Μάθημα: Στοιχεία Δικαίου της Πληροφορίας

Θέμα εργασίας: Καταγραφή γνωστών περιπτώσεων επιθέσεων σε κρατικά πληροφοριακά συστήματα και ανάλυση των νομικών δυνατοτήτων αντιμετώπισής τους με βάση το εθνικό νομοθετικό πλαίσιο.

Ομάδα:

Ανδρινόπουλος Κωνσταντίνος 3190009

Κοτσιφός Γεώργιος 3190093

Τσάμη Κωνσταντίνα 3190322

Εισαγωγή

Τα τελευταία χρόνια παρατηρείται ένας αυξανόμενος αριθμός επιθέσεων σε κρατικά συστήματα πληροφοριών. Οι επιθέσεις αυτές μπορεί να έχουν σημαντικό αντίκτυπο στην κυβέρνηση, συμπεριλαμβανομένης της διακοπής των υπηρεσιών, της κλοπής δεδομένων και της πρόκλησης οικονομικών απωλειών.

Σκοπός της συγκεκριμένης εργασίας είναι να καταγράψει γνωστές περιπτώσεις επιθέσεων σε κρατικά πληροφοριακά συστήματα και θα αναλύσει τις νομικές δυνατότητες αντιμετώπισής τους με βάση το εθνικό νομικό πλαίσιο. Αρχικά θα προσδιορίζουμε τους διάφορους τύπους επιθέσεων που έχουν πραγματοποιηθεί σε κρατικά συστήματα πληροφοριών και στη συνέχεια θα παρουσιαστεί το εθνικό νομικό πλαίσιο που ισχύει για την αντιμετώπιση αυτών των επιθέσεων.
Οι συχνότερες και πιο γνωστές επιθέσεις σε κρατικά πληροφοριακά συστήματα είναι οι ακόλουθες:

- **Distributed Denial of Service Attack(DDoS)**

Επιθέσεις άρνησης εξυπηρέτησης ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες. Η κυριότερη μορφή των επιθέσεων αυτών χρησιμοποιεί πολλαπλές επιθέσεις μέσω άλλων θυμάτων ή και θυτών και είναι γνωστή σαν κατανεμημένη επίθεση άρνησης εξυπηρέτησης(DDoS)

Κάποια γνωστά περιστατικά επιθέσεων DDoS είναι τα εξής:

Κυβερνοεπίθεση Υπ. Ψηφιακής Διακυβέρνησης:

Μια από τις μεγαλύτερες κυβερνοεπιθέσεις δέχτηκαν τα πληροφοριακά συστήματα του υπουργείου Ψηφιακής Διακυβέρνησης, με επίκεντρο το TAXISnet, του οποίου η λειτουργία

μπλοκαρίστηκε για πάνω από 48 ώρες.Επρόκειτο για πρωτοφανή επίθεση αυτού του τύπου, που σύμφωνα με πηγές προήλθε από την Ολλανδία και μέσω της οποίας οι άγνωστοι κυβερνοεγκληματίες επιχείρησαν να «ρίξουν» προσωρινά ή και να διακόψουν εντελώς τη λειτουργία περίπου 800 ιστοτόπων του Δημοσίου. Σημειωτέον, ότι με τη χρήση των κωδικών TAXISnet λειτουργούν εκατοντάδες υπηρεσίες του Gov.gr, όπως και οι πιστοποιήσεις (αυθεντικοποιήσεις) για υπηρεσίες των τραπεζικών ιδρυμάτων.

Viasat Hack :

Το hack της Viasat, το οποίο συνέβη μεταξύ 5 π.μ. και 9 π.μ. ώρα Ελλάδας στις 24 Φεβρουαρίου, μπορεί να είχε ως στόχο να διαταράξει τα ουκρανικά στρατιωτικά δίκτυα, τα οποία χρησιμοποιούσαν το δίκτυο της Viasat για να τους παρέχει υπηρεσίες επικοινωνίας. Η επίθεση "κατέστησε μη λειτουργικά χιλιάδες δορυφορικά ευρυζωνικά μόντεμ της Viasat KA-SAT στην Ουκρανία, συμπεριλαμβανομένων εκείνων που χρησιμοποιούνταν από στρατιωτικές και άλλες κυβερνητικές υπηρεσίες, προκαλώντας σημαντική απώλεια στην επικοινωνία μέσω διαδικτύου.

