριών και να εφαρμόζει τις προβλεπόμενες διαδικασίες προς άμεση επίλυση του περιστατικού και περιορισμό του αντίκτυπου αυτού διασφαλίζοντας τη συνέχιση παροχής υπηρεσιών της επιχείρησης.

Ιδιαίτερο ρόλο κατά την αντιμετώπιση περιστατικών ασφάλειας φέρουν οι ομάδες CSIRT και CERT των οποίων ο κύριος ρόλος είναι ο συντονισμός των δράσεων κατά τη διαχείριση ενός περιστατικού επίθεσης από τους εμπλεκόμενους φορείς, βάσει καθορισμένων ρόλων, αρμοδιοτήτων και διαδικασιών αλλά και επιχειρησιακών και επικοινωνιακών δυνατοτήτων. Σε εθνικό επίπεδο ήδη λειτουργούν ή μπορούν να δημιουργηθούν και άλλες ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών ανά τομέα.

Επιπρόσθετα, το Εθνικό CERT αποσκοπεί στη βελτιστοποίηση του επιπέδου πρόληψης, αξιολόγησης και ανάλυσης των απειλών μεταξύ των φορέων που συμμετέχουν στην Εθνική Στρατηγική. Το Εθνικό CERT, σε συνεργασία με τα άλλα CSIRT/CERT που λειτουργούν εντός της χώρας αλλά και με άλλα εθνικά CSIRT/CERT με τα οποία έχει συγκροτήσει ένα δίκτυο συνεργασίας, παρακολουθεί διαρκώς σε εθνικό και διεθνές επίπεδο τις απειλές και τις ευπάθειες των συστημάτων επικοινωνιών και πληροφορικής, τις αναλύει και τις αξιολογεί, με βάση τις ιδιαιτερότητες της χώρας, και ενημερώνει τους φορείς ώστε να ενισχυθεί η ετοιμότητά τους στην αντιμετώπιση περιστατικών ασφάλειας (Παππάς, 2018, σ. 13).

Σημαντικό επίσης είναι η επιχειρήσεις να κοινοποιούν το συμβάν στην Εθνική αρχή κυβερνοασφάλειας χωρίς αδικαιολόγητη καθυστέρηση και εντός 24 ωρών αφότου λάβουν γνώση του περιστατικού.

Η αποτελεσματική αντιμετώπιση δεν περιορίζεται μόνο στον μετριασμό των ζημιών, αλλά και στον προσδιορισμό των υπευθύνων για τις επιθέσεις. Η παρακολούθηση και ο εντοπισμός των επιτιθέμενων, μπορεί να παρουσιάσουν μεγάλες δυσκολίες λόγω της αυξανόμενης χρήσης εργαλείων ανωνυμοποίησης, και κρυπτογράφησης. Το πρόβλημα αυτό είναι γνωστό ως πρόβλημα απόδοσης ευθυνών. Το ζήτημα δεν είναι μόνο τεχνικό, αλλά δημιουργεί προκλήσεις και για την ποινική δικαιοσύνη.

Οι ποινικές έρευνες και η δίωξη των υπόπτων μπορεί να προσκρούουν στις νομικές και διαδικαστικές διαφορές μεταξύ των διαφόρων χωρών. Για την αντιμετώπιση του προβλήματος αυτού απαιτείται μια πιο τυποποιημένη επιχειρησιακή ανταλλαγή πληροφοριών, στο πλαίσιο σαφέστερων διαδικασιών, με την Ευρωπόλ ή με το Ευρωπαϊκό δικαστικό δίκτυο για το έγκλημα στον κυβερνοχώρο της Eurojust (Μονάδα δικαστικής συνεργασίας της ΕΕ).

Το στίγμα που αφορά τη φήμη μιας επιχείρησης μετά από ένα περιστατικό ψηφιακής παραβίασης παραμένει, αν και περιορισμένο. Αυτό όμως που εξακολουθεί να έχει μεγάλη σημασία για όλους, είναι η απώλεια δεδομένων. Οι άμεσες κινήσεις που πρέπει να κάνουν οι επιχειρήσεις έπειτα από μια παραβίαση. Οι κινήσεις αυτές είναι οι εξής

(Γεωργόπουλος):

- Να κατανοήσουν πώς συνέβη η επίθεση
- Να καταλάβουν πώς κλάπηκαν τα δεδομένα
- Να αποσυνδέσουν τους μολυσμένους υπολογιστές, για να αποφευχθεί η περαιτέρω προσβολή τους.
- Να προβούν σε αναβάθμιση πολιτικής ασφαλείας και μέτρων εφαρμογής
- Να προβούν σε επανεκπαίδευση του προσωπικού

Καίρια σημασία έχει επίσης και η έγκαιρης συμμετοχής των αρχών επιβολής του νόμου στην αρχική αντίδραση σε πιθανολογούμενα κυβερνοεγκλήματα, καθώς και η προληπτική ανταλλαγή πληροφοριών με τις CSIRT. Αυτό σημαίνει ότι καλούνται οι επιχειρήσεις να ανταλλάσσουν πληροφορίες που αφορούν στα συστήματα επικοινωνιών και πληροφορικής που χρησιμοποιούν, στις πολιτικές ασφαλείας που

έχουν υλοποιήσει, στις ευπάθειες, στις απειλές και στα περιστατικά ασφάλειας που αντιμετωπίζουν.

Αντίστοιχα, οι δημόσιοι φορείς καλούνται να ανταλλάσσουν πληροφορίες που έχουν συλλέξει οι επιχειρήσεις, γεγονός που ενδέχεται να θέσει σε κίνδυνο το επιθυμητό επίπεδο κυβερνοασφάλειας. Με τον συσχετισμό όμως αυτών των πληροφοριών είναι δυνατή η ανάλυση της εξέλιξης των απειλών που σχετίζονται με την Κυβερνοασφάλεια της χώρας.

Στόχος αυτής της συνεργασίας είναι η ανταλλαγή εμπειριών και βέλτιστων πρακτικών, καθώς και η διαπίστωση των δυνατοτήτων για την από κοινού ανάπτυξη κατάλληλων μέσων, με σκοπό την αντιμετώπιση απειλών και προκλήσεων που αφορούν την ασφάλεια του κυβερνοχώρου. Επίσης θα αξιοποιηθεί, στο μέγιστο δυνατό βαθμό, η συμβολή της χώρας μας στη διαμόρφωση και υλοποίηση σχετικών αποφάσεων που έχουν υιοθετηθεί στο πλαίσιο διεθνών Οργανισμών στους οποίους συμμετέχει η Ελλάδα, με σκοπό τόσο την ενίσχυση της κυβερνοασφάλειας σε εθνικό επίπεδο, όσο και τον εναρμονισμό μεταξύ των συναφών διεθνών μηχανισμών και δράσεων, λαμβάνοντας υπ' όψιν και την αυτονομία λήψης αποφάσεων σε εθνικό επίπεδο (Παππάς, 2018, σ. 16).

9. Νομοθετικό πλαίσιο

Από το 2002 έχουν εγκριθεί διάφορες νομοθετικές πράξεις που σχετίζονται σε διαφορετικό βαθμό με την κυβερνοασφάλεια. Η σημαντικότερη νομοθετική πράξη και κεντρικός πυλώνας της στρατηγικής για την κυβερνοασφάλεια του 2013 είναι η οδηγία του 2016 για την ασφάλεια δικτύων και πληροφοριών (οδηγία NIS) η πρώτη σε επίπεδο ΕΕ για την κυβερνοασφάλεια. Η οδηγία, η οποία έπρεπε να μεταφερθεί στο εθνικό δίκαιο έως τον Μάιο του 2018, επιδιώκει να επιτύχει ένα ελάχιστο επίπεδο εναρμονισμένων ικανοτήτων, υποχρεώνοντας τα κράτη μέλη να θεσπίσουν εθνικές στρατηγικές για την ασφάλεια δικτύων και πληροφοριών και να δημιουργήσουν ενιαία κέντρα επαφής και ομάδες απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (computer security incident response team - CSIRT)

Ακόμη, θεσπίζει απαιτήσεις ασφάλειας και κοινοποίησης για τους φορείς εκμετάλλευσης βασικών υπηρεσιών σε κρίσιμους τομείς και για τους παρόχους ψηφιακών υπηρεσιών.

