Info Quest TECHNOLOGIES

Security in a Cloud World? Challenge Accepted!

Quest GROUP 35 YEARS

Αντώνης Σταματόπουλος
Commercial Director

Agenda

- **Cloud: Ένα νέο τοπίο**
  - Το Οικοσύστημα
  - Τα Workflows
  - Οι απειλές
  - Η άμυνα
  - Social Engineering

Κυβερνοεπιθέσεις θα συμβαίνουν.
Αδυναμίες στα συστήματα θα αποκαλύπτονται διαρκώς.
Ο σωστός σχεδιασμός Συστημάτων, Διαδικασιών και Εκπαίδευσης θα διασφαλίσει την ελαχιστοποίηση της έκθεσης σε κίνδυνο, αλλά και των απωλειών.

Το Οικοσύστημα

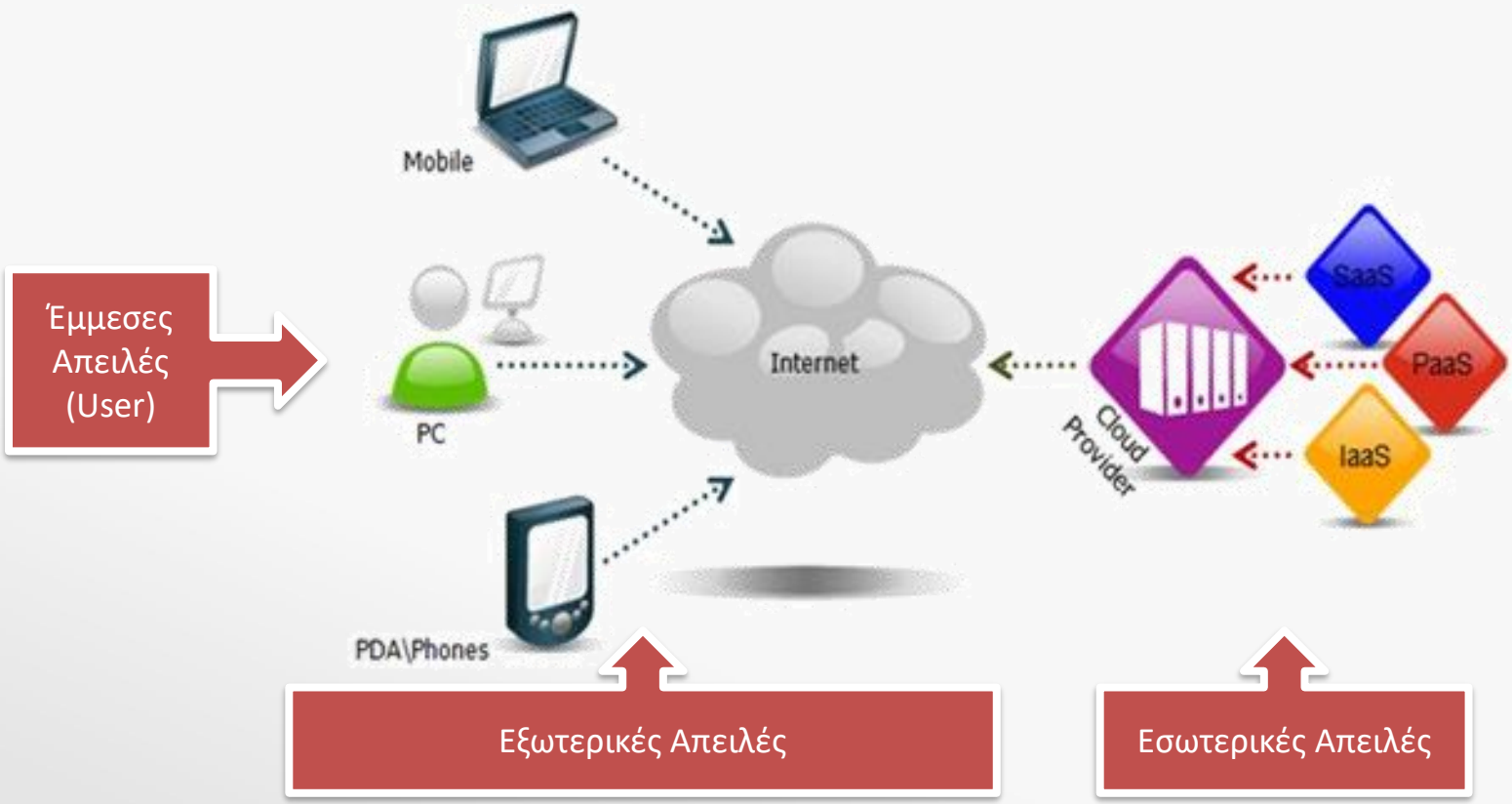
- **Υποδομές:**
  - Private Cloud On-Premise
  - Private Cloud Off-Premise
  - Hybrid Cloud
  - Public Cloud
- **Συνδεσιμότητα (Αρχιτεκτονική)**
  - Local Network
  - Wide Area Network
  - Virtual Private Network
- **Συνδεσιμότητα (Πρωτόκολλο)**
  - Ethernet
  - USB
  - Wi-Fi
  - Bluetooth
  - NFC
  - M2M (z-wave, Zigbee etc)

