1 – Βασικές Έννοιες Κυβερνοασφάλειας

Εθνική Σχολή Δημόσιας Διοίκησης & Αυτοδιοίκησης
Απρίλιος 2021

Ενότητες

- Εισαγωγή στην κυβερνοασφάλεια
- Αρχές κυβερνοασφάλειας
- Απαιτήσεις ασφάλειας
- Ορισμοί
- Είδη επιθέσεων
- Ιομορφικό λογισμικό

Κυβερνοχώρος

Τι είναι Αυτό;

BATTLESPACE

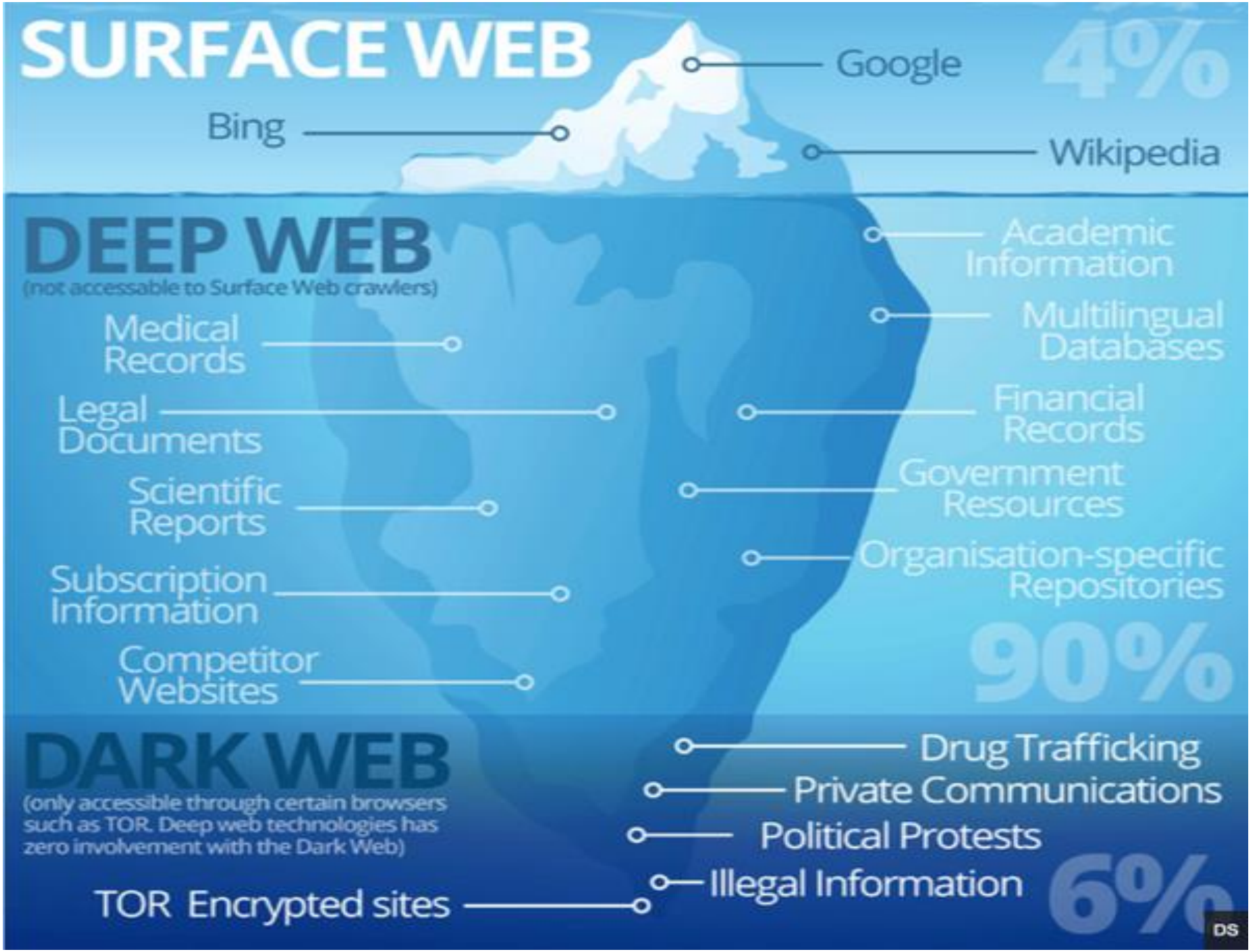
Cyber Space
- C4I

Μεγαλύτερη Πρόκληση = **ΚΑΤΑΝΟΗΣΗ** κυβερνοχώρου

ΚΥΒΕΡΝΟΧΩΡΟΣ

- Internet
- Μεμονωμένα Δίκτυα
- Μεμονωμένοι Η/Υ
- Συσκευές με ενσωματωμένο Η/Υ (tablets, smart phones, routers, etc)
- Περιφερειακές Συσκευές (modems, printers, monitors, etc)
- Μέσα αποθήκευσης (HD, USB Flash Drives, CD/DVD, etc)
- Ψηφιακά Δεδομένα
- Μέσα Κοινωνικής Δικτύωσης (Facebook, tweeter, Instagram, Linked-in κλπ)
- **IoT** Internet of Things = Λοιπές Διασυνδεδεμένες Συσκευές