2007 Κυβερνοεπιθέσεις στην Εσθονία:

Από τις 27 Απριλίου 2007, μια σειρά κυβερνοεπιθέσεων στόχευσε ιστότοπους Εσθονικών οργανισμών, συμπεριλαμβανομένου του εσθονικού κοινοβουλίου, τραπεζών, υπουργείων, εφημερίδων και ραδιοτηλεοπτικών φορέων, εν μέσω της διαφωνίας της χώρας με τη Ρωσία σχετικά με τη μετακίνηση του Χάλκινου Στρατιώτη του Ταλίν, ενός περίτεχνου ταφικού μνημείου της σοβιετικής εποχής, καθώς και πολεμικών τάφων στο Ταλίν. Οι περισσότερες από τις επιθέσεις που είχαν κάποια επιρροή στο ευρύ κοινό ήταν κατανεμημένες επιθέσεις τύπου άρνησης παροχής υπηρεσιών, οι οποίες κυμαίνονταν από μεμονωμένα άτομα που χρησιμοποιούσαν διάφορες μεθόδους, όπως πλημμύρες ping, μέχρι ακριβές ενοικιάσεις botnets που χρησιμοποιούνται συνήθως για τη διανομή spam. Μετά την επίθεση, η Εσθονία έχει ταχθεί

υπέρ της αύξησης της προστασίας και του πρωτοκόλλου αντιμετώπισης της ασφάλειας στον κυβερνοχώρο.

Νόμοι για DDoS:

Για αρχή, ας δούμε τον ορισμό του DdOS: Σύμφωνα με το Άρθρο 2 - Απόφαση ΕΕΤΤ 750/2/19.02.2015 η Άρνηση Παροχής Υπηρεσίας ή Αποκεντρωμένη Άρνηση Παροχής Υπηρεσίας [Denial of Service (DoS) ή Distributed Denial of Service (DDoS)] είναι η τεχνική με την οποία υπηρεσίες και πόροι ενός υπολογιστή καθίστανται μη διαθέσιμοι στους προοριζόμενους χρήστες.

Με τον ν. 4619/2019 στο άρθρο 292Β έχουμε:

1. Όποιος χωρίς δικαίωμα παρεμποδίζει σοβαρά ή διακόπτει τη λειτουργία συστήματος πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά, τιμωρείται με φυλάκιση και χρηματική ποινή.

2. Η πράξη της πρώτης παραγράφου τιμωρείται: α) με φυλάκιση τουλάχιστον ενός έτους και χρηματική ποινή, αν τελέστηκε με τη χρήση εργαλείου που έχει σχεδιαστεί κατά κύριο λόγο για πραγματοποίηση επιθέσεων που επηρεάζουν μεγάλο αριθμό συστημάτων πληροφοριών ή επιθέσεων που προκαλούν σοβαρές ζημίες και ιδίως επιθέσεων που προκαλούν μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημιά ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων, β) με φυλάκιση τουλάχιστον δύο ετών και χρηματική ποινή, αν προκάλεσε σοβαρές ζημίες και ιδίως μεγάλης έκτασης ή για μεγάλο χρονικό διάστημα διατάραξη των υπηρεσιών των συστημάτων πληροφοριών, οικονομική ζημία ιδιαίτερα μεγάλης αξίας ή σημαντική απώλεια δεδομένων και γ) με φυλάκιση τουλάχιστον τριών ετών και χρηματική ποινή, αν τελέστηκε κατά συστημάτων πληροφοριών που αποτελούν μέρος υποδομής για την προμήθεια του πληθυσμού με ζωτικής σημασίας αγαθά ή υπηρεσίες. Ως ζωτικής σημασίας αγαθά ή υπηρεσίες νοούνται ιδίως η εθνική άμυνα, η υγεία, οι συγκοινωνίες, οι μεταφορές και η ενέργεια.

Οπότε, ένα DDoS attack επιφέρει αυτά τα πρόστιμα της 2η παραγράφου λόγο τον αποκλεισμό της πρόσβασης στα δεδομένα.

- **Data Breaches: DNS hijacking, Info-stealer malware**

Η παραβίαση δεδομένων είναι ένα περιστατικό κατά το οποίο πληροφορίες εκλάπησαν ή λήφθηκαν από ένα σύστημα χωρίς τη γνώση ή την εξουσιοδότηση του ιδιοκτήτη του συστήματος. Μια μικρή εταιρεία ή ένας μεγάλος οργανισμός μπορεί να υποστεί παραβίαση δεδομένων. Τα κλεμμένα δεδομένα μπορεί να αφορούν ευαίσθητες, ιδιόκτητες ή εμπιστευτικές πληροφορίες, όπως αριθμούς πιστωτικών καρτών, δεδομένα πελατών, εμπορικά μυστικά ή θέματα εθνικής ασφάλειας.

