Μάθημα: Στοιχεία Δικαίου της Πληροφορίας

Τίτλος Εργασίας:

Κυβερνοεπιθέσεις σε κρατικά Πληροφοριακά Συστήματα και νομικοί τρόποι αντιμετώπισης

Ομάδα:

Σπυρίδων Μπάζιος (3170113)
Διογένης Τσολάκου (3170164)
Χρήστος Αργυρόπουλος (3170010)

Εισαγωγή

Οι στόχοι της έρευνας είναι η καταγραφή των πιο γνωστών κυβερνοεπιθέσεων σε κρατικά πληροφοριακά συστήματα και η ανάλυση των πιθανών νομοθετικών τρόπων αντιμετώπισης σύμφωνα με το εθνικό νομοθετικό πλαίσιο.

Συγκεκριμένα αναλύονται κάποιες από τις πιο συνηθισμένες και σημαντικές κατηγορίες επιθέσεων και αναφέρονται τα σημαντικότερα διεθνή παραδείγματα αυτών αλλά και τις συνέπειες τους και τα μέτρα που θεσπίστηκαν λόγω αυτών. Μετά την αναφορά τους γίνεται αναφορά στον τρόπο που ορίζονται από την ελληνική νομοθεσία, σε ποιους νόμους εμπίπτουν και τους πιθανούς τρόπους αντιμετώπισης μέσω της αντίστοιχης νομοθεσίας.

Επιθέσεις και ανάλυση αυτών

Οι σημαντικότερες και γνωστότερες επιθέσεις σε κρατικά ΠΣ που βρέθηκαν είναι οι παρακάτω.

Επιθέσεις DDoS

2007 Cyberattacks on Estonia.

Οι κυβερνοεπιθέσεις του 2007 στην Εσθονία ήταν μια σειρά από επιθέσεις που ξεκίνησαν στα τέλη του Απριλίου το 2007 και είχαν ως στόχο μία πληθώρα ιστοσελίδων εσθονικών οργανισμών. Κάποιοι από αυτούς ήταν της κυβέρνησης, διάφορων τραπεζών και υπουργείων. Ο λόγος των επιθέσεων υποπτεύεται ότι ήταν οι διαπληκτισμοί της χώρας με την Ρωσία όσον αφορά κάποια μνημεία του 2ου Παγκοσμίου Πολέμου.

Οι περισσότερες επιθέσεις ήταν τύπου DDoS μέσω της μεθόδου ping flooding[1]. Τα συστήματα που στοχεύθηκαν αποτελούσαν συστήματα των οποίων οι διευθύνσεις δικτύου δεν ήταν κοινώς γνωστές, το οποίο σύμφωνα με ειδικούς που έχουν σχολιάσει τις επιθέσεις υποδεικνύει ότι μπορεί να προήλθαν από κρατικές ομάδες χάκερ της Ρωσίας.

Λόγω των επιθέσεων αυτών η Εσθονία δημιούργησε μία ομάδα άμυνας από κυβερνοεπιθέσεις και το εγχειρίδιο του Ταλίν, το οποίο αναφέρει διεθνείς νόμους οι οποίοι μπορούν να εφαρμοστούν σε τέτοιες υποθέσεις.

1. Ping flooding : η αποστολή ενός μεγάλου αριθμού πακέτων εντοπισμού προς έναν διακομιστή, υπό κανονικές συνθήκες ένα τέτοιο πακέτο χρησιμοποιείται για την εύρεση ενός υπολογιστή ή διακομιστή ο οποίος απαντάει στον αποστολέα ώστε να υπάρξει σύνδεση μεταξύ τους

Επιθέσεις Ransomware

2017 Cyberattacks on Ukraine.

Οι κυβερνοεπιθέσεις του 2017 στην Ουκρανία ήταν μια σειρά πολύ ισχυρών επιθέσεων μέσω της χρήσης του malware Petya στοχεύοντας ουκρανικές τράπεζες, υπουργεία, εφημερίδες και εταιρείες ηλεκτρισμού.

Ο Petya είναι malware που εμφανίζεται ως ransomware[1] ενώ έχει ως πραγματικό σκοπό την πρόκληση όσο μεγαλύτερης δυνατής ζημιάς. Σύμφωνα με ειδικούς η επίθεση προήλθε από ενημέρωση ενός προγράμματος που χρησιμοποιείται από πολλές λογιστικές εταιρείες στην Ουκρανία. Οι επιτιθέμενοι είχαν καταφέρει να προσπεράσουν το αυτόματο σύστημα ενημέρωσης της εταιρείας που ανέπτυξε το πρόγραμμα, αντικαθιστώντας την πραγματική ενημέρωση με τον ιό.

Ο ιός χρησιμοποιούσε το Server Message Block[2] (SMB) πρωτόκολλο ώστε να εντοπίσει και μολύνει υπολογιστές στο τοπικό δίκτυο και υπολογιστές συνδεδεμένους εξ' αποστάσεως στο τοπικό δίκτυο. Λόγω της εκτεταμένης αυτής μόλυνσης ο ιός κατάφερε να επηρεάσει αρκετά υπουργεία, τράπεζες, το μετρό μέχρι και τηλεφωνικές εταιρείες, ταχυδρομεία αλλά και το σύστημα επίβλεψης του πυρηνικού σταθμού του Τσέρνομπιλ.