Παράλληλα, ο γενικός κανονισμός για την προστασία των δεδομένων (ΓΚΠΔ) τέθηκε σε ισχύ το 2016 και σε εφαρμογή τον Μάιο του 2018.

Σύμφωνα με το ΓΚΠΔ «Δεδομένα προσωπικού χαρακτήρα» αποτελούν κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο. Το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα, ιδίως μέσω αναφοράς σε αναγνωριστικό στοιχείο ταυτότητας, όπως όνομα, σε αριθμό ταυτότητας, σε δεδομένα θέσης, σε επιγραμμικό αναγνωριστικό ταυτότητας ή σε έναν ή περισσότερους παράγοντες που προσιδιάζουν στη σωματική, φυσιολογική, γενετική, ψυχολογική, οικονομική, πολιτιστική ή κοινωνική ταυτότητα του εν λόγω φυσικού προσώπου. Ενώ «Προσωπικά δεδομένα ειδικών κατηγοριών» είναι τα δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν (Ένωση

Ασφαλιστών Εταιριών Ελλάδος ΕΑΕΕ, σ. 9):

- Φυλετική ή εθνοτική καταγωγή,
- Πολιτικά φρονήματα,
- Θρησκευτικές ή φιλοσοφικές πεποιθήσεις
- Συμμετοχή σε συνδικαλιστική οργάνωση
- Γενετικά δεδομένα
- Βιομετρικά δεδομένα
- Δεδομένα που αφορούν την υγεία
- Δεδομένα που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό

Στόχος του ΓΚΠΔ είναι η προστασία όλων των δεδομένων προσωπικού χαρακτήρα των ευρωπαίων πολιτών, μέσω του καθορισμού κανόνων για την επεξεργασία και τη διάδοσή τους. Παρέχει στα υποκείμενα των δεδομένων ορισμένα δικαιώματα και συνεπάγεται υποχρεώσεις για τους υπεύθυνους επεξεργασίας δεδομένων σχετικά με τη χρήση και τη διαβίβαση πληροφοριών. Επιπλέον, επιβάλλει απαιτήσεις κοινοποίησης σε περίπτωση παραβίασης και σε ορισμένες περιπτώσεις, προβλέπει πρόστιμα.

Η μη τήρηση των κανόνων του ΓΚΠΔ μπορεί να οδηγήσει σε σημαντικά πρόστιμα που μπορούν να φθάσουν μέχρι τα 20 εκατομμύρια ευρώ ή το 4% του συνολικού κύκλου εργασιών της επιχείρησης για ορισμένες παραβάσεις. Η Αρχή Προστασίας Δεδομένων μπορεί επίσης να επιβάλει συμπληρωματικά διορθωτικά μέτρα όπως η απαίτηση διακοπής της επεξεργασία προσωπικών δεδομένων (Ευρωπαϊκή Ένωση, 2021).

Το νομοθετικό πλαίσιο που καλύπτει την κυβερνοασφάλεια και ισχύει για την Ελλάδα καλύπτεται από το νόμο 4577, (ΦΕΚ Α' 199/03-12-2018) και περιλαμβάνει την ενσωμάτωση (στην ελληνική νομοθεσία) της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις. (Υπουργείο Ψηφιακής Διακυβέρνησης, 2018). Πιο αναλυτικά στην παραπάνω νομοθεσία αναφέρονται:

- Σύμφωνα με το άρθρο 2 της Οδηγίας 2016/1148/ΕΕ, η επεξεργασία δεδομένων προσωπικού χαρακτήρα, που γίνεται κατά τον παρόντα νόμο, διενεργείται σύμφωνα με τον Κανονισμό (ΕΚ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 (ΕΕ L 119) και το ν. 2472/1997 (Α' 50)
- Σύμφωνα με το άρθρο 7, 8 και 9 της Οδηγίας 2016/1148/ΕΕ, αναφέρονται οι αρμόδιες αρχές που είναι υπεύθυνες για το χειρισμό κινδύνων και συμβάντων βάσει καθορισμένων διαδικασιών.
- Σύμφωνα με τα άρθρα 11, 12 και 15 καθορίζονται οι απαιτήσεις ασφαλείας που πρέπει να τηρούνται και κοινοποίησης των συμβάντων καθώς και οι κυρώσεις αν δεν εφαρμοστούν οι απαιτήσεις αυτές.

Ενώ σύμφωνα με το άρθρο 4 του νόμου 4577/ 2018 (Α' 199), για τις βασικές απαιτήσεις ασφαλείας, οι ελληνικές επιχειρήσεις πρέπει να κατανοούν τη σχετική διακινδύνευση για την ασφάλεια των συστημάτων δικτύου και πληροφοριών και τους επιτρέπουν να εστιάσουν τις προσπάθειές τους και να διαχειριστούν τους πόρους τους, με αποτελεσματικό και αποδοτικό τρόπο. Στα πλαίσια του νόμου αυτού πρέπει να τηρηθούν μια σειρά από απαιτήσεις, οι σημαντικότερες εκ των οποίων είναι οι εξής

(Υπουργείο Ψηφιακής Διακυβέρνησης, 2019, σ. 2):

1. Αποτίμηση διακινδύνευσης: Η διακινδύνευση για την ασφάλεια των συστημάτων δικτύου και πληροφοριών αναγνωρίζεται, αναλύεται και αποτιμάται μέσω κατάλληλης, τεκμηριωμένης και αποτελεσματικής διεργασίας.

2. Στρατηγική διαχείρισης διακινδύνευσης: Καθορίζονται οι προτεραιότητες, περιορισμοί, ανοχές διακινδύνευσης και λοιπές παραδοχές οι οποίες χρησιμοποιούνται για την αιτιολόγηση των αποφάσεων σχετικά με τα επιλεγόμενα μέτρα διαχείρισης και μετριασμού της διακινδύνευσης για την ασφάλεια των συστημάτων δικτύου και πληροφοριών.
3. Διαχείριση διακινδύνευσης αλυσίδας εφοδιασμού: Η διακινδύνευση που αφορά στην αλυσίδα εφοδιασμού (προμηθευτές υλικού ή υπηρεσιών) εντοπίζεται, αξιολογείται και μετριάζεται. Ειδικότερα διασφαλίζεται, μέσω Συμφωνιών Επιπέδου Υπηρεσιών (Service Level Agreements - SLA) ή/και επιθεωρήσεις, ότι οι προμηθευτές εφαρμόζουν κατάλληλα και αναλογικά μέτρα ασφάλειας
4. Αυτοαξιολόγηση – Βελτίωση: Για την παρακολούθηση και συνεχή βελτίωση της ασφάλειας των συστημάτων δικτύου και πληροφοριών, συντάσσεται αναφορά αυτοαξιολόγησης συνοδευόμενης και από σχετικό πλάνο διορθωτικών ή βελτιωτικών ενεργειών, τα οποία κοινοποιούνται στην Εθνική Αρχή Κυβερνοασφάλειας
5. Χρήση κατάλληλων μηχανισμών αυθεντικοποίησης και διαδικασιών ελέγχου πρόσβασης.
6. Ασφάλεια δεδομένων: Τα δεδομένα διαχειρίζονται σύμφωνα με τη στρατηγική διαχείρισης διακινδύνευσης με σκοπό την προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητάς τους. Για το σκοπό αυτό εφαρμόζονται κατάλληλες πολιτικές και διαδικασίες
7. Αντίγραφα ασφαλείας. Τα δεδομένα τα οποία είναι απαραίτητα για την παροχή των βασικών υπηρεσιών διασφαλίζονται από πιθανή απώλειά τους μέσω της τήρησης αντιγράφων ασφαλείας σε κατάλληλη μορφή, η οποία δίνει τη δυνατότητα για άμεση ανάκτησή τους. Για το σκοπό αυτό εφαρμόζονται κατάλληλες πολιτικές, διαδικασίες και αυτοματοποιημένα συστήματα λήψης και διατήρησης αντιγράφων ασφαλείας.
8. Δοκιμές συστημάτων. Για την διασφάλιση της ανθεκτικότητας των συστημάτων που υποστηρίζουν βασικές υπηρεσίες έναντι απειλών, εφαρμόζονται κατάλληλες διαδικασίες δοκιμών και τεχνικών ελέγχων

10. Εκτίμηση Ρίσκου

Οι τουριστικές επιχειρήσεις όπως και οι περισσότερες επιχειρήσεις τα τελευταία χρόνια εξαρτώνται ολοένα και περισσότερο από τεχνολογίες πληροφορικής και επικοινωνιών για να εκτελούν την καθημερινή τους λειτουργία. Οι τεχνολογίες αυτές όμως υπόκεινται όπως είδαμε σε διάφορες απειλές, οι οποίες εκμεταλλεύονται γνωστές και άγνωστες ευπάθειες των συστημάτων με ενδεχόμενες σοβαρές επιπτώσεις στην επιχειρησιακή λειτουργία, στα πρόσωπα και στις κρίσιμες υποδομές λόγω της παραβίασης της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας της πληροφορίας όπου τα συστήματα αυτά επεξεργάζονται, αποθηκεύουν ή μεταδίδουν.