Τα Νέα Workflows

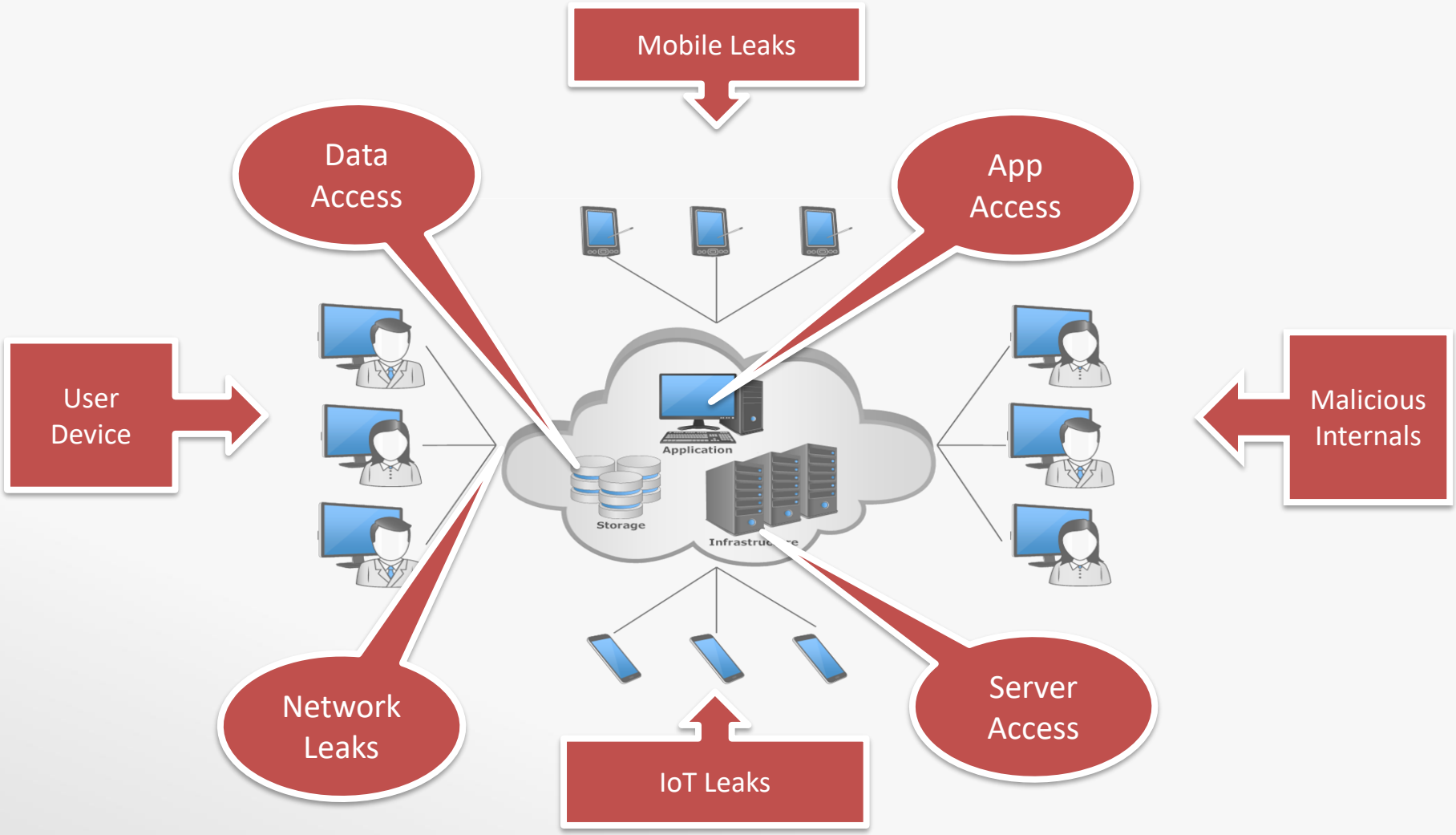
- Cloud Accessibility Process
  - Internal Network
  - Wi-Fi
  - VPN
  - 4-5G Mobile
- Upload-Download Data Transfer
  - Backup
  - Disaster Recovery
  - Collaboration
- IoT / M2M Networks
  - Sensors
  - Beacons
  - Hubs
- Financial Transactions
  - Credit Card Clearance
  - Block Chain-Crypto Currency

Οι νέες απειλές

- **Εσωτερικές:** Malicious Insiders, Internal Leaks
- **Εξωτερικές:** Cyber Attacks, Network Attacks, DoS Attacks
- **Έμμεσες:** Social Engineering (User targeted attack)

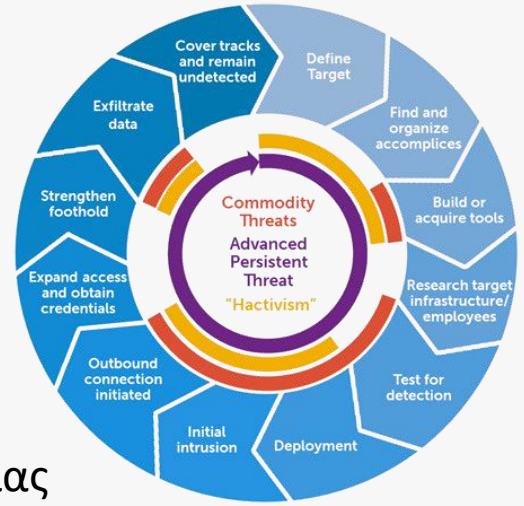


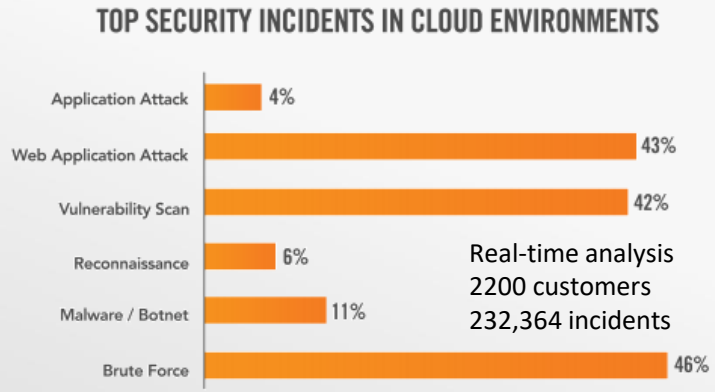
Οι νέες απειλές



Οι νέες απειλές

Data breaches: Διαρροή Δεδομένων
Weak identity, credential and access management: Κενά Ασφαλείας στην Πρόσβαση
Insecure interfaces and APIs: Κενά στα APIs
System and application vulnerability: Ευάλωτες υποδομές
Account hijacking: Υποκλοπή Κωδικών
Malicious insiders: Κακόβουλοι Εσωτερικοί Πόροι
Advanced persistent threats: →
Data loss: Απώλεια Δεδομένων
Insufficient due diligence: Ανεπαρκής Έλεγχος
Abuse/nefarious cloud service use: Κακή χρήση Cloud Services
Denial of service: Τεχνητή Απαγόρευση παροχής Cloud Υπηρεσίας
Shared technology issues: Κενά από σύνθεση Τεχνολογικών Μονάδων