Λόγω της έκτασης και της εκλεπτυσμένης φύσης της επίθεσης θεωρείται ότι δεν είχε ως σκοπό το χρηματικό κέρδος όπως οι περισσότερες τέτοιες επιθέσεις, αλλά την αποδυνάμωση του Ουκρανικού κράτους. Αυτό φαίνεται από το γεγονός ότι η επίθεση ξεκίνησε σε ημέρα εθνικής εορτής καθώς οι περισσότερες κρατικές και κυβερνητικές υπηρεσίες δεν θα ήταν ανοιχτές αλλά και ότι υπήρξαν περιπτώσεις που ο ιός δεν κρυπτογραφούσε τα δεδομένα των υπολογιστών αλλά τα διέγραφε ή τα κρυπτογραφούσε με τρόπους ώστε η αποκρυπτογράφηση να ήταν αδύνατη.

Εκτός αυτών, μετά από αναλύσεις και έρευνες στα συστήματα από όπου προήλθε ο ιός ανακαλύφθηκε ότι υπήρχαν backdoors[3] ώς και 2 μήνες πριν την έναρξη της επίθεσης. Όλα αυτά δείχνουν ότι η επίθεση ήταν σχεδιασμένη με μεγάλη λεπτομέρεια και προσοχή και γι' αυτό το λόγο κατηγορήθηκε η Ρωσία λόγω των σχέσεων της με την Ουκρανία μετά το 2014[4]. Οι ζημιές από τον ιό εκτιμούνται γύρω στα 10δις δολάρια και επηρέασε κι άλλες ευρωπαϊκές χώρες σε μικρότερο βαθμό. Η εταιρεία του λογιστικού προγράμματος κατηγορήθηκε για εγκληματική αμέλεια λόγω των χαλαρών μέτρων ασφαλείας της.

WannaCry Ransomware Attack

Τον Μάιο του 2017 εξαπλώθηκε παγκόσμια ένας ιός λυτρισμικού ονόματι WannaCry, δηλαδή κακόβουλο λογισμικό με σκοπό την απόσπαση χρημάτων από τα θύματα.

Το WannaCry εκμεταλλευόταν την ίδια ευπάθεια του SMB πρωτοκόλλου των WIndows όπως ο Petya και κρυπτογραφούσε πολλούς -τους πιο συνηθισμένους- τύπους

αρχείων στον υπολογιστή του θύματος καθιστώντας τους μη προσπελάσιμους. Ο μοναδικός τρόπος να αποκτήσει ξανά πρόσβαση ο χρήστης ήταν να πληρώσει 300$ (που αργότερα έγινε 600$) σε Bitcoin στους επιτιθέμενους, ώστε αυτοί να ξεκλειδώσουν τα αρχεία του. Σε αντίθετη περίπτωση οι επιτιθέμενοι απειλούσαν να διαγράψουν τα αρχεία του θύματος εντός ολίγων ημερών. Στην πραγματικότητα φημολογείται πως λόγω ενός προβλήματος στον κώδικα του ιού, κανείς που πλήρωσε τα λύτρα δεν απέκτησε ξανά πρόσβαση σε αυτά διότι δεν υπήρχε τρόπος συσχέτισης του υπολογιστή του θύματος με την εκάστοτε πληρωμή.

Υπολογίζεται πως πάνω από 230.000 υπολογιστές παγκόσμια έπεσαν θύμα του WannaCry, μεταξύ αυτών το Υπουργείο Εσωτερικών της Ρωσίας, μερικές κυβερνήσεις πολιτειών στην Ινδία και τα εθνικά συστήματα υγείας στην Αγγλία και την Σκωτία.

1. Ransomware : τύπος ιού που κρυπτογραφεί τα δεδομένα του χρήστη και απαιτεί λύτρα σε κρυπτονομίσματα για την αποκρυπτογράφηση τους
2. SMB : πρωτόκολλο επικοινωνίας για την κοινή πρόσβαση σε αρχεία και συσκευές από τους κόμβους εντός ενός δικτύου
3. Backdoor : κρυφός τρόπος εισόδου παρακάμπτοντας τις απαιτούμενες μεθόδους αυθεντικοποίησης για την εξ αποστάσεως πρόσβαση σε ένα σύστημα
4. Κρίση της Κριμαίας : η ρωσική εισβολή στην Κριμαία και η προσάρτηση της στη Ρωσία

Data Breaches

Democratic National Committee Cyber Attacks

Οι κυβερνοεπιθέσεις στην Εθνική Δημοκρατική Επιτροπή έλαβαν μέρος την περίοδο 2015-2016, όπου Ρώσοι χάκερ διείσδυσαν στο δίκτυο της Επιτροπής για την παραβίαση και δημοσιοποίηση προσωπικών δεδομένων. Οι επιθέσεις ήταν μέρος ενός μεγαλύτερου συνόλου επιθέσεων για την υποκλοπή πληροφοριών από Αμερικανικούς πολιτικούς οργανισμούς.

Οι δύο ομάδες που εκτέλεσαν τις επιθέσεις κατασκόπευαν τις επικοινωνίες της Επιτροπής, υπέκλεψαν την έρευνα της αντιπολίτευσης για τον Ντόναλντ Τράμπ και διάβασαν όλα τα e-mail και τις συνομιλίες. Επιπλέον, οι ομάδες ήταν ήδη γνωστές ως επιτιθέμενοι πολιτικής και οικονομικής κατασκοπίας για τα συμφέροντα της Ρωσίας, έχοντας επιτεθεί σε πολλούς τομείς της Αμερικής αλλά και άλλων χωρών ανά τα χρόνια και έχουν άρτια κατάρτιση που υποδεικνύει ότι είναι πολύ πιθανό να είναι κρατικές ομάδες.