Οι απειλές όπως ήδη έχει αναφερθεί για τις τεχνολογίες πληροφορικής περιλαμβάνουν τόσο τις κυβερνοεπιθέσεις όσο και τα ανθρώπινα λάθη είτε αυτά προκύπτουν από λάθος ενός υπαλλήλου είτε από το διοικητικό προσωπικό. Για το λόγο αυτό, αποτελεί επιτακτική ανάγκη για τις επιχειρήσεις να συνειδητοποιήσουν την ευθύνη που φέρουν και να καθιερώσουν μία στρατηγική διαχείρισης προστασίας και αντιμετώπισης των κινδύνων σχετική με τη λειτουργία και τη χρήση των πληροφοριακών τους συστημάτων.

Ο οικονομικός αντίκτυπος της κυβερνοεγκληματικότητας από το 2013 ως το 2017 πενταπλασιάστηκε, πλήττοντας κυβερνήσεις και επιχειρήσεις, ανεξαρτήτως μεγέθους. Ενδεικτική της τάσης αυτής είναι η πρόβλεψη για αύξηση των κυβερνοασφαλίσεων από 3 δισεκατομμύρια ευρώ το 2018 σε 8,9 δισεκατομμύρια ευρώ το 2020 (Ευρωπαϊκή Ένωση, 2020, σσ. 12-20).

Ενώ ο οικονομικός αντίκτυπος των κυβερνοεπιθέσεων συνεχίζει να αυξάνεται, είναι εξαιρετικά ανησυχητική η απόκλιση μεταξύ του κόστους της εξαπόλυσης μιας επίθεσης και του κόστους της πρόληψης, της διερεύνησης και της αποκατάστασης μιας βλάβης.

Για παράδειγμα, μια επίθεση DDoS μπορεί να κοστίσει ακόμη και μόλις 15 ευρώ τον μήνα, ενώ οι ζημιές για τις επιχειρήσεις που έχουν μπει στο στόχο των κυβερνοεγκληματιών, συμπεριλαμβανομένης της προσβολής της φήμης τους, είναι σημαντικά υψηλότερες. Μολονότι το 80% των επιχειρήσεων της ΕΕ βίωσε τουλάχιστον ένα περιστατικό κυβερνοασφάλειας το 2016, η αναγνώριση των κινδύνων παραμένει σε ανησυχητικά χαμηλά επίπεδα.

Το 69% των επιχειρήσεων της Ευρωπαϊκής ένωσης αγνοεί ή κατανοεί ελάχιστα τους κινδύνους στους οποίους εκτίθεται στο διαδίκτυο ενώ το 60 % δεν έχει ποτέ προβεί σε

εκτίμηση των δυνητικών οικονομικών ζημιών. Επιπλέον, σύμφωνα με παγκόσμια έρευνα, το ένα τρίτο των επιχειρήσεων θα προτιμούσε να καταβάλει τα λύτρα παρά να πραγματοποιήσει επενδύσεις στην ασφάλεια πληροφοριών του κρατά.

Από κοινού, οι επιθέσεις με το λυτρισμικό WannaCry και το κακόβουλο λογισμικό διαγραφής δεδομένων (wiper) NotPetya το 2017 είχαν περισσότερα από 320 000 θύματα σε περίπου 150 χώρες.

Οι επιθέσεις αυτές είχαν ως αποτέλεσμα την αφύπνιση της παγκόσμιας κοινότητας σχετικά με την απειλή των κυβερνοεπιθέσεων, δημιουργώντας νέα δυναμική για την ενσωμάτωση της διάστασης της κυβερνοασφάλειας στον επίσημο σχεδιασμό πολιτικής. Πλέον, μάλιστα, το 86% των πολιτών της Ευρωπαϊκής Ένωσης πιστεύει ότι ο κίνδυνος να πέσουν θύματα κυβερνοεγκλήματος αυξάνεται.

Όσον αφορά την Ελλάδα είναι γνωστό ότι την αγορά κατακλύζουν μικρές και μεσαίες επιχειρήσεις πολλές εκ των οποίων είναι οικογενειακές. Γνωστό είναι επίσης ότι η Ελλάδα είναι ένας τόπος ο οποίος αποτελεί τουριστικό θέρετρο που δέχεται ετησίως εκατομμύρια τουρίστες από όλο τον κόσμο.

Οι τουριστικές επιχειρήσεις είτε λειτουργούν 6 μήνες το χρόνο είτε 12 θα πρέπει να έχουν κατά νου ότι οι κυβερνοαπειλές υπάρχουν και μπορούν να προκαλέσουν ζημιά οποιαδήποτε στιγμή. Η πίεση χρόνου που δέχονται κυρίως οι εποχιακές επιχειρήσεις και η σημασία που δίνουν για την προετοιμασία λειτουργίας τους αλλά και για την συντήρηση τους δεν πρέπει να τους αποπροσανατολίζει από τον υπάρχον κίνδυνο του διαδικτύου.

Μολονότι οι συνέπειες για τους οργανισμούς και επιχειρήσεις του ιδιωτικού τομέα μπορεί να είναι σοβαρές, οι αδυναμίες στη διακυβέρνηση του κυβερνοχώρου είναι πάρα πολλές. Σχεδόν εννέα στους δέκα οργανισμούς δηλώνουν ότι οι δραστηριότητές τους στον τομέα της κυβερνοασφάλειας δεν ανταποκρίνονται πλήρως στις ανάγκες τους. Για το λόγο αυτό θα πρέπει να εφαρμόζεται από όλες τις επιχειρήσεις μια εκτίμηση κινδύνου.

Η εκτίμηση κινδύνου σε μία επιχείρηση, αποτελεί μια συστηματική εξέταση κάθε διεξαγόμενης εργασίας, με σκοπό να εντοπισθούν οι πηγές που είναι ευπαθή ή μη αλλά μπορούν να αποτελέσουν κινδύνου. Η Εκτίμηση κινδύνου, αποτελεί ένα από τα

σημαντικότερα εργαλεία για την αποτελεσματική διαχείριση της ασφάλειας των συστημάτων μιας επιχείρησης και κατ' επέκταση της ίδιας.

Συγκεκριμένα, με την Εκτίμηση κινδύνου μπορεί να εντοπιστεί πως ενδέχεται να προκληθεί κίνδυνος για την ασφάλεια των συστημάτων και της επιχείρησης, να διαπιστωθεί ποια μέτρα πρέπει να ληφθούν και κατά πόσο μπορούν να αποφευχθούν ή να εξαλειφθούν οι κίνδυνοι και οι πηγές τους. Αν αυτό δεν είναι δυνατόν, θα πρέπει να καταγραφούν τα μέτρα πρόληψης που ήδη εφαρμόζονται, και να προταθούν αυτά που πρέπει να ληφθούν συμπληρωματικά, για τον έλεγχο των κινδύνων και την προστασία της δεδομένων της επιχείρησης.