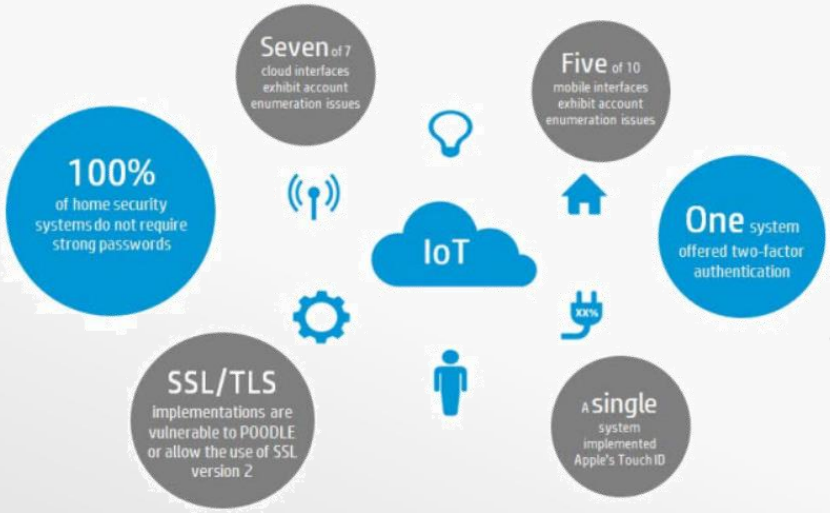


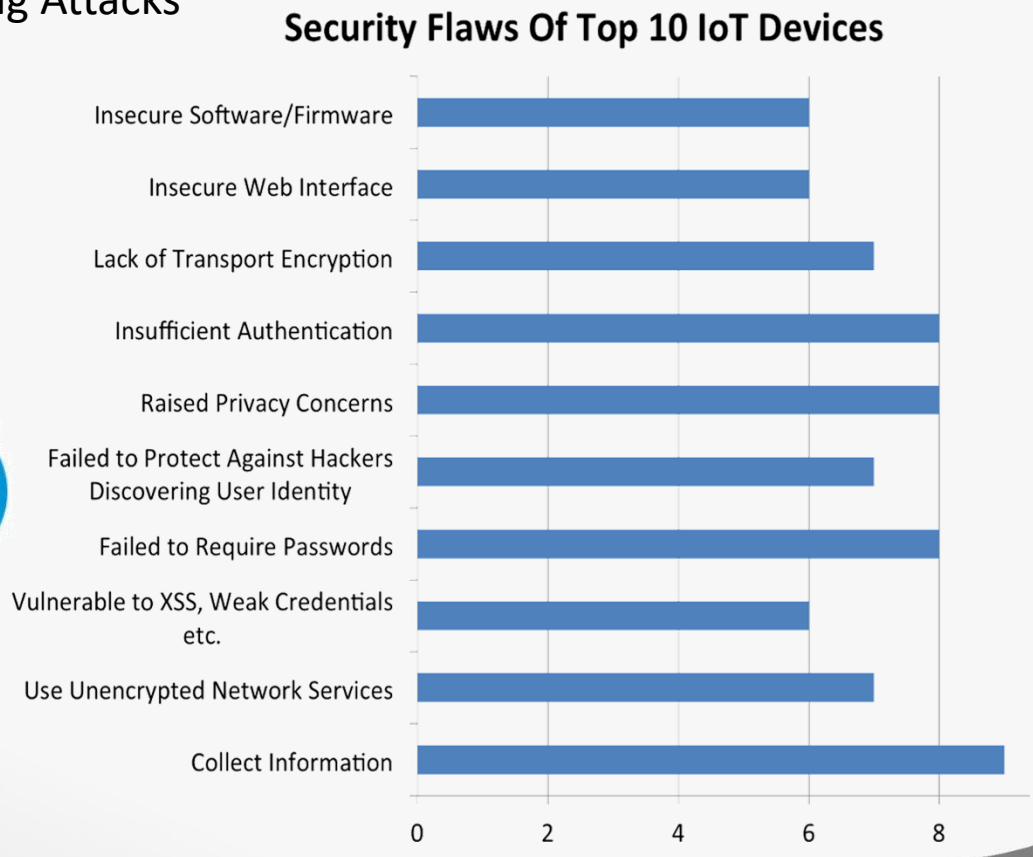
Πηγή: Alert Logic Cloud Security Report 2014

Οι νέες απειλές

IoT & M2M Communication Vulnerabilities

- Smart Home Devices:
  - Προστασία με απλά 8char Passwords
  - Σπάνια χρήση Two Factor Authentication
  - Account Enumeration by Timing Attacks
  - Smart Hubs με USB Ports
  - Wireless Cameras
  - Sensors





Quest GROUP 35 YEARS

Info Quest TECHNOLOGIES

Η άμυνα: IT Manager

Deter: Αποθαρρύνετε πιθανούς εισβολείς

- **SECURE POLICIES AND PROCEDURES:** Εφαρμόστε Πολιτικές Ασφαλείας και τήρησης της Ιδιωτικότητας
- **STANDARDIZATION COMPLIANCE:** Εφαρμόστε και Γνωστοποιήστε την τήρηση Ασφαλών Προτύπων
- **INTERNAL AUDIT:** Εφαρμόστε διαδικασίες εσωτερικών ελέγχων
- **STAY INFORMED: Παραμείνετε ενημερωμένοι για νέες απειλές**

Prevent: Εμποδίστε τη διείσδυση στα συστήματά σας

- **CODE SECURITY:** Ασφαλίστε τον κώδικά σας
- **ACCESS MANAGEMENT POLICY:** Δημιουργήστε Φυσικό και Role έλεγχο πρόσβασης
- **SECURITY TOOLKIT:** Δημιουργήστε Ολοκληρωμένο Πλαίσιο Ασφαλείας
- **STAY INFORMED: Παραμείνετε ενημερωμένοι για νέες απειλές**

Detect: Ανιχνεύστε άμεσα την πιθανή απειλή

- **MONITORING:** Ελέγχετε συνεχώς τη ροή δεδομένων στο σύστημά σας και τις εισόδους σε αυτό
- **LOG MANAGEMENT:** Ελέγξτε την πρόσβαση
- **STAY INFORMED: Παραμείνετε ενημερωμένοι για νέες απειλές**

Correct: Διορθώστε τόσο το πρόβλημα όσο και την πηγή του

- **PATCH MANAGEMENT:** Υιοθετήστε μηχανισμό μαζικής προσθήκης Patches
- **FORENSICS ANALYSIS**: Αναπτύξτε μηχανισμό αναγνώρισης της εισβολής
- **STAY INFORMED: Παραμείνετε ενημερωμένοι για νέες απειλές**

Η άμυνα: Cloud User

Change Your **Password** Like Clockwork

- Η συχνή αλλαγή του Password αποτρέπει την κακόβουλη χρήση του ακόμα και εάν κλαπεί.

Screen Your **Email** With Neurotic Energy

- Το email αποτελεί βασικό παράθυρο για Εισβολή. Ελέγχετε τα εισερχόμενα σχολαστικά.