Μερικά γνωστά περιστατικά παραβίασης δεδομένων είναι τα εξής:

ΕΥΠ, Μαξίμου, ΕΛ.ΑΣ το 2020:

Τον Απρίλιο του 2019 στο στόχαστρο χάκερ μπήκε το Μέγαρο Μαξίμου, το υπουργείο Εσωτερικών, η ΕΥΠ και η Ελληνική Αστυνομία, στο πλαίσιο μιας διεθνούς εκστρατείας κυβερνοκατασκοπείας με την κωδική ονομασία «Θαλάσσια Χελώνα» (Sea Turtle). Οι επιτιθέμενοι κατάφεραν να αποκτήσουν πρόσβαση στα εσωτερικών δίκτυα των κρατικών υπηρεσιών, που περιέχουν την ηλεκτρονική τους αλληλογραφία.
Η επίθεση των χάκερ έγινε αντιληπτή από στελέχη της ομάδας κυβερνοασφάλειας, καθώς διαπιστώθηκε ασυνήθιστη δυσλειτουργία στη χρήση των emails. Η αυτοψία επιβεβαίωσε πως βρισκόταν σε εξέλιξη επίθεση τύπου DNS Hijacking.

Φεβρουάριος 2023. Η βορειοκορεατική ομάδα hacking Lazarus διεξήγαγε εκστρατεία κατασκοπείας μεταξύ Αυγούστου και Νοεμβρίου 2022:

Μια νέα εκστρατεία κατασκοπείας στον κυβερνοχώρο με την ονομασία "No Pineapple!" αποδίδεται στην ομάδα hacking Lazarus της Βόρειας Κορέας, επιτρέποντας στους δράστες απειλών να κλέψουν κρυφά 100GB δεδομένων χωρίς να προκαλέσουν καμία καταστροφή.
Η εκστρατεία διήρκεσε από τον Αύγουστο έως τον Νοέμβριο του 2022, στοχεύοντας οργανισμούς στον τομέα της ιατρικής έρευνας, της υγειονομικής περίθαλψης, της χημικής μηχανικής, της ενέργειας, της άμυνας και ένα κορυφαίο ερευνητικό πανεπιστήμιο.

Το Βουλγαρικό Personal Tax Revenue office υπέστη παραβίαση δεδομένων που εκθέτει προσωπικές αναγνωριστικές πληροφορίες:

Οι αρχές αναγνώρισαν ότι η εθνική φορολογική υπηρεσία της Βουλγαρίας υπέστη παραβίαση. Εκλάπησαν προσωπικά δεδομένα σχεδόν κάθε ενήλικα, τα ονόματα, οι διευθύνσεις, τα εισοδήματα και τα στοιχεία κοινωνικής ασφάλισης έως και πέντε εκατομμυρίων Βουλγάρων και κατοίκων. Ανεξάρτητα από το ποιος διέπραξε την παραβίαση, οι ειδικοί δήλωσαν ότι η παραβίαση ανέδειξε τον ολοένα αυξανόμενο κίνδυνο που αντιμετωπίζουν τόσο οι κυβερνήσεις όσο και οι πολίτες τους σε έναν ολοένα και πιο ψηφιοποιημένο κόσμο.
Η παραβίαση ήταν η μεγαλύτερη κλοπή προσωπικών δεδομένων που έχει αναφερθεί ποτέ στα Βαλκάνια.

Ransomware attacks

Το ransomware είναι ένα είδος κακόβουλου λογισμικού που απειλεί να δημοσιοποιήσει τα προσωπικά δεδομένα του θύματος ή να διακόψει την πρόσβασή του θύματος σε αυτά, μέχρι να δοθούν λύτρα από το θύμα.