Η επίθεση είχε εντοπιστεί από το καλοκαίρι του 2015 αλλά η έλλειψη ορθής επικοινωνίας μεταξύ των πολιτικών οργανώσεων και της κυβέρνησης αποτέλεσε τον λόγο για τον αργοπορημένο ορισμό μέτρων για την αντιμετώπιση των επιθέσεων και της ενημέρωσης των αρχηγών της Επιτροπής τον Απρίλιο του 2016, ένα χρόνο αργότερα. Η επίθεση είχε ως απώτερο σκοπό την λεπτομερέστερη γνώση στον τρόπο λειτουργίας του πολιτικού συστήματος των ΗΠΑ, τις πολιτικές και πιθανές τάσεις πολιτικών αρχηγών αλλά και τις στρατηγικές και πρακτικές της κυβέρνησης.

Οι ειδικοί ανέφεραν ότι το σύνολο των επιθέσεων το 2015-2016 (μαζί με την συγκεκριμένη) είχαν ως στόχο τη διασπορά αβεβαιότητας για το Δημοκρατικό κόμμα ώστε να βοηθήσουν τον Τραμπ να κερδίσει στις εκλογές του 2016.

Μετά τις επιθέσεις, το Κογκρέσο προχώρησε στην έγκριση μέτρων για την περαιτέρω ασφάλεια της χώρας από προσπάθειες προπαγάνδας ενώ ο τότε Πρόεδρος Μπαράκ Ομπάμα διέταξε τη διεξαγωγή έρευνας για τις προσπάθειες επιρροής των εκλογών του 2016 από τη Ρωσία.

Office of Personnel Management Data Breach

Τον Απρίλιο του 2015 το Γραφείο Διαχείρισης Προσωπικού (ΓΔΠ) των ΗΠΑ, η υπηρεσία που διαχειρίζεται το εργατικό δυναμικό της χώρας, ανακάλυψε πως είχαν κλαπεί μερικά από τα αρχεία που αφορούσαν προσωπικά στοιχεία εκατομμύρια πολιτών, από όνομα έως δακτυλικά αποτυπώματα.

Η επίθεση ξεκίνησε τον Νοέμβριο του 2013 και τον Μάρτιο του 2014 έγινε αντιληπτή από το ΓΔΠ. Τότε, αποφασίστηκε πως δεν διακινδυνεύονταν σημαντικές πληροφορίες και επιτράπηκε η παραμονή των επιτιθέμενων στο δίκτυο ώστε να συλλεχθούν πληροφορίες.

Δύο μήνες αργότερα έγινε απόπειρα εκδίωξής τους από το σύστημα, η οποία όμως εν άγνοια του ΓΔΠ απέτυχε και η κλοπή δεδομένων συνεχίστηκε ως και τον Απρίλιο του 2015, όταν τελικά εντοπίστηκε. Οι επιτιθέμενοι είχαν εξασφαλίσει ένα backdoor που τους επέτρεψε

την εγκατάσταση κρυφού κακόβουλου λογισμικού. Μετά από έρευνα οι αρχές κατέληξαν πως η επίθεση έγινε από hackers συνεργαζόμενους με το κινέζικο κράτος.

Ακολούθησαν αγωγές στο ΓΔΠ από δύο ενώσεις δημοσίων υπαλλήλων, όμως στα δικαστήρια δεν δικαιώθηκαν καθώς ο νόμος περί ιδιωτικότητας δεν κάλυπτε περιπτώσεις που τα δεδομένα κλέβονται μεν, δεν δημοσιοποιούνται δε. Η κυβέρνηση των ΗΠΑ για να μετριαστεί η ζημία όσων κλάπηκαν τα στοιχεία τους θα τους προσφέρει υπηρεσίες όπως η προστασία ταυτότητας έως το 2025 με το συνολικό κόστος να ανέρχεται στο 1 δισεκατομμύριο δολάρια.

Cyber-warfare

Stuxnet / Operation Olympic Games

Το Stuxnet είναι ένα από τα πιο γνωστά κακόβουλα λογισμικά που έχουν χρησιμοποιηθεί ποτέ στον χώρο των πληροφοριακών συστημάτων σε διακρατικό επίπεδο. Πρόκειται για ένα malware το οποίο ήταν σχεδιασμένο για να μολύνει υπολογιστές λειτουργικού συστήματος Windows και ο στόχος του αρχικά ήταν η επίθεση σε βιομηχανικά συστήματα (programmable logic controllers) της Siemens.

Για την ανάπτυξή του Stuxnet είχαν χρησιμοποιηθεί τέσσερεις επιθέσεις 'zero-day'[1] και τελικά αποδείχθηκε ότι το payload του, ήταν η απότομη μεταβολή συχνοτήτων λειτουργίας φυγόκεντρων σε πυρηνικό εργοστάσιο στο Ιράκ. Η απότομη αυτή μεταβολή ερυθρέ με το χρόνο τους φυγόκεντρους και προκάλεσε βλάβη σε ποσοστό 20% επί του συνόλου αυτών.

Αξίζει να σημειωθεί πως το Stuxnet έκανε χρήση rootkit[2] που απέτρεπε την επιτήρηση των πραγματικών συνθηκών λειτουργίας των φυγόκεντρων από το αρμόδιο προσωπικό, κάνοντας το έτσι απίθανο να ανιχνευτεί πριν φανούν τα αποτελέσματα της δράσης του.

1. Επίθεση zero-day: επιθέσεις που εκμεταλλεύονται ευπάθειες πληροφοριακών συστημάτων τις οποίες οι προγραμματιστές δεν έχουν επίγνωση της ύπαρξης τους.
2. Rootkit: Ένα rootkit είναι λογισμικό που επιτρέπει την συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη.