10.1. Τι περιλαμβάνει η Εκτίμηση Κινδύνου

Η εκτίμηση του κινδύνου περιλαμβάνει την αναγνώριση και την καταγραφή των κινδύνων που υπάρχουν, καθώς και αυτών που ενδέχεται να εμφανισθούν. Τα στοιχεία που θα πρέπει οπωσδήποτε να συλλέγονται και να καταγράφονται είναι τα εξής:

- Όνομα και ιδιότητα του ατόμου (ή των ατόμων) που διεξάγει την εκτίμηση.
- Κίνδυνοι και πηγές κινδύνου που εντοπίστηκαν.
- Ομάδες εργαζομένων που εκτίθενται σε συγκεκριμένους κινδύνους.
- Απαραίτητα μέτρα προστασίας.
- Στοιχεία που αφορούν τη θέσπιση μέτρων, όπως το όνομα του υπευθύνου και η ημερομηνία.
- Λεπτομέρειες για τις ρυθμίσεις παρακολούθησης και αναθεώρησης, συμπεριλαμβανομένων των ημερομηνιών και των ατόμων που είναι αρμόδια για αυτές.
- Στοιχεία σχετικά με τη συμμετοχή των εργαζομένων και των εκπροσώπων τους στη διαδικασία εκτίμησης κινδύνου.

Ενδεικτικά οι κίνδυνοι που αφορούν τις τουριστικές επιχειρήσεις μπορεί να είναι:

- Οικονομικές επιπτώσεις / Απώλεια εσόδων
- Προσωπική προβολή / προβολή κοινωνικής ατζέντας
- Οικονομική κατασκοπία
- Λήψη / Αποστολή κακόβουλου λογισμικού

- Υποκλοπή εταιρικών πληροφοριών ή προσωπικών δεδομένων τόσο του προσωπικού της επιχείρησης όσο και των πελατών της.
- Εκβιασμός αποκάλυψης δεδομένων
- Διακοπή εργασιών / Επίθεση άρνησης υπηρεσιών / εξυπηρέτησης
- Δυσφήμιση

Η επιλογή όμως για το πώς θα προσεγγίσει μια επιχείρηση την εκτίμηση κινδύνου εξαρτάται κυρίως από τη φύση της εργασίας και το είδος των διαδικασιών που εκτελεί. Σε ορισμένες περιπτώσεις μπορεί να κριθεί κατάλληλη μία ενιαία προσέγγιση που να καλύπτει όλους τους κινδύνους σε ένα χώρο εργασίας ή μια δραστηριότητα ενώ σε άλλες περιπτώσεις, να χρειάζεται να πραγματοποιηθούν διαφορετικές προσεγγίσεις για το χώρο εργασίας και για τις δραστηριότητες που εκτελούνται εκεί (Καραμπέκιος, 2012).

Η ικανότητα των επιχειρήσεων να ανιχνεύουν κακόβουλες επιθέσεις, να τις αντιμετωπίζουν και να ανακτούν τη λειτουργικότητά τους μετά από μία παραβίαση στα συστήματά τους αποτελεί προτεραιότητα και οδηγεί στη διασφάλιση της επιχειρησιακής συνέχειας και στην αδιάλειπτη παροχή των υπηρεσιών της. Οι επιπτώσεις από τη μη υλοποίηση ενός επαρκούς σχεδίου διαχείρισης περιστατικών κυβερνοασφάλειας μπορεί να είναι ιδιαίτερα σοβαρές όσον αφορά (Υπουργείο Ψηφιακής Διακυβέρνησης, 2021, σ. 45):

- Την αδυναμία περιορισμού της ζημιάς: είτε επειδή δεν έχει αντιληφθεί ότι λαμβάνει χώρα περιστατικό ή είτε ήδη έχει συμβεί και υπάρχει περιορισμένη ικανότητα για την αποτελεσματική αντιμετώπιση. Το γεγονός αυτό μπορεί να οδηγήσει σε διακοπή λειτουργίας συστημάτων άρα και σε πώλεια χρημάτων ή περιουσιακών στοιχείων από τη μη εξουσιοδοτημένη πρόσβαση στους τραπεζικούς λογαριασμούς της επιχείρησης αλλά και σε απώλεια κερδών σε περίπτωση συμβάντος διακοπής εργασιών.
- Τη φήμη της επιχείρησης: η αδυναμία παροχής διασφάλισης των προσωπικών δεδομένων των πελατών αλλά και γενικότερα των αρχείων μιας επιχείρησης μπορεί να επηρεάσει τη φήμη της.
- Τις συνεχείς διαταραχές λειτουργίας: μια επιχείρηση που αδυνατεί να αντιμετωπίσει τη ριζική αιτία του περιστατικού (ελλιπείς τεχνολογίες, ευπάθειες σε συστήματα και εφαρμογές κ.α) θα παραμένει εκτεθειμένη σε επαναλαμβανόμενα συμβάντα παραβιάσεων.

- Την ανάγκη για νέο εξοπλισμό: εφόσον τα δεδομένα ή το υλικό υποστούν βλάβη η επιχείρηση θα είναι αναγκαίο να προχωρήσει σε έξοδα για την αγορά νέου υλικού.
- Τις διοικητικές και οικονομικές κυρώσεις: ένα περιστατικό που έχει σαν αποτέλεσμα την παραβίαση ευαίσθητων δεδομένων μπορεί να οδηγήσει σε σημαντικές κυρώσεις, όταν μετά από έλεγχο προκύψει ότι η επιχείρηση δεν είχε συμμορφωθεί με συγκεκριμένες νομικές και κανονιστικές διατάξεις.

Για να μπορέσει να υπάρξει μια στρατηγική απέναντι στις κυβερνοαπειλές αρχικά είναι απαραίτητη η αξιολόγηση του κινδύνου που έχει να αντιμετωπίσει η κάθε επιχείρηση.

Σε επίπεδο Ευρωπαϊκής Ένωσης δεν υφίστανται παγιωμένοι κανόνες σχετικά με τον τρόπο διεξαγωγής της εκτίμησης κινδύνου η κάθε χώρα φέρει την δική της νομοθεσία όσον αφορά την εκτίμηση κινδύνου από κυβερνοεπιθέσεις παρόλα αυτά κατά την προσέγγιση μιας εκτίμησης κινδύνου θα πρέπει πάντοτε να λαμβάνονται υπόψη οι εξής δύο αρχές (EU-OSHA , 2021):

- Η διάρθρωση της εκτίμησης θα πρέπει να διασφαλίζει την κάλυψη όλων των συναφών πηγών κινδύνων και πιθανών κινδύνων.
- Μόλις προσδιοριστεί ένας κίνδυνος, η διαδικασία της εκτίμησης οφείλει να ξεκινήσει από τις βασικές αρχές της εξετάζοντας καταρχάς εάν μπορεί να εξαλειφθεί εντελώς.

Οι κατευθυντήριες γραμμές της Ευρωπαϊκής Ένωσης σχετικά με την εκτίμηση κινδύνου στις επιχειρήσεις προτείνουν μια σταδιακή προσέγγιση που βασίζεται σε μια σειρά βημάτων. Φυσικά δεν πρόκειται για τη μοναδική μέθοδο διεξαγωγής της εκτίμησης κινδύνου, υπάρχουν πολλές και διαφορετικές μεθοδολογίες για την επίτευξη του ίδιου σκοπού, στις περισσότερες όμως επιχειρήσεις, κυρίως στις μικρές και μικρομεσαίες επιχειρήσεις, μια απλή ποσοτική προσέγγιση της εκτίμησης κινδύνου που ενσωματώνει στοιχεία διαχείρισης κινδύνου όπως η παρακάτω προσέγγιση, είναι συνήθως επιτυχής (EU-OSHA , 2021).

10.2. Προσέγγιση εκτίμησης κινδύνου

Βήμα 1ο: Προσδιορισμός των πηγών κινδύνων καθώς και των ατόμων που απειλούνται από αυτές.

Στο πρώτο αυτό βήμα περιλαμβάνεται η αναζήτηση στον εργασιακό χώρο των παραγόντων εκείνων οι οποίοι θα μπορούσαν να προκαλέσουν βλάβη και προσδιορισμός των εργαζομένων οι οποίοι μπορεί να εκτίθενται σε κάποια πηγή κινδύνου. Πιο συγκεκριμένα για τον προσδιορισμό των πηγών κινδύνου θα πρέπει:

- Να εντοπιστούν οι πηγές απειλών που σχετίζονται με την επιχείρηση (κακόβουλες ομάδες, ανταγωνιστές, φυσικές απειλές, ανθρώπινα λάθη)
- Να εντοπιστούν οι ενέργειες που θα μπορούσαν να συμβούν από τις παραπάνω πηγές απειλών (κυβερνοεπιθέσεις, φυσικές καταστροφές, βλάβη υλικού/λογισμικού)
- Να εντοπιστούν τα αδύναμα σημεία (ευπάθειες) της επιχείρησης που θα μπορούσε κάποια πηγή να τις εκμεταλλευτεί μέσω συγκεκριμένων ενεργειών.