Passwords With **Real Words** In Them **Are** The **Slightest Secure**

- Μη χρησιμοποιείτε κοινές λέξεις στα Passwords ούτε αλληλουχία χαρακτήρων (12345678).

A few Records Will Enroll **Upper** And **Lower Case**

- Όπου επιτρέπεται συστημικά, αλλοιώστε τη σειρά μεταξύ Κεφαλαίων και Μικρών Χαρακτήρων.

Simply **Utilize** A Mystery Answer **Once**

- Στην Ερώτηση Ασφαλείας, χρησιμοποιείστε Μία Λανθασμένη απάντηση και απομνημονεύστε την.

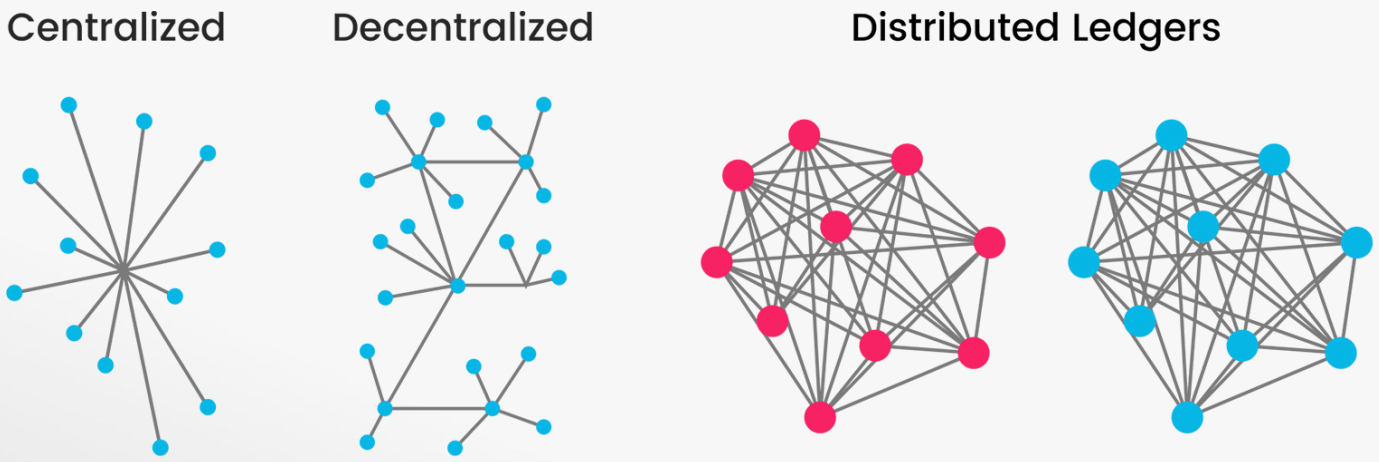
UNDERSTAND YOUR CLOUD SERVICE PROVIDER SECURITY MODEL: Κατανοείστε το Μοντέλο του SP σας

Ασφάλεια μέσω αποκέντρωσης: Το Blockchain

"The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value."
Don & Alex Tapscott, authors Blockchain Revolution (2016)

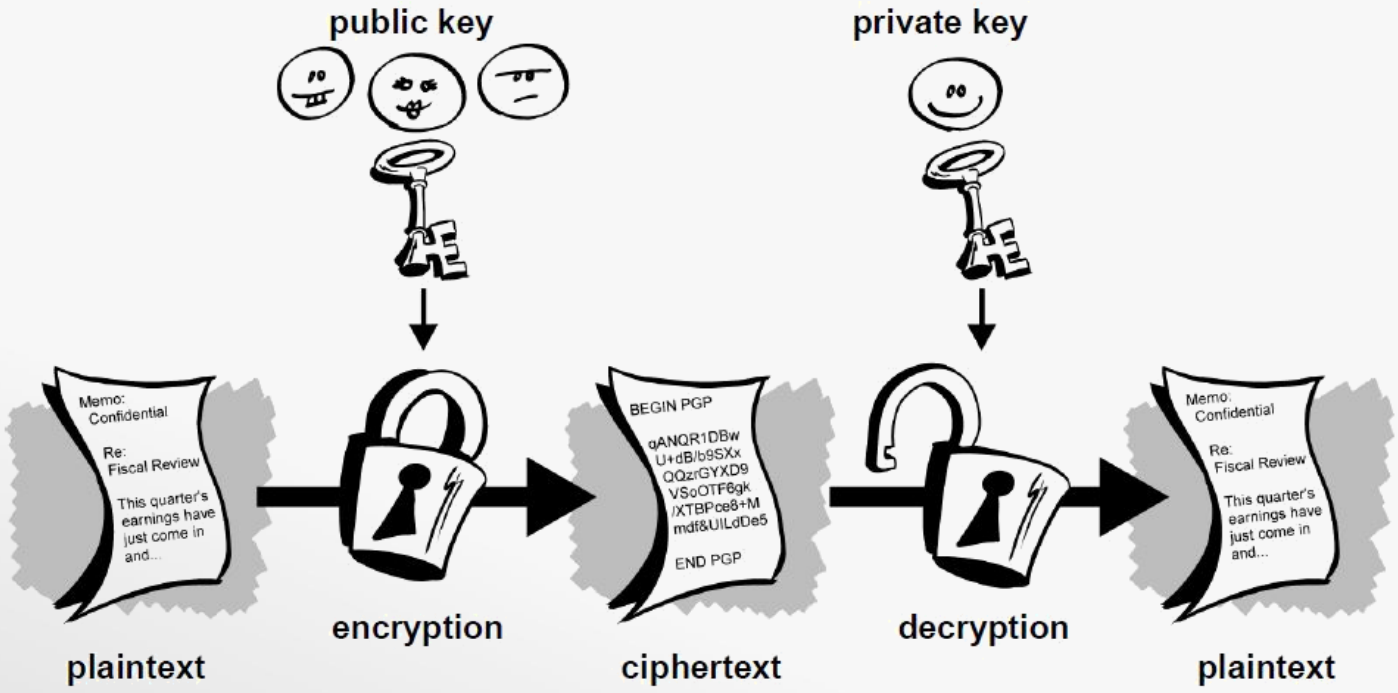
By storing blocks of information that are identical across its network, the blockchain cannot:

- Be controlled by any single entity.
- Has no single point of failure.