Hacktivism

2013 Singapore Cyberattacks

Τον Νοέμβριο του 2013, σειρά κυβερνοεπιθέσεων έλαβε χώρα στην Σιγκαπούρη ως απάντηση στην σύσταση αρμόδιας αρχής από την έκτοτε κυβέρνηση, για λογοκρισία περιεχομένου ιστοσελίδων (Media Development Authority) με πάνω από 50.000 μοναδικούς χρήστες κάθε μήνα. Την επίθεση πραγματοποίησε μέλος της ακτιβιστικής οργάνωσης Anonymous με το ψευδώνυμο 'Μεσσίας'.

Οι επιθέσεις ξεκίνησαν στις 28 Οκτωβρίου του 2013 με στόχο την σελίδα του κοινοτικού ιδρύματος, PAP Community Foundation και της περιοχής Ang Mo Kio της Σιγκαπούρης. Επίθεση παραποίησης της όψης ιστοσελίδας δέχτηκε επίσης και το ειδησεογραφικό πρακτορείο Straits Times μετά από κριτική που δημοσίευσε για τα συμβάντα. Οι επιθέσεις συνεχίστηκαν με στόχο το αεροδρόμιο Seletar της Σιγκαπούρης του οποίου η ιστοσελίδα παραποιήθηκε με συμβολικές εικόνες των Anonymous.

Στις 5 Νοεμβρίου παραβιάστηκαν οι λογαριασμοί Youtube και Twitter του κωμικού Ridhwan Azman για αντιπαραθέσεις που είχε με την ακτιβιστική οργάνωση (Anonymous). Την σειρά αυτή επιθέσεων κλείνει 2 μέρες αργότερα ο βανδαλισμός της επίσημης ιστοσελίδας του πρωθυπουργού της Σιγκαπούρης Lee Hsien Loong. Αξίζει να σημειωθεί ότι αργότερα στις 20 Νοεμβρίου σελίδες 13 σχολείων που λειτουργούσαν με κοινό server δέχτηκαν επίσης επιθέσεις παραμόρφωσης περιεχομένου για μικρό χρονικό διάστημα εντός της ημέρας.

Νομικές δυνατότητες αντιμετώπισης

Επιθέσεις DDoS (Επιθέσεις άρνησης υπηρεσιών)

Άρνηση Παροχής Υπηρεσίας ή Αποκεντρωμένη Άρνηση Παροχής Υπηρεσίας [Denial of Service (DoS) ή Distributed Denial of Service (DDoS)] ορίζεται η τεχνική με την οποία υπηρεσίες και πόροι ενός υπολογιστή καθίστανται μη διαθέσιμοι στους προοριζόμενους χρήστες (άρθρο 2 της υπ' αρ.750/2/19-02-2015 Απόφασης της ΕΕΤΤ, ΦΕΚ 412/Β/24-03-2015). Η διαφορά απλής και αποκεντρωμένης επίθεσης έγκειται στο ότι η τελευταία λαμβάνει χώρα από περισσότερα σημεία εκκίνησης. Η συντριπτική πλειονότητα των επιθέσεων DoS ανήκει στην κατηγορία των αποκεντρωμένων επιθέσεων.

Για την αντιμετώπιση - ποινική δίωξη της πράξης απαιτείται έγκληση πράγμα το οποίο σημαίνει ότι από τη στιγμή που θα παρέλθει άπρακτη η αποκλειστική προθεσμία των τριών μηνών για την υποβολή εγκλήσεως, τότε χάνεται εξ' ολοκλήρου το δικαίωμα προσφυγής στην ποινική δικαιοσύνη, με αποτέλεσμα ο παθών να μην μπορεί να κινηθεί νομικά στα ποινικά δικαστήρια. Το άρθρο 292Β παρ. 2 (όπως και το άρθρο 381Α παρ.2), καθιστά ποινικό αδίκημα τις επιθέσεις κατά πληροφοριακών συστημάτων, απλές ή αποκεντρωμένες (DoS ή DDoS). Αξίζει να τονιστεί πως στην περίπτωση που μας απασχολεί (επίθεση σε κρατικό οργανισμό), το παραπάνω άρθρο, προβλέπει φυλάκιση τουλάχιστον δύο (2) ετών, αφού η επίθεση προσβάλει ζωτικής σημασίας υπηρεσία.

Data Breaches (Παραβιάσεις προσωπικών δεδομένων)

Παραβίαση προσωπικών δεδομένων συνιστά κάποιο συμβάν ασφαλείας σε σχέση με δεδομένα τα οποία διαχειρίζεται ένας οργανισμός, μία εταιρεία ή ένα κράτος (από εδώ και πέρα θα αναφέρεται ως οργανισμός), έχοντας ως αποτέλεσμα την παραβίαση του απορρήτου των δεδομένων αυτών.

Αν αυτή η παραβίαση μπορεί να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες ενός (φυσικού) προσώπου τότε σύμφωνα με το άρθρο 33 του Γενικού Κανονισμού Προσωπικών Δεδομένων (GDPR) ο οργανισμός που είναι αρμόδιος αυτών των δεδομένων οφείλει να ειδοποιήσει την αρμόδια εποπτική αρχή, σύμφωνα με το άρθρο 55 του ΓΚΠΔ, μέσα σε 72 ώρες και όχι αργότερα από την στιγμή που έγινε αντιληπτή η παραβίαση. Κάτι το οποίο δεν έγινε στο πρώτο παράδειγμα παραβίασης προσωπικών δεδομένων που αναφέρθηκε μιας και εκτός του γεγονότος ότι δεν είχε ψηφιστεί τότε ο ΓΚΠΔ , δεν θα είχε ισχύ αφού ισχύει μόνο σε χώρες της Ευρωπαϊκής Ένωσης.