Κυβερνοχώρος: **Επηρεάζεται από εξελίξεις Τεχνολογίας**
Διαρκώς επεκτείνεται


SURFACE WEB
Google
Bing
Wikipedia
4%
DEEP WEB
(not accessable to Surface Web crawlers)
Medical Records
Legal Documents
Scientific Reports
Subscription Information
Competitor Websites
Academic Information
Multilingual Databases
Financial Records
Government Resources
Organisation-specific Repositories
90%
DARK WEB
(only accessible through certain browsers such as TOR. Deep web technologies has zero involvement with the Dark Web)
TOR Encrypted sites
Drug Trafficking
Private Communications
Political Protests
Illegal Information
6%
DS

Surface Web - Deep Web - Dark Web

Surface Web [Διαδίκτυο (Internet)] 4%

Οτιδήποτε μπορεί να καταγραφεί από τυπική μηχανή αναζήτησης (Google, Bing, Yahoo)

Deep Web 90%

Οτιδήποτε ΔΕΝ μπορεί να βρεθεί από τις μηχανές αναζήτησης. Γιατί:

- Απαιτείται αλληλεπίδραση (interaction) με χρήστη (πχ. Taxisnet, e-banking)

- Δεν υπάρχει σύνδεσμος από ιστοσελίδα που ανήκει στο Surface Web

- Ιδιωτική ιστοσελίδα (είσοδος με “κωδικό”)

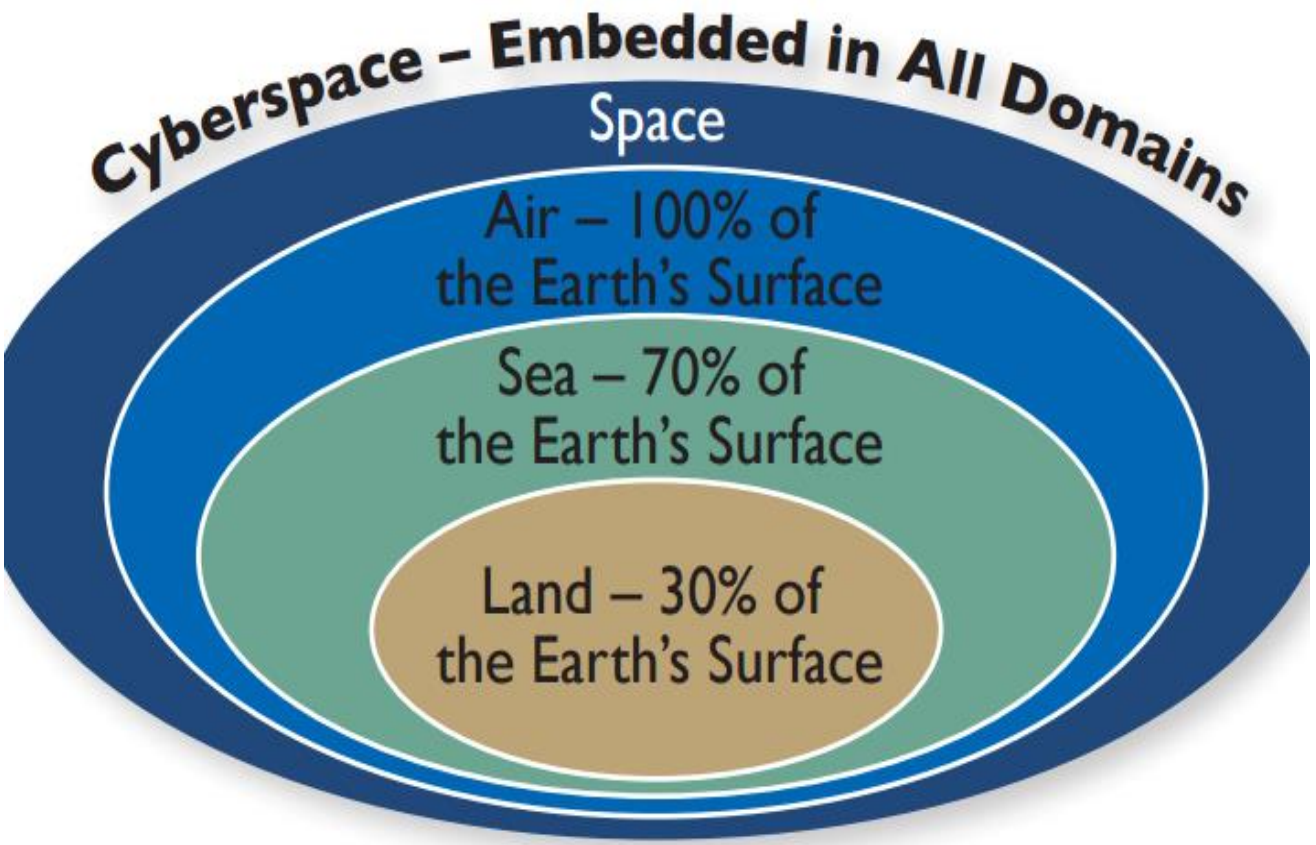
- Περιορισμός πρόσβασης σε μηχανές αναζήτητησης με τεχνικό τρόπο (robots.txt)

Dark Web 6%

Μικρό τμήμα του “Deep Web”, μη προσβάσιμο με συμβατικά προγράμματα περιήγησης (browsers). Κρυπτογραφημένη σύνδεση με ειδικά προγράμματα (**Tor**)

Παρέχει ΑΝΩΝΥΜΙΑ (Δεν εντοπίζεται η πραγματική θέση μίας ιστοσελίδας ή του επισκέπτη, εφόσον τηρούνται οι κανόνες ασφαλείας)

ΚΥΒΕΡΝΟΧΩΡΟΣ



ΚΥΒΕΡΝΟΧΩΡΟΣ:

- **ΝΕΑ (5η) Διάσταση Πεδίου Επιχ/σεων**
- **Ευρύτερη κάλυψη → Συμπεριλαμβάνεται στις άλλες**
- **Συνεχώς Εξελίσσεται / Επεκτείνεται**

Κυβερνοασφάλεια

- Ο όρος **κυβερνοασφάλεια**, περιλαμβάνει τις δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων

Αρχή της αναλογικότητας

- **Αρχή της αναλογικότητας (proportionality principle)**

- Τα **μέτρα προστασίας** πρέπει να είναι αντίστοιχα:
  - των κινδύνων που απειλούν ένα ψηφιακό σύστημα
  - της πιθανότητας υλοποίησης των απειλών
  - της σοβαρότητας των αντίστοιχων συνεπειών

  - Πχ Mail-Bank Account password for transactions

Πως επιτυγχάνεται η απόλυτη ασφάλεια;

Η απόλυτη ασφάλεια δεν είναι εφικτή

- **Η επίτευξη απόλυτης ασφάλειας δεν είναι εφικτός στόχος, σε πραγματικές συνθήκες**

- Ποιο είναι το επίπεδο ή το ποσοστό ασφάλειας (ή το ποσοστό επικινδυνότητας) που είμαστε διατεθειμένοι να αποδεχθούμε, εφαρμόζοντας την αρχή της αναλογικότητας;

Η αρχή του ελάχιστου προνομίου

- **Αρχή του ελάχιστου προνομίου**

- Κάθε χρήστης πρέπει να έχει τα **ελάχιστα δικαιώματα πρόσβασης** στα δεδομένα και στους πόρους πληροφορικής που απαιτούνται για την εκπλήρωση των καθηκόντων του, δηλαδή τις ενέργειες για τις οποίες είναι **εξουσιοδοτημένος**
- Προστασία από εσωτερικές αλλά και εξωτερικές **επιθέσεις μη εξουσιοδοτημένης πρόσβασης**

Η αρχή της ασφάλειας από τον σχεδιασμό

- **Αρχή της ασφάλειας από τον σχεδιασμό (security by design)**

- Ένα ψηφιακό σύστημα θα πρέπει να υλοποιείται έχοντας ενσωματώσει στις προδιαγραφές σχεδίασης όλες τις απαιτήσεις ασφάλειας που είναι αναγκαίες για την εύρυθμη λειτουργία του

Η αρχή της ασφάλειας εξ ορισμού

- **Αρχή της ασφάλειας εξ ορισμού (security by default)**

- Όλες οι ρυθμίσεις προστασίας θα πρέπει να είναι εξ ορισμού ενεργοποιημένες και μόνο εφόσον απαιτείται θα πρέπει να απενεργοποιούνται

Ο κανόνας του ασθενέστερου κρίκου

- **Κανόνας του ασθενέστερου κρίκου**

- Το επίπεδο της ασφάλειας ενός ψηφιακού συστήματος εξαρτάται από την ασφάλεια του **ασθενέστερου σημείου**
- Η αποτελεσματική θωράκιση ενός ψηφιακού συστήματος απαιτεί **ολιστική προσέγγιση** και χάραξη **ενιαίας πολιτικής** ασφάλειας σε επίπεδο οργανισμού

Μείωση της επιφάνειας επίθεσης

- **Ελαχιστοποίηση της επιφάνειας επίθεσης**

- Μείωση της **επιφάνειας επίθεσης**, η οποία αποτελείται από το εύρος των λειτουργικών πόρων που είναι προσπελάσιμοι από έναν επιτιθέμενο

Η αρχή του Kerckhoffs

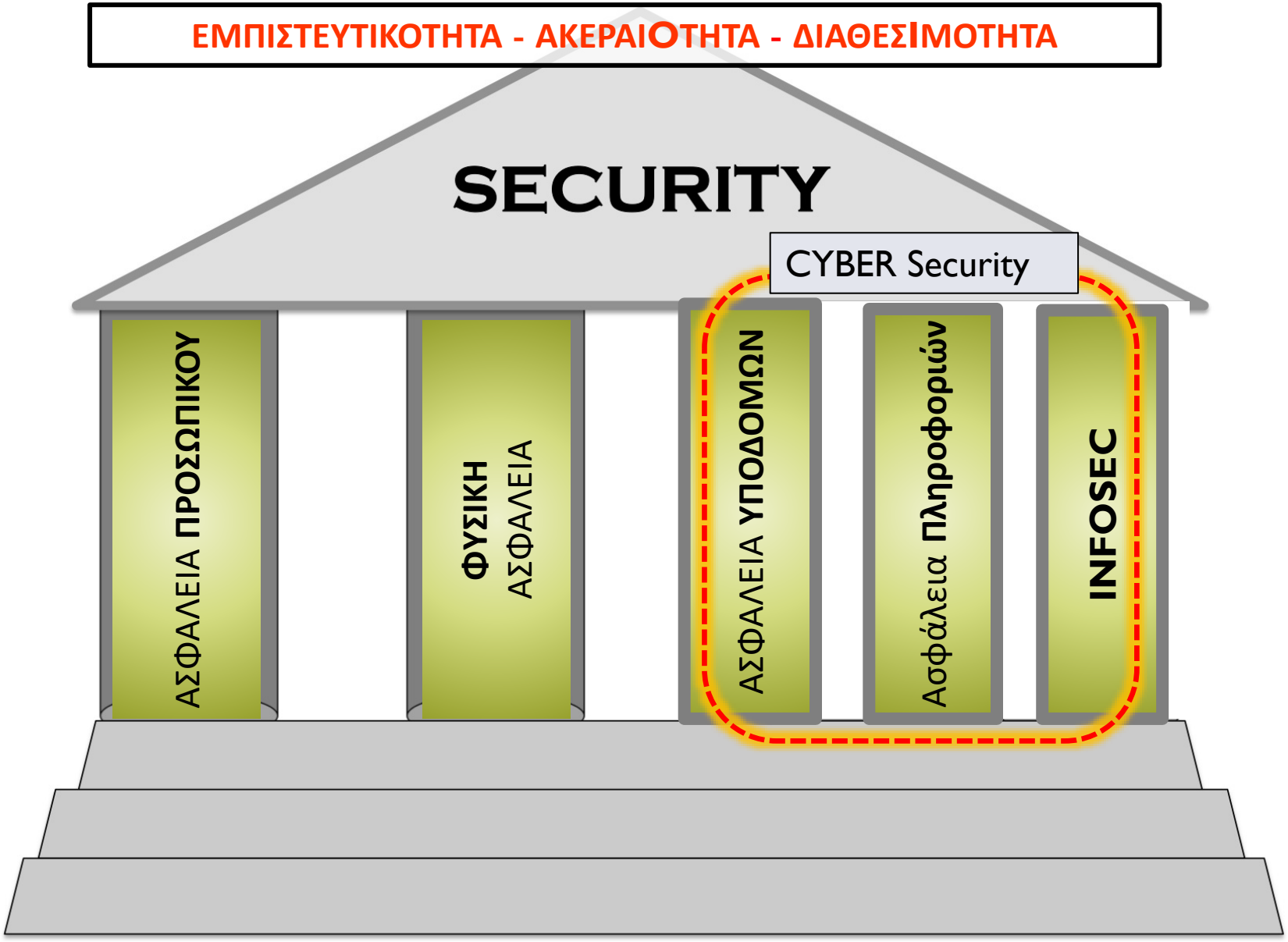
Στην κρυπτογραφία τι προστατεύουμε;