Κάποια γνωστά περιστατικά επιθέσεων ransomware είναι τα εξής:

Επιθέσεις ransomware στην Ουκρανία:

Μια σειρά ισχυρών κυβερνοεπιθέσεων με τη χρήση του κακόβουλου λογισμικού Petya ξεκίνησε στις 27 Ιουνίου 2017 και κατέκλυσε ιστότοπους ουκρανικών οργανισμών, συμπεριλαμβανομένων τραπεζών, υπουργείων, εφημερίδων και επιχειρήσεων ηλεκτρικής ενέργειας.Κατά τη διάρκεια της επίθεσης το σύστημα παρακολούθησης της ραδιενέργειας στον πυρηνικό σταθμό του Τσερνομπίλ στην Ουκρανία τέθηκε εκτός λειτουργίας. Αρκετά ουκρανικά υπουργεία, τράπεζες, συστήματα μετρό και κρατικές επιχειρήσεις επηρεάστηκαν. Σημαντικά αρχεία των μολυσμένων υπολογιστών αντικαταστάθηκαν και έτσι υπέστησαν μόνιμη βλάβη,

παρά το μήνυμα που εμφανιζόταν από το κακόβουλο λογισμικό στον χρήστη που ανέφερε ότι όλα τα αρχεία θα μπορούσαν να ανακτηθούν "με ασφάλεια και ευκολία", ικανοποιώντας τις απαιτήσεις των επιτιθέμενων και καταβάλλοντας την αιτούμενη πληρωμή σε νόμισμα Bitcoin.

Wiper malware επίθεση:

Λίγο πριν από τις 5 μ.μ. της 23ης Φεβρουαρίου, εντοπίστηκε κακόβουλο λογισμικό data wiper σε εκατοντάδες υπολογιστές που ανήκαν σε πολλούς ουκρανικούς οργανισμούς, μεταξύ άλλων στους τομείς των χρηματοοικονομικών, της άμυνας, των αερομεταφορών και των υπηρεσιών πληροφορικής. Το wiper φέρεται να συντάχθηκε στις 28 Δεκεμβρίου 2021, ενώ η Symantec ανέφερε κακόβουλη δραστηριότητα ήδη από τον Νοέμβριο του 2021, γεγονός που υποδηλώνει ότι η επίθεση είχε σχεδιαστεί μήνες νωρίτερα. Η Symantec ανέφερε επίσης επιθέσεις wiper εναντίον συσκευών στη Λιθουανία και ότι ορισμένοι οργανισμοί είχαν εκτεθεί μήνες πριν από την επίθεση wiper. Παρόμοια με την επίθεση Whisper Gate του Ιανουαρίου, το ransomware συχνά αναπτύσσεται ταυτόχρονα με το wiper ως δόλωμα και το wiper καταστρέφει το κύριο αρχείο εκκίνησης της συσκευής.

Νόμοι για τα Data Breaches και τα Ransomware Attacks

Στον Νόμο 4619/2019 αναφέρετε το:

Άρθρο 370Β:

1. Όποιος κατά παράβαση μέτρου προστασίας και χωρίς δικαίωμα αποκτά πρόσβαση σε μέρος ή στο σύνολο συστήματος πληροφοριών ή σε ηλεκτρονικά δεδομένα τιμωρείται με φυλάκιση έως δύο έτη ή χρηματική ποινή. Σε ιδιαίτερα ελαφρές περιπτώσεις η πράξη μένει ατιμώρητη.

2. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του συστήματος πληροφοριών ή των δεδομένων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του.

3. Αν η πράξη της παραγράφου 1 αναφέρεται σε επιστημονικά ή επαγγελματικά απόρρητα επιχείρησης του δημόσιου ή ιδιωτικού τομέα τιμωρείται με φυλάκιση έως τρία έτη ή χρηματική ποινή.

4. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου των στοιχείων καθώς και αν το απόρρητο είναι ιδιαίτερα μεγάλης οικονομικής αξίας, επιβάλλεται φυλάκιση και χρηματική ποινή.

5. Για την ποινική δίωξη των πράξεων των παραγράφων 1 και 4 απαιτείται έγκληση.

Και το:

Άρθρο 370Δ:

1. Όποιος χωρίς δικαίωμα αντιγράφει ή χρησιμοποιεί προγράμματα υπολογιστών, τιμωρείται με χρηματική ποινή ή παροχή κοινωφελούς εργασίας.
2. Όποιος χωρίς δικαίωμα αποκτά πρόσβαση στο σύνολο ή τμήμα πληροφοριακού συστήματος ή σε στοιχεία που μεταδίδονται με συστήματα τηλεπικοινωνιών, παραβιάζοντας απαγορεύσεις ή μέτρα ασφαλείας που έχει λάβει ο νόμιμος κάτοχος του, τιμωρείται με φυλάκιση.
3. Αν ο δράστης είναι στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος ή των στοιχείων, η πράξη της προηγούμενης παραγράφου τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου.