Από τη στιγμή όμως που στη χώρα μας ο συγκεκριμένος κανονισμός έχει πλήρη ισχύ από τον Μάιο του 2018, σε μια παρόμοια περίπτωση στη χώρα μας οι αντίστοιχοι οργανισμοί που προσβλήθηκαν από μία τέτοια επίθεση όπως της Εθνικής Δημοκρατικής Επιτροπής και του Γραφείου Διαχείρισης Προσωπικού θα ήταν υποχρεωμένοι να το αναφέρουν χωρίς καθυστέρηση.

Επιπλέον, θα έπρεπε μαζί με την ειδοποίηση της παραβίασης να περιγράψουν την φύση της παραβίασης και αν είναι δυνατό τον κατά προσέγγιση αριθμό επηρεαζόμενων προσώπων και αρχείων δεδομένων. Εκτός αυτού, πρέπει να αναφέρει το όνομα και τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων (Data Protection Officer, DPO) ώστε να μπορούν να ληφθούν περισσότερες πληροφορίες.

Τέλος, θα πρέπει να αναφερθούν και οι συνέπειες που μπορεί να προκύψουν από αυτή την παραβίαση αλλά και τα μέτρα που έχουν ληφθεί ή πρόκειται να ληφθούν για την αντιμετώπιση της παραβίασης ή την μείωση των επιπτώσεων των συνεπειών σε χείριστη περίπτωση όπου ο περιορισμός των συνεπειών δεν προβλέπεται.

Η όποια παράβαση αυτών τιμωρείται με διοικητικά πρόστιμα σύμφωνα με το άρθρο 83 του ΓΚΠΔ. Για την επιβολή των προστίμων αυτών λαμβάνονται υπόψη η φύση, η βαρύτητα, η διάρκεια της παράβασης αλλά και ο αριθμός των επηρεαζόμενων προσώπων. Συγκεκριμένα τα πρόστιμα μπορούν να φτάσουν τα 10.000.000 € ή το 2% του συνολικού ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους σε περιπτώσεις που ο παραβάτης είναι εταιρεία, από τις δύο αυτές τιμές επιβάλλεται αυτή που είναι υψηλότερη. Η μη συμμόρφωση στις εντολές της εποπτικής αρχής επιφέρει πρόστιμα της τάξεως των 20.000.000€ ή του 4% του κύκλου εργασιών και επιβάλλεται όπως αναφέρθηκε παραπάνω.

Hacktivism (Ακτιβισμός μέσω του χάκινγκ)

Ο ακτιβισμός μέσω του χάκινγκ έχει πολλές μορφές, οι πιο συνηθισμένες είναι αυτές της άρνησης παροχής υπηρεσιών (DDoS), οι οποίες αναλύθηκαν παραπάνω, η παραποίηση της όψης των ιστοσελίδων, το mirroring και το doxxing.

Το mirroring είναι η αντιγραφή άλλων ιστοσελίδων ή δικτυακών κόμβων για την αποφυγή λογοκρισίας που μπορεί να μπλοκάρει την λειτουργία μίας ιστοσελίδας. Για παράδειγμα ιστοσελίδες με πειρατικό περιεχόμενο αλλά και ιστοσελίδες όπως το WikiLeaks χρησιμοποιούν αυτή τη τεχνική για να αποφύγουν εμπόδια σε χώρες που τα έχουν απαγορεύσει και για την καλύτερη αποθήκευση και συντήρηση του περιεχομένου τους σε περίπτωση που η κύρια ιστοσελίδα πέσει. Από τη στιγμή που μία ιστοσελίδα έχει μπλοκαριστεί λόγω του περιεχομένου της, τότε και τα mirror της υπόκεινται στην ίδια νομοθεσία. Παραδείγματος χάρη η Επιτροπή για τη Διαδικτυακή Προσβολή της Πνευματικής Ιδιοκτησίας (ΕΔΠΠΙ) έχει μπλοκάρει ένα σημαντικό αριθμό ιστοσελίδων (τελευταία πρόσβαση στις 8.5.2021), παρόλα αυτά αρκετές από αυτές διατηρούν mirrors για την αποφυγή της λογοκρισίας αυτής.

Το doxxing είναι η αποκάλυψη ιδιωτικών προσωπικών δεδομένων μέσω του διαδικτύου που αφορούν ένα πρόσωπο ή έναν οργανισμό, συνήθως γίνεται για λόγους hacktivism ή για εκβιασμό ή για το λεγόμενο vigilantism, όπου απλοί πολίτες προσπαθούν να απονείμουν δικαιοσύνη. Δυστυχώς, στις περισσότερες χώρες του κόσμου δεν υπάρχει νομοθεσία συγκεκριμένα για το doxxing και τι προβλέπεται για τα πρόσωπα που το επιχειρούν. Όσες χώρες έχουν κάποιο σχετικό νόμο, κινούνται κυρίως στη περιοχή της δημόσιας εξύβρισης και συκοφαντίας, π.χ. η δημοσιοποίηση φωτογραφίας ενός προσώπου χωρίς την άδεια του και η πρόσαψη κατηγοριών. Επομένως, τα νομικά βήματα στα οποία μπορεί να κινηθεί κάποιος είναι αμφιλεγόμενα μιας και υπάρχει η περίπτωση να μην έχει λάβει χώρα εξύβριση του ατόμου που δέχεται doxxing. Πιο συγκεκριμένα, οι ΗΠΑ έχουν νόμους που σχετίζονται με το stalking (Interstate Stalking Statute) και μπορούν να σχετιστούν έμμεσα με το doxxing, ενώ η Νότιος Κορέα έχει το άρθρο 49 του "Νόμου για την προώθηση της χρήσης του δικτύου πληροφοριών και επικοινωνιών και την προστασία των πληροφοριών" (τελευταία πρόσβαση στις 8.5.2021) που αναφέρει ότι απαγορεύεται η άνομη συλλογή και διάδοση ιδιωτικών πληροφοριών όπως το ονοματεπώνυμο, η ημερομηνία γέννησης, η διεύθυνση και άλλες πληροφορίες που μπορεί να θεωρηθούν αρκετές ώστε να αναγνωρίσουν ένα πρόσωπο, αν και όπως αναφέρθηκε είναι δύσκολο να γίνει τέτοια συσχέτιση και στους δύο νόμους των δύο χωρών.