- Τον κρυπτογραφικό αλγόριθμο
- Το κρυπτογραφικό κλειδί
- Όλα τα παραπάνω
- Κανένα από τα παραπάνω

Η αρχή του Kerckhoffs

- Η **ασφάλεια** ενός **κρυπτοσυστήματος** δεν εξαρτάται από τη μυστικότητα του αλγορίθμου κρυπτογράφησης αλλά μόνο από τη διατήρηση της μυστικότητας του κλειδιού κρυπτογράφησης

CYBER - SECURITY



Απαιτήσεις Ασφάλειας

Ορισμοί

- **Εμπιστευτικότητα (Confidentiality)**. Η διασφάλιση ότι μία πληροφορία ή ένας υπολογιστικός πόρος δεν γίνονται διαθέσιμα και δεν αποκαλύπτονται χωρίς την έγκριση του ιδιοκτήτη τους
- **Ακεραιότητα (Integrity)**. Η διασφάλιση της ακρίβειας και της πληρότητας των πληροφοριών, καθώς και η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας
- **Διαθεσιμότητα (Availability)**. Η διασφάλιση ότι μία πληροφορία ή ένας υπολογιστικός πόρος βρίσκεται πάντοτε στη διάθεση ενός εξουσιοδοτημένου ατόμου όταν τη ζητήσει

Ορισμοί

- **Αυθεντικοποίηση (authentication)**. Είναι η διαδικασία πιστοποίησης και επιβεβαίωσης της ταυτότητας των χρηστών, η οποία σε κάθε περίπτωση βασίζεται στα διαπιστευτήρια που κατέχει ο χρήστης
- Οι χρήστες μπορεί να είναι φυσικά πρόσωπα, υπηρεσίες, διαδικασίες ή υπολογιστές

Ορισμοί

- **Εξουσιοδότηση (Authorization)**. Είναι η διαδικασία που διέπει τα μέσα και τις λειτουργίες ελέγχου πρόσβασης σε πόρους από αυθεντικοποιημένους χρήστες
- Οι **πόροι** περιλαμβάνουν αρχεία, βάσεις δεδομένων, πίνακες κ.ά., σε συνδυασμό με πόρους σε επίπεδο συστήματος, όπως κλειδιά μητρώου (registry keys) και δεδομένα ρυθμίσεων (configuration data)

Ορισμοί

- **Μη-άρνηση της ευθύνης (Non-Repudiation)**. Είναι η αδυναμία αποποίησης (άρνησης) της ευθύνης για την εκτέλεση μίας πράξης (ενέργειας), όπως για παράδειγμα την εκτέλεση μίας ηλεκτρονικής συναλλαγής
- **Ανθεκτικότητα (Resilience)**. Αναφέρεται στην ικανότητα ενός συστήματος να παράγει συνεχώς το επιδιωκόμενο αποτέλεσμα παρά τα όποια αντίξοα περιστατικά

Ορισμοί

- Με τον όρο **συνθηματικά (credentials)** προσδιορίζουμε το όνομα χρήστη (user name) και τον κωδικό πρόσβασης (password) που δίνουμε για να αποκτήσουμε δικαίωμα πρόσβασης (εξουσιοδότηση) σε ένα ψηφιακό σύστημα

Ορισμοί

- **Ταυτοποίηση** σημαίνει η διαδικασία αναζήτησης της ύπαρξης του συγκεκριμένου χρήστη στη βάση του συστήματος
- Ουσιαστικά, δηλώνεται στο σύστημα το όνομα χρήστη (user name)