Αυτά τα άρθρα εστιάζουν περισσότερο στη παράνομη απόκτηση πρόσβασης σε ένα πληροφοριακό σύστημα και τα αντίστοιχα πρόστιμα, που μπορούμε να το αναφέρουμε ως το πρώτο βήμα για να δημιουργηθούν 2 προβλήματα: Data Breach και RansomWare.
Data Breach έχουμε όταν υπάρχει κλοπή δεδομένων ενώ RansomWare έχουμε όταν τα δεδομένα μιας επιχείρησης κρυπτογραφούνται από έναν τρίτο χρήστη, οπότε δεν μπορούν να τα δουν οι κανονικοί χρήστες, και τα αποκρυπτογραφούν αν και μόνο αν δοθούν λύτρα για αυτά.

Πιο συγκεκριμένα, όταν υπάρχει κίνδυνος παραβίασης προσωπικών στοιχείων, τότε μπαίνει σε ισχύ ο ΓΚΠΔ και ο ν. 4624/2019 ο οποίος είναι η εφαρμογή του ΓΚΠΔ. Οι κανονισμοί που θα

αναφέρουμε μεταξύ 4624/2019 και ΓΚΠΔ μοιάζουν, όπως είναι φυσικό. Για αρχή ας δούμε τα άρθρα 33, 34, και 83 για του ΓΚΠΔ,τα οποία υπάρχουν αντίστοιχα στον ν. 4264/2019:
Το άρθρο 33 του ΓΚΠΔ αναφέρει πως ο οργανισμός χρειάζεται να δηλώσει το συμβάν Ο εκτελών την επεξεργασία ενημερώνει τον υπεύθυνο επεξεργασίας αμελλητί, μόλις αντιληφθεί παραβίαση δεδομένων προσωπικού χαρακτήρα χωρίς κάποια καθυστέρηση.
Το άρθρο 34 του ΓΚΠΔ αναφέρει πως ο οργανισμός χρειάζεται να ενημερώσει και στους χρήστες που παραβιάστηκαν τα δεδομένα τους.
Το άρθρο 83 του ΓΚΠΔ πραγματεύεται τους γενικούς όρους επιβολής διοικητικών προστίμων ο οποίος λέει τα εξής: Κάθε εποπτική αρχή μεριμνά ώστε η επιβολή διοικητικών προστίμων να είναι για κάθε μεμονωμένη περίπτωση αποτελεσματική, αναλογική και αποτρεπτική. Το ύψος του προστίμου εξαρτάται από τη σοβαρότητα της παράβασης, τον αριθμό των υποκειμένων των δεδομένων που θίγονται και τον βαθμό της ζημίας που υπέστησαν. Άλλοι παράγοντες που μπορεί να ληφθούν υπόψη περιλαμβάνουν τη φύση της επεξεργασίας, οι κατηγορίες δεδομένων προσωπικού χαρακτήρα που επηρεάζει η παράβαση, το βαθμό συνεργασίας με την εποπτική αρχή και το κατά πόσο ο υπεύθυνος επεξεργασίας ή ο εκτελών της επεξεργασίας έχει ιστορικό παραβάσεων. Το συνολικό ποσό του προστίμου για πολλαπλές παραβάσεις δεν μπορεί να υπερβαίνει το ποσό που ορίζεται για την πιο σοβαρή παράβαση. Οι πιο σοβαρές παραβιάσεις είναι αυτές που συνεπάγονται θεμελιώδη παραβίαση του ΓΚΠΔ, όπως η επεξεργασία δεδομένων προσωπικού χαρακτήρα χωρίς συγκατάθεση ή η μη αναφορά παραβίασης δεδομένων στην εποπτική αρχή εντός 72 ωρών.
Το ύψος του προστίμου για λιγότερο σοβαρή παραβίαση περιορίζεται σε 10 εκατ. ευρώ ή σε περίπτωση επιχειρήσεων, έως το 2 % του συνολικού παγκόσμιου ετήσιου κύκλου εργασιών του προηγούμενου οικονομικού έτους, ανάλογα με το ποιο είναι υψηλότερο, ενώ σε πιο σοβαρές περιπτώσεις αγγίζουν τα 20 εκατ. ευρώ ή σε περίπτωση επιχειρήσεων έως το 4 %. Ωστόσο, κάθε κράτος μέλος μπορεί να καθορίσει τους κανόνες σχετικά με το αν και σε ποιο βαθμό μπορούν να επιβληθούν διοικητικά πρόστιμα σε δημόσιες αρχές και φορείς που είναι εγκατεστημένοι στο εν λόγω κράτος μέλος.