Επιθέσεις Ransomware (Επιθέσεις λυτρισμικού)

Οι επιθέσεις λυτρισμικού μπορούν αναλόγως την έκταση τους και τα θύματα τους να εμπίπτουν σε πληθώρα νόμων, από φθορά ηλεκτρονικών δεδομένων έως πλαστογραφία, και εκβιασμό.

Η βασική επίπτωση μιας τέτοιας επίθεσης είναι η κρυπτογράφηση του συστήματος του θύματος, συνεπώς διακόπτεται η λειτουργία του και συχνά η ζημιά είναι μη αναστρέψιμη. Σύμφωνα με το άρθρο 292Β του νόμου 4619/2019 του νέου Ποινικού Κώδικα που τέθηκε σε ισχύ τον Ιούλιο του 2019, η παρεμπόδιση ή διακοπή της λειτουργίας ενός πληροφοριακού συστήματος με αλλοίωση ψηφιακών δεδομένων και αποκλεισμό πρόσβασης σε αυτά τιμωρείται με φυλάκιση από ένα (1) έως τρία (3) έτη και χρηματική ποινή.

Οι επιθέσεις λυτρισμικού συχνά χρησιμοποιούν τεχνικές phishing (ηλεκτρονικού ψαρέματος) για να εξαπατήσουν τα θύματα τους κάνοντας να νομίζουν πως βρίσκονται υπό έρευνα της αστυνομίας και πρέπει να πληρώσουν ένα χρηματικό ποσό για να εξασφαλίσουν την αθωότητά τους. Η παράγραφος 3 του άρθρου 216 του νόμου 4619/2019 προβλέπει την τιμωρία με φυλάκιση έως δέκα (10) έτη και επιπλέον χρηματική ποινή, αν κάποιος χρησιμοποιήσει πλαστά έγγραφα με σκοπό να βλάψει κάποιον για δικό του περιουσιακό όφελος. Η παράγραφος 4 του ίδιου άρθρου προβλέπει πως αν η πράξη έχει στόχο το νομικό πρόσωπο του ελληνικού Δημοσίου, όπως θα συνέβαινε σε περίπτωση επίθεσης σε κρατικό σύστημα, τότε επιβάλλεται κάθειρξη τουλάχιστον δέκα (10) ετών και χρηματική ποινή έως χίλιες ημερήσιες μονάδες.

Στις περισσότερες περιπτώσεις οι επιτιθέμενοι αλλοιώνουν τα ψηφιακά δεδομένα των θυμάτων τους αποκλείοντας την πρόσβαση, με σκοπό την απόσπαση χρηματικού ποσού για να τους επιτραπεί ξανά η πρόσβαση σε αυτά. Σύμφωνα με το άρθρο 385 του νόμου 4619/2019 ο εξαναγκασμός κάποιου με απειλή σε πράξη ή παράλειψη με σκοπό την αποκόμιση ιδίου παράνομου περιουσιακού οφέλους τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή. Αν ο υπαίτιος μεταχειρίστηκε απειλή βλάβη της επιχείρησης του θύματος, τότε προβλέπεται φυλάκιση τριών (3) ετών και επιπλέον χρηματική ποινή. Τέλος, σε περίπτωση που επέλθει θάνατος ή βαριά σωματική βλάβη κάποιου προσώπου, όπως είναι δυνατόν να συμβεί αν το θύμα της επίθεσης είναι κρίσιμη κρατική υποδομή, τότε επιβάλλεται ισόβια κάθειρξη ή πρόσκαιρη για τουλάχιστον δέκα (10) έτη και επιπλέον χρηματική ποινή.

Cyber-warfare

Το cyber-warfare αποτελεί μια ειδική περίπτωση επίθεσης λόγω του διακρατικού του χαρακτήρα. Εκδηλώνετε με την χρήση cyber-weapons που είναι malwares τα οποία προκαλούν φυσικές καταστροφές και είναι συνήθως αρκετά εξελιγμένα και προσεκτικά μελετημένα κάνοντας τα σχεδόν αδύνατον να δημιουργηθούν από μικρές ομάδες hacker. Για αυτό το λόγο η νομική αντιμετώπιση τους είναι στην διακριτική ευχέρεια κάθε κράτους να αξιολογήσει την σοβαρότητα μιας δεχόμενης επίθεσης και να απαντήσει αναλόγως.