Βήμα 2ο: Εκτίμηση των κινδύνων και καθορισμός προτεραιοτήτων.

Αφού αποτυπωθούν οι παράγοντες από τους οποίους μπορεί να προκληθεί κίνδυνος ακολουθεί ο υπολογισμός της σοβαρότητας και της πιθανότητας πρόκλησης βλάβης από την κάθε πηγή κινδύνου ξεχωριστά και ο καθορισμός προτεραιοτήτων με βάση τη σοβαρότητα του κάθε κινδύνου. Στη διαδικασία αυτή συμπεριλαμβάνεται και:

- Ο υπολογισμός της πιθανότητας ότι οι αναγνωρισμένες πηγές μπορούν να ξεκινήσουν συγκεκριμένες ενέργειες αλλά και η πιθανότητα επιτυχούς πραγματοποίησης τους.
- Η εκτίμηση και ο υπολογισμός των επιπτώσεων (στις λειτουργίες και στα συστήματα της επιχείρησης αλλά και σε πρόσωπα, υπαλλήλους και πελάτες) εάν οι ενέργειες πραγματοποιηθούν. Π.χ Γεγονότα όπως επίθεση άρνησης παροχής υπηρεσιών, ξαφνική πτώση της ταχύτητας του δικτύου, αλλά και φυσικές καταστροφές όπως σεισμός, φωτιά ή πλημμύρα μπορούν να προκαλέσουν πρόσκαιρη ή και παρατεταμένη διακοπή των επιχειρηματικών λειτουργιών.

Για τον σκοπό αυτό, χρησιμοποιείται ο παρακάτω πίνακας - Εικόνα 7 - σύμφωνα με τον οποίο μπορεί να αποφασιστεί ο βαθμός της επικινδυνότητας που ενέχει κάθε πιθανός κίνδυνος.

ΣΟΒΑΡΟΤΗΤΑ	ΠΙΘΑΝΟΤΗΤΑ
------------	------------

ΣΥΝΕΠΕΙΩΝ	Απίθανο	Απομακρυσμένο	Πιθανό	Πολύ Πιθανό
Πολύ Χαμηλή	Αμελητέα	Χαμηλή	Χαμηλή	Μέτρια
Χαμηλή	Χαμηλή	Χαμηλή	Μέτρια	Μέτρια
Μέτρια	Χαμηλή	Μέτρια	Μέτρια	Υψηλή
Υψηλή	Μέτρια	Μέτρια	Υψηλή	Υψηλή

Εικόνα 7 Πίνακας Επικινδυνότητας

Κριτήρια κατάταξης Πιθανότητας:

Απίθανο: Ενδέχεται να μην παρουσιαστεί κίνδυνος.

Απομακρυσμένο: Το ενδεχόμενο να παρουσιαστεί κίνδυνος είναι χαμηλό.

Πιθανό: Ενδέχεται η πηγή να αποτελέσει κίνδυνο αρκετές φορές.

Πολύ Πιθανό: Το ενδεχόμενο να αποτελέσει κίνδυνο η πηγή αυτή είναι υψηλό και με πιθανότητα επανάληψης.

Κριτήρια κατάταξης Σοβαρότητας Συνεπειών:

Πολύ Χαμηλή: Επικίνδυνα συμβάντα τα οποία όμως δεν προκαλούν βλάβη ή απειλή για την επιχείρηση, τους εργαζομένους ή τους πελάτες αλλά ενδεχομένως θα μπορούσαν να προκαλέσουν δυνητικά.

Χαμηλή: Βλάβη ή απειλή η οποία δεν προκαλεί σημαντική απώλεια ή ζημιά στην επιχείρηση, στους εργαζομένους ή στα ψηφιακά συστήματα π.χ μόλυνση ενός μεμονωμένου υπολογιστικού συστήματος, ή διέρευση κρυπτογραφημένων πληροφοριών. Συμβάντα που μπορούν να τεθούν άμεσα υπό έλεγχο.

Μέτρια: Βλάβες ή απειλές που προκαλούν μικρή, μέτρια, παρατεταμένη ή συχνά επαναλαμβανόμενη απειλή όπως μόλυνση από κακόβουλο λογισμικό τύπου ransomware όπου απαιτείται η καταβολή αντιτίμου για να επανέλθει η κανονική ροή λειτουργίας των ψηφιακών συστημάτων.

Υψηλή: Βλάβες ή απειλές σοβαρές ή μόνιμες για την συνέχιση λειτουργίας της επιχείρησης όπως διαρροή ευαίσθητων δεδομένων. Επιβάλλεται η γνωστοποίησή τους στην Εθνική Αρχή Κυβερνοασφάλειας και στο αρμόδιο CSIRT με βάση τη σχετική νομοθεσία.

Βήμα 3ο: Λήψη αποφάσεων σχετικά με προληπτική δράση

Στο τρίτο βήμα γίνεται ο προσδιορισμός των κατάλληλων μέτρων που πρέπει να ακολουθηθεί από την επιχείρηση ώστε οι κίνδυνοι που ενδεχομένως να υπάρξουν να μπορέσουν να εξαλειφθούν ή να τεθούν υπό έλεγχο άμεσα.

Ανάλογα με τη διαβάθμιση της Επικινδυνότητας του κινδύνου που θα προκύψει με βάση τον παραπάνω πίνακα δίνονται και οι αντίστοιχες επεξηγήσεις:

Υψηλή Επικινδυνότητα: Αν η επικινδυνότητα είναι μεγάλη και έχει εκτιμηθεί ως Υψηλή (δηλαδή κρίνεται ως ανεπίτρεπτη), οι ενέργειες εκ μέρους του εργοδότη και η λήψη προτεινόμενων μέτρων για την μείωση της επικινδυνότητας πρέπει να είναι άμεσες.

Μέτρια Επικινδυνότητα: Αν η επικινδυνότητα είναι μέτρια και έχει εκτιμηθεί ως επιτρεπτή, η εισήγηση είναι να προγραμματιστεί ο σχεδιασμός ενεργειών για μείωση του επιπέδου επικινδυνότητας σε Χαμηλή, μέσα σε εύλογα χρονικά διαγράμματα που καθορίζει ο εργοδότης λαμβάνοντας υπόψη του διάφορες παραμέτρους (π.χ. απλότητα λήψης των μέτρων από τον ίδιο, ανάγκη για ανάθεση λήψης μέτρων μέσω εξωτερικού συνεργάτη, συχνότητα χρήσης του χώρου και έκθεσης εργαζομένων κ.ά. μέτρων).

Χαμηλή Επικινδυνότητα: Αν η επικινδυνότητα είναι μικρή και έχει εκτιμηθεί ως επιτρεπτή, είναι αναγκαίο να επιβεβαιωθεί ότι η επικινδυνότητα θα παραμείνει στα ίδια επίπεδα.

Αμελητέα Επικινδυνότητα: Αν η επικινδυνότητα είναι αμελητέα, ο εργοδότης δεν υποχρεούται να λάβει συγκεκριμένα προληπτικά και προστατευτικά μέτρα.

Βήμα 4ο: Ανάληψη δράσης

Υποχρεωτική τήρηση μέτρων πρόληψης και προστασίας μέσω στρατηγικής που θα ορίζει η επιχείρηση σύμφωνα με τις προτεραιότητες που έχει θέσει.

Βήμα 5ο: Παρακολούθηση και αναθεώρηση

Η εκτίμηση κινδύνου θα πρέπει να αναθεωρείται ανά τακτά χρονικά διαστήματα, ώστε να είναι επίκαιρη και ενήμερη σύμφωνα με τις τελευταίες τεχνολογικές βελτιώσεις και εξελίξεις.