Ας επιστρέψουμε στα Ransomware Attacks, και στους νόμους. Εκτός από τους νόμους που προαναφέρθηκαν στα άρθρα 370Β και 370Δ, θα πρέπει να λάβουμε υπόψη και τον εκβιασμό

που εμπεριέχει η φύση των Ransomware attack. Ο εκβιασμός τιμωρείται με το άρθρο 385 στον ν. 4619/2019. Πιο συγκεκριμένα αναφέρει στις παραγράφους 1 και 3 πως:

1. Όποιος, με σκοπό να αποκομίσει ο ίδιος ή τρίτος παράνομο περιουσιακό όφελος, εξαναγκάζει άλλον με βία ή απειλή σε πράξη, παράλειψη ή ανοχή από την οποία επέρχεται ζημία στην περιουσία του εξαναγκαζομένου ή άλλου τιμωρείται με φυλάκιση τουλάχιστον ενός (1) έτους και χρηματική ποινή.

3. Η εκβίαση τιμωρείται με φυλάκιση τουλάχιστον τριών (3) ετών και χρηματική ποινή αν ο υπαίτιος μεταχειρίστηκε βία ή απειλή βλάβης της επιχείρησης, του επαγγέλματος, του λειτουργήματος ή άλλης δραστηριότητας που ασκεί ο εξαναγκαζόμενος ή άλλος ή προσφέρθηκε να παρέχει ή παρέχει προστασία για την αποτροπή πρόκλησης τέτοιας βλάβης από τρίτον. Αν την παραπάνω πράξη τέλεσε πρόσωπο που διαπράττει τέτοιες πράξεις κατ' επάγγελμα, επιβάλλεται κάθειρξη έως δέκα έτη και χρηματική ποινή.

- **Hacktivism**

Οι Anonymous και οι επιθέσεις στην Τυνησία:

Το 2011, οι Anonymous εξαπέλυσαν μια σειρά επιθέσεων κατά των πληροφοριακών συστημάτων της κυβέρνησης της Τυνησίας για την υποστήριξη των διαδηλώσεων της Αραβικής Άνοιξης. Η ομάδα χακτιβιστών παραμόρφωσε κυβερνητικούς ιστότοπους συμπεριλαμβανομένων εκείνων του προέδρου, του πρωθυπουργού, του υπουργείου βιομηχανίας, του υπουργείου εξωτερικών και του χρηματιστηρίου, διέρρευσε ευαίσθητες πληροφορίες και εξαπέλυσε επιθέσεις DDoS εναντίον βασικών κυβερνητικών διακομιστών. Η επίθεση συνέπεσε με μια εθνική απεργία, που είχε προγραμματιστεί να πραγματοποιηθεί τη Δευτέρα, η οποία, σύμφωνα με τους διοργανωτές, θα ήταν η μεγαλύτερη λαϊκή εκδήλωση αυτού του μεγέθους από τότε που ο Ζιν Ελ Αμπιντίν Μπεν Αλί ανέλαβε την προεδρία. Οι επιθέσεις αυτές συνέβαλαν στο να προσελκύσουν την προσοχή στη λογοκρισία και τις παραβιάσεις των ανθρωπίνων δικαιωμάτων της κυβέρνησης και έπαιξαν ρόλο στην τελική ανατροπή του προέδρου Ζιν Ελ Αμπιντίν Μπεν Αλί. Η επιχείρηση "Τυνησία" πραγματοποιήθηκε μόλις λίγες ημέρες μετά από μια παρόμοια επίθεση σε ιστότοπους της

κυβέρνησης της Ζιμπάμπουε. Σε εκείνη την περίπτωση, οι Anonymous δήλωσαν ότι στόχευσαν την κυβέρνηση του Ρόμπερτ Μουγκάμπε για τις ενέργειες που έλαβαν οι αξιωματούχοι για την καταστολή των πληροφοριών σχετικά με τα χιλιάδες απόρρητα διπλωματικά τηλεγραφήματα των ΗΠΑ που δημοσίευσε το WikiLeaks. "Οι επιθέσεις στον κυβερνοχώρο θα συνεχιστούν έως ότου η κυβέρνηση της Τυνησίας σεβαστεί το δικαίωμα όλων των Τυνήσιων πολιτών στην ελευθερία του λόγου και της πληροφόρησης και σταματήσει τη λογοκρισία στο διαδίκτυο" σχολίασαν για την επίθεση η ομάδα χακτιβιστών Anonymous. Το αποτέλεσμα των επιθέσεων ήταν να εγκαταλείψει τη χώρα ο Μπεν Αλί τον ίδιο μήνα που οι διαδηλώσεις κατέκλυσαν τη χώρα.