Συμπέρασμα

Τα κυβερνητικά πληροφοριακά συστήματα βρίσκονται υπό την διαρκή απειλή να δεχθούν επίθεση. Οι επιτιθέμενοι ποικίλουν από ερασιτεχνικές ολιγομελείς ομάδες έως και επαγγελματικές ομάδες χρηματοδοτούμενες από άλλα κράτη ώστε να εξυπηρετήσουν τα συμφέροντα τους ενάντια στο κράτος-στόχο. Οι τρόποι επίθεσης εξαρτώνται από τον σκοπό αυτής, ο οποίος μπορεί να είναι μεταξύ άλλων η υποκλοπή απόρρητων πληροφοριών, η διακοπή κρίσιμων διαδικασιών και η οικονομική ζημία. Για αυτό τον λόγο, το Υπουργείο Εθνικής Άμυνας οφείλει να λάβει τα κατάλληλα μέτρα ώστε να προετοιμασθεί κατάλληλα για κάθε τύπο απειλής.

Το κάθε κράτος έχει τους δικούς του νόμους και τρόπους αντιμετώπισης επιθέσεων, ωστόσο κρίνεται σημαντικό να καθιερωθεί ένα διεθνές νομικό πλαίσιο για τις κυβερνοεπιθέσεις. Με αυτό τον τρόπο, δίνεται η δυνατότητα να υπάρξουν διακρατικές κυρώσεις και να αποφασισθεί τι μπορεί να θεωρηθεί αιτία πολέμου μεταξύ κρατών. Αυτή τη στιγμή, είναι στην διακριτική ευχέρεια κάθε κράτους να αξιολογήσει την σοβαρότητα μιας δεχόμενης επίθεσης και να απαντήσει αναλόγως, γεγονός που μπορεί να προκαλέσει δυσανάλογες αντιδράσεις και να προκύψουν ανεξέλεγκτες επιπτώσεις. Παρόλα αυτά, σε πολλές από τις επιθέσεις που αναφέρθηκαν δεν υπήρξαν νομικά αντίποινα στους επιτιθέμενους, αφού οι περισσότερες εκτελέσθηκαν από έμπειρα άτομα υποστηριζόμενα από κράτη, επομένως δεν γνωστοποιήθηκαν ποτέ οι επιτιθέμενοι.

Λεξικό Όρων

DDoS – Distributed Denial of Service (Αποκεντρωμένη Άρνηση Παροχής Υπηρεσιών): Η τεχνική με την οποία υπηρεσίες και πόροι ενός υπολογιστή καθίστανται μη διαθέσιμοι στους προοριζόμενους χρήστες.

Ping flooding : Η αποστολή ενός μεγάλου αριθμού πακέτων εντοπισμού προς έναν διακομιστή, υπό κανονικές συνθήκες ένα τέτοιο πακέτο χρησιμοποιείται για την εύρεση ενός υπολογιστή ή διακομιστή ο οποίος απαντάει στον αποστολέα ώστε να υπάρξει σύνδεση μεταξύ τους

Ransomware (Λυτρισμικό) : Τύπος ιού που κρυπτογραφεί τα δεδομένα του χρήστη και απαιτεί λύτρα σε κρυπτονομίσματα για την αποκρυπτογράφηση τους

SMB : Πρωτόκολλο επικοινωνίας για την κοινή πρόσβαση σε αρχεία και συσκευές από τους κόμβους εντός ενός δικτύου

Backdoor (Κερκόπορτα) : Κρυφός τρόπος εισόδου παρακάμπτοντας τις απαιτούμενες μεθόδους αυθεντικοποίησης για την εξ αποστάσεως πρόσβαση σε ένα σύστημα

Επίθεση zero-day: Επιθέσεις που εκμεταλλεύονται ευπάθειες πληροφοριακών συστημάτων τις οποίες οι προγραμματιστές δεν έχουν επίγνωση της ύπαρξης τους.

Rootkit: Λογισμικό που επιτρέπει την συνεχή πρόσβαση σε έναν υπολογιστή με προνόμια υπερχρήστη.

Περίληψη

Στο παρόν έγγραφο παρουσιάζονται αναλυτικά μέσα και τρόποι προσβολής που χρησιμοποιήθηκαν σε κάποιες από τις πιο γνώστες περιπτώσεις επιθέσεων με στόχο κρατικά πληροφοριακά συστήματα ανά τον κόσμο, καλύπτοντας τις κατηγορίες ransomware, DDoS, hacktivism, Cyber-warfare και Data Breaches. Σκοπός είναι ο εντοπισμός διαδικτυακών απειλών που το υπουργείο εθνικής άμυνας μπορεί να κληθεί να αντιμετωπίσει.

Στην συνέχεια η έρευνα περιλαμβάνει ανάγωγη στα ελληνικά δεδομένα εξετάζοντας νομικές δυνατότητες αντιμετώπισής τους με βάση το εθνικό νομοθετικό πλαίσιο ανά κατηγορία επίθεσης. Πιο συγκεκριμένα για κάθε κατηγορία επίθεσης εξετάζονται οι παραβάσεις που προκύπτουν και πως αυτές διώκονται ποινικά στην χώρα μας. Επιπλέον γίνεται αναφορά και στις ποινές που προβλέπει ο νόμος για κάθε μια.