Τα αποτελέσματα των εκτιμήσεων κινδύνου θα πρέπει να καταγράφονται από τις επιχειρήσεις προκειμένου να αποτελέσουν βάση για:

- Αξιολόγηση και παρακολούθηση και για το κατά πόσο έχουν θεσπιστεί τα απαραίτητα μέτρα.
- Τυχόν αναθεώρηση σε περίπτωση μεταβολής των συνθηκών.
- Διαβίβαση πληροφοριών στις αρμόδιες αρχές.
- Αποδεικτικά στοιχεία και προσκόμιση σε εποπτικές αρχές.

Προκειμένου ένα σύστημα διαχείρισης ασφάλειας πληροφοριών να υλοποιηθεί με αποτελεσματικότητα, θα πρέπει η εκάστοτε επιχείρηση να δημιουργήσει κατάλληλη οργανωτική δομή με αρμοδιότητα την ασφάλεια των πληροφοριακών συστημάτων, όπου θα πρέπει:

- Να οριστούν οι κατάλληλοι ρόλοι και αρμοδιότητες στο προσωπικό διοικητικό και μη.
- Να είναι επαρκώς στελεχωμένη με πρόσωπα που κατέχουν τεχνική και νομική εξειδίκευση στα θέματα της ασφάλειας του κυβερνοχώρου και
- Να διατεθούν οι απαιτούμενοι πόροι για την υλοποίηση των στόχων που έχουν τεθεί για την κυβερνοασφάλεια.

Ενώ για να προσδιοριστεί η σοβαρότητα του αντίκτυπου ενός συμβάντος, λαμβάνονται υπόψη οι παρακάτω παράμετροι:

1. Ο αριθμός των χρηστών που επηρεάζονται από τη διατάραξη της βασικής υπηρεσίας.
2. Η διάρκεια του συμβάντος.
3. Το γεωγραφικό εύρος της περιοχής που επηρεάζεται από το συμβάν.
4. Η έκταση των επιπτώσεων στις οικονομικές και κοινωνικές δραστηριότητες.

Οι καταγραφές των εκτιμήσεων θα πρέπει να καταρτίζονται κατόπιν διαβούλευσης και συμμετοχής των εργαζομένων ή και των εκπροσώπων τους και στη συνέχεια να

διατίθενται προς ενημέρωση. Σε κάθε περίπτωση, οι ενδιαφερόμενοι εργαζόμενοι πρέπει να ενημερώνονται για το αποτέλεσμα κάθε εκτίμησης που αφορά τη θέση εργασίας τους και για τα μέτρα που πρόκειται να ληφθούν ως αποτέλεσμα της εκτίμησης.

Με βάση τον υπολογισθέντα κίνδυνο, η επιχείρηση μπορεί να προβεί σε επιλογή των ανάλογων μέτρων προστασίας, προκειμένου οι κίνδυνοι να αντιμετωπιστούν επαρκώς.

Παράλληλα η επιχείρηση οφείλει να αναπτύξει πολιτική ασφάλειας, που θα ορίζει σε υψηλό επίπεδο τους στόχους ασφάλειας και την επίτευξή τους έπειτα από την εκτίμηση που διεξήγαγε ενώ θα παραπέμπει σε ειδικότερες θεματικές πολιτικές και διαδικασίες που θα εξειδικεύουν την υλοποίηση και εφαρμογή των επιλεγμένων μέτρων προστασίας.

Η διαχείριση του κινδύνου αποτελεί πάντα το σημείο εκκίνησης για μία αποτελεσματική προσέγγιση στην κυβερνοασφάλεια. Έτσι, οι επιχειρήσεις οφείλουν να καθιερώσουν ένα σύστημα διαχείρισης ασφάλειας πληροφοριών (information security management system), το οποίο:

- ✓ Θα υλοποιείται με την εφαρμογή τεχνικών και οργανωτικών μέτρων ασφάλειας που θα βασίζονται στη διαχείριση του κινδύνου (risk based).
- ✓ Θα έχει την πλήρη οικονομική και οργανωτική υποστήριξη της διοικητικής ηγεσίας.
- ✓ Θα επιθεωρείται και θα ανανεώνεται σε τακτά χρονικά διαστήματα.
- ✓ Θα διαμορφώνει μία κουλτούρα κυβερνοασφάλειας σε όλους τους εμπλεκόμενους (ανώτερη Διοίκηση, σύνολο του προσωπικού, παρόχους και προμηθευτές).

Όσο μεγαλύτερος είναι ο όγκος πληροφοριών και δεδομένων που καλείται να διαχειριστεί μια επιχείρηση τόσο αυξάνονται οι ευθύνες και η ανάγκη για μεγαλύτερη ασφάλεια και ειδικά όταν πρόκειται για επιχειρήσεις που κρατούν δεδομένα μεγάλης κλίμακας.

Σε αυτήν την προσπάθεια των επιχειρήσεων μπορούν να συνεισφέρουν οι υπεύθυνοι συνεργάτες ασφαλείας πληροφοριακών συστημάτων και δικτύων με κατάλληλα τεχνικά και οργανωτικά προσόντα, όπως.

DPO (Data Protection Officer), Υπεύθυνος Ασφάλειας Πληροφοριών και Δικτύων. Ο DPO:

- Αποτελεί το σημείο επαφής με την Εθνική Αρχή Κυβερνοασφάλειας και το αρμόδιο CSIRT.
- Συνεργάζεται με την Εθνική Αρχή Κυβερνοασφάλειας και με το αρμόδιο CSIRT.
- Συντονίζει και επιβλέπει τον Οργανισμό ως προς τις υποχρεώσεις που απορρέουν από τον ν. 4577/2018 (Α' 199), από την παρούσα υπουργική απόφαση και από άλλες διατάξεις της Ευρωπαϊκής Ένωσης ή της Εθνικής Αρχής Κυβερνοασφάλειας σχετικά με την Ασφάλεια Συστημάτων Δικτύων και Πληροφοριών.
- Εποπτεύει την υλοποίηση της Ενιαίας Πολιτικής Ασφάλειας και την ικανοποίηση των βασικών απαιτήσεων ασφάλειας, την εκπαίδευση και ευαισθητοποίηση των υπαλλήλων του Οργανισμού σε θέματα ασφάλειας πληροφοριών και δικτύων καθώς, και τη σύνταξη της αναφοράς αυτοαξιολόγησης του Οργανισμού που αποστέλλεται στην Εθνική Αρχή Κυβερνοασφάλειας.
- Παρίσταται στους ελέγχους που πραγματοποιεί η Ομάδα Επιθεώρησης Ελέγχου, όπως αυτή ορίζεται από την Εθνική Αρχή Κυβερνοασφάλειας, και της παρέχει όλα τα κατάλληλα μέσα για να διευκολύνει το έργο της. Ο ρόλος του στην οργανωτική δομή του Οργανισμού προτείνεται να είναι ανεξάρτητος και να μην έγκειται σε σύγκρουση συμφερόντων με άλλους εργασιακούς ρόλους που τυχόν κατέχει.

CISO (Chief Information Security Officer) υπεύθυνος ασφάλειας πληροφοριακών συστημάτων. Ο CISO είναι τυπικά υπεύθυνος για την παροχή στρατηγικού επιπέδου οδηγιών για τα θέματα κυβερνοασφάλειας της επιχείρησης, την επίβλεψη και παρακολούθηση του συστήματος διαχείρισης ασφάλειας πληροφοριών και τη διασφάλιση της συμμόρφωσης της επιχείρησης με τις αντίστοιχες νομοθετικές και κανονιστικές ρυθμίσεις όπως αυτές ορίζονται από το κάθε κράτος. Πρόκειται για ρόλο με αναγκαία ηγετικά χαρακτηριστικά και με ευθύνη να συντονίζει τους στόχους της κυβερνοασφάλειας με τους επιχειρησιακούς στόχους εντός της επιχείρησης.

Από τη μεριά της η Εθνική Αρχή Κυβερνοασφάλειας, σε συνεργασία με την αρμόδια CSIRT και τους λοιπούς ανά τομέα βασικής υπηρεσίας, εμπλεκόμενους φορείς:

1. Αξιολογεί τα τεχνικά και οργανωτικά μέτρα που λαμβάνουν οι επιχειρήσεις για τη διαχείριση των κινδύνων που αφορούν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούν στις δραστηριότητές τους, ως προς την καταλληλότητα και την αναλογικότητά τους.