Ορισμοί

- **Αυθεντικοποίηση** είναι η διαδικασία ελέγχου της ταυτότητας του χρήστη
- Ζητείται δηλαδή από το χρήστη να αποδείξει ότι είναι ο πραγματικός κάτοχος της ταυτότητας
- Εισάγοντας τον κωδικό (password) αποδεικνύουμε στο σύστημα ότι είμαστε ο νόμιμος χρήστης με το συγκεκριμένο όνομα (user name)

Ορισμοί

- **Εξουσιοδότηση** είναι η απονομή στο χρήστη συγκεκριμένων δικαιωμάτων πρόσβασης στο σύστημα
- Το σύστημα αφού ελέγξει τα συνθηματικά μας επιτρέπει (εξουσιοδότηση) την πρόσβαση σε συγκεκριμένους πόρους, σύμφωνα με τα δικαιώματα που έχουν δοθεί στον χρήστη
- Η διαδικασία με την οποία αποκτούμε πρόσβαση σε ένα ψηφιακό σύστημα είναι πρώτα η ταυτοποίηση, ακολουθεί η αυθεντικοποίηση και τέλος η εξουσιοδότηση

Διαδικασία πρόσβασης σε ψηφιακό σύστημα

Μελέτη Περίπτωσης 1

Ποιες είναι οι **απαιτήσεις ασφάλειας** μιας τραπεζικής συναλλαγής με τη χρήση εφαρμογής ηλεκτρονικής τραπεζικής;

Μελέτη Περίπτωσης 1

Εισάγουμε το όνομα χρήστη (**ταυτοποίηση**) και τον κωδικό πρόσβασης (**αυθεντικοποίηση**) και αποκτούμε πρόσβαση στα στοιχεία του τραπεζικού μας λογαριασμού (**εξουσιοδότηση**). Επιλέγουμε να μεταφέρουμε το ποσό των 10€ από τον λογαριασμό μας σε αυτόν του παραλήπτη, επιβεβαιώνοντας τα στοιχεία της συναλλαγής. Για την εκτέλεση της χρηματικής μεταφοράς μας ζητείται να εισάγουμε στο σύστημα έναν επιπλέον κωδικό μιας χρήσης (one time password – otp), τον οποίο λαμβάνουμε στο κινητό μας μέσω sms από την τράπεζα. Πρόκειται για μία αυθεντικοποίηση δύο επιπέδων (two factor authentication), χρησιμοποιώντας κάτι που ξέρω (password) και κάτι που έχω (otp μέσω sms που λαμβάνω στο κινητό μου).

Εφόσον η παραπάνω διαδικασία ολοκληρωθεί με επιτυχία, η συναλλαγή εκτελείται με τη μεταφορά ακριβώς του ποσού που ζητήθηκε από το χρήστη (**ακεραιότητα**). Σε περίπτωση που αμφισβητήσουμε τη εν λόγω συναλλαγή, ισχυριζόμενοι ότι ποτέ δεν δώσαμε συγκατάθεσή για τη μεταφορά χρημάτων από το λογαριασμό μας, η τράπεζα θα παρουσιάσει το αρχείο καταγραφής του συστήματος (log file), αποδεικνύοντας την ολοκλήρωση της συναλλαγής, από τον συγκεκριμένο χρήστη, τη δεδομένη χρονική στιγμή, με τη χρήση των κωδικών μας, καταρρίπτοντας έτσι τον ισχυρισμό μας (**μη αποποίηση ευθύνης**).

Επιπλέον, κατά τη διάρκεια της συναλλαγής μας θα θέλαμε η υπηρεσία ηλεκτρονικής τραπεζικής να βρίσκεται συνεχώς σε λειτουργία (**διαθεσιμότητα**) και το ψηφιακό σύστημα της τράπεζάς μας να παραμένει αξιόπιστο και λειτουργικό σε ενδεχόμενες κυβερνοεπιθέσεις (**ανθεκτικότητα**).

Μελέτη Περίπτωσης 2

Ποιες είναι οι **απαιτήσεις ασφάλειας** μιας υποθετικής ηλεκτρονικής υπηρεσίας, η οποία θα παρέχεται από την ΕΣΔΔΑ για την υποστήριξη της διαδικασίας υποβολής των εργασιών των σπουδαστών, προς αξιολόγηση από τους εκπαιδευτές, στο πλαίσιο των μαθημάτων;

Μελέτη Περίπτωσης 2

Οι απαιτήσεις ασφάλειας της υπηρεσίας είναι:

- η **αυθεντικοποίηση** του συντάκτη
- η **ακεραιότητα** του κειμένου
- η **μη αποποίηση της ευθύνης**
- η **εμπιστευτικότητα** της επικοινωνίας

Είδη Επιθέσεων

- **Παθητικές** & **Ενεργητικές** επιθέσεις
- Η **παθητική επίθεση** στοχεύει στη συλλογή και χρήση πληροφοριών του συστήματος χωρίς να γίνει αντιληπτό και χωρίς να επηρεαστεί η ομαλή λειτουργία του
- Η **ενεργητική επίθεση** έχει στόχο να παρέμβει και να τροποποιήσει τον τρόπο λειτουργίας του συστήματος

Είδη Επιθέσεων

- Τα δύο κύρια είδη **παθητικής επίθεσης** είναι η **υποκλοπή μηνύματος** και η **παρακολούθηση της κίνησης** δεδομένων
- **Υποκλοπή μηνύματος** έχουμε για παράδειγμα στην περίπτωση καταγραφής μιας τηλεφωνικής κλήσης, ενός μηνύματος ηλεκτρονικού ταχυδρομείου ή ενός μεταφερόμενου αρχείου
- Ένα άλλο παράδειγμα είναι οι **επιθέσεις κρυπτανάλυσης** με τις οποίες γίνεται προσπάθεια να αποκρυπτογραφηθεί ένα κρυπτογραφημένο μήνυμα, χωρίς να είναι γνωστό το κλειδί αποκρυπτογράφησης