Η Αρχή των «Κλειδιών»

- The basis are the so-called public and private “keys”.
- A “public key” (a long, randomly-generated string of numbers) is a users’ address on the blockchain.
- Bitcoins sent across the network gets recorded as belonging to that address.
- The “private key” is like a password that gives its owner access to their Bitcoin or other digital assets.
- Store your data on the blockchain and it is incorruptible.



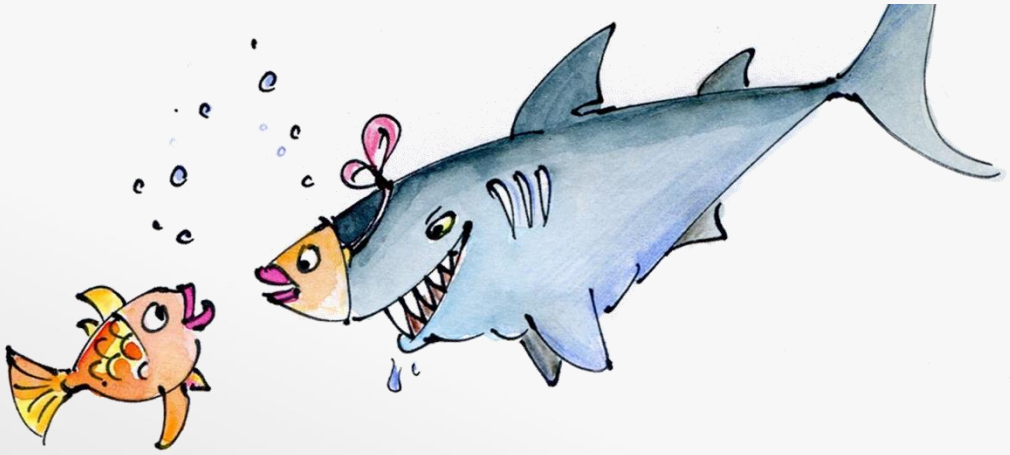
Το Social Engineering: Μία νέα απειλή

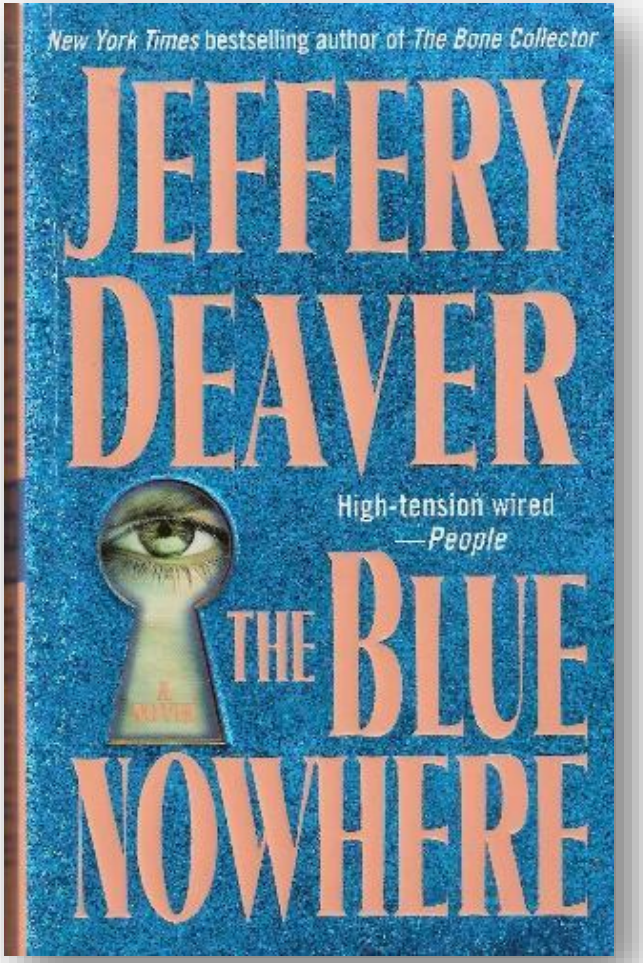
“It takes 20 years to build a reputation and 5 minutes to ruin it”

Warren Buffet

Η Αρχή

- Κάθε σύστημα ασφαλείας έχει **Κενά**
- Ακόμα και αν δεν έχει Τεχνικά Κενά, έχει **Διαχειριστικά**
- Ακόμα και αν έχει πιστοποιηθεί η Διαχειριστική Διαδικασία, ο Υπεύθυνος Παρακολούθησής της έχει **Προσωπική Ζωή**





Παραδείγματα Social Engineering

- Εικονικά Μηνύματα από Τράπεζες
- Προσωπικό μήνυμα εμπιστοσύνης και επενδυτική πρόταση
- Τηλεφωνικές κλήσεις αναζήτησης βοήθειας από «οικείο» πρόσωπο, λόγω ατυχήματος ή αιφνιδίου προβλήματος υγείας
- Μήνυμα από εικονική Αρχή για συνέπειες μίας παράβασης
- Μπλε Φάλαινα (Blue Whale Suicide Game)

Blue Whale Levels

14. Cut the lip
15. Poke the needle arm
16. Make yourself hurt
17. Go to the roof of the largest and stand on the edge
18. Going to the bridge
19. Climb on the crane

Παράγοντες Επιτυχίας

- Τα θύματα δεν αναγνωρίζουν εγκαίρως την απειλή
- Η σύνθεση πολλών ετερογενών πηγών «αθώας» πληροφορίας δε δημιουργεί υποψίες
- Τα θύματα υποτιμούν την αξία της πληροφορίας που δίνουν
- Ο μεσάζων «στόχος» δεν έχει άμεσο προσωπικό συμφέρον στον τελικό «στόχο»
- Τα θύματα αναζητούν προσωπική αναγνώριση
- Τα θύματα δε συνειδητοποιούν τις συνέπειες των πράξεών τους