Βιβλιογραφία

Πηγές πληροφόρησης επιθέσεων

- Stuxnet
  1. https://en.wikipedia.org/wiki/Stuxnet (τελευταία πρόσβαση 8.5.2021)
  2. http://large.stanford.edu/courses/2015/ph241/holloway1/ (τελευταία πρόσβαση 8.5.2021)

- Επιθέσεις στην Εσθονία
  1. https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia (τελευταία πρόσβαση 8.5.2021)
  2. https://en.wikipedia.org/wiki/Tallinn_Manual (τελευταία πρόσβαση 8.5.2021)
  3. https://www.bbc.com/news/39655415 (τελευταία πρόσβαση 8.5.2021)

- Επιθέσεις στη Σιγκαπούρη
  1. https://www.reuters.com/article/us-singapore-hacker/singapore-on-alert-for-cyber-attacks-after-websites-hacked-idUKBRE9A30FP20131104 (τελευταία πρόσβαση 8.5.2021)
  2. https://en.wikipedia.org/wiki/The_Straits_Times (τελευταία πρόσβαση 8.5.2021)
  3. https://en.wikipedia.org/wiki/2013_Singapore_cyberattacks (τελευταία πρόσβαση 8.5.2021)
  4. https://en.wikipedia.org/wiki/Media_Development_Authority (τελευταία πρόσβαση 8.5.2021)

- Επιθέσεις στην Ουκρανία
  1. https://en.wikipedia.org/wiki/2017_cyberattacks_on_Ukraine (τελευταία πρόσβαση 8.5.2021)
  2. https://en.wikipedia.org/wiki/Annexation_of_Crimea_by_the_Russian_Federation (τελευταία πρόσβαση 8.5.2021)
  3. https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine (τελευταία πρόσβαση 8.5.2021)

- WannaCry
  1. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry (τελευταία πρόσβαση 8.5.2021)
  2. https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html (τελευταία πρόσβαση 8.5.2021)

- Επιθέσεις DNC
  1. https://en.wikipedia.org/wiki/Democratic_National_Committee_cyber_attacks (τελευταία πρόσβαση 8.5.2021)
  2. https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html (τελευταία πρόσβαση 8.5.2021)

- Office of Personnel Management data breach
  1. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html (τελευταία πρόσβαση 8.5.2021)

- Πληροφορίες για την αντιμετώπιση της παραβίασης προσωπικών δεδομένων και ΓΚΠΔ
  1. https://www.lawspot.gr/nomika-nea/ti-einai-i-paraviasi-dedomenon-data-breach-kai-poies-einai-oi-shetikes-ypohreoseis (τελευταία πρόσβαση 8.5.2021)
  2. https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-33-genikos-kanonismos-gia-tin-prostasia-dedomenon?lspt_context=gdpr (τελευταία πρόσβαση 8.5.2021)
  3. https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-55-genikos-kanonismos-gia-tin-prostasia-dedomenon?lspt_context=gdpr (τελευταία πρόσβαση 8.5.2021)
  4. https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-34-genikos-kanonismos-gia-tin-prostasia-dedomenon?lspt_context=gdpr (τελευταία πρόσβαση 8.5.2021)
  5. https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-83-genikos-kanonismos-gia-tin-prostasia-dedomenon-genikoi?lspt_context=gdpr (τελευταία πρόσβαση 8.5.2021)
  6. https://www.lawspot.gr/nomikes-plirofories/nomothesia/genikos-kanonismos-gia-tin-prostasia-dedomenon?lspt_context=gdpr (τελευταία πρόσβαση 8.5.2021)

- Πληροφορίες για το hacktivism και νομοθεσία περί αυτού
  1. https://en.wikipedia.org/wiki/Hacktivism (τελευταία πρόσβαση 8.5.2021)
  2. https://opi.gr/edppi1/apofaseis-edppi (τελευταία πρόσβαση 8.5.2021)
  3. https://en.wikipedia.org/wiki/Mirror_site (τελευταία πρόσβαση 8.5.2021)
  4. https://en.wikipedia.org/wiki/Doxing (τελευταία πρόσβαση 8.5.2021)
  5. https://www.privacy.go.kr/cmm/fms/FileDown.do?atchFileId=FILE_000000000830762&fileSn=0#:~:text=Article%201%20(Purpose)%20The%20purpose,communications%20networks%20in%20order%20to (τελευταία πρόσβαση 8.5.2021)

- Πληροφορίες και νομική αντιμετώπιση επιθέσεων άρνησης υπηρεσιών
  1. https://lawandtech.eu/2016/05/21/information-systems-attacks/ (τελευταία πρόσβαση 8.5.2021)

2. https://www.crimetimes.gr/%CE%B5%CF%80%CE%B9%CE%B8%CE%AD%CF%83%CE%B5%CE%B9%CF%82-%CE%AC%CF%81%CE%BD%CE%B7%CF%83%CE%B7%CF%82-%CF%80%CE%B1%CF%81%CE%BF%CF%87%CE%AE%CF%82-%CF%85%CF%80%CE%B7%CF%81%CE%B5%CF%83%CE%B9%CF%8E%CE%BD-dos/ (τελευταία πρόσβαση 8.5.2021)
3. https://www.lawspot.gr/nomikes-plirofories/nomothesia/pk/arthro-381a-poinikos-kodikas-fthora-ilektronikon-dedomenon (τελευταία πρόσβαση 8.5.2021)

- Νομική αντιμετώπιση για τις επιθέσεις ransomware (λυτρισμικού)
  1. https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-292v-poinikos-kodikas-nomos-4619-2019-parakolysi (τελευταία πρόσβαση 8.5.2021)
  2. https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-216-poinikos-kodikas-nomos-4619-2019-plastografia (τελευταία πρόσβαση 8.5.2021)
  3. https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-385-poinikos-kodikas-nomos-4619-2019-ekviasi (τελευταία πρόσβαση 8.5.2021)

- Περισσότερες πληροφορίες
  1. https://ec.europa.eu/home-affairs/what-we-do/policies/cybercrime_en (τελευταία πρόσβαση 8.5.2021)
  2. https://www.dcaf.ch/sites/default/files/publications/documents/CyberPaper_3.6.pdf (τελευταία πρόσβαση 8.5.2021)
  3. https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx (τελευταία πρόσβαση 8.5.2021)