2. Αξιολογεί την καταλληλότητα των μέτρων που λαμβάνουν οι επιχειρήσεις για την αποτροπή και την ελαχιστοποίηση του αντίκτυπου συμβάντων που επηρεάζουν την ασφάλεια των συστημάτων δικτύου και πληροφοριών που χρησιμοποιούνται για την παροχή των βασικών υπηρεσιών, με σκοπό τη διασφάλιση της επιχειρησιακής τους συνέχειας.
3. Καθορίζει τη διαδικασία κοινοποίησης που πρέπει να τηρούν προκειμένου να κοινοποιήσουν στην Εθνική Αρχή Κυβερνοασφάλειας και στην αρμόδια CSIRT συμβάντα με σοβαρές επιπτώσεις στην επιχειρησιακή συνέχεια των βασικών υπηρεσιών που αυτοί παρέχουν.

Η ασφαλιστική κάλυψη ως εργαλείο διαχείρισης κινδύνου

Δεδομένου ότι τα παραδοσιακά ασφαλιστήρια που χρησιμοποιούνται για την ασφαλιστική κάλυψη των ξενοδοχειακών μονάδων δεν είναι πλέον αρκετά, γιατί περιέχουν καλύψεις οι οποίες δεν μπορούν να ανταποκριθούν πλήρως σε πιθανές κυβερνοεπιθέσεις, δημιουργήθηκε η ανάγκη για εξειδικευμένα ασφαλιστήρια.

Έτσι επιπτώσεις από παραβίαση συστημάτων και διαρροής ευαίσθητων δεδομένων μπορούν πλέον να καλυφθούν από τα εξειδικευμένα ασφαλιστήρια τα οποία μπορούν να αντιμετωπίσουν ολοκληρωτικά τις συνέπειες κινδύνους που προκαλούν παραβιάσεις συστημάτων. Η σωστή οργάνωση, ο προγραμματισμός, η λήψη κατάλληλων μέτρων πρόληψης και προστασίας, η ύπαρξη διαδικασιών και ενός πλάνου αντιμετώπισης περιστατικών είναι απαραίτητα συστατικά, όμως ακόμα και μια πολύ καλά οργανωμένη επιχείρηση δεν μπορεί να αντιμετωπίσει πλήρως το σύνολο των επιπτώσεων αποτελεσματικά λόγω της έλλειψης εμπειρίας σε ανάλογες καταστάσεις.

Για την αντιμετώπιση και διαχείριση περιστατικών παραβίασης συστημάτων, απώλειας δεδομένων και άρνησης παροχής υπηρεσίας απαιτούνται να καλυφθούν άμεσα και έμμεσα κόστη όπως:

Άμεσα κόστη τα οποία περιλαμβάνουν, επαγγελματικές αμοιβές εξειδικευμένων συμβούλων διαχείρισης περιστατικών παραβίασης συστημάτων, πρόστιμα και έξοδα όπως:

- Αμοιβές εξειδικευμένου δικηγόρου

- Υπηρεσίες ειδικών ψηφιακής εγκληματολογίας
- Υπηρεσίες δημοσίων σχέσεων και επικοινωνίας
- Υπηρεσίες τηλεφωνικού κέντρου
- Credit monitoring παρακολούθηση συναλλαγών πιστωτικών καρτών
- Έξοδα αντικατάστασης στοιχείων ενεργητικού όπως αντικατάσταση της πιστωτικής κάρτας του πελάτη και αντικατάσταση υλικού hardware ή software κ.λπ.
- Πρόστιμα για μη τήρηση της νομοθεσίας περί προσωπικών δεδομένων
- Έξοδα για την επίτευξη επιχειρησιακής συνέχειας

Έμμεσα κόστη μπορεί να είναι ακόμα πιο σημαντικά, συμπεριλαμβανομένων:

- Μείωση της φήμης της εταιρίας
- Την πτώση των εσόδων
- Χαμένων επιχειρηματικών ευκαιριών
- Απώλειας πελατών
- Απώλειας συνεργατών
- Αύξηση των αμοιβών των υπηρεσιών τρίτων παρόχων
- Κόστη εκπαίδευσης και ευαισθητοποίησης σε θέματα ασφάλειας πληροφοριών του ανθρώπινου δυναμικού της εταιρίας,
- Πρόσθετα επαναλαμβανόμενα έξοδα για ελέγχους ασφάλειας.

Δυστυχώς, πολλά από αυτά τα κόστη είναι απρογραμμάτιστα και μπορούν να έχουν αρνητική επίπτωση στην ρευστότητα και τις ταμειακές ροές μιας επιχείρησης.

Τα κόστη που μπορούν να προκύψουν όμως δεν είναι πάντα μόνο οικονομικά. Το 57% των συμβάντων απώλειας δεδομένων είχε αρνητικό αντίκτυπο στη συνολική λειτουργία της επιχείρησης. Επίσης, πάνω από τα μισά περιστατικά απώλειας δεδομένων (56%) έχουν αρνητικό αντίκτυπο στη φήμη και την αξιοπιστία μιας εταιρείας. Όπως προκύπτει από έρευνα, το 61% των ερωτηθέντων αντιμετώπισε προβλήματα με ιούς, worms, Trojans και άλλα είδη κακόβουλου λογισμικού.

Τα διαθέσιμα συμβόλαια στην Ελληνική ασφαλιστική αγορά προσφέρουν τις ακόλουθες βασικές καλύψεις (Παπαγεωργίου):

- Αστικής ευθύνης έναντι τρίτων, συνεπεία κυβερνοεπίθεσης
- Δαπανών διοικητικών υποχρεώσεων (νομική προστασία και διοικητικά πρόστιμα)

- Δαπανών διαχείρισης γεγονότων

Προαιρετικά παρέχονται καλύψεις όπως:

- Απώλειας καθαρού κέρδους, συνεπεία διακοπής λειτουργίας του δικτύου
- Δαπανών εκβιασμού
- Παραβίασης πνευματικής ιδιοκτησίας

Ενώ στις διεθνείς αγορές υπάρχει και η δυνατότητα κάλυψης φυσικής ζημιά στα πάγια περιουσιακά στοιχεία μιας επιχείρησης, συνεπεία μιας κυβερνοεπίθεσης. Ο κίνδυνος αυτός αναμένεται να λάβει σημαντικές διαστάσεις με την αύξηση των τεχνολογιών διασύνδεσης και εκείνη του Internet of Things (IoT).

Η ασφάλιση αποτελεί ένα εργαλείο διαχείρισης κινδύνου και αποτελεσματικής διαχείρισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων πελατών. Λαμβάνοντας υπόψη ότι δεν μπορούμε να εξαλείψουμε την πιθανότητα πραγματοποίησης συμβάντων θα πρέπει να μπορούμε να διαχειριστούμε αποτελεσματικά περιστατικά απώλειας δεδομένων και εμπιστευτικών πληροφοριών.

Η ασφάλιση Cyber Insurance προσφέρει εκτός από την κάλυψη των χρηματοοικονομικών επιπτώσεων της εταιρίας και πρόσβαση σε ομάδες ειδικών οι οποίες έχουν αντιμετωπίσει πλήθος περιστατικών. Η πρόσβαση σε ομάδες ειδικών μπορεί να βοηθήσει και να ελαχιστοποιήσει την οικονομική καταστροφή και τη βλάβη της φήμης που μπορεί να συντελεστεί σε σύντομο χρονικό διάστημα.

