GDPR

«Η προστασία των προσωπικών δεδομένων και η ασφάλεια των πληροφοριακών συστημάτων»

Φώτης Ρωμούδης

Senior IT Consultant

Τρίτη 20/03/2018

Ασφάλεια Προσωπικών Δεδομένων

- Τι είναι τα δεδομένα; (data)

Τα δεδομένα είναι ένα σύνολο από σύμβολα τα οποία έχουν καταγραφεί.

- Τι είναι η πληροφορία; (information)

Πληροφορία ονομάζεται το σύνολο των δεδομένων τα οποία συνδέονται από την έννοια τους.

- Τι είναι τα προσωπικά δεδομένα;

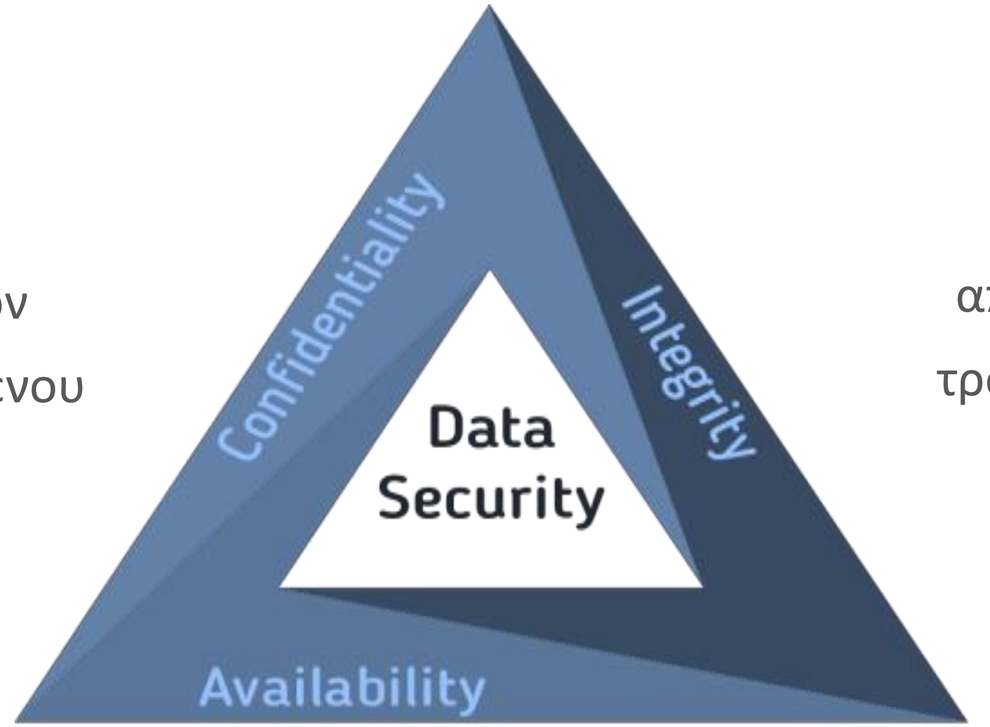
Κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»). Δεδομένα όπως διευθύνσεις διαδικτυακού πρωτοκόλλου (IP), αναγνωριστικά cookies ή άλλα αναγνωριστικά στοιχεία όπως ετικέτες αναγνώρισης μέσω ραδιοσυχνοτήτων μπορούν να χρησιμοποιηθούν για την ταυτοποίηση φυσικών προσώπων

www.eugdpr.gr

CIA

Εμπιστευτικότητα (confidentiality)

Εμπιστευτικότητα είναι η αποκάλυψη πληροφοριών χωρίς την άδεια του υποκειμένου



Ακεραιότητα (integrity)

Ακεραιότητα ονομάζεται η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας

Διαθεσιμότητα (availability)

Διαθεσιμότητα δεδομένων ονομάζεται η αποφυγή της καθυστέρησης ενός εξουσιοδοτημένου υποκειμένου να αποκτήσει πρόσβαση σε πληροφορίες ή υπολογιστικούς πόρους

ΟΡΙΣΜΟΣ
Τι είναι η ασφάλεια προσωπικών δεδομένων ?
(Information Security)

Ασφάλεια προσωπικών δεδομένων
είναι η προστασία
της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας

Η απώλεια έστω και μιας από τις αρχές
της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας
αποτελεί παραβίαση
της ασφάλειας προσωπικών δεδομένων

Βασικοί Κανόνες Ασφαλείας

- PASSWORDS
- ANTI - VIRUS
- UPDATES
- ATTACHMENTS
- BACKUP

Social impact

Let me in: «Άσε το κακό να μπεί»