Kevin Mitnick

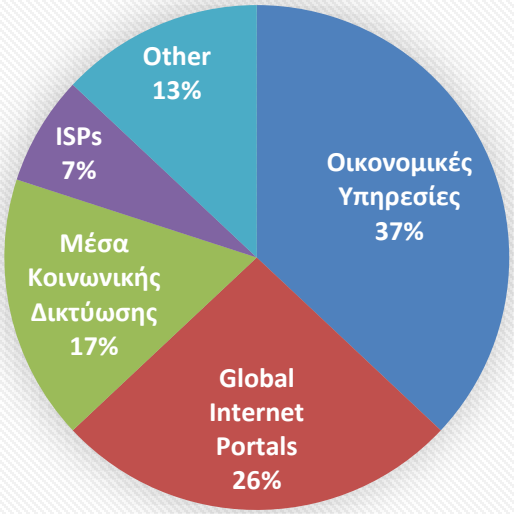
Μέθοδοι Διείσδυσης

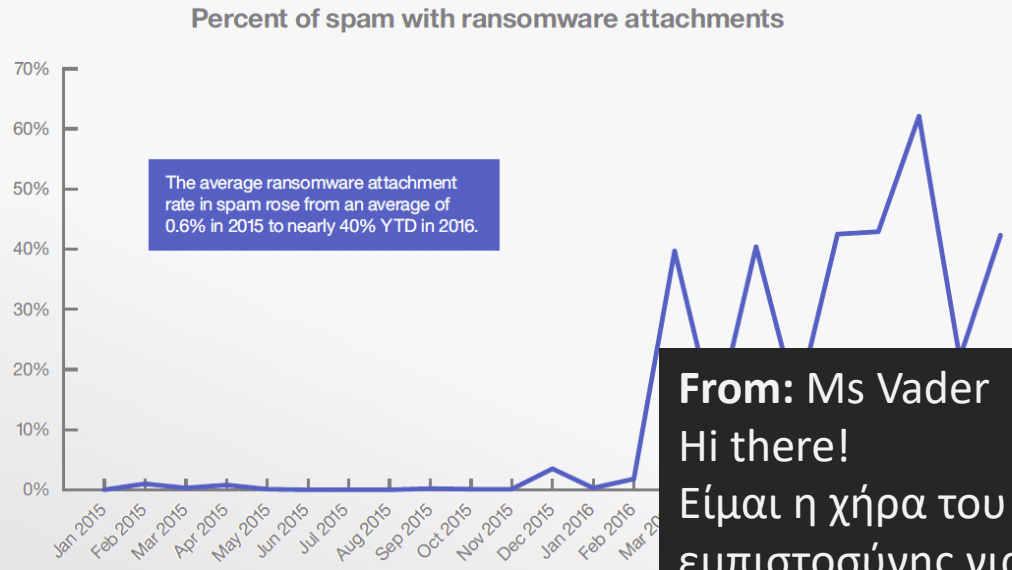
- Phishing
- Spear Phishing
- Vishing
- SMiShing
- Man-to-Man Middle Attack
- Man-to-Man Browser Attack
- Social Media Mining

Phishing

Mail από «Φίλο»

- Διαδεδομένο σε επιθέσεις προς Financial Institutes και ISPs
- Αν και τεχνολογικά θεωρείται παρωχημένο, παραμένει επιτυχής μέθοδος διείσδυσης





From: Ms Vader
Hi there!
Είμαι η χήρα του Darth Vader και αναζητώ άτομο εμπιστοσύνης για να μεταβιβάσω τα χρυσορυχεία του άνδρα μου στο Φεγγάρι. Στείλε μου τα στοιχεία σου!

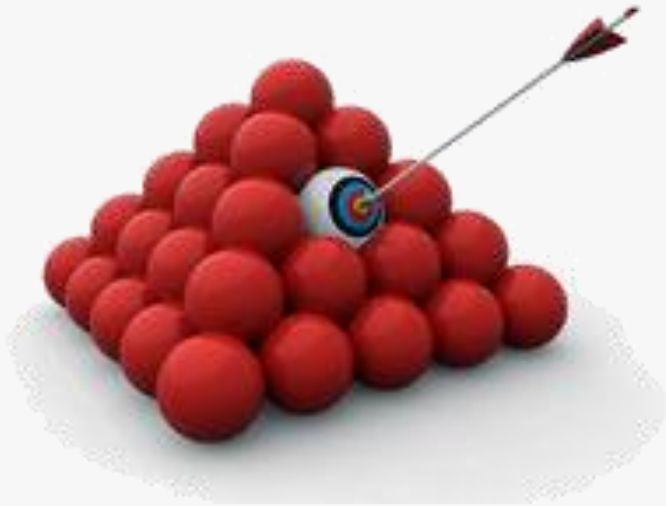
Quest GROUP 35 YEARS

Info Quest TECHNOLOGIES

Spear Phishing

Επώνυμο Στοχευμένο Mail σε επιλεγμένο κοινό

- 91% των τεχνολογικά εξελιγμένων Κυβερνοεπιθέσεων ξεκινούν από ένα Στοχευμένο Phishing Mail
- Έχει αυξημένη επιτυχία έναντι του απλού Phishing, δεδομένης της εξατομικευμένης προσέγγισης του θύματος



From: Ms Vader
Hi Antonis! Όλα καλά στην Athens, Greece?
Είμαι η χήρα του Darth Vader και αναζητώ άτομο από το IT για να μεταβιβάσω τα χρυσορυχεία του άνδρα μου στο Φεγγάρι.

Vishing

Κλήση από εικονική Αρχή (Phising+Voice)

Εντός του 2014, 21 εκατομμύρια Στερλίνες διέρρευσαν από τις Βρετανικές Τράπεζες μέσω Vishing