Οι Anonymous και άλλες ομάδες χάκερ καταρρίπτουν ιρανικούς κυβερνητικούς ιστότοπους:

Το 2022, ακολουθώντας τις υποστηρικτικές εξεγέρσεις για το θάνατο της 22-χρονης Mahsa Amini, η οποία υπέστη εγκεφαλικό επεισόδιο και αρκετές καρδιακές προσβολές ενώ βρισκόταν υπό την επιτήρηση της λεγόμενης αστυνομίας ηθικής του Ιράν για το "ακατάλληλο" χιτζάμπ που φορούσε, οι Ιρανικές κυβερνητικές και κρατικές ιστοσελίδες τέθηκαν εκτός λειτουργίας από τους Anonymous και άλλες παγκόσμιες ομάδες hacking σε μια κίνηση υποστήριξης αυτής της πανεθνικής διαμαρτυρίας. Αυτοί ισχυρίστηκαν ότι παραβίασαν τη βάση δεδομένων του ιρανικού κοινοβουλίου, αποκτώντας τα προσωπικά στοιχεία των βουλευτών. Στην εφαρμογή ανταλλαγής μηνυμάτων Telegram, η Atlas Intelligence Group, μια άλλη ομάδα χάκερ, λέει ότι διέρρευσε αριθμούς τηλεφώνων και διευθύνσεις ηλεκτρονικού ταχυδρομείου Ιρανών αξιωματούχων και διασημοτήτων, μια τακτική γνωστή ως "doxing". Η ίδια προσφέρθηκε επίσης να πουλήσει προφανή δεδομένα τοποθεσίας για το Σώμα Φρουρών της Ισλαμικής Επανάστασης, έναν κλάδο των ενόπλων δυνάμεων του Ιράν, σύμφωνα με την Check Point, η οποία έχει καταγράψει τις προσπάθειες των χακτιβιστών στο Ιράν. Ορισμένοι κρατικοί ιστότοποι στο Ιράν, όπως το ειδησεογραφικό πρακτορείο Fars που συνδέεται με το IRGC και ο ειδησεογραφικός ιστότοπος του κρατικού ραδιοτηλεοπτικού φορέα, είχαν περιορίσει την πρόσβαση στις σελίδες τους από το εξωτερικό, επειδή φοβόντουσαν μήπως δεχτούν επίθεση από τις ομάδες χακτιβιστών. Οι Anonymous, εκτός από την επίθεση, προέτρεψαν τους Ιρανούς να μην σταματήσουν την "επανάσταση". Η "επανάσταση" αυτή σύμφωνα με ομάδες ανθρωπίνων δικαιωμάτων, οδήγησε σε θάνατο τουλάχιστον επτά ανθρώπων οι οποίοι έχασαν

τη ζωή τους στις διαδηλώσεις, όλοι από τους οποίους σκοτώθηκαν από τις δυνάμεις ασφαλείας, ενώ οι ιρανικές αρχές έκαναν λόγο για τρεις νεκρούς.

Νόμοι για το Hacktivism:

Το Hacktivism μπορεί να πάρει πολλές μορφές, οπότε μπορεί να έχει διάφορους νόμους, θα εστιάσουμε στους νόμους που παραβιάζουν οι 2 επιθέσεις που έχουμε δώσει ως παραδείγματα. Για τις επιθέσεις των Anonymous στην Τυνησία έχουμε 1) παραμόρφωση κυβερνητικών ιστότοπων, 2) διέρευση ευαίσθητων δεδομένων, 3) DDoS σε διακομιστές της κυβέρνησης. Για το δεύτερο παράδειγμα, οι Anonymous και άλλες ομάδες χάκερ καταρρίπτουν ιρανικούς κυβερνητικούς ιστότοπους, έχουμε: 1) DDoS για να ρίξουν τις Ιρανικές κυβερνητικές ιστοσελίδες, 2) Data Breach και Data Leaks μέσω Doxing.
Για την παραμόρφωση κυβερνητικών ιστότοπων έχουμε για αρχή τον Νόμο 4619/2019 τα άρθρα 370Β και 370Δ που προαναφέρθηκαν. Για την διέρευση δεδομένων ισχύουν τα άρθρα 33, 34 και 83 για το τι πρέπει να κάνουν και τα αντίστοιχα πρόστιμα, τα οποία έχουν και αυτά προαναφερθεί. Τέλος, στο DDoS έχουμε τον ν. 4619/2019 στο άρθρο 292Β που επίσης έχουμε αναφέρει.