Είδη Επιθέσεων

- Η **ανάλυση κίνησης** εφαρμόζεται στην περίπτωση ανταλλαγής κρυπτογραφημένων δεδομένων, όπου ο επιτιθέμενος προσπαθεί να ανιχνεύσει πρότυπα στη μορφή και τη συχνότητα των μηνυμάτων, ώστε να εξάγει με έμμεσο τρόπο πληροφορίες σχετικά με τη φύση της επικοινωνίας
- Οι **παθητικές επιθέσεις** ανιχνεύονται πολύ δύσκολα επειδή δεν προκαλούν τροποποίηση των δεδομένων
- Αντιμετωπίζονται με αποτρεπτικά μέτρα ασφάλειας όπως για παράδειγμα η **κρυπτογράφηση** και η **ανωνυμοποίηση** δεδομένων

Είδη Επιθέσεων

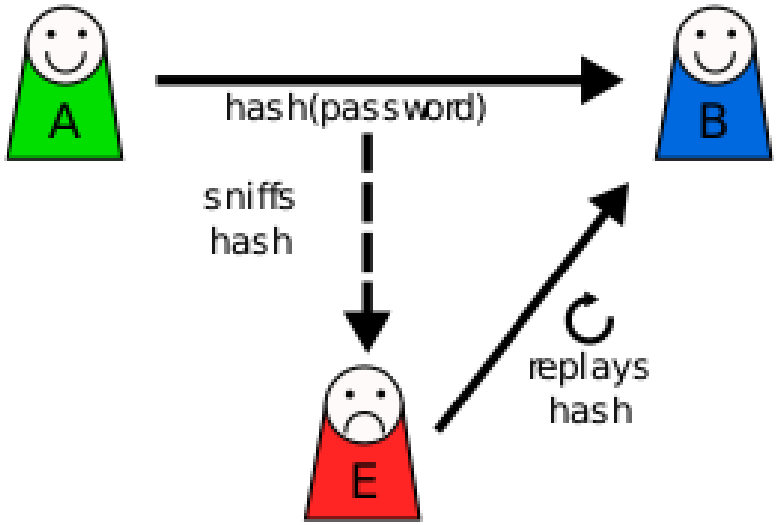
- Οι **ενεργητικές επιθέσεις** περιλαμβάνουν:
  - τη **μεταμφίεση**
  - την **επανεκπομπή**
  - την **τροποποίηση**
  - την **άρνηση υπηρεσίας**
  - την **εξαντλητική αναζήτηση κωδικού**

Είδη Επιθέσεων

- Η **μεταμφίεση** μπορεί να αφορά την αλλαγή της IP διεύθυνσης (IP Spoofing) των πακέτων που στέλνει ο επιτιθέμενος ή την αλλαγή της φυσικής (MAC) διεύθυνσης (MAC Address Spoofing) της κάρτας δικτύου του επιτιθέμενου
- Η πρώτη περίπτωση εφαρμόζεται κυρίως σε επιθέσεις τύπου **Άρνησης Υπηρεσίας**, προσφέροντας το επιπλέον πλεονέκτημα ότι αποκρύπτεται η πραγματική διεύθυνση του επιτιθέμενου
- Στη δεύτερη περίπτωση ο επιτιθέμενος συνήθως ενδιαφέρεται να λάβει την απάντηση του θύματος, οπότε η τεχνική αυτή χρησιμοποιείται κυρίως για επιθέσεις τύπου **Man-In-The-Middle**

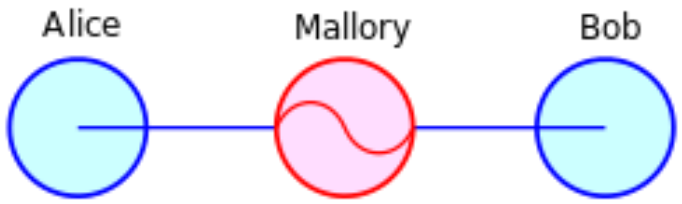
Είδη Επιθέσεων

- Η **επανεκπομπή (replay attack)** συνίσταται αρχικά στην παθητική υποκλοπή ενός μηνύματος και μετέπειτα στην επαναμετάδοσή του ώστε να επιτύχει μία μη εξουσιοδοτημένη ενέργεια



Είδη Επιθέσεων

- Η **τροποποίηση μηνυμάτων ή επίθεση διαμεσολαβητή (Man in the Middle attack)** εκδηλώνεται όταν ο επιτιθέμενος παρεμβάλλεται στην επικοινωνία μεταξύ δύο κόμβων, υποκλέπτοντας και αλλοιώνοντας τις πληροφορίες που ανταλλάσσονται



Είδη Επιθέσεων

- Η **εξαντλητική αναζήτηση κωδικού (Brute-force attack)** εφαρμόζεται στην περίπτωση που ο επιτιθέμενος χρειάζεται να δοκιμάσει όλους τους διαφορετικούς συνδυασμούς πιθανών κωδικών μέχρι να ανακαλύψει τον σωστό
- Οι επιθέσεις αυτές βασίζονται σε αυτόματο λογισμικό με χρήση εμπλουτισμένου λεξικού
- Οι κωδικοί πρόσβασης που επιλέγουμε θα πρέπει να είναι δύσκολο για κάποιον να τους μαντέψει