SMiShing

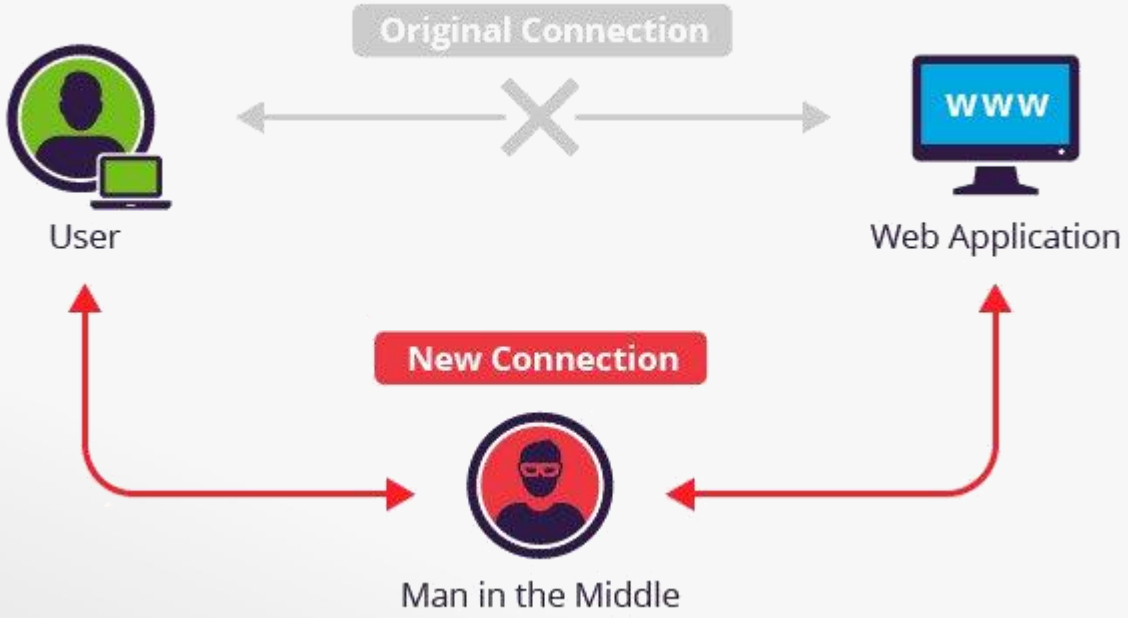
Phishing μέσω SMS

200 εκατομμύρια SMiShing μηνύματα
αποστέλλονται παγκοσμίως καθημερινά

Man-to-Man Middle Attack

Αποστολή Email μέσω υπαρκτού αποστολέα από υποκλοπή SSL σύνδεσης μεταξύ Browser και Web Server

Μία μοναδική Rogue DNS Attack χτύπησε ταυτόχρονα 70+ Οικονομικές Υπηρεσίες



Man-to-Man Browser Attack

Αποστολή Email μέσω υπαρκτού αποστολέα εκμεταλλευόμενοι Browser Vulnerability

90% των Επιχειρήσεων είναι εκτεθειμένες σε επιθέσεις Man-In-A-Browser

The Man-in-the-Browser attack is the same approach as Man-in-the-middle attack, but in this case a Trojan Horse is used to intercept and manipulate calls between the main application's executable (ex: the browser) and its security mechanisms or libraries on-the-fly.

Social Media Mining

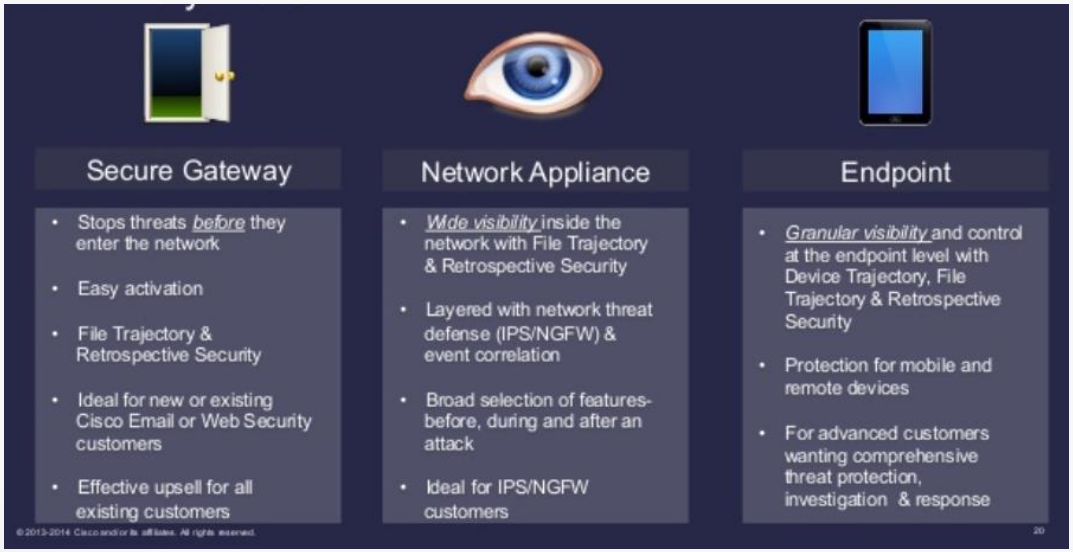
Ενδελεχής Έρευνα για Profiling του θύματος.
Χρησιμοποιείται ως προεργασία για το Spear Phishing και το Vishing

100 εκατομμύρια Facebook Accounts είναι Ψευδή ή Αντίγραφα

Η άμυνα

Information Systems Security

- Ασφάλεια Πολλαπλών επιπέδων
- Advanced Malware Protection
  - DNS Layer Protection
  - Endpoint Protection
  - Email Threat Protection
  - Sophisticated Segmentation
- Διασφάλιση συναλλαγών
  - 2-Way Validation
  - Transaction Authorization
- Ψηφιακή Σήμανση

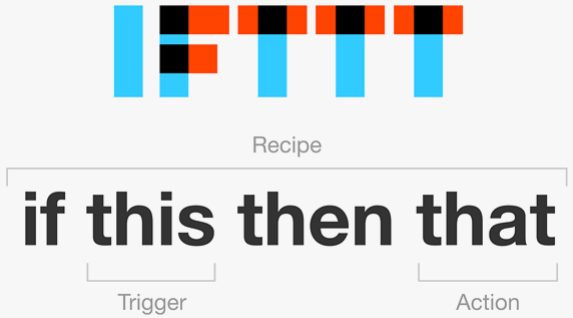


Η άμυνα

Context Security:

Τι είναι:

- Συνδυασμός Άμυνας και Καταστολής
- Αξιοποίηση του IoT προς όφελος της Ασφάλειάς μας
- IFTTT M2M Triggered Actions



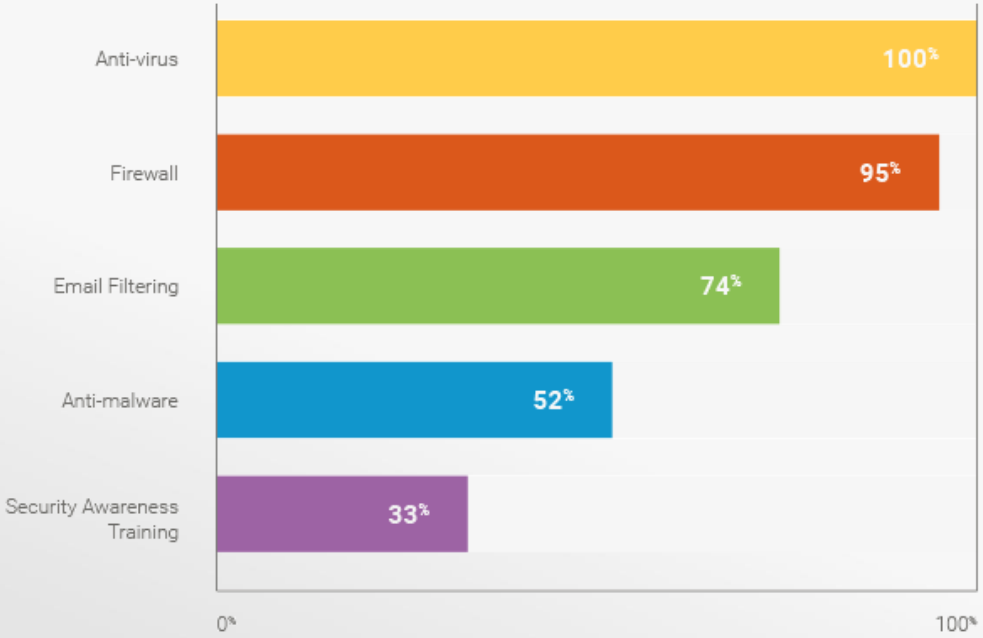
Πώς λειτουργεί:

- Αξιοποιεί συνδεδεμένες συσκευές
- Σε περίπτωση που ένας αισθητήρας (π.χ. Πόρτα του Computer Room) δηλώσει παραβίαση, ενεργοποιείται συγκεκριμένο Flow που προλαμβάνει την έκθεση των ευαίσθητων δεδομένων μας στον εισβολέα (π.χ. άμεση διαγραφή αρχείων, κρυπτογράφηση δεδομένων)

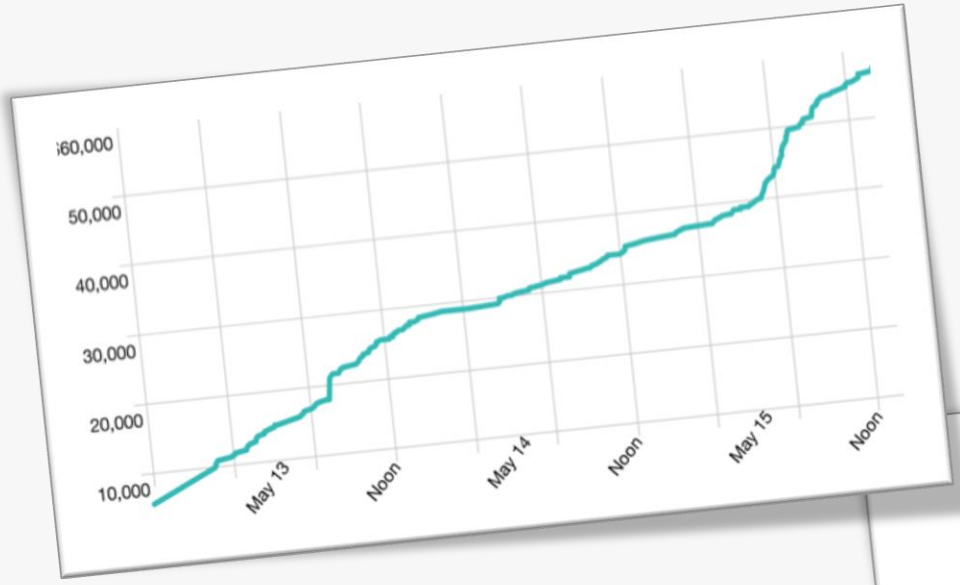
Η άμυνα

Εκπαίδευση:

- «Δεν παίρνουμε καραμέλες από ξένους»
- Δε μοιραζόμαστε στοιχεία Ταυτοποίησής μας
- Ενημερώνουμε το IT τμήμα μας για ύποπτα Requests
- Δημιουργούμε Κουλτούρα γύρω από την Εταιρική μας Επικοινωνία
- Διαχωρίζουμε το Επαγγελματικό από το Προσωπικό Οικοσύστημα

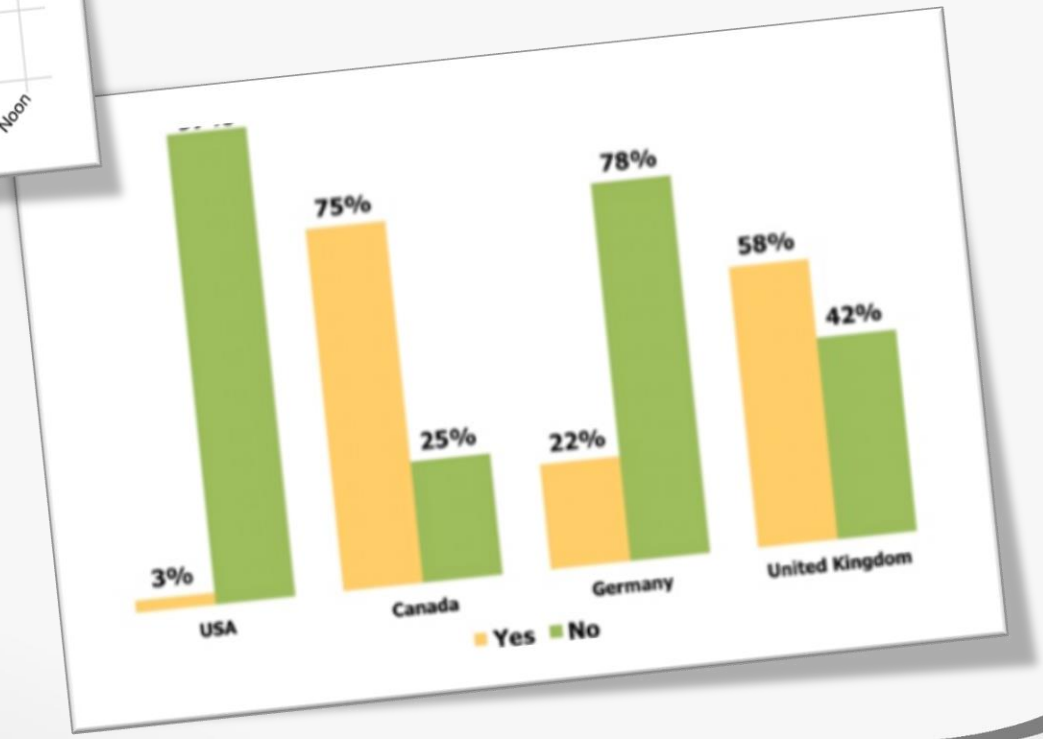


Some Facts:



WannaCry
Bitcoin
Payments

Total
Ransomware
Payments



Quest GROUP

Info Quest TECHNOLOGIES

uni systems

Υπερήφανος Χορηγός Εθνικής Ομάδας Κυβερνοασφάλειας

HELLENIC CYBER SECURITY TEAM

Ευχαριστώ

Quest GROUP 35 YEARS

Info Quest TECHNOLOGIES