Σύνοψη

Στην παρούσα εργασία παρουσιάσαμε τρόπους και περιστατικά επιθέσεων σε κρατικά πληροφοριακά συστήματα ανά τον κόσμο και για κάθε κατηγορία επίθεσης (Ransomware, Data breach, Hacktivism, DDoS attack) αναλύθηκαν οι νομικές δυνατότητες αντιμετώπισής τους με βάση το εθνικό νομοθετικό πλαίσιο.

Βιβλιογραφία

- DDoS
  https://www.lawspot.gr/nomikes-plirofories/nomothesia/750-2-eett/arthro-2-apofasi-eett-750-2-19022015-orismoi (τελευταία πρόσβαση στις 5.5.2023)

  https://www.secnews.gr/434338/kivernoepithesi-ipourgeio-psifiakis-diakivernisis-stoxos-istotopoi-dimosiou/ (τελευταία πρόσβαση στις 5.5.2023)

https://www.grtimes.gr/politiki/chakaran-toys-istotopoys-tis-el-as-kai-toy (τελευταία πρόσβαση στις 5.5.2023)

https://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia(τελευταία πρόσβαση στις 5.5.2023)

https://en.wikipedia.org/wiki/2022_Ukraine_cyberattacks (τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-292v-poinikos-kodikas-nomos-4619-2019-parakolysi (τελευταία πρόσβαση στις 5.5.2023)

- Data Breaches και Ransomware attacks
https://www.cnn.gr/ellada/story/208656/agnosti-kyvernoepithesi-se-maximoy-eyp-kai-el-as-pos-ypeklapisan-eggrafa (τελευταία πρόσβαση στις 5.5.2023)

https://www.bleepingcomputer.com/news/security/north-korean-hackers-stole-research-data-in-two-month-long-breach/ (τελευταία πρόσβαση στις 5.5.2023)

https://www.nytimes.com/2019/07/17/world/europe/bulgaria-hack-cyberattack.html (τελευταία πρόσβαση στις 5.5.2023)

https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019 (τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-370v-poinikos-kodikas-nomos-4619-2019-paranomi(τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-370d-poinikos-kodikas-nomos-4619-2019 (τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-33-genikos-kanonismos-gia-tin-prostasia-dedomenon (τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-34-genikos-kanonismos-gia-tin-prostasia-dedomenon (τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-83-genikos-kanonismos-gia-tin-prostasia-dedomenon-genikoi (τελευταία πρόσβαση στις 5.5.2023)

https://en.wikipedia.org/wiki/2017_Ukraine_ransomware_attacks (τελευταία πρόσβαση στις 6.5.2023)

https://en.wikipedia.org/wiki/2022_Ukraine_cyberattacks (τελευταία πρόσβαση στις 6.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-385-poinikos-kodikas-nomos-4619-2019-ekviasi (τελευταία πρόσβαση στις 6.5.2023)

- Hacktivism

https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-370v-poinikos-kodikas-nomos-4619-2019-paranomi(τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-370d-poinikos-kodikas-nomos-4619-2019 (τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-33-genikos-kanonismos-gia-tin-prostasia-dedomenon (τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-34-genikos-kanonismos-gia-tin-prostasia-dedomenon (τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/gdpr/arthro-83-genikos-kanonismos-gia-tin-prostasia-dedomenon-genikoi (τελευταία πρόσβαση στις 5.5.2023)

https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4619-2019/arthro-292v-poinikos-kodikas-nomos-4619-2019-parakolysi (τελευταία πρόσβαση στις 5.5.2023)

https://www.aljazeera.com/news/2011/1/3/hackers-hit-tunisian-websites (τελευταία πρόσβαση στις 6.5.2023)

https://www.reuters.com/article/uk-tunisia-hacking/anonymous-says-hacks-tunisia-prime-ministers-emails-idUKBRE8370FA20120408 (τελευταία πρόσβαση στις 6.5.2023)

https://www.newarab.com/news/mahsa-amini-anonymous-claims-cyberattack-iran-websites (τελευταία πρόσβαση στις 6.5.2023)

https://www.iranintl.com/en/202209255133 (τελευταία πρόσβαση στις 6.5.2023)

https://www.cnbc.com/2022/10/05/how-anonymous-and-other-hacking-groups-are-aiding-protests-in-iran.html (τελευταία πρόσβαση στις 6.5.2023)