# Κυβερνοεπιθέσεις σε κρατικά πληροφοριακά συστήματα και νομικοί τρόποι αντιμετώπισης

Μάθημα: Στοιχεία δικαίου της πληροφορίας
Ομάδα: Σπυρίδων Μπάζιος (3170113)
Διογένης Τσολάκου (3170164)
Χρήστος Αργυρόπουλος (3170010)

# Εισαγωγή

- Στην παρουσίαση αυτή συνοψίζεται η έρευνα πάνω στις κυβερνοεπιθέσεις σε κρατικά πληροφοριακά συστήματα
- Αναφέρονται οι πιο δημοφιλείς κατηγορίες επιθέσεων και τα πιο σημαντικά παραδείγματα αυτών
- Γίνεται αναφορά των νομικών τρόπων αντιμετώπισης σύμφωνα με το εθνικό νομοθετικό πλαίσιο

# Επιθέσεις DDoS

**2007 Cyberattacks on Estonia**

*Σειρά επιθέσεων με στόχο πληθώρα ιστοσελίδων εθνικών οργανισμών της Εσθονίας.*

Τύπος επιθέσεων: DDOS (με μέθοδο ping flooding)

Αποτέλεσε την αφορμή για το διεθνές εγχειρίδιο νόμων του Ταλίν

# Νομική Αντιμετώπιση DDoS

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)

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.

*Για την αντιμετώπιση - ποινική δίωξη της πράξης απαιτείται έγκληση*

# Cyber-Warfare

**Stuxnet / Operation Olympic Games**

*Cyber-weapon που χρησιμοποιήθηκε κατά του Ιράν.*

Exploit: 4 ‘zero-day’ επιθέσεις σε βιομηχανικά συστήματα

Payload : Απότομη μεταβολή συχνοτήτων λειτουργίας φυγόκεντρων σε πυρηνικό εργοστάσιο στο Ιράκ με σκοπό την πρόκληση βλάβης.

# Νομική Αντιμετώπιση Cyber-Warfare

Το cyber-warfare αποτελεί μια ειδική περίπτωση επίθεσης λόγω του διακρατικού του χαρακτήρα. Εκδηλώνεται 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.

# Επιθέσεις Ransomware

- Τρόπος Επίθεσης: Windows OS - SMB protocol

- Petya (2017)
  - Λογιστικές Εταιρείες, Υπουργεία, Τράπεζες, Τσέρνομπιλ
  - Αποδυνάμωση Ουκρανικού Κράτους, 10 δις δολλάρια ζημιά

- WannaCry (2017)
  - 230.000 Η/Υ παγκοσμίως
  - ΥΠ.ΕΣ Ρωσίας, Πολιτείες Ινδίας, ΕΣΥ Αγγλίας, ΕΣΥ Σκωτίας

# Νομική Αντιμετώπιση Ransomware

- Φθορά Ψηφιακών Δεδομένων & Διακοπή Λειτουργίας ΠΣ
  - Α.292Β Ν.4619/2019 - Φυλάκιση & Χρηματική Ποινή
- Πλαστογραφία (Phishing)
  - Α.216 Ν.4619/2019 - Φυλάκιση & Χρηματική Ποινή
- Εκβίαση για Περουσιακό Όφελος
  - Α.385 Ν.4619/2019 - Φυλάκιση & Χρηματική Ποινή

# Data Breaches

**Επιθέσεις στην Εθνική Δημοκρατική Επιτροπή**

Μέρος συνόλου επιθέσεων για την υποκλοπή πληροφοριών Αμερικανικών πολιτικών οργανισμών από ρωσικές κρατικές ομάδες χάκερ, έχοντας ως απώτερο σκοπό την επιρροή στις εκλογές του 2016

**Επίθεση στο Γραφείο Διαχείρισης Προσωπικού**

Υποκλοπή προσωπικών στοιχείων εκατομμύριων Αμερικανών πολιτών από το κινέζικο κράτος

Ξεκίνησε τον Νοέμβριο του 2013, έγινε αντιληπτή μισό χρόνο αργότερα, δεν αντιμετωπίστηκε σωστά μέχρι το 2015 λόγω ύπαρξης backdoor

# Νομική Αντιμετώπιση Data Breaches

**Παραβίαση του απορρήτου των προσωπικών δεδομένων**

- Σωστή τήρηση του ΓΚΠΔ, ειδικά των άρθρων 33 και 55 για την σωστή αντιμετώπιση της επίθεσης
- Λεπτομερής περιγραφή της επίθεσης και των επιπτώσεων της
- Επικοινωνία μεταξύ εποπτικής αρχής και υπευθύνου προστασίας δεδομένων
- Αναφορά μέτρων που λήφθηκαν ή πρόκειται να ληφθούν για την αντιμετώπιση και την μείωση των συνεπειών της επίθεσης

# Hacktivism

**2013 Singapore Cyberattacks**

Σειρά επιθέσεων από μέλος των Anonymous ως απάντηση στη λογοκρισία στο περιεχόμενο ιστοσελίδων

- Παραποίηση της όψης των ιστοσελίδων του PAP Community Foundation, του ειδησεογραφικού πρακτορείου Straits Times και του αεροδρομίου Seletar
- Βανδαλισμός ιστοσελίδας πρωθυπουργού

# Νομική Αντιμετώπιση Hacktivism

- Ίδιοι τρόποι που αναφέρθηκαν για το DDoS, στην περίπτωση όπου γίνεται τέτοιου είδους επίθεση ως hacktivism
- Ίδια νομοθεσία περί λογοκρισίας σε περιπτώσεις mirroring για την αποφυγή της λογοκρισίας της αρχικής ιστοσελίδας
- Σε περιπτώσεις doxxing δεν υπάρχει επαρκής νομοθεσία παρά μόνο σχετικά με τη δημόσια εξύβριση ή το stalking και είναι δύσκολο να γίνει συσχέτιση αυτών με το doxxing καθώς για να ισχύσουν χρειάζεται η πιθανή πρόκλησης κακού στο άτομο που υπόκειται σε αυτό

# Συμπέρασμα

- Υπάρχει ένας διαρκής κυβερνοπόλεμος μεταξύ κρατών του οποίου οι επθέσεις έχουν στόχο την υποκλοπή δεδομένων ή την διακοπή κρίσιμων λειτουργιών

- Είναι αναγκαίο να αναπτυχθεί ένα διεθνώς αποδεκτό νομικό πλαίσιο για την αντιμετώπιση των κυβερνοεπιθέσεων και να οριστούν σαφώς οι νομικές επιπτώσεις τους