Είδη Επιθέσεων

- Η **Άρνηση Υπηρεσίας (DoS)** και η **Κατανεμημένη Άρνηση Υπηρεσίας (DDoS)** αποσκοπούν στο να θέσουν εκτός λειτουργίας το σύστημα στόχο της επίθεσης, ώστε να μην είναι σε θέση να παρέχει υπηρεσίες στους εξουσιοδοτημένους χρήστες του, αποστέλλοντας έναν μεγάλο αριθμό αιτημάτων εξυπηρέτησης προκαλώντας την υπερφόρτωση και την κατάρρευσή του
- Αν η επίθεση πραγματοποιείται συντονισμένα από πολλές διαφορετικές τοποθεσίες ταυτόχρονα, τότε πρόκειται για μια **Κατανεμημένη Άρνηση Εξυπηρέτησης (Distributed Denial of Service)**

Είδη Επιθέσεων

- Οι επιθέσεις **Κοινωνικής Μηχανικής (Social Engineering)** στοχεύουν στον ανθρώπινο παράγοντα, δηλαδή στους ίδιους τους χρήστες των ψηφιακών συστημάτων
- Ο επιτιθέμενος προσπαθεί να εκμεταλλευτεί τις αδυναμίες του ανθρώπινου χαρακτήρα χρησιμοποιώντας μεθόδους εκβιασμού, χειραγώγησης ή παραπλάνησης για την επίτευξη του στόχου

Είδη Επιθέσεων

- Οι επιθέσεις **Ηλεκτρονικής Εξαπάτησης (Phishing)** βασίζονται στην αποστολή ενός παραπλανητικού μηνύματος ηλεκτρονικού ταχυδρομείου ή μιας παραπλανητικής διαδικτυακής τοποθεσίας με στόχο να ωθήσει τους παραλήπτες θύματα να αποκαλύψουν προσωπικά δεδομένα ή οικονομικά στοιχεία
- Οι πληροφορίες αυτές χρησιμοποιούνται συνήθως για υποκλοπή ταυτότητας

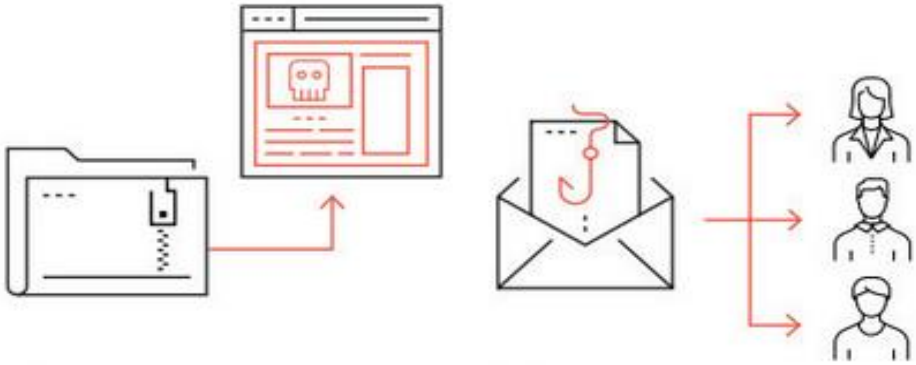
Χαρακτηριστική Περίπτωση Επίθεσης

- Τοποθέτηση ενός μολυσμένου CD ή USB σε κάποιο πολυσύχναστο σημείο του οργανισμού στόχου
- Η περιέργεια όποιου εργαζομένου τύχει να το βρει θα τον ωθήσει να το συνδέσει στον υπολογιστή του για να δει το περιεχόμενό του
- Το αποτέλεσμα είναι να μολυνθεί με ιομορφικό λογισμικό προσφέροντας στον κακόβουλο πρόσβαση στα ψηφιακά συστήματα του οργανισμού

1. The legitimate website is cloned

2. The login page is changed to point to a credential-stealing script

3. The modified files are bundled into a zip file to make a phishing kit



4. The phishing kit is uploaded to the hacked website, files are unzipped

5. Emails are sent with links pointing to the new spoofed website

Anatomy of a Phishing Kit

What is a phishing kit?

The availability of phishing kits makes it easy for cyber criminals, even those with minimal technical skills, to launch phishing campaigns. A phishing kit bundles phishing website resources and tools that need only be installed on a server. Once installed, all the attacker needs to do is send out emails to potential victims. Phishing kits as well as mailing lists are available on the dark web. A couple of sites, Phishtank and OpenPhish, keep crowd-sourced lists of known phishing kits.

Ιομορφικό Λογισμικό

- **Ιομορφικό** ή **κακόβουλο** είναι το λογισμικό που περιέχει κώδικα εντολών και στοχεύει στην παραβίαση της ασφάλειας (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) ενός ψηφιακού συστήματος

Virus (Ιός)

- Εκτελέσιμο λογισμικό που ενσωματώνει τον κώδικά του σε ένα πρόγραμμα και αναπαράγεται με την αντιγραφή του εαυτού του σε άλλα προγράμματα

Trojan Horse (Δούρειος Ίππος)

- Πρόγραμμα το οποίο περιέχει πρόσθετη μη αναμενόμενη λειτουργικότητα άγνωστη στον χρήστη του ψηφιακού συστήματος
- Σε αντίθεση με τον ιό δεν αναπαράγεται μόνο του

Worm (Αναπαραγωγός)

- Αυτόνομο πρόγραμμα που διαδίδει τον εαυτό του σε άλλους υπολογιστές μέσω δικτύου δημιουργώντας αντίγραφα

