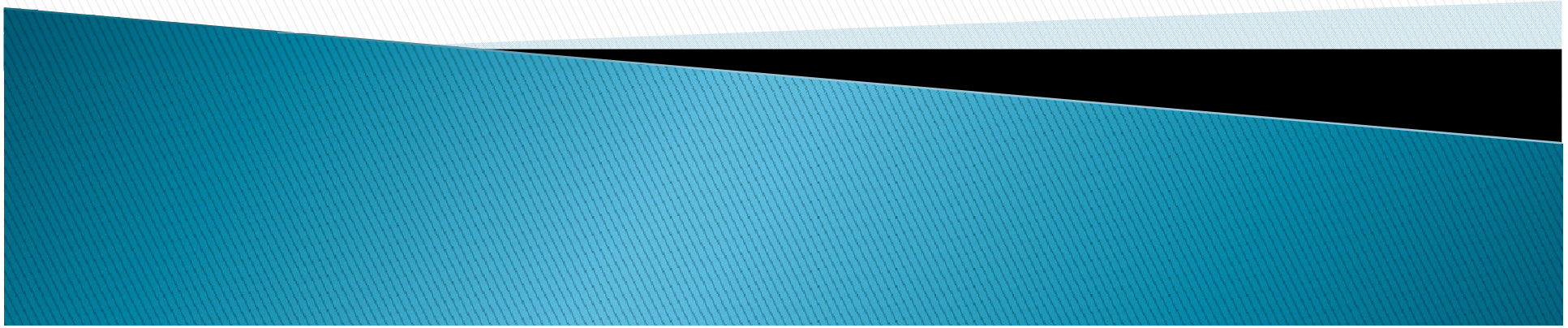
encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ
ΤΡΑΠΕΖΩΝ

# Το Πρότυπο PCI DSS

23 Σεπτεμβρίου 2009



# Ατζέντα

- Εισαγωγή
- Το Πρότυπο PCI DSS
- Περιβάλλον Δεδομένων Καρτούχων
- Καθορισμός Εύρους Εφαρμογής
- Ανάλυση Απαιτήσεων Προτύπου
- Τεχνολογικοί Μηχανισμοί

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Βασικοί Στόχοι Έργου

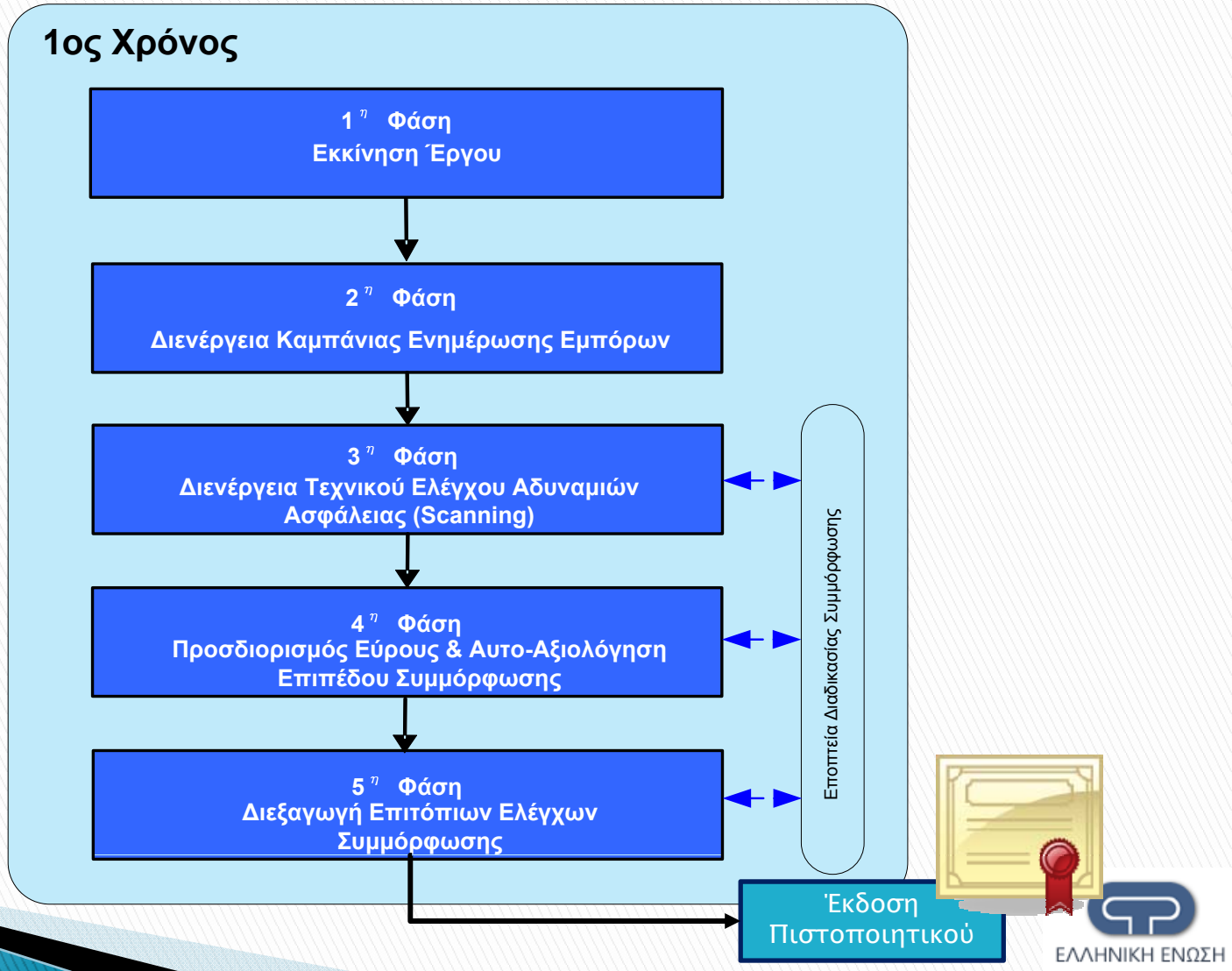
Προκειμένου να επιτευχθεί η προστασία και εύρυθμη λειτουργία των εμπορικών επιχειρήσεων, οι βασικοί στόχοι του έργου είναι :

- η ουσιαστική ενημέρωση των εμπορικών επιχειρήσεων,
- η πιστοποίηση συμμόρφωσης των εμπορικών επιχειρήσεων με το πρότυπο ασφαλείας PCI DSS, και
- η διατήρηση πιστοποίησης της συμμόρφωσής τους για τρία τουλάχιστον έτη.

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

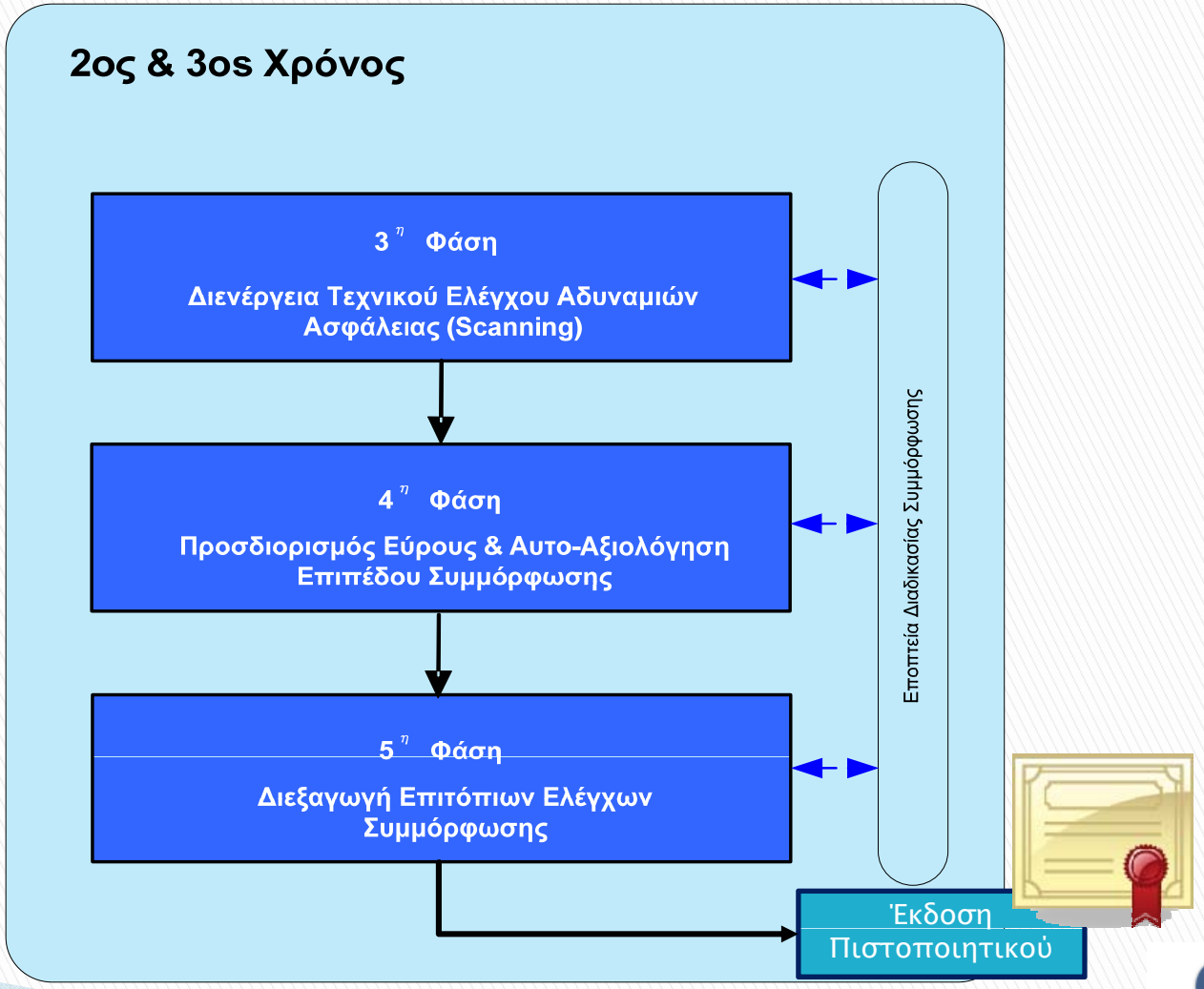
# Μεθοδολογία Έργου…




encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# ...Μεθοδολογία Έργου




encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# ENCODE

Η ENCODE, αποτελεί τη μεγαλύτερη & πλέον εξειδικευμένη στην Ελλάδα εταιρεία, με **αποκλειστικό αντικείμενο** την παροχή υπηρεσιών ασφάλειας και διαχείρισης κινδύνου πληροφοριών.

- Ίδρυση: Απρίλιος 2001
- Έδρα : Αθήνα
- Θυγατρικές: ENCODE Middle East: Dubai, Ηνωμένα Αραβικά Εμιράτα
- Παραρτήματα: ENCODE UK: Λονδίνο, Αγγλία
- Περιοχές παροχής υπηρεσιών: Δυτική & ΝΑ Ευρώπη, Μέση Ανατολή, Βαλκάνια και ΗΠΑ
- Στελέχωση: Περισσότερους από 30 ειδικούς στην Ασφάλεια Πληροφοριών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Πιστοποιητικά

- ISO 9001:2000
- ISO 27001/BS7799
- PCI QSA & ASV
- CISSP/CISM/CISA…

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Οι Πελάτες μας

- **Περισσότερες από 25 μεγάλες Τράπεζες**
  - 6 μεγαλύτερες τράπεζες στην Ελλάδα,
  - 8 από τις μεγαλύτερες τράπεζες της Μέσης Ανατολής
- **10 μεγάλοι τηλεπικοινωνιακοί οργανισμοί**
  - 4 μεγάλοι τηλεπικοινωνιακοί οργανισμοί στην Ελλάδα
  - 5 από τους μεγαλύτερους τηλεπικοινωνιακούς οργανισμούς της Μέσης Ανατολής
- **Πάνω από 80 μεγάλοι πελάτες ανά τον κόσμο**
  - Η μεγαλύτερη πετρελαϊκή εταιρία της Μέσης Ανατολής
  - Η μεγαλύτερη μη-πετρελαϊκή κατασκευαστική εταιρία της Μέσης Ανατολής
  - Η δεύτερη παγκοσμίως μεγαλύτερη εταιρεία ολοκληρωμένων συστημάτων τυχερών παιχνιδιών & διαχείρισης συναλλαγών
  - Μεγάλοι Δημόσιοι Οργανισμοί & Υπηρεσίες στην Ελλάδα και τη Μέση Ανατολή

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Παρεχόμενες Υπηρεσίες

## Στρατηγική Ασφάλειας Πληροφοριών

Information Security Management & Strategy

## Αρχιτεκτονική Ασφάλειας Πληροφοριακής Υποδομής

IT Security Architecture

## Έλεγχος Ασφάλειας Πληροφοριακής Υποδομής

Information Security Assurance

## Διαχείριση & Παρακολούθηση Υποδομής Ασφαλείας

Managed Security Services

## Εκπαίδευση στην Ασφάλεια Πληροφοριών

Information Security Training

## Έρευνα και Ανάπτυξη

Information Security R&D


encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Ατζέντα

- Εισαγωγή
- Το Πρότυπο PCI DSS
- Περιβάλλον Δεδομένων Καρτούχων
- Καθορισμός Εύρους Εφαρμογής
- Ανάλυση Απαιτήσεων Προτύπου
- Τεχνολογικοί Μηχανισμοί

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

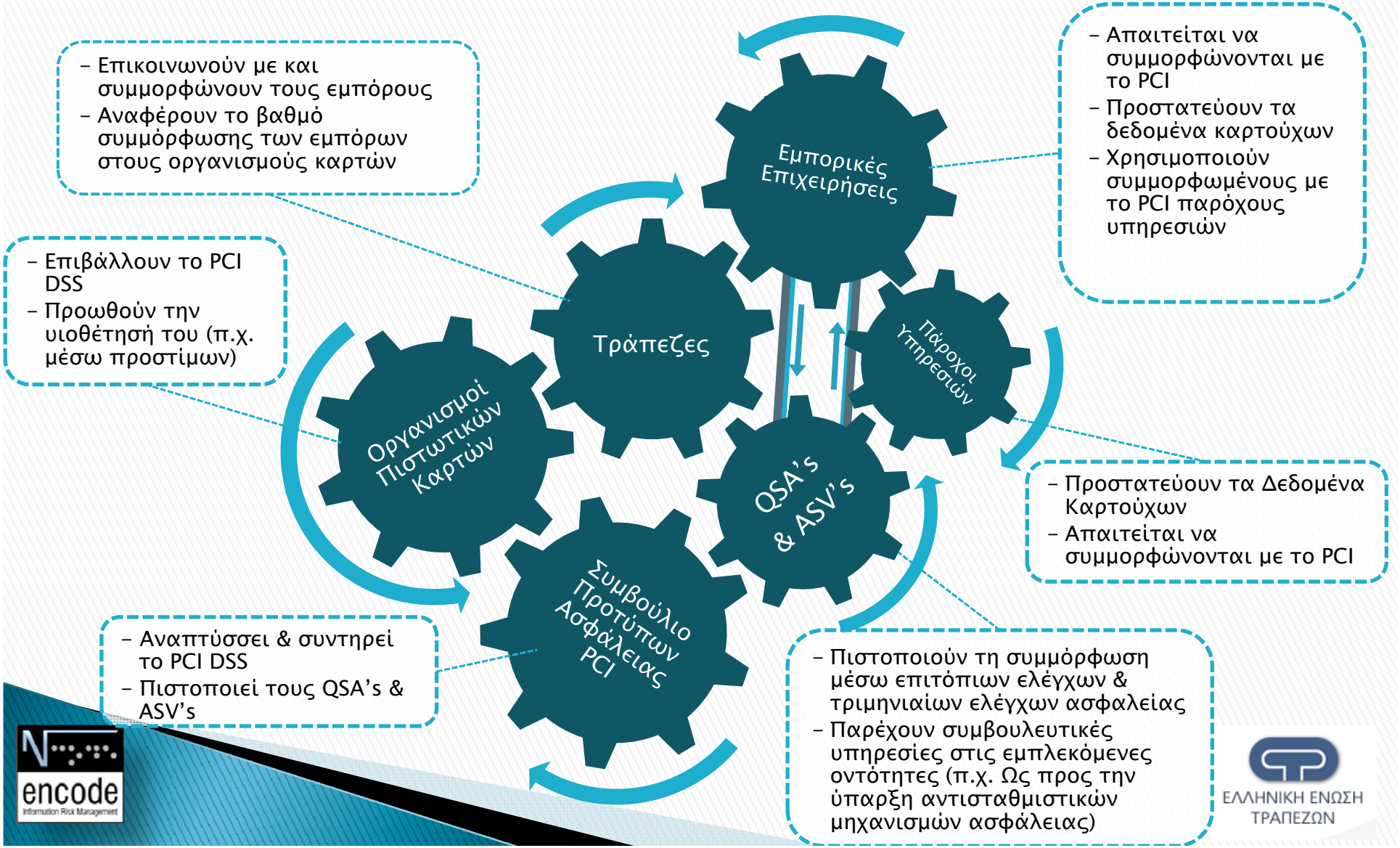
# Κανονιστική Απαίτηση ή Πρότυπο?

- Το PCI DSS αποτελεί συμβατική υποχρέωση μεταξύ των εμπορικών επιχειρήσεων και των Τραπεζών
- Αφορά σε όλες τις οντότητες που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα κατόχων καρτών πληρωμής καθώς και σε όλα τα κανάλια πληρωμών (ταχυδρομείο, τηλέφωνο, e-commerce / Internet)
- Καλύπτει τεχνικά και λειτουργικά τμήματα των συστημάτων που περιλαμβάνονται ή συνδέονται με τα δεδομένα των καρτούχων
- Μια εμπορική επιχείρηση που δέχεται ή επεξεργάζεται κάρτες πληρωμών, πρέπει να συμμορφωθεί με τις απαιτήσεις του Προτύπου Ασφάλειας Δεδομένων PCI
- Μη συμμόρφωση μπορεί να οδηγήσει σε πρόστιμα και ενδεχομένως στην απώλεια του δικαιώματος αποδοχής συναλλαγών με κάρτες πληρωμών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Εμπλεκόμενα Μέρη



# Βασικοί Όροι…

| | |
|---|---|
| Δεδομένα Καρτούχων | • Πλήρης Αριθμός Λογαριασμού (PAN),<br>• Όνομα Καρτούχου, Ημερομηνία Λήξης,<br>• Κωδικός Υπηρεσίας |
| Ευαίσθητα Δεδομένα Αυθεντικοποίησης | • Security code (CVV2/CVC2/CID),<br>• Δεδομένα Μαγνητικής Ταινίας,<br>• PIN/PIN block |
| Εμπορική Επιχείρηση | • Οντότητα η οποία λαμβάνει και χρησιμοποιεί δεδομένα καρτούχων ή ευαίσθητα δεδομένα αυθεντικοποίησης για δικούς της σκοπούς |
| Πάροχος Υπηρεσιών | • Επιχειρηματική οντότητα η οποία εμπλέκεται άμεσα στην επεξεργασία, αποθήκευση, ή μετάδοση δεδομένων καρτούχων για λογαριασμό τρίτων |

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# ...Βασικοί Όροι

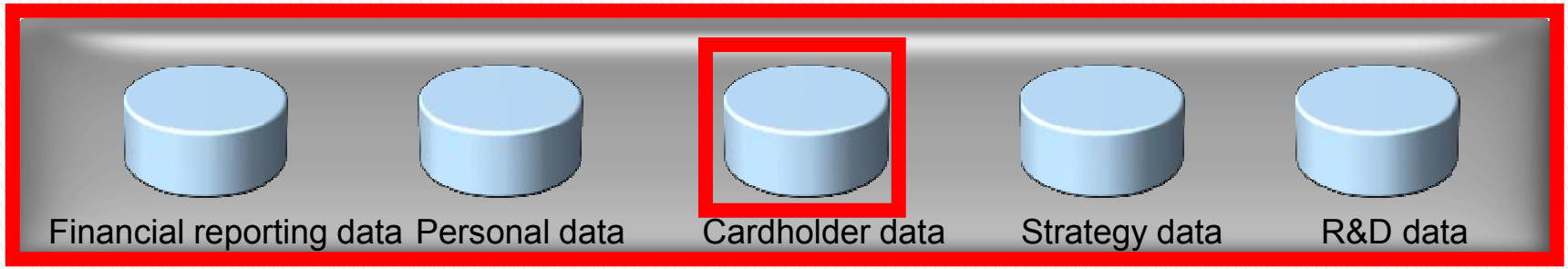
| | |
|---|---|
| Περιβάλλον Δεδομένων Καρτούχων | • Τμήμα του δικτύου όπου υπάρχουν δεδομένα καρτούχων ή ευαίσθητα δεδομένα αυθεντικοποίησης, καθώς και τα άμεσα συνδεδεμένα συστήματα ή τμήματα του δικτύου |
| Συστατικά Μέρη Συστήματος | • Κάθε συστατικό μέρος του δικτύου, διακομιστής ή εφαρμογή που συμπεριλαμβάνεται ή συνδέεται στο περιβάλλον δεδομένων καρτούχων |
| Συμμόρφωση | • Κάλυψη όλων των απαιτήσεων του PCI DSS<br>• Συνεχής διεργασία |
| Επικύρωση | • Επικυρώνει τη συμμόρφωση<br>• Διενεργείται σε τριμηνιαία και ετήσια βάση ανάλογα με τη δραστηριότητα |

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Απαιτήσεις Μηχανισμών Ασφάλειας

- Το πρότυπο καλύπτει ευρύ φάσμα μηχανισμών ασφάλειας:
  - Διοικητικούς Μηχανισμούς (πολιτικές και διαδικασίες),
  - Τεχνολογικούς Μηχανισμούς (passwords, κρυπτογράφηση δεδομένων),
  - Μηχανισμούς Φυσικής Ασφάλειας

