«ΠΕΡΙΣΤΑΤΙΚΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΑΡΑΒΙΑΣΕΙΣ/ΔΙΑΡΡΟΕΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ»

ΤΕΧΝΟΛΟΓΙΚΕΣ ΚΑΙ ΟΡΓΑΝΩΤΙΚΕΣ ΠΤΥΧΕΣ, ΣΥΜΦΩΝΑ ΜΕ ΤΟΝ Γ.Κ.Π.Δ. ΚΑΙ Ν. 4624/2019

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Anastasios Papathanasiou, B.Sc, M.Sc., PhD(c) in Computer Science

Έγκλημα στον Κυβερνοχώρο

Το Έγκλημα στον Κυβερνοχώρο

- Αποτελεί **βασική πρόκληση για την ψηφιακή οικονομία και την κοινωνία**.
  - Europol: *Έκθεση αξιολόγησης απειλών από το Σοβαρό και Οργανωμένο έγκλημα (2018)*

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος

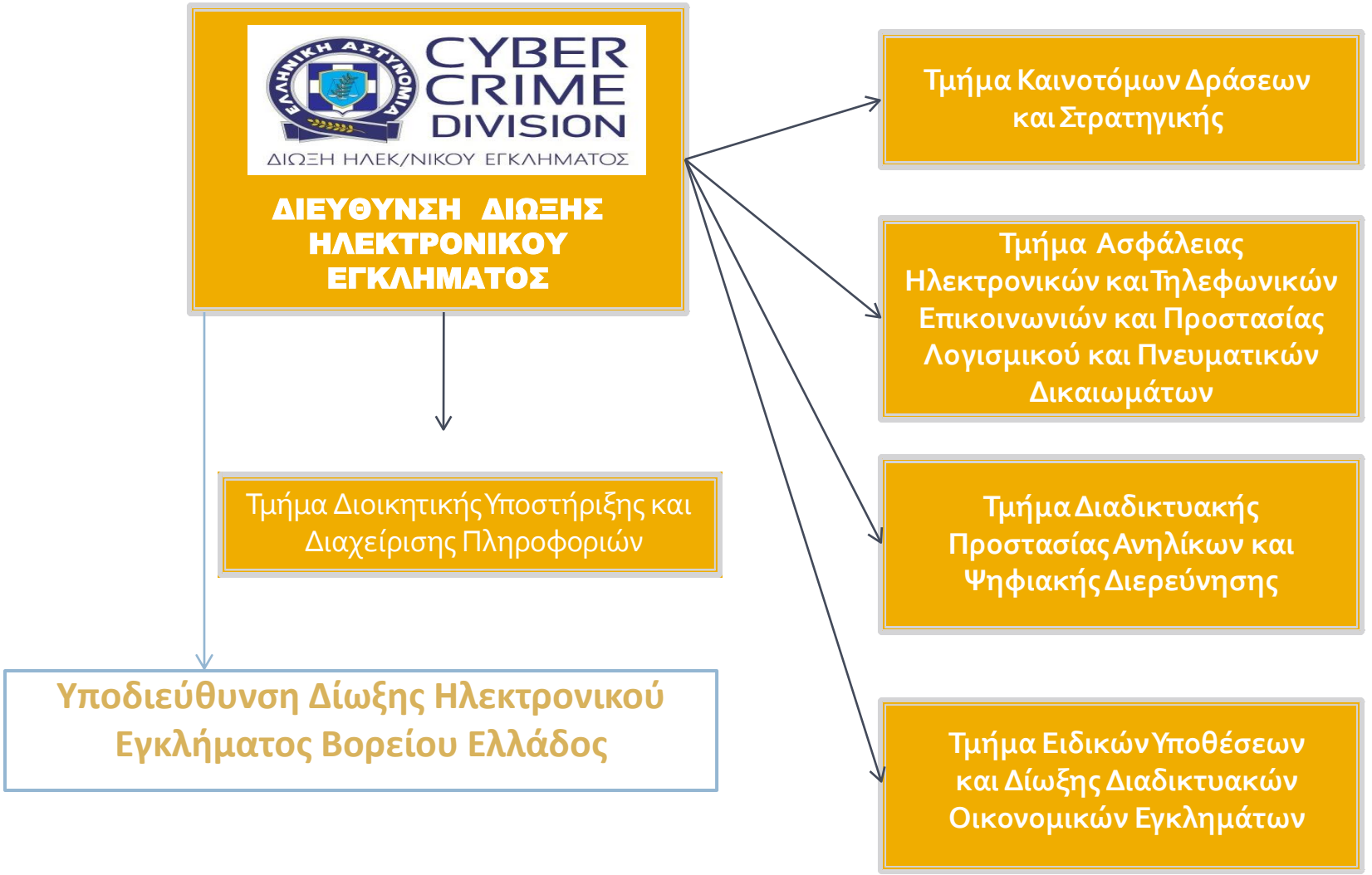
- Αρχικά ξεκίνησε ως **Τμήμα** το **2004** [Π.Δ. 100/2004]

- Το **2010** προσελήφθησαν **25 Αξιωματικοί Ειδικών Καθηκόντων**

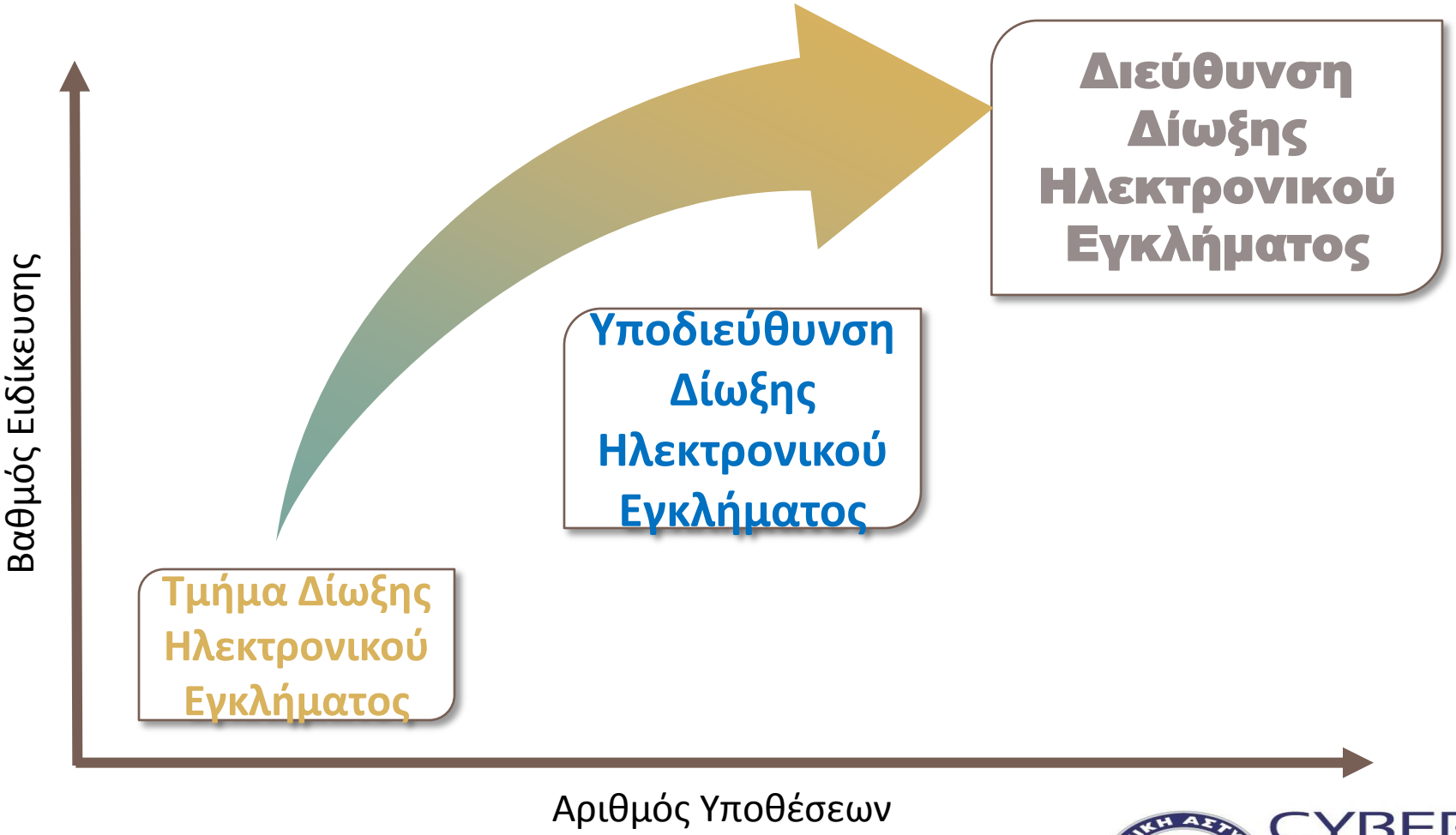
- Με το **Π.Δ. 9/2011** επεκτάθηκε σε **Υποδιεύθυνση** με τέσσερα (4) Τμήματα

- Με το αρ. 17 του **Ν. 4249/2014** αναβαθμίστηκε σε **Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος** και **έτσι λειτουργεί σήμερα**.

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος



Από Τμήμα, Υποδιεύθυνση και σήμερα
Διεύθυνση



CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Μορφές Κυβερνοεγκλήματος

- **Πορνογραφία ανηλίκων**
- **Οικονομικά Εγκλήματα (απάτες κ.τ.λ.)**
- **Cracking and Hacking**
- **Εγκλήματα που παραβιάζουν την πνευματική ιδιοκτησία**
- **Διακίνηση ναρκωτικών-φαρμάκων**
- **Κλοπή Διαδικτυακής Ταυτότητας**
- **Παραβιάσεις/διαρροές προσωπικών δεδομένων στον Κυβερνοχώρο**

Παραβιάσεις/διαρροές δεδομένων προσωπικού χαρακτήρα

Top Threats 2016, 2017, 2018 (Πηγή: ENISA)

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	↑	1. Malware	→	1. Malware	→	→
2. Web based attacks	↑	2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web application attacks	↑	3. Web Application Attacks	↑	3. Web Application Attacks	→	→
4. Denial of service	↑	4. Phishing	↑	4. Phishing	↑	→
5. Botnets	↑	5. Spam	↑	5. Denial of Service	↑	↑
6. Phishing	→	6. Denial of Service	↑	6. Spam	→	↓
7. Spam	↓	7. Ransomware	↑	7. Botnets	↑	↑
8. Ransomware	→	8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	→	9. Insider threat	→	9. Insider Threat	↓	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/ damage/ theft/loss	→	10. Physical manipulation/ damage/ theft/loss	→	→
11. Exploit kits	↑	11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Data breaches	↑	12. Identity Theft	↑	12. Identity Theft	↑	→
13. Identity theft	↓	13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Information leakage	↑	14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber espionage	↓	15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasin
Ranking: ↑ Going up, → Same, ↓ Going do

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Παραβίαση δεδομένων (Data Breach)

- **Μόνο όταν υπάρχουν προσωπικά δεδομένα** (σύμφωνα και με τον ΓΚΠΔ)

Τύποι περιστατικών παραβίασης προστασίας δεδομένων:

Παραβίαση: { Εμπιστευτικότητας / Διαθεσιμότητας / Ακεραιότητας } ή συνδυασμός

Παραβίαση δεδομένων (Data Breach)

- Παραβίαση δεδομένων προσωπικού χαρακτήρα (Τι νοείτε παραβίαση σύμφωνα και με τον Γ.Κ.Π.Δ. και Ν. 4624/2019)
  - *«Η **παραβίαση της ασφάλειας** που οδηγεί σε **τυχαία ή παράνομη***
    - ***καταστροφή,***
    - ***απώλεια,***
    - ***αλλοίωση,***
    - ***μη εξουσιοδοτημένη διάδοση ή***
    - ***προσπέλαση δεδομένων*** *προσωπικού χαρακτήρα που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά οποιονδήποτε άλλο τρόπο σε επεξεργασία»*

Περιστατικά παραβίασης δεδομένων (1)

- **Διακοπή** της ομαλής λειτουργίας ενός συστήματος ή μιας υπηρεσίας ή ενός δικτύου και, συνήθως,
- **πλήρης διακοπή** της πρόσβασης στους εξουσιοδοτημένους χρήστες

Μια **επίθεση DDoS** έχει σαν στόχο ένα σύστημα, συνήθως έναν server ή ένα ολόκληρο κέντρο δεδομένων (datacenter). Η επίθεση "βομβαρδίζει" το σύστημα με ένα **τεράστιο όγκο δεδομένων από διαφορετικές πηγές.**

Περιστατικά παραβίασης δεδομένων (2)

- Περιστατικά **μη εξουσιοδοτημένης/παράνομης πρόσβασης** και **επιθέσεις** σε συστήματα ή πληροφορίες, με διάφορα τεχνολογικά μέσα (πχ hacking, επιθέσεις με ιούς, worms, trojans

Περιστατικά παραβίασης δεδομένων (3)

- Περιστατικά «**μόλυνσης**» ή «**κλειδώματος**» αρχείων/δεδομένων με **ιομορφικό/κακόβουλο λογισμικό** (ransomware)

Το Ransomware είναι κακόβουλο λογισμικό που χρησιμοποιούν οι Κυβερνοεγκληματίες για να κλειδώσουν μια συσκευή ή να κρυπτογραφήσουν τα περιεχόμενά της, προκειμένου να εξαναγκάσουν τον ιδιοκτήτη ή τον χρήστη σε καταβολή λύτρων με την, χωρίς εγγυήσεις, υπόσχεση αποκατάστασης της πρόσβασης

Τεχνικές ransomware

- Οι Κυβερνοεγκληματίες χρησιμοποιούν πολλές τεχνικές ransomware, οι οποίες περιλαμβάνουν τα παρακάτω:
  - Το **screen lock ransomware** αποκλείει την πρόσβαση στην οθόνη της συσκευής (εκτός από το interface του κακόβουλου λογισμικού)
  - Το **PIN locker ransomware** αλλάζει τον κωδικό PIN της συσκευής, καθιστώντας το περιεχόμενο και τη λειτουργικότητά του απρόσιτα.
  - Το **ransomware κωδικοποίησης** δίσκων κρυπτογραφεί τις δομές MBR (Master Boot Record) ή/και τις κρίσιμες δομές του συστήματος αρχείων και επομένως εμποδίζει τον χρήστη να έχει πρόσβαση στο λειτουργικό σύστημα.
  - Το **Crypto-ransomware** κρυπτογραφεί τα αρχεία χρηστών που είναι αποθηκευμένα στο δίσκο.

Περιστατικά παραβίασης δεδομένων (4)

- Περιστατικά **απώλειας ή κλοπής ψηφιακών συσκευών** που **περιέχουν προσωπικά δεδομένα του οργανισμού/επιχείρησης** (πχ Laptop, USB κτλ)

Περιστατικά παραβίασης δεδομένων (5)

- **Η εκ των έσω απειλή (insider threat)**
- Εσωτερικές παραβιάσεις, από προσωπικό, πρώην προσωπικό, social engineering, phishing

Ανεπαρκή μέτρα ασφάλειας (6)

- **Ανεπαρκή μέτρα ασφάλειας/προστασίας** (**τεχνικά, οργανωτικά** κτλ), απουσία εκπαίδευσης, παραλείψεις, αμέλειες με αποτέλεσμα να **μην** προστατεύονται επαρκώς τα δεδομένα.

Προστασία προσωπικών δεδομένων – Εθνική νομοθεσία

Προστασία προσωπικών δεδομένων

Εξέλιξη της νομοθεσίας στην Ελλάδα

- Κύρωση με το Ν.2068/1992 της σύμβασης 108
  - ατελές καθεστώς προστασίας των προσωπικών πληροφοριών
- **Ν. 2472/1997** «Προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα»,
  - εναρμόνιση με οδηγία 95/46/ΕΚ
  - Συνταγματικές αναφορές: άρθρα 2§1, 5§1, 9§1 και 19 του Συντάγματος 1975/1986
- 2001: άρθρο 9Α Συντάγματος

«Καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως νόμος ορίζει. Η προστασία των προσωπικών δεδομένων διασφαλίζεται από ανεξάρτητη αρχή, που συγκροτείται και λειτουργεί, όπως νόμος ορίζει.»

- **Ν. 3471/2006** «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών»
  - Εναρμόνιση με οδηγία 2002/58/ΕΚ (Ν. 2774/1999 για την παλαιότερη οδηγία)
  - Με το ν. 4070/2012 τροποποιήθηκε ο ν. 3471/2006, βάσει της 2009/136/ΕΚ
- **Ν. 3917/2011** Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών (εναρμόνιση με 2006/24/ΕΚ), χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις.
- **Κανονισμός (ΕΕ) 2016/679 - Γ.Κ.Π.Δ.**
- **Ν. 4624/2019** - Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 και άλλες διατάξεις

Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR)

- Ο Κανονισμός, καταργώντας την Οδηγία 95/46/ΕΚ, αποτελεί μια **κανονιστική εξέλιξη στο ρυθμιστικό περιβάλλον της προστασίας προσωπικών δεδομένων**, η οποία επήλθε ένεκα της τεχνολογικής ανάπτυξης που κατέστησε την Οδηγία παρωχημένη
  - **ψηφιακή επανάσταση,**
  - **διαδίκτυο,**
  - **κινητή τηλεφωνία,**
  - **big data κ.ά.**

Τα βασικά χαρακτηριστικά του Κανονισμού

- **α**) Έχει **γενική εφαρμογή**
  - αφορά τόσο τις επιχειρήσεις του **ιδιωτικού τομέα** (ανεξαρτήτως μεγέθους και κλάδου δραστηριοποίησης)
  - όσο και τους φορείς του **δημοσίου**.
- **β**) Είναι **άμεσα εφαρμοστέος**
- **γ**) Αρκετές διατάξεις στη **διακριτική ευχέρεια των κρατών-μελών για περαιτέρω εξειδίκευση**
- **δ**) Προβλέπει **υψηλά διοικητικά πρόστιμα**
- **ε**) Έντονες και πολυετείς **διαπραγματεύσεις για το τελικό κείμενο**

Νέος Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων (GDPR)

- **Απαιτεί** από τους **οργανισμούς/φορείς/επιχειρήσεις** να :
  - Έχουν **κατάλληλα μέτρα ασφαλείας** και **αναγκαίες πολιτικές** για την προστασία -ασφάλεια των πληροφοριών
  - Κάνουν **αναλύσεις των επιπτώσεων** που μπορούν να προκύψουν λόγω παραβίασης ιδιωτικότητας
  - Έχουν ορίσει **υπεύθυνο για την προστασία των δεδομένων** (Data Protection Officer)
  - **Ενημερώνουν τις αρμόδιες αρχές εντός 72 ωρών** από τον εντοπισμό συμβάντος παραβίασης δεδομένων
  - Επίσης προβλέπει **πρόστιμα** τα οποία μπορούν να φθάσουν
    - **έως 4% του τζίρου ή**
    - **20εκ€ όποιο από τα δύο είναι μεγαλύτερο, ανάλογα με την σπουδαιότητα της παραβίασης.**

Αντιμετώπιση Περιστατικών Παραβίασης σύμφωνα με τον ΓΚΠΔ και Ν.4624/19

Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή (Άρθρο 33 ΓΚΠΔ Άρθρο 63 Ν.4624/19)

- Σε **περίπτωση παραβίασης** δεδομένων προσωπικού χαρακτήρα, ο **υπεύθυνος επεξεργασίας** γνωστοποιεί **αμελλητί** και, αν είναι δυνατό, **εντός 72 ωρών** από τη στιγμή που **αποκτά γνώση** του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην **εποπτική αρχή**

Τι περιλαμβάνει η γνωστοποίηση (Άρθρο 33 ΓΚΠΔ και άρθρο 63 Ν.4624/19)

- Η γνωστοποίηση περιλαμβάνει:
  - **α) φύση της παραβίασης,**
  - **β) όνομα και τα στοιχεία επικοινωνίας** του υπευθύνου προστασίας δεδομένων,
  - **γ) ενδεχόμενες συνέπειες** της παραβίασης ,
  - **δ) ληφθέντα ή τα προτεινόμενα προς λήψη μέτρα,** για την αντιμετώπιση της παραβίασης

Ειδική Φόρμα Γνωστοποίησης Περιστατικών Παραβίασης στην Αρχή (1)

- Για τη γνωστοποίηση περιστατικού παραβίασης προσωπικών δεδομένων στην Εποπτεύουσα Αρχή, ο υπεύθυνος επεξεργασίας πρέπει
  - να συμπληρώσει ειδική φόρμα που βρίσκεται στο παράρτημα 1 και στην ιστοσελίδα www.dpa.gr
  - η οποία υποβάλλεται ηλεκτρονικά στην ηλεκτρονική διεύθυνση: databreach@dpa.gr

- https://www.dpa.gr/portal/page?_pageid=33,211125&_dad=portal&_schema=PORTAL

Ειδική Φόρμα Γνωστοποίησης Περιστατικών Παραβίασης στην Αρχή (2)

Φόρμα υποβολής γνωστοποίησης περιστατικού παραβίασης προσωπικών δεδομένων

Σύμφωνα με το άρ. 33 του Γενικού Κανονισμού (ΕΕ) 679/2016

0. Γενικές Πληροφορίες		Επεξηγηματικά Σχόλια
Είδος γνωστοποίησης (Αρχική/Συμπληρωματική/Πλήρης)	☑ ΑΡΧΙΚΗ ☐ ΣΥΜΠΛΗΡΩΜΑΤΙΚΗ ☐ ΠΛΗΡΗΣ	1) Αρχική, αν πρόκειται για υποβολή κάποιων πρώτων διαθέσιμων στοιχείων, ενώ εκκρεμούν κάποια γιατί ακόμη δεν είναι διαθέσιμα 2) Συμπληρωματική, αν συμπίπτουν συμπληρωματικά στοιχεία από προηγούμενης υποβολή(ούσ)ες αρχικής 3) Πλήρης, αν παρέχονται όλες οι πληροφορίες από τον περιστατικό
Αναγνωριστικός αριθμός		Συμπληρώνεται από την Αρχή
1. Ποιος υποβάλει την παρούσα γνωστοποίηση περιστατικού		
1.1 Στοιχεία φυσικού/νομικού επικοινωνίας		
Όνομα οργανισμού/φορέα	GDPR A.E.	
Αριθμός ΓΕΜΗ (αν υπάρχει)	000-000-000	
ΑΦΜ	990099001.23	
Διεύθυνση οργανισμού/φορέα για επικοινωνία	Διεύθυνση Διαδικτύου	
Αρμόδιο πρόσωπο για επικοινωνία με την Αρχή (ονοματεπώνυμο - θέση στον οργανισμό/φορέα)	Ιωάννης Παπαδόπουλος	
Ηλεκτρονική διεύθυνση	gpapapodoulos@gdpras-greece.gr	
Τηλέφωνο	2109821212	
Ταχυδρομική διεύθυνση	Παπαδόπουλου 4, 11523, Αθήνα	
1.2 Πληροφορίες σχετικά τρίτων εμπλεκομένων μερών		
Για την εν λόγω επεξεργασία προσωπικών δεδομένων συμμετέχει και τρίτος, πέραν του οργανισμού σας; (ΝΑΙ/ΟΧΙ)	☑ ΝΑΙ ☐ ΟΧΙ	
Όνομα (επωνυμία) και ρόλος του τρίτου μέρους	Best Hosting Hellas A.E. - Συντήρηση εφαρμογής διαδικτύου	Συμπληρώνεται υποχρεωτικά εάν στο προηγ. πεδίο έχει δηλωθεί ΝΑΙ
2. Πληροφορίες για το χρονοδιάγραμμα του περιστατικού		
Το περιστατικό είναι σε εξέλιξη; (ΝΑΙ/ΟΧΙ)	☑ ΝΑΙ ☐ ΟΧΙ	
Χρόνος έναρξης του περιστατικού (μήνας/μήνες/έτος έτη) (πχ. 14/3/2018 15:00)	Άγνωστο	
Χρόνος που λάβατε γνώση του περιστατικού (μήνας/μήνες/έτος έτη) (πχ. 14/3/2018 15:00)	22/4/18 15:00	
Τρόπος με τον οποίο λάβατε γνώση του περιστατικού	Ενημέρωση με τηλέφωνο από την Best Hosting Hellas A.E.	
Χρόνος που ενημερωθήκατε από τον εκτελούντα την επεξεργασία για το περιστατικό (ώρα/μήνας/μήνες/έτος)	22/4/18 15:00	Προαιρετικό πεδίο - συμπληρώνεται μόνο εάν υπήρξε ενημέρωση από τον εκτελούντα
Λοιπές επεξηγηματικές πληροφορίες επί του χρονοδιαγράμματος		Προαιρετικό πεδίο - συμπληρώνεται αν ο υπεύθυνος επεξεργασίας κρίνει ότι χρειάζονται επεξηγηματικές πληροφορίες
3. Πληροφορίες για τη φύση του περιστατικού		
Απώλεια της εμπιστευτικότητας των προσωπικών δεδομένων;	☑ ΝΑΙ ☐ ΟΧΙ	Συμπληρώνεται ΝΑΙ εφόσον αποκτήθηκε μη εξουσιοδοτημένη πρόσβαση σε προσωπικά δεδομένα ή μη εξουσιοδοτημένη αποκάλυψη αυτών
Απώλεια της ακεραιότητας των προσωπικών δεδομένων;	☐ ΝΑΙ ☑ ΟΧΙ	Συμπληρώνεται ΝΑΙ εφόσον πραγματοποιήθηκε μη εξουσιοδοτημένη τροποποίηση/αλλοίωση σε προσωπικά δεδομένα
Απώλεια της διαθεσιμότητας των προσωπικών δεδομένων;	☐ ΝΑΙ ☑ ΟΧΙ	Συμπληρώνεται ΝΑΙ εφόσον τα προσωπικά δεδομένα κατέστησαν μη διαθέσιμα ή καταστράφηκαν

Πότε **δεν** απαιτείται γνωστοποίηση παραβίασης δεδομένων στην εποπτική αρχή;

- **Δεν γίνεται γνωστοποίηση** παραβίασης δεδομένων στην εποπτική αρχή, εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα:

  - **δεν ενδέχεται να προκαλέσει κίνδυνο**

    - **για τα δικαιώματα** και
    - τις **ελευθερίες των φυσικών προσώπων**.

Ανακοίνωση παραβίασης στα **υποκείμενα** των δεδομένων (Άρθρο 33 ΓΚΠΔ και άρθρο 64 Ν.4624/19)

- Όταν η παραβίαση δεδομένων προσωπικού χαρακτήρα ενδέχεται να **θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων**

  - ο **υπεύθυνος επεξεργασίας** ανακοινώνει **αμελλητί** την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο **υποκείμενο των δεδομένων**

  - **περιγράφεται** με σαφήνεια η **φύση της παραβίασης**

Ενημέρωση Αρχών Επιβολής του Νόμου

- Ενημέρωση **Αρχών Επιβολής του Νόμου** (Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος) για **ποινική διερεύνηση** (Άρθρο 38 Κ.Π.Δ.)

Εναρμόνιση με τις απαιτήσεις του Κανονισμού

Καθορισμός Διαδικασιών και Σχεδίου

- **Καθορισμός Διαδικασιών** και **Δημιουργία Σχεδίου Αντιμετώπισης Περιστατικών Παραβίασης** (σύμφωνα με άρθρα 33 κ 34 ΓΚΠΔ και άρθρο 63 και 64 του Ν.4624/19)

Καθορισμός διαδικασιών (1)

- Ο **υπεύθυνος επεξεργασίας** οφείλει να διαθέτει **διαδικασίες** για την **έγκαιρη**
  - **αναγνώριση**,
  - **αναφορά** και
  - **άμεση αντιμετώπιση** των περιστατικών παραβίασης της ασφάλειας των προσωπικών δεδομένων στο πλαίσιο του χρησιμοποιούμενου συστήματος επεξεργασίας, όπως :
    - ***τυχαία ή αθέμιτη καταστροφή,***
    - ***τυχαία απώλεια,***
    - ***αλλοίωση,***
    - ***απαγορευμένη διάδοση ή πρόσβαση και***
    - ***κάθε άλλη μορφή αθέμιτης επεξεργασίας***.

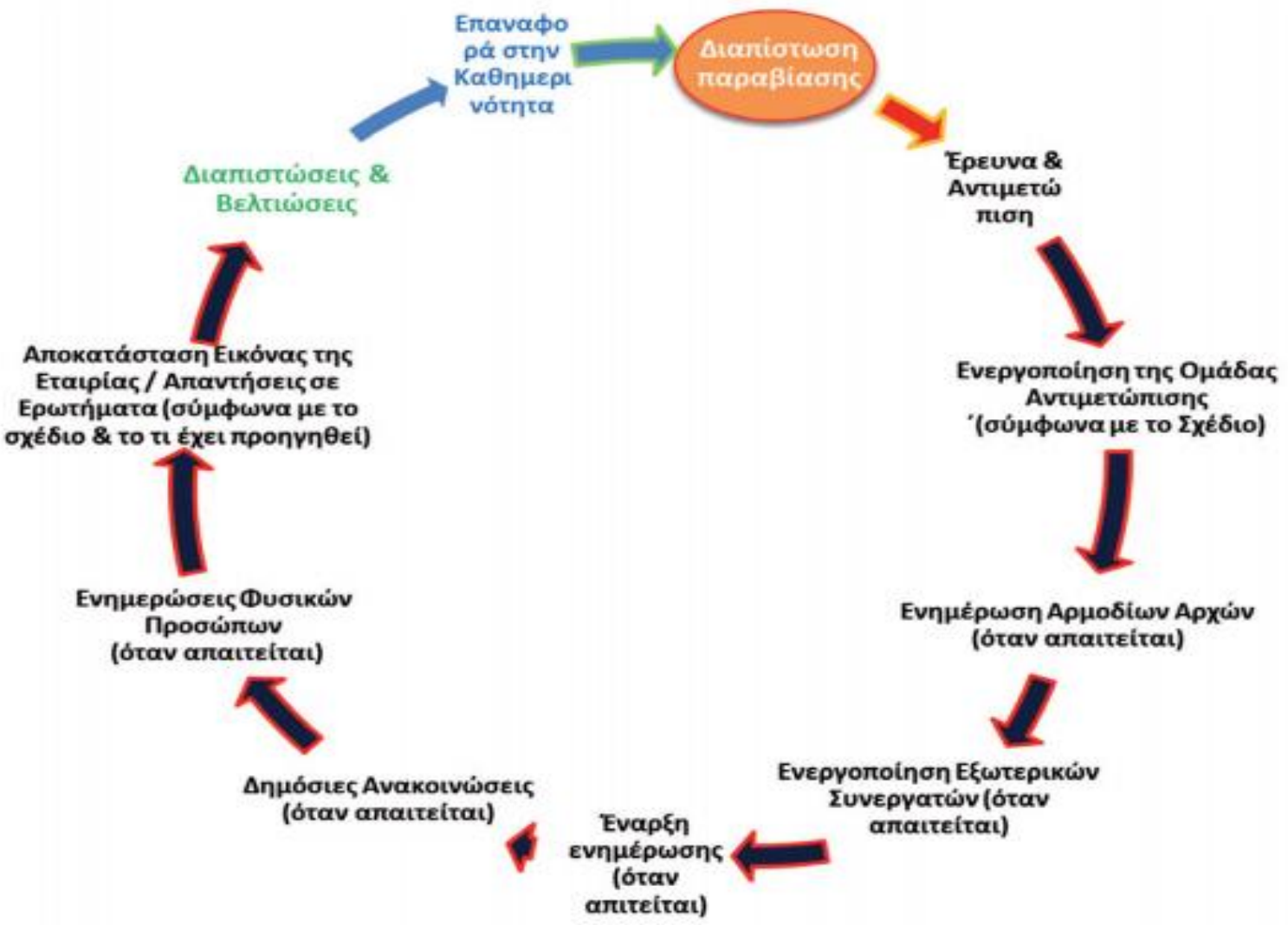
Καθορισμός διαδικασιών (2)

- Στις διαδικασίες αυτές πρέπει να περιλαμβάνονται κατ' αρχάς οι **ενέργειες** που είναι αναγκαίες για τη **διερεύνηση του εκάστοτε περιστατικού**
  - **τρόπος αναφοράς** περιστατικού,
  - **προσωπικό/ομάδα** που θα **ενεργοποιηθεί**,
  - **αρχεία-συστήματα** που θα πρέπει να **διερευνηθούν**

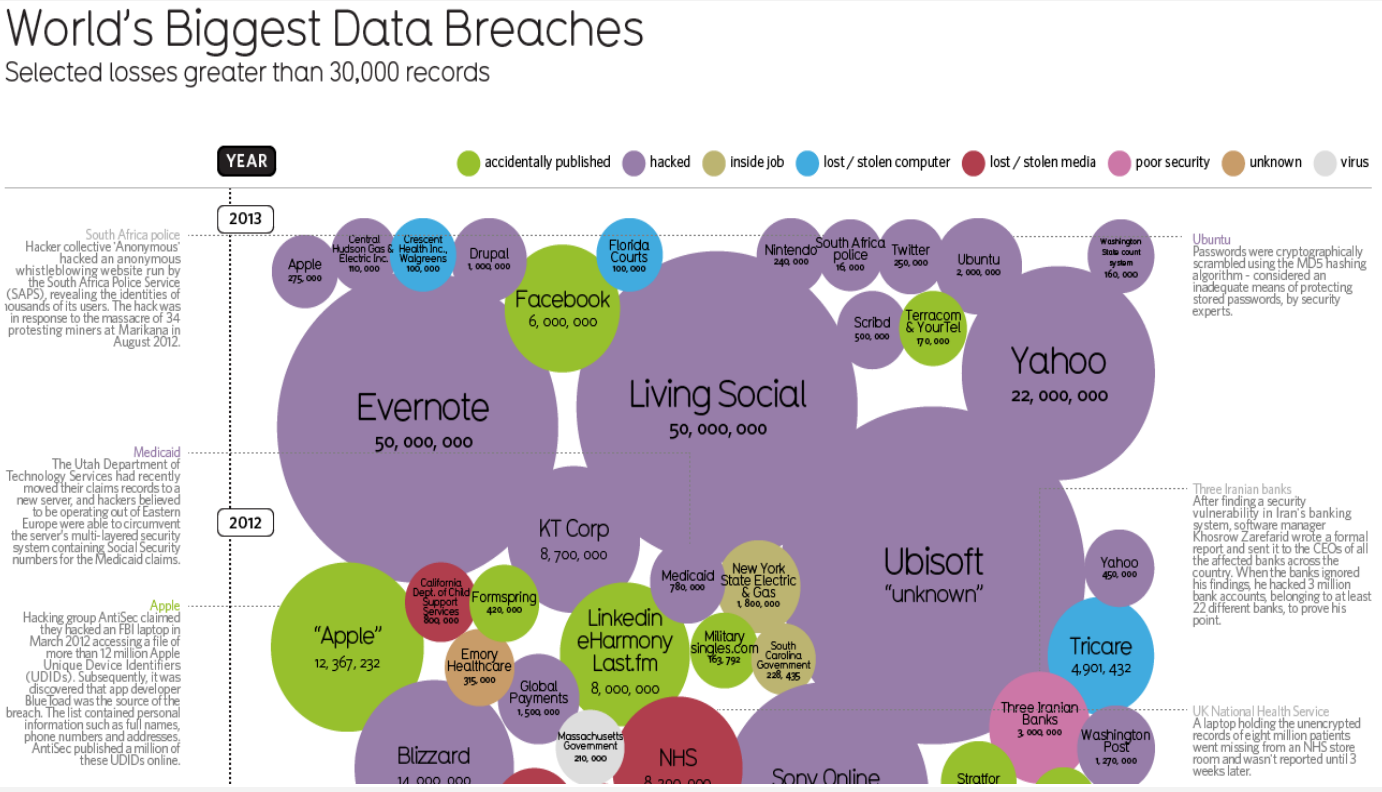
Καθορισμός διαδικασιών (3)

- Θα πρέπει να υπάρχει καταγραφή του κάθε συμβάντος σε **σχετικό αρχείο**, που θα περιλαμβάνει
  - τη **χρονική στιγμή** που έλαβε χώρα,
  - το **πρόσωπο που το ανέφερε** και **σε ποιον το ανέφερε**,
  - **εκτίμηση** των συνεπειών και της **κρισιμότητας** του περιστατικού,
  - **διαδικασίες ανάκαμψης/διόρθωσης** που ακολουθήθηκαν, καθώς και
  - **ενδεχόμενη διαδικασία ενημέρωσης των θιγομένων ατόμων** (υποκείμενα των δεδομένα) ανάλογα με την έκταση του περιστατικού

Κύκλος αντιμετώπισης μιας παραβίασης προσωπικών δεδομένων

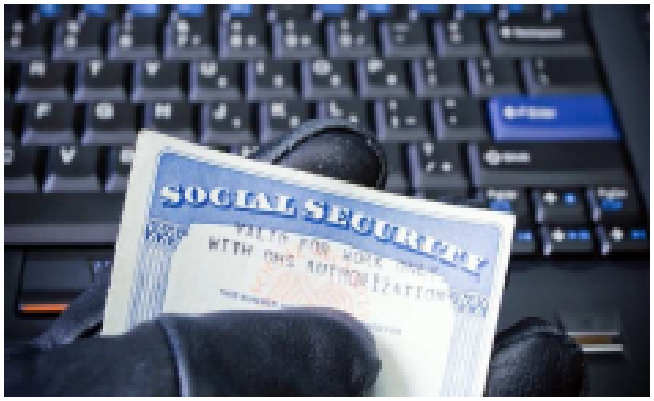


Μελέτες - Περιστατικά παραβίασης προσωπικών δεδομένων (εν γένει)



Premera

- Αμερικάνικη ασφαλιστική εταιρεία υγείας
- Μη εγκεκριμένη πρόσβαση σε
  - Προσωπικά Δεδομένα 11 εκ. πελατών
  - Στοιχεία επικοινωνίας, αριθμός κοινωνικής ασφάλισης, αριθμός μέλους, δεδομένα αιτήσεων κάλυψης εξόδων για ιατρική περίθαλψη και, σε μερικές περιπτώσεις, στοιχεία τραπεζικού λογαριασμού
- Κυβερνοεπίθεση -> **5/5/2014**
- Ανακάλυψη περιστατικού -> **29/1/2015**
- Ανακοίνωση περιστατικού -> **17/3/2015**
- Τρόπος επίθεσης -> Κακόβουλο λογισμικό
- Κίνδυνος κλοπής ιατρικής ταυτότητας



Διαχείριση περιστατικού παραβίασης

- Πρόσληψη εξειδικευμένης εταιρείας αντιμετώπισης / διερεύνησης περιστατικών ασφαλείας
- Συνεργασία με FBI
- Δημοσιοποίηση περιστατικού
- Δημιουργία ειδικής σελίδας ενημέρωσης
- Προσωπική ενημέρωση πελατών

Υποκλοπή και παράνομη επεξεργασία δεδομένων – στοιχείων από ελληνική επιχείρηση

- Άτομο, εκμεταλλευόμενο τη θέση εργασίας του σε ελληνική επιχείρηση (δραστηριοποιημένη στον τουρισμό), **υπέκλεψε το σύνολο του πελατολογίου**
  - *Ονοματεπώνυμα και στοιχεία πιστωτικών καρτών*

- Από τον Αύγουστο έως τον Νοέμβριο του 2016, χρησιμοποιώντας τα στοιχεία των υποκλαπέντων καρτών, προέβη
  - είτε ο ίδιος,
  - είτε χρησιμοποιώντας τρίτα-παρένθετα πρόσωπα, σε **πληθώρα απατηλών συναλλαγών**

Έρευνες

- Σε **έρευνα** που πραγματοποιήθηκε στην οικία του, παρουσία **δικαστικού λειτουργού**, βρέθηκαν και κατασχέθηκαν :
  - **(900) περίπου ψηφιακά αρχεία** με **προσωπικά δεδομένα ημεδαπών και αλλοδαπών υπηκόων**, στα οποία περιέχονται μεταξύ άλλων και τα στοιχεία των πιστωτικών τους καρτών
  - Από την έρευνα, τα αρχεία με δεδομένα που βρέθηκαν, αφορούσαν **τουλάχιστον (1.900) άτομα-υποκείμενα**

Παραπομπή υπόθεσης Ποινική Δικαιοσύνη– Ενημέρωση θιγομένων υποκειμένων

- Συλληφθείς, με τη δικογραφία που σχηματίσθηκε σε βάρος του, οδηγήθηκε στον **αρμόδιο Εισαγγελέα**, ο οποίος τον παρέπεμψε σε **Τακτικό Ανακριτή**.

- Οι έρευνες για την διακρίβωση του εύρους της παράνομης δραστηριότητας και την **ενημέρωση υποκειμένων** ιδιαίτερα **δυσχερής** και πραγματοποιήθηκε σε συνεργασία με
  - τη Διεύθυνση Διεθνούς Αστυνομικής Συνεργασίας,
  - την Ένωση Ελληνικών Τραπεζών,
  - ημεδαπά Τραπεζικά Ιδρύματα

Περιστατικό Παραβίασης Προσωπικών Δεδομένων σε πελάτες Ελληνικού Ξενοδοχείου

- Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια των Δικτύων και Πληροφοριών (ENISA) ενημέρωσε την Αρχή Προστασίας Προσωπικών Δεδομένων σχετικά με:
  - **περιστατικό διαρροής δεδομένων πιστωτικών καρτών ατόμων**
  - **τα οποία πραγματοποίησαν, από ξεχωριστές τοποθεσίες (διαφορετικά κράτη), ηλεκτρονική κράτηση σε ξενοδοχείο.**

- ΑΠΟΦΑΣΗ **85/2015** της Αρχής Προστασίας Προσωπικών Δεδομένων για το περιστατικό παραβίασης προσωπικών δεδομένων.

Περιστατικό Παραβίασης Προσωπικών Δεδομένων σε πελάτες Ελληνικού Ξενοδοχείου

- Κατά την εξέταση της υπόθεσης, προέκυψε ότι
  - η ηλεκτρονική πλατφόρμα που χρησιμοποιείται για τις διαδικτυακές κρατήσεις, **τηρούσε το σύνολο των δεδομένων των πιστωτικών καρτών** (*αριθμό κάρτας, αριθμό ασφαλείας, ημερομηνία λήξης*) χωρίς μέτρα ασφάλειας
  - ενώ παράλληλα **δεν είχαν υιοθετηθεί τα πλέον ενδεδειγμένα μέτρα για την ασφάλεια της επεξεργασίας**, όπως δηλ.
    - *να επιτρέπονται προσβάσεις που επιχειρούνται από συγκεκριμένες στατικές IP διευθύνσεις,*
    - *να τηρούνται αρχεία καταγραφής ενεργειών χρηστών, και*
    - *να χρησιμοποιούνται συνθηματικά (password) με επαρκή πολυπλοκότητα.*

Παραδείγματα εφαρμογής

Το backup αρχείων με προσωπικά δεδομένα αποθηκεύεται κρυπτογραφημένα σε ένα DVD. Γίνεται κλοπή και το CD φαίνεται να λείπει	ΟΧΙ	ΟΧΙ
Μετά από «κυβερνοεπίθεση» hackers εξάγουν προσωπικά δεδομένα από ένα ιστότοπο που λειτουργεί με https	ΝΑΙ	ΠΟΛΥ ΠΙΘΑΝΟ
Μετά από σύντομη διακοπή ρεύματος παρατηρείται βλάβη στο τηλεφωνικό κέντρο. Οι πολίτες δεν μπορούν να ασκήσουν τα δικαιώματά τους	ΟΧΙ	ΟΧΙ
Ransomware προσβάλει Η/Υ κρυπτογραφώντας αρχεία με προσωπικά δεδομένα. Για τα αρχεία αυτά δεν υπάρχουν πρόσφατα backup. Η έρευνα δείχνει ότι αυτή ήταν η μόνη κακόβουλη ενέργεια	ΝΑΙ	ΑΝΑΛΟΓΑ...
Πολίτης τηλεφωνεί ενημερώνοντας ότι έλαβε επιστολή που προοριζόταν για άλλο παραλήπτη, από λάθος στη διεύθυνση. Το περιεχόμενο της επιστολής περιέχει οικονομικά στοιχεία.	ΝΑΙ	ΜΟΝΟ ΕΝΑΣ
Οι ηλεκτρονικοί φάκελοι ενός νοσοκομείου παραμένουν χωρίς πρόσβαση για 30 ώρες, λόγω τεχνικού προβλήματος	ΝΑΙ	ΝΑΙ
Από λάθος, αρχείο με προσωπικά δεδομένα 500 πολιτών στέλνεται σε λίστα ηλεκτρονικού ταχυδρομείου με 300 παραλήπτες	ΝΑΙ	ΑΝΑΛΟΓΑ...

Μέτρα Ασφάλειας

Πολιτική και Σχέδιο ασφάλειας

- **Πολιτική ασφάλειας**
  - **Επίσημο έγγραφο** του οργανισμού
  - **εγκεκριμένο** από τη Διοίκηση
  - αποτυπώνονται **βασικές αρχές** προστασίας προσωπικών δεδομένων και ασφάλειας που εφαρμόζονται.

- **Σχέδιο ασφάλειας**
  - Περιγράφει την **υλοποίηση των αρχών της πολιτικής ασφάλειας** στα επιμέρους συστήματα επεξεργασίας προσωπικών δεδομένων

Ενδεικτικά μέτρα που μπορεί να προβλέπονται σε μία πολιτική ασφάλειας

1. *Υπεύθυνος ασφαλείας*
2. *Σχέδιο ανάκαμψης από καταστροφές*
3. *Υποχρέωση εμπιστευτικότητας του προσωπικού*
4. *Διαχείριση πληροφοριακών αγαθών*
5. *Διαχείριση χρηστών*
6. *Εκτελούντες την επεξεργασία.*
7. *Καταστροφή δεδομένων*
8. *Διαχείριση αλλαγών*
9. *Διαχείριση περιστατικών παραβίασης προσωπικών δεδομένων*
10. *Εκπαίδευση του προσωπικού*
11. *Μέτρα φυσικής ασφάλειας*
12. *Σχεδιασμός εφαρμογών του πληροφοριακού συστήματος*
13. *Αναγνώριση και αυθεντικοποίηση*
14. *Αρχεία καταγραφής*
15. *Αντίγραφα ασφαλείας*
16. *Διαμόρφωση περιβάλλοντος υπολογιστών*
17. *Ασφάλεια επικοινωνιών*

Οργανωτικά

Τεχνικά

Πηγές - Βιβλιογραφία

Κάτσικας Σ. (2014): «Διαχείριση ασφάλειας πληροφοριών», Εκδόσεις ΠΕΔΙΟ.

- http://www.dpa.gr/
- http://www.astynomia.gr/
- https://dpoacademy.gr/
- http://money.cnn.com/2015/03/17/technology/security/premera-hack/index.html

ONLY THREE THINGS ARE CERTAIN IN LIFE: DEATH, TAXES, AND ..... DATA BREACHES!!!

ΣΑΣ ΕΥΧΑΡΙΣΤΩ ΓΙΑ ΤΗΝ ΠΡΟΣΟΧΗ ΣΑΣ !

Αστυνόμος Α΄ Αναστάσιος ΠΑΠΑΘΑΝΑΣΙΟΥ, MSc, PhD(c)

a.papathanasiou@cybercrimeunit.gr

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος / Α.Ε.Α.

ccu@cybercrimeunit.gov.gr