Backdoors (Κερκόπορτες)

- Μετατροπή ενός προγράμματος με τη δημιουργία σημείων εισόδου ώστε να επιτυγχάνεται μη εξουσιοδοτημένη πρόσβαση σε ένα ψηφιακό σύστημα

Logic Bomb (Λογική Βόμβα)

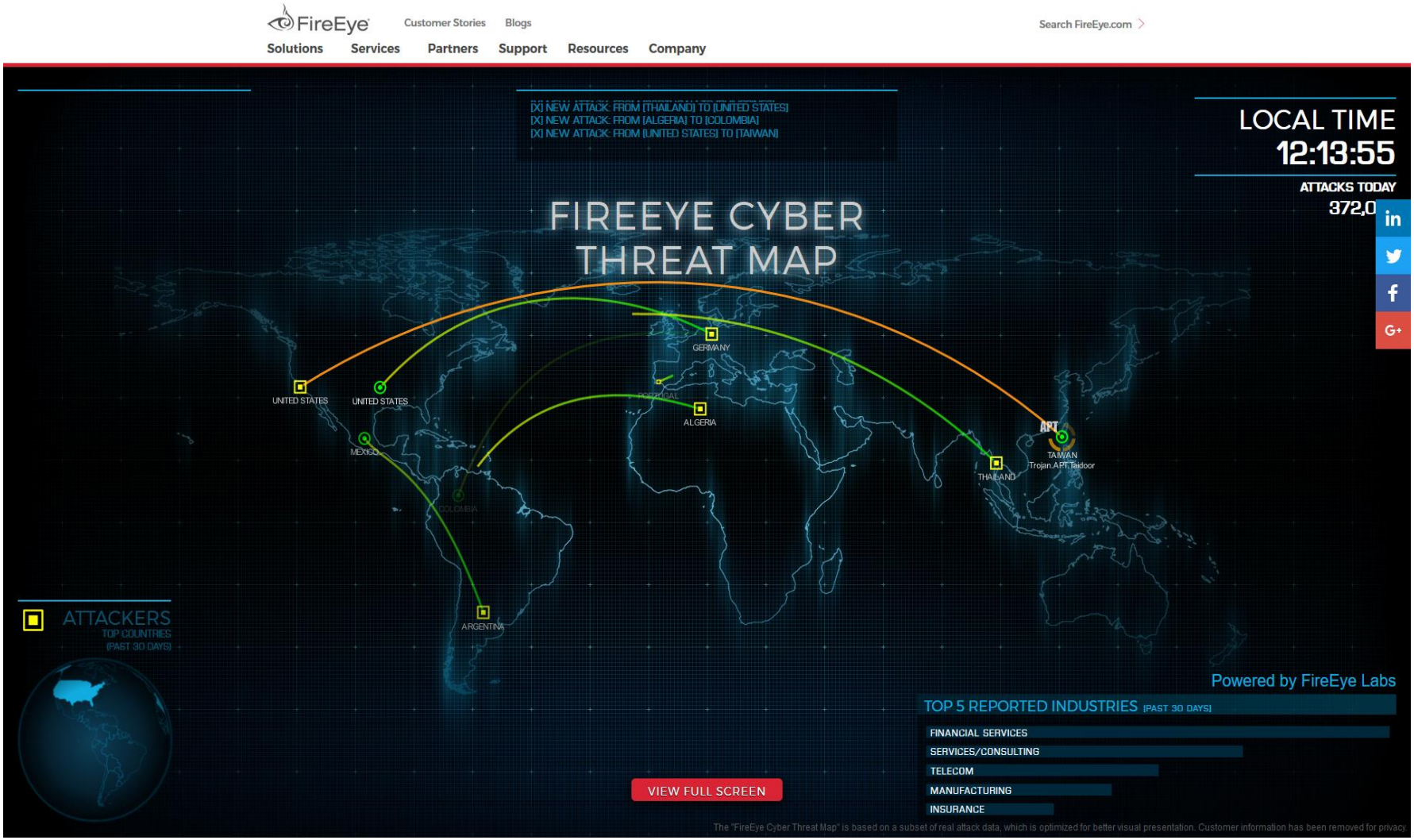
- Πρόγραμμα το οποίο ενεργοποιείται υπό συγκεκριμένες συνθήκες (π.χ. ορισμένη λογική συνθήκη, ημερομηνία, ώρα) παραβιάζοντας την ασφάλεια του ψηφιακού συστήματος

Bacteria (Βακτήρια)

- Προγράμματα τα οποία αναπαράγονται αυτόνομα, χωρίς να προκαλούν επιβλαβείς ενέργειες, με σκοπό την κατανάλωση πόρων του ψηφιακού συστήματος (επεξεργαστική ισχύ, μνήμη, χώρο στο σκληρό δίσκο)
- Κατά συνέπεια, μειώνεται η διαθεσιμότητα του συστήματος οδηγώντας το σε κατάρρευση

Case Studies

- Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών
  - http://www.adae.gr/cybersecurity/enimerosi-christon-kai-syndromiton/piges-pliroforisis-gia-tin-asfaleia-stis-ilektronikes-epikoinonies/koyiz-gnoseon/
  - http://www.adae.gr/quiz/
- Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
  - https://www.dpa.gr/



ΚΥΝΕΡΝΟΕΠΙΘΕΣΕΙΣ ΣΕ ΠΡΑΓΜΑΤΙΚΟ ΧΡΟΝΟ

https://www.fireeye.com/cyber-map/threat-map.html

https://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=18166&view=map

Ευχαριστώ για την προσοχή σας

Ερωτήσεις