Το 84% των χρηστών του Google δήλωσε ότι του άρεσε αυτή η ταινία

Κωδικοί Ασφαλείας (Passwords)

SplashData 2017 Top 20 worst passwords

1	123456 (top 2016 list)		11	admin (up 4)
2	password (top 2016 list)		12	welcome (unchanged)
3	12345678 (up 1)		13	monkey (new)
4	qwerty (up 2)		14	login (down 3)
5	12345 (down 2)		15	abc123 (down 1)
6	123456789 (new)		16	starwars (new)
7	letmein (new)		17	23123 (new)
8	1234567 (Unchanged)		18	dragon (up 1)
9	football (down 4)		19	passw0rd (down 1)
10	iloveyou (new)		20	master (up 1)

Κωδικοί Ασφαλείας (Passwords)

- Ισχυροί Κωδικοί
- Διαφορετικοί Κωδικοί ανά Εφαρμογή
- Password Manager
- 2FA
- Αλλαγή Κωδικού ανά 2 Μήνες

Εγκατάσταση αντιϊκού προγράμματος (Anti-virus)

- Τακτικός έλεγχος αρχείων
- Τακτική ενημέρωση του προγράμματος
- Κρυπτογράφηση αρχείων
- Κρυπτογράφηση πληρωμών

Ενημερώσεις Προγραμμάτων

- Έλεγχος συμβατότητας με τις κρίσιμες εφαρμογές
- Αυτόματη ενημέρωση προγραμμάτων
- Εγκατάσταση νέων εκδόσεων λειτουργικών συστημάτων

Αποφυγή εκτέλεσης συνημμένων μέσω μηνυμάτων ηλεκτρονικής αλληλογραφίας (e-mail attachments)

- Έλεγχος αποστολέα
- Διασταύρωση με τον αποστολέα για την αποστολή συνημένου
- Ενεργοποίηση εμφάνισης κατάληξης αρχείων
- Έλεγχος συνημμένου σε διαδικτυακές υπηρεσίες ανίχνευσης ιών

Διατήρηση αντιγράφων ασφαλείας (Backup)

- Backup σε φυσικό έγγραφο
- Backup σε φυσικό αποθηκευτικό μέσο (USB, Σκληρός δίσκος, DVD κ.α.
- Backup σε cloud υπηρεσίες

Συνήθεις Κυβερνο-επιθέσεις

- Κακόβουλο Λογισμικό
- Επιθέσεις Phishing
- Ransomware
- Επιθέσεις άρνησης υπηρεσιών
- Επίθεση Man-in-the-Middle
- Επαναχρησιμοποίηση κωδικών
- Προηγούμενη επίμονη απειλή
- Προεπιλεγμένοι Κωδικοί
- Επίθεση SQL Injection
- Μη εξουσιοδοτημένη πρόσβαση

Κακόβουλο Λογισμικό (malicious software – malware)

Μεταδίδεται κυρίως μέσω:

- E-mail
- USB
- Παραβιασμένης Ιστοσελίδας
- Πειρατικού Λογισμικού

Τύποι:

- **Ιός (virus):** μπορεί να αλλοιώσει, κλέψει ή να διαγράψει τα δεδομένα του χρήστη
- **Worm**: αντιγράφει τον εαυτό του από τον έναν υπολογιστή στον άλλον χωρίς την ανθρώπινη παρέμβαση
- **Δούρειος Ίππος (Trojan horse**): μπορεί να αποθηκεύσει κωδικούς μέσω
  της καταγραφής της κίνησης του πληκτρολογίου
  και να καταγράψει βίντεο μέσω της κάμερας
- **Rootkits**: επιτρέπει την πρόσβαση σε ένα υπολογιστικό σύστημα με δικαιώματα υπερχρήστη

Επιθέσεις Phishing

Ο επιτιθέμενος
χρησιμοποιώντας συνήθως μηνύματα μέσω
e-mail ξεγελά το υποκείμενο με σκοπό την
εκτέλεση ιομορφικού λογισμικού

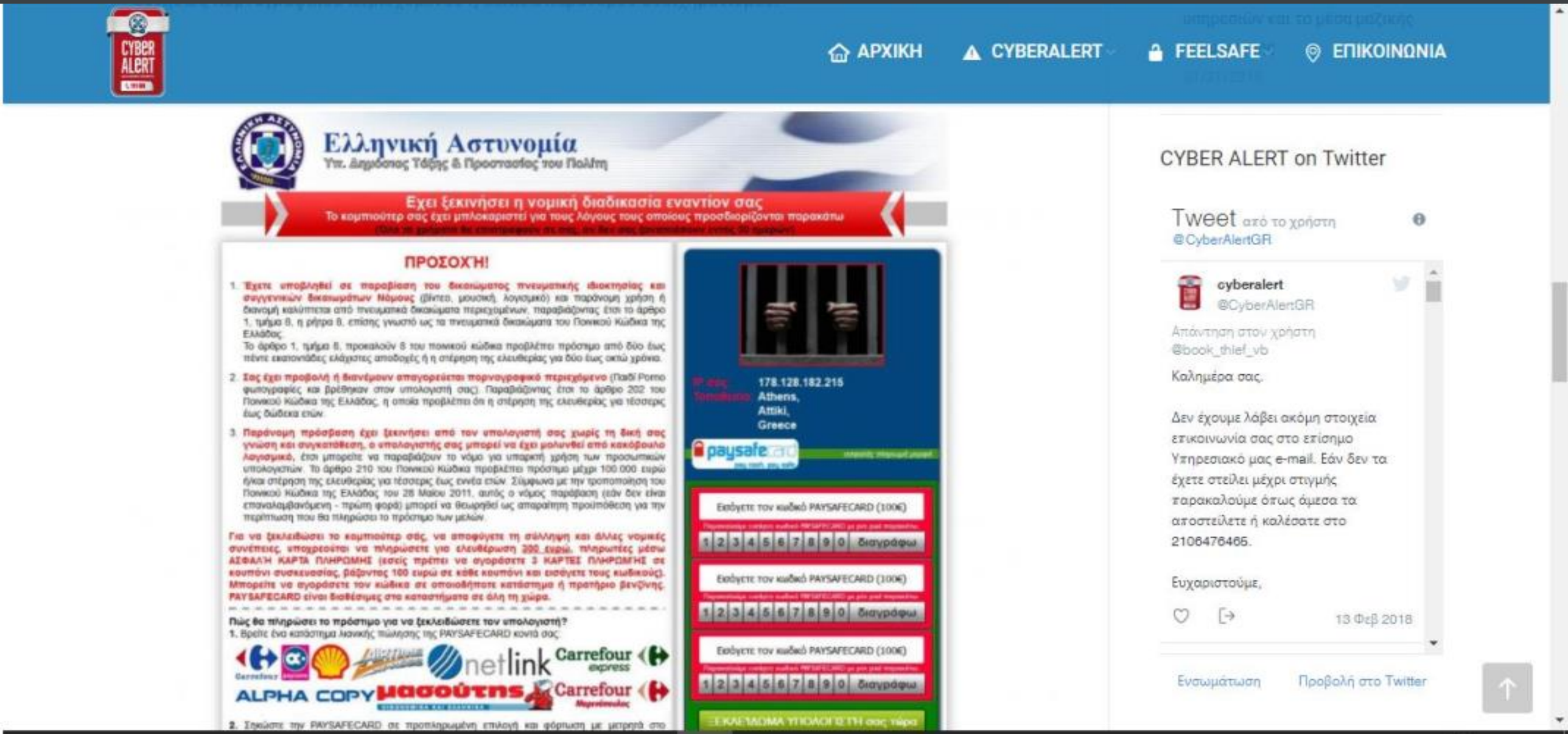
Στηρίζονται στην:

- Έλλειψη γνώσεων
- Έλλειψη προσοχής
- Οπτική εξαπάτηση

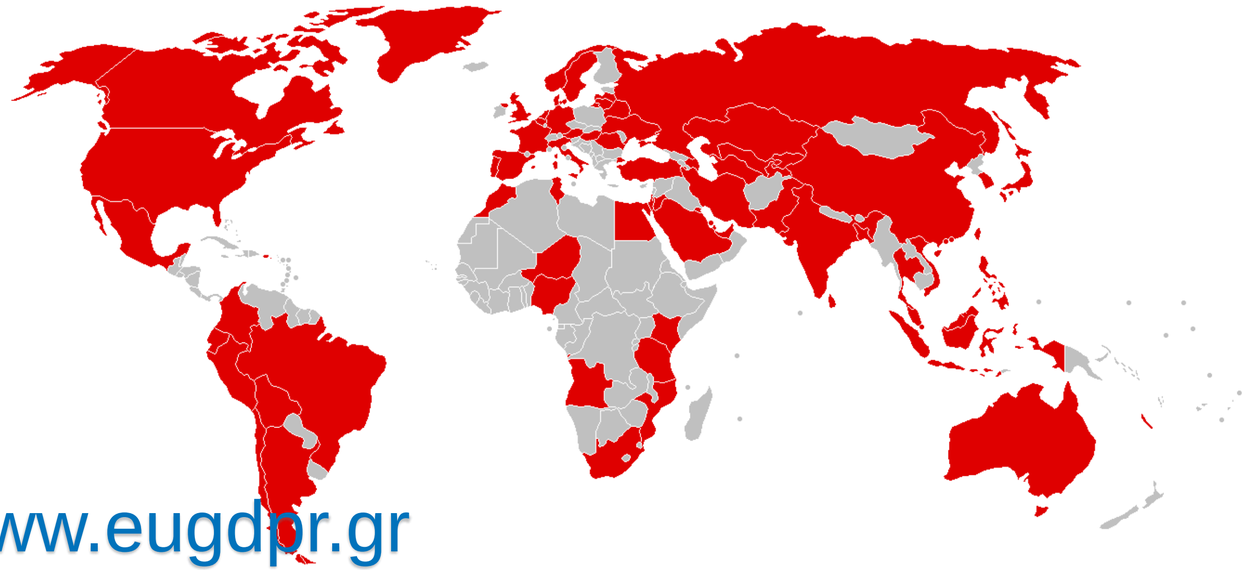
Υλοποιούνται με:

- Παραπλανητικό κείμενο όπως λάθος σύνταξη ή αναγραμματισμούς
- Παραπλανητικές εικόνες όπως παρεμφερή λογότυπα
- Παραπλανητικός σχεδιασμός ιστοσελίδας

Ransomware


CYBER ALERT
ΑΡΧΙΚΗ
CYBERALERT
FEELSAFE
ΕΠΙΚΟΙΝΩΝΙΑ
Ελληνική Αστυνομία
Υπ. Δημόσιας Τάξης & Προστασίας του Πολίτη
Έχει ξεκινήσει η νομική διαδικασία εναντίον σας
Το κομπιούτερ σας έχει μπλοκαριστεί για τους λόγους τους οποίους προσδιορίζονται παρακάτω
ΠΡΟΣΟΧΗ!
1. Έχετε υποβληθεί σε παραβίαση του δικαιώματος πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων Νόμους (βίντεο, μουσική, λογισμικό) και παράνομη χρήση ή διανομή καλύπτεται από πνευματικά δικαιώματα περιεχομένων, παραβιάζοντας έτσι το άρθρο 1, τμήμα 8, η ρήτρα 8, επίσης γνωστό ως τα πνευματικά δικαιώματα του Ποινικού Κώδικα της Ελλάδας.
Το άρθρο 1, τμήμα 8, προκαλούν 8 του ποινικού κώδικα προβλέπει πρόστιμο από δύο έως πέντε εκατονιάδες ελάχιστες αποδοχές ή η στέρηση της ελευθερίας για δύο έως οκτώ χρόνια.
2. Σας έχει προβολή ή διανέμουν απαγορεύεται πορνογραφικό περιεχόμενο (Παιδί Porno φωτογραφίες και βρέθηκαν στον υπολογιστή σας). Παραβιάζοντας έτσι το άρθρο 202 του Ποινικού Κώδικα της Ελλάδας, η οποία προβλέπει ότι η στέρηση της ελευθερίας για τέσσερις έως δώδεκα ετών.
3. Παράνομη πρόσβαση έχει ξεκινήσει από τον υπολογιστή σας χωρίς τη δική σας γνώση και συγκατάθεση, ο υπολογιστής σας μπορεί να έχει μολυνθεί από κακόβουλο λογισμικό, έτσι μπορείτε να παραβιάζουν το νόμο για υπαρκτή χρήση των προσωπικών υπολογιστών. Το άρθρο 210 του Ποινικού Κώδικα προβλέπει πρόστιμο μέχρι 100 000 ευρώ ή/και στέρηση της ελευθερίας για τέσσερις έως εννέα ετών. Σύμφωνα με την τροποποίηση του Ποινικού Κώδικα της Ελλάδας του 28 Μαΐου 2011, αυτός ο νόμος παράβαση (εάν δεν είναι επαναλαμβανόμενη - πρώτη φορά) μπορεί να θεωρηθεί ως απαραίτητη προϋπόθεση για την περίπτωση που θα πληρώσει το πρόστιμο των μελών.
Για να ξεκλειδώσει το κομπιούτερ σας, να αποφύγετε τη σύλληψη και άλλες νομικές συνέπειες, υποχρεούται να πληρώσετε για ελευθέρωση 200 ευρώ, πληρωτές μέσω ΑΣΦΑΛΗ ΚΑΡΤΑ ΠΛΗΡΩΜΗΣ (εσείς πρέπει να αγοράσετε 3 ΚΑΡΤΕΣ ΠΛΗΡΩΜΗΣ σε κουπόνι συσκευασίας, βάζοντας 100 ευρώ σε κάθε κουπόνι και εισάγετε τους κωδικούς). Μπορείτε να αγοράσετε τον κώδικα σε οποιοδήποτε κατάστημα ή πρατήριο βενζίνης. PAYSAFECARD είναι διαθέσιμες στο καταστήματα σε όλη τη χώρα.
Πώς θα πληρώσει το πρόστιμο για να ξεκλειδώσετε τον υπολογιστή?
1. Βρείτε ένα κατάστημα λιανικής πώλησης της PAYSAFECARD κοντά σας
netlink
Carrefour express
ALPHA COPY
μασούτης
Carrefour
2. Σηκώστε την PAYSAFECARD σε προπληρωμένη επιλογή και φόρτιση με μετρητά στο
178.128.182.215
Athens,
Attiki,
Greece
paysafecard
Εισάγετε τον κωδικό PAYSAFECARD (100€)
1 2 3 4 5 6 7 8 9 0 διαγράφω
Εισάγετε τον κωδικό PAYSAFECARD (100€)
1 2 3 4 5 6 7 8 9 0 διαγράφω
Εισάγετε τον κωδικό PAYSAFECARD (100€)
1 2 3 4 5 6 7 8 9 0 διαγράφω
CYBER ALERT on Twitter
Tweet από το χρήστη @CyberAlertGR
cyberalert
@CyberAlertGR
Απάντηση στον χρήστη @book_thief_vb
Καλημέρα σας.
Δεν έχουμε λάβει ακόμη στοιχεία επικοινωνία σας στο επίσημο Υπηρεσιακό μας e-mail. Εάν δεν τα έχετε στείλει μέχρι στιγμής παρακαλούμε όπως άμεσα τα αποστείλετε ή καλέσατε στο 2106476465.
Ευχαριστούμε,
13 Φεβ 2018
Ενσωμάτωση
Προβολή στο Twitter

WannaCry ransomware



12-15 Μάϊου 2017

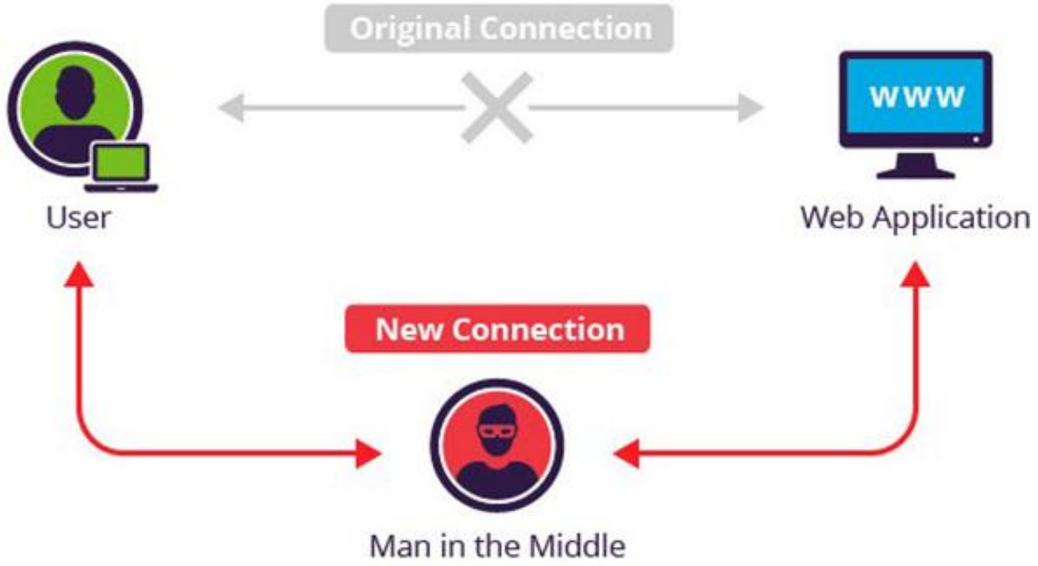
Επηρέασε 300.000 υπολογιστές σε 150 χώρες

Τα διαφυγόντα κέρδη των επιχειρήσεων που μολύνθηκαν από το ransomware υπολογίστηκαν γύρω στα 3M $

Το WannaCry ransomware ήταν μια κυβερνοεπίθεση λυτρισμικού (ransomware) σε υπολογιστές σε όλο τον κόσμο που τρέχουν το λειτουργικό σύστημα Windows.
Το ransomware κρυπτογραφούσε αρχεία και ζητούνταν λύτρα 300-600 δολαρίων μέσω Bitcoin για να αποκτήσει ο χρήστης και πάλι πρόσβαση στα αρχεία του.
Η επίθεση κράτησε τέσσερις μέρες, από τις 12 Μαΐου μέχρι τις 15 Μαΐου 2017.

Επίθεση Man-in-the-middle (MITM)

Κατά την επίθεση Man-in-the-middle (MITM) ο κακόβουλος χρήστης παρεμποδίζει την επικοινωνία δυο μερών, ελέγχοντας την ροή της επικοινωνίας με σκοπό την απόσπαση των πληροφοριών που αποστέλλονται.



Η επίθεση MITM γίνεται συνήθως με 2 τρόπους:

- Την υποκλοπή των δεδομένων (eavesdropping attack)
- Την αλλοίωση του μηνύματος από τον αποστολέα στον παραλήπτη και αντίστροφα

Μέτρα Προστασίας που ορίζει το GDPR

- Ψευδονυμοποίηση
- Ελαχιστοποίηση
- Ανωνυμοποίηση
- Προστασία εξ’ ορισμού & προστασία από τον σχεδιασμό

Ψευδονυμοποίηση

Σκοπός

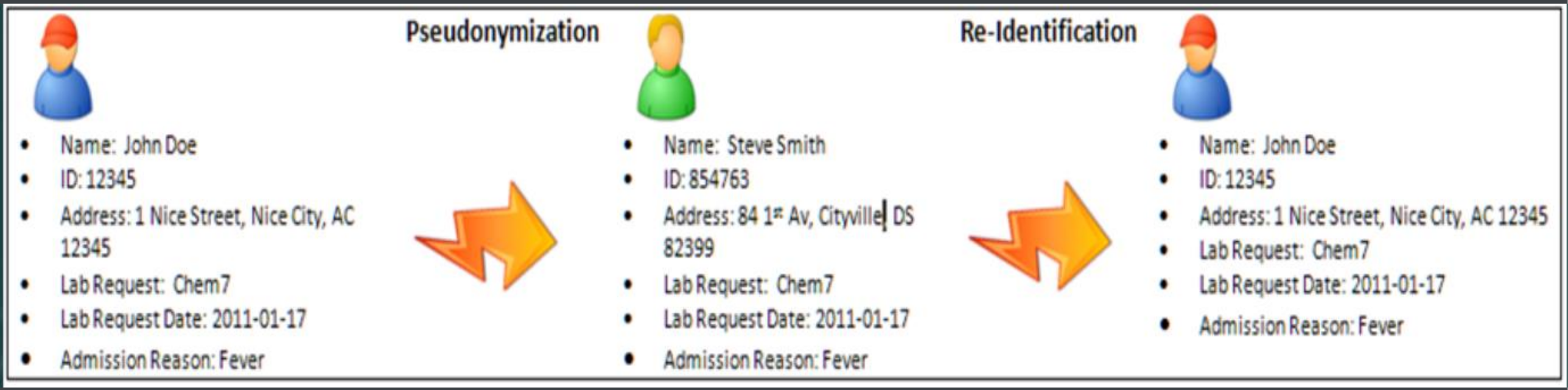
Η ευχέρεια της συλλογής δεδομένων για το υποκείμενο χωρίς η ταυτότητα του τελευταίου να γνωστοποιείται στον υπεύθυνο επεξεργασίας

Υλοποίηση

- ✓ Μέσω κρυπτογράφησης
- ✓ Με αποχαρακτηρισμό των δεδομένων
- ✓ Με διαχωρισμό των βάσεων δεδομένων

Ψευδονυμοποίηση ορίζεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μην μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και επόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο

Ψευδονυμοποίηση - παράδειγμα



Ελαχιστοποίηση

Σκοπός

Ο σκοπός της ελαχιστοποίησης των δεδομένων είναι ο μετριασμός της επεξεργασίας περιττών δεδομένων
Ελαχιστοποιείται η περίπτωση της γενικευμένης διαρροής δεδομένων από μια παραβίαση πληροφοριακών συστημάτων

Υλοποίηση

- ✓ **Μέσω αποκλεισμού**: αποφυγή της επεξεργασίας δεδομένων
- ✓ **Μέσω επιλογής**: επεξεργασία συγκεκριμένων μόνο δεδομένων
- ✓ **Μέσω αφαίρεσης**: διαγραφή δεδομένων που δεν είναι απαραίτητα
- ✓ **Μέσω καταστροφής**: η πλήρης καταστροφή των δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα πρέπει να είναι κατάλληλα, συναφή και να περιορίζονται στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.

Η παραπάνω πρόταση ορίζεται από τον κανονισμό ως ελαχιστοποίηση των δεδομένων

Ανωνυμοποίηση

Ως ανωνυμοποίηση ορίζονται όλες οι ενέργειες που εκτελεί ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία πάνω σε σύνολο προσωπικών δεδομένων, με αποκλειστικό γνώμονα τη μη-αναστρέψιμη παραμόρφωση του μέρους εκείνου των δεδομένων που επιτρέπει τον προσδιορισμό ενός φυσικού προσώπου.

Προστασία εξ ορισμού και από το σχεδιασμό

Από το σχεδιασμό:

Οργανωτικά, τεχνικά & διοικητικά μέτρα

σχεδιασμένα για την εξυπηρέτηση των αρχών προστασίας δεδομένων

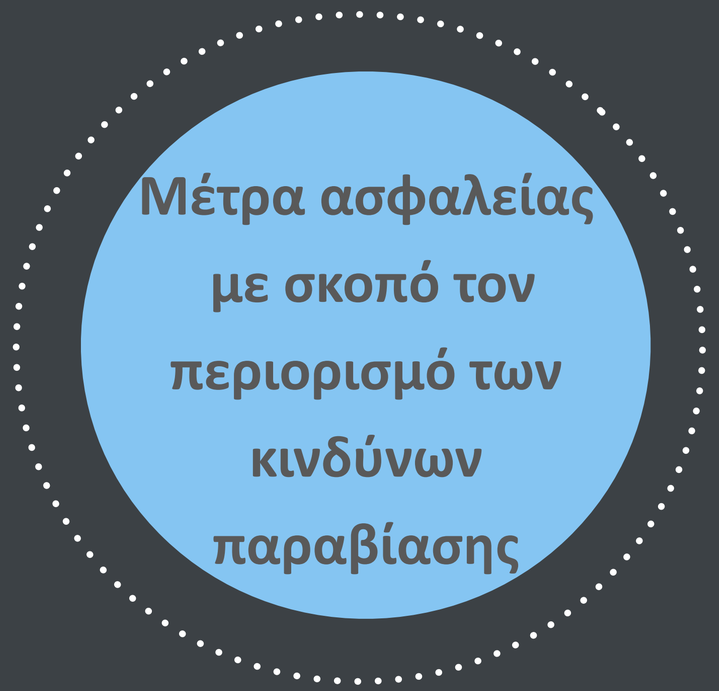
- Ψευδωνυμοποίηση
- Confidentiality, Integrity, Availability (CIA)
- Πίνακες ιδιωτικότητας (privacy dashboards)

Εξ'ορισμού:

Κάθε πράξη επεξεργασίας, κάθε ρύθμιση, κάθε εργαλείο

ΘΑ ΠΡΕΠΕΙ εξ'ορισμού ΝΑ ΕΞΥΠΗΡΕΤΟΥΝ την ιδιωτικότητα

- Ρυθμίσεις
- Εύκολη πρόσβαση και ενημέρωση επί των ρυθμίσεων (πχ. Whatsapp cloud)



Αποφυγή πολιτικής Bring your own device

Διαμόρφωση διαχειριστικών δικαιωμάτων

Διεξαγωγή τεκτικών ελέγχων ασφαλείας

Τοίχος προστασίας (Firewall)

Intrusion Detection System

Intrusion prevention system

Τμηματοποίηση και απομόνωση δικτύου

Data leak prevention

Κρυπτογράφηση δεδομένων

Επιμόρφωση προσωπικού

Αποφυγή πολιτικής Bring your own device (BYOD)

Ελαχιστοποιείται:

- ❑ Η πιθανότητα απώλειας εταιρικών δεδομένων
- ❑ Η πιθανότητα μόλυνσης του εσωτερικού εταιρικού δικτύου

Κίνδυνοι:

- ❑ Κλοπή ή απώλεια συσκευής
- ❑ Απουσία τοίχους προστασίας ή αντιικού
- ❑ Πρόσβαση σε μη ασφαλή δίκτυα

Διεξαγωγή τακτικών ελέγχων ασφαλείας

- ❑ Αξιολόγηση ευπαθειών
- ❑ Έλεγχος διείσδυσης
- ❑ Προσομοίωση κυβερνοεπίθεσης (stress test – read team)
- ❑ Προσομοίωση άμυνας κυβερνοεπίθεσης (διαχείριση κρίσης – blue team)

Πλεονεκτήματα:

- ➢ Εύρεση ευπαθειών
- ➢ Πρόταση αντιμέτρων
- ➢ Αξιολόγηση κατάστασης πληροφοριακών συστημάτων
- ➢ Αξιολόγηση ετοιμότητας προσωπικού

Τοίχος προστασίας (firewall)

Τεχνολογία λογισμικού ή υλικού με σκοπό τον έλεγχο της εισερχόμενης ή εξερχόμενης κίνησης μέσω της ανάλυσης των διερχόμενων πακέτων και ανάλογα με την πολιτική τα απορρίπτει ή τα αποδέχεται

Πλεονεκτήματα:

✓ Πρόληψη απώλειας δεδομένων

✓ Απόρριψη κακόβουλων πακέτων

✓ Απόρριψη κακόβουλων διευθύνσεων IP

✓ Δρομολόγηση στο εσωτερικό του εταιρικού δικτύου

✓ Ανάλυση δικτύου (logs, timestamps κ.τ.λ.)

Τμηματοποίηση και απομόνωση δικτύου

Η τμηματοποίηση του δικτύου περιλαμβάνει τον διαχωρισμό του δικτύου σε μικρότερα δίκτυα και η απομόνωση καθορίζει μέσω των κανόνων ποιές συσκευές επιτρέπει να επικοινωνούν με άλλες συσκευές στο δίκτυο

- Διαχωρισμός του δικτύου σε μικρότερα δίκτυα
- Ποιές συσκευές επιτρέπεται να επικοινωνούν με άλλες συσκευές στο δίκτυο

  - Περιορισμός παραβίασης
  - Απομόνωση της πρόσβασης εξωτερικών χρηστών από το εσωτερικό δίκτυο
  - Περιορισμός πρόσβασης σε ευαίσθητα δεδομένα μόνο σε εξουσιοδοτημένα τμήματα
  - Βελτιστοποίηση ταχύτητας δικτύου

Κρυπτογράφηση δεδομένων

Η κρυπτογράφηση των δεδομένων μέσω έγκυρων κρυπτογραφικών αλγορίθμων ενισχύει την εμπιστευτικότητα των δεδομένων.
Διατηρείται η εμπιστευτικότητα και η εγκυρότητα των Δεδομένων.

Υλοποιείται σε:

- Βάσεις δεδομένων (MD5)
- Απομακρυσμένη επικοινωνία (VPN)
- Διαδικτυακή επικοινωνία (HTTPS)
- Μεταφορά αρχείων (SFTP)

Επιμόρφωση προσωπικού

Η επιμόρφωση του προσωπικού είναι το μοναδικό μη τεχνικό μέσο περιορισμού των κινδύνων παραβίασης αλλά ίσως και το σημαντικότερο

Μέσω της επιμόρφωσης περιορίζεται η πιθανότητα επιτυχούς επίθεσης κοινωνικής μηχανής

- Εκπαίδευση μέσω σεμιναρίων
- Ενημέρωση για νέες τεχνολογίες από τη διεύθυνση μηχανογράφησης
- Επιμόρφωση του προσωπικού πάνω σε προσομοίωση ρεαλιστικού σεναρίου κυβερνοεπίθεσης

Σκοπός είναι η ευαισθητοποίηση σε θέματα ασφαλείας (security awareness)

Υπηρεσίες Πληροφορικής για το GDPR

- Προετοιμασία – Αποτύπωση υφιστάμενης κατάστασης
- Αξιολόγηση επιπτώσεων / Αξιολόγηση Κινδύνων
- Υλοποίηση Λύσεων λογισμικού για παρακολούθηση του GDPR
- Υλοποίηση λύσεων κρυπτογράφησης δεδομένων
- Αξιολόγηση Πολιτικών Ασφάλειας Δεδομένων & Δικτύων

Υπηρεσίες Πληροφορικής για το GDPR

File & Email Encryption	Κρυπτογράφηση αρχείων & μηνυμάτων ηλεκτρονικής αλληλογραφίας
Backup Systems	Συστήματα δημιουργίας αντιγράφων ασφαλείας
Electronic Encryption Mechanism	Κρυπτογράφηση ηλεκτρονικών συναλλαγών
Document Management System (DMS)	Σύστημα ασφαλούς ψηφιοποίησης και αρχειοθέτησης εγγράφων

Υπηρεσίες Πληροφορικής για το GDPR

Penetration & Vulnerability Test (Cyber-attack simulation)	Έλεγχος διείσδυσης και ευπάθειας δικτύων & πληροφοριακών συστημάτων (Προσομοίωση κυβερνοεπίθεσης)
Intrusion Detection and Prevention Systems (IDS - IPS)	Συστήματα ανίχνευσης & αποτροπής εισβολών
Secure Filesharing & Email File Transfer (Zero Knowledge – Fragmentation)	Ασφαλής αποστολή αρχείων δεδομένων μέσω ηλεκτρονικής αλληλογραφίας και δυνατότητα διαμοιρασμού/συγχρονισμού αρχείων με χρήση private data rooms ανά τμήμα κλινικής (Expiration date for files & data rooms)
Network Inventory Tools	Εργαλεία network discovery, inventory & audit

SIGMASOFT

Ερωτήσεις - Απορίες

Ευχαριστούμε πολύ