11. Συμπεράσματα

Συνοψίζοντας λοιπόν βλέπουμε ότι η ψηφιοποίηση όλο και περισσότερων διαδικασιών προκάλεσε την αποδυνάμωση των υπαρχόντων μέτρων ασφάλειας στον κυβερνοχώρο μέσω αλλαγών στα πρότυπα εργασίας και υποδομής που προκλήθηκαν από την πανδημία COVID-19 και δημιουργήθηκαν ευκαιρίες για εξατομικευμένες επιθέσεις από τους ιδιαίτερα «έξυπνους» εγκληματίες του κυβερνοχώρου με τη χρήση προηγμένων μεθόδων και τεχνικών. Οι τεχνικές επιθέσεων έρχονται σε πολλές διαφορετικές μορφές και μπορούν να εκτελεσθούν οπουδήποτε εμπλέκεται η ανθρώπινη αλληλεπίδραση. Οι επιθέσεις αυτές γίνεται αντιληπτό ότι μπορούν να είναι εξαιρετικά δαπανηρές για τις επιχειρήσεις. Το κίνητρο των κυβερνοεπιθέσεων σε κάθε περίπτωση μπορεί να

διαφέρει η ανάγκη όμως για ασφάλεια είναι πάντα ίδια για όλες τις επιχειρήσεις. Για το λόγο αυτό είναι απαραίτητο οι επιχειρήσεις να σχεδιάζουν μια στρατηγική προστασίας η οποία ως κατευθυντήρια γραμμή θα έχει το σχέδιο εκτίμησης κινδύνου, βάσει του οποίου θα λάβει όλα τα απαραίτητα μέτρα πρόληψης και αντιμετώπισης. Επιχειρήσεις οι οποίες διαθέτουν ελλιπείς σχέδια εκτίμησης ρίσκου διακυβεύουν ουσιαστικά τα κέρδη τους αλλά και την ίδια τη βιωσιμότητά τους. Στόχος είναι να προλαμβάνουν τον κίνδυνο λαμβάνοντας μέτρα κατάλληλα για την πρόληψη τέτοιων επιθέσεων βελτιώνοντας την ασφάλεια των ψηφιακών συστημάτων και εφαρμογών τους και διασφαλίζοντας της επιχειρησιακή τους συνέχιση.

Παράλληλα η θεσμική θωράκιση του εθνικού πλαισίου κυβερνοασφάλειας, για την αποτελεσματική αντιμετώπιση περιστατικών κυβερνοεπιθέσεων και την ελαχιστοποίηση των επιπτώσεων από απειλές στον κυβερνοχώρο βοηθά στο συντονισμό των δράσεων κατά τη διαχείριση ενός περιστατικού επίθεσης, βάσει καθορισμένων διαδικασιών, αρμοδιοτήτων αλλά και επιχειρησιακών και επικοινωνιακών δυνατοτήτων.

Νέοι κίνδυνοι προκύπτουν και θα προκύπτουν συνέχεια όσο εξελίσσεται η τεχνολογία γι' αυτό οι επιχειρήσεις πρέπει να κατανοήσουν ότι η καλύτερη αντίδραση είναι η συνειδητοποίηση του κινδύνου και η έγκαιρη διαχείρισή του.

12. Βιβλιογραφία

Brewster, T. (2018, 12 1). *capital*. Ανάκτηση από www.capital.gr:

<https://www.capital.gr/forbes/3330856/kubernoeipithesi-sti-marriott-ektetheimenoi-500-ekat-pelates-se-pano-apo-ekato-xores>

Check Point Research CPR. (n.d.). <https://research.checkpoint.com>. Ανάκτηση από

<https://research.checkpoint.com>: <https://blog.checkpoint.com/2022/01/10/checkpoint-research-cyber-attacks-increased-50-year-over-year/>

CISA. (2021, 09 22). Ανάκτηση από <https://www.cisa.gov/uscert/ncas/alerts/aa21-265a>

CNN. (2022, 01 10). *Cnn.gr*. Ανάκτηση από <https://www.cnn.gr>:

<https://www.cnn.gr/tech/story/296881/poso-ayxithikan-oi-kyvernoepitheseis-se-ellinikes-epixeiriseis>

ENISA. (2021, 10). *ENISA*. Ανάκτηση από www.enisa.europa.eu:

<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>

- EU-OSHA . (2021). *oiraproject*. Ανάκτηση από <https://oiraproject.eu/el:https://oiraproject.eu/el/how-carry-out-risk-assessment>
- Kaspersky. (2021, 07 29). *www.capital.gr*. Ανάκτηση από [www.capital.gr](https://www.capital.gr/epixeiriseis/3573057/kaspersky-sxedon-8-stous-10-ellines-den-exoun-ekpaideutei-se-themata-psifiakis-asfaleias):
<https://www.capital.gr/epixeiriseis/3573057/kaspersky-sxedon-8-stous-10-ellines-den-exoun-ekpaideutei-se-themata-psifiakis-asfaleias>
- Sean O'Neill, S. (2020, 08 21). Ανάκτηση από <https://skift.com/2020/08/21/ransomware-attacks-on-travel-companies-spread-sparking-complacency-fears/>
- Skai.gr. (2017, 05 22). *Skai*. Ανάκτηση από Skai: <https://www.skai.gr/news/world/syllipsi-20-roson-xaker-gia-ilektronikes-epitheseis-se-trapezes>
- Thomas, I. (2021, 09 02). *IRONSCALES*. Ανάκτηση από <https://ironscales.com/blog/ransomware-in-hospitality-industry/>
- WOLFF, O. (2017, 02 01). Ανάκτηση από <https://slate.com/technology/2017/02/the-ransomware-attack-that-locked-hotel-guests-out-of-their-rooms.html>
- Γεωργόπουλος, Ν. (n.d.). *www.cyberinsurancegreece.com*. Ανάκτηση από [www.cyberinsurancegreece.com](http://www.cyberinsurancegreece.com:https://www.cyberinsurancegreece.com/ereynes/hotels/):
<https://www.cyberinsurancegreece.com/ereynes/hotels/>
- Ένωση Ασφαλιστών Εταιριών Ελλάδος ΕΑΕΕ. (n.d.). Ανάκτηση από http://www1.eaee.gr/sites/default/files/%CE%BF%CE%B4%CE%B7%CE%B3%CF%8C%CF%82_%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B9%CF%83%CE%B7%CF%82_cyber_20210907.pdf
- Ευρωπαϊκή Ένωση. (2020). *www.eca.europa.eu*. Ανάκτηση από [www.eca.europa.eu](https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EL.pdf):
https://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_EL.pdf
- Ευρωπαϊκή Ένωση. (2021, 03 26). Ανάκτηση από https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_el.htm
- Καραμπέκιος, Δ. (2012). *Cyberedge*. Αθήνα: ΑΙΓ.
- Παπαγεωργίου, Γ. (n.d.). *AON*. Ανάκτηση από [www.aon.com](http://www.aon.com:https://www.aon.com/greece/articles/cyber-insurance.jsp):
<https://www.aon.com/greece/articles/cyber-insurance.jsp>
- Παππάς, Ν. (2018, 03 07). Έγκριση της Εθνικής Στρατηγικής Κυβερνοασφάλειας. (ΑΔΑ: Ψ4Ρ7465Χ00-Ζ6Ω). Αθήνα, Ελλάδα. Ανάκτηση από <https://mindigital.gr/kyvernoasfaleia>
- Σιούτη, Λ. (2017, 01 29). *Protothema*. Ανάκτηση από [www.protothema.gr](http://www.protothema.gr:https://www.protothema.gr/world/article/649599/austria-haker-kleidosan-ta-domatia-xenodoheiou-zitodas-lutra-gia-na-ta-anoixoun/):
<https://www.protothema.gr/world/article/649599/austria-haker-kleidosan-ta-domatia-xenodoheiou-zitodas-lutra-gia-na-ta-anoixoun/>

Υπουργείο Ψηφιακής Διακυβέρνησης. (2021, 06). *mindigital.gr*. Ανάκτηση από <https://mindigital.gr/>: <https://mindigital.gr/wp-content/uploads/2021/06/%CE%95%CE%B3%CF%87%CE%B5%CE%B9%CF%81%CE%AF%CE%B4%CE%B9%CE%BF-%CE%9A%CF%85%CE%B2%CE%B5%CF%81%CE%BD%CE%BF%CE%B1%CF%83%CF%86%CE%AC%CE%BB%CE%B5%CE%B9%CE%B1%CF%82.pdf>

Υπουργείο Ψηφιακής Διακυβέρνησης. (2018, 12 3). *mindigital*. (Π. Νικόλας, Επιμ.) Ανάκτηση από <https://mindigital.gr/>: https://mindigital.gr/wp-content/uploads/2019/09/N.4577_2018.pdf

Υπουργείο Ψηφιακής Διακυβέρνησης. (2019, 10 8). *mindigital*. Ανάκτηση από mindigital.gr: <https://mindigital.gr/wp-content/uploads/2020/01/3739B-19-1.pdf>

Υπουργείο Ψηφιακής Διακυβέρνησης. (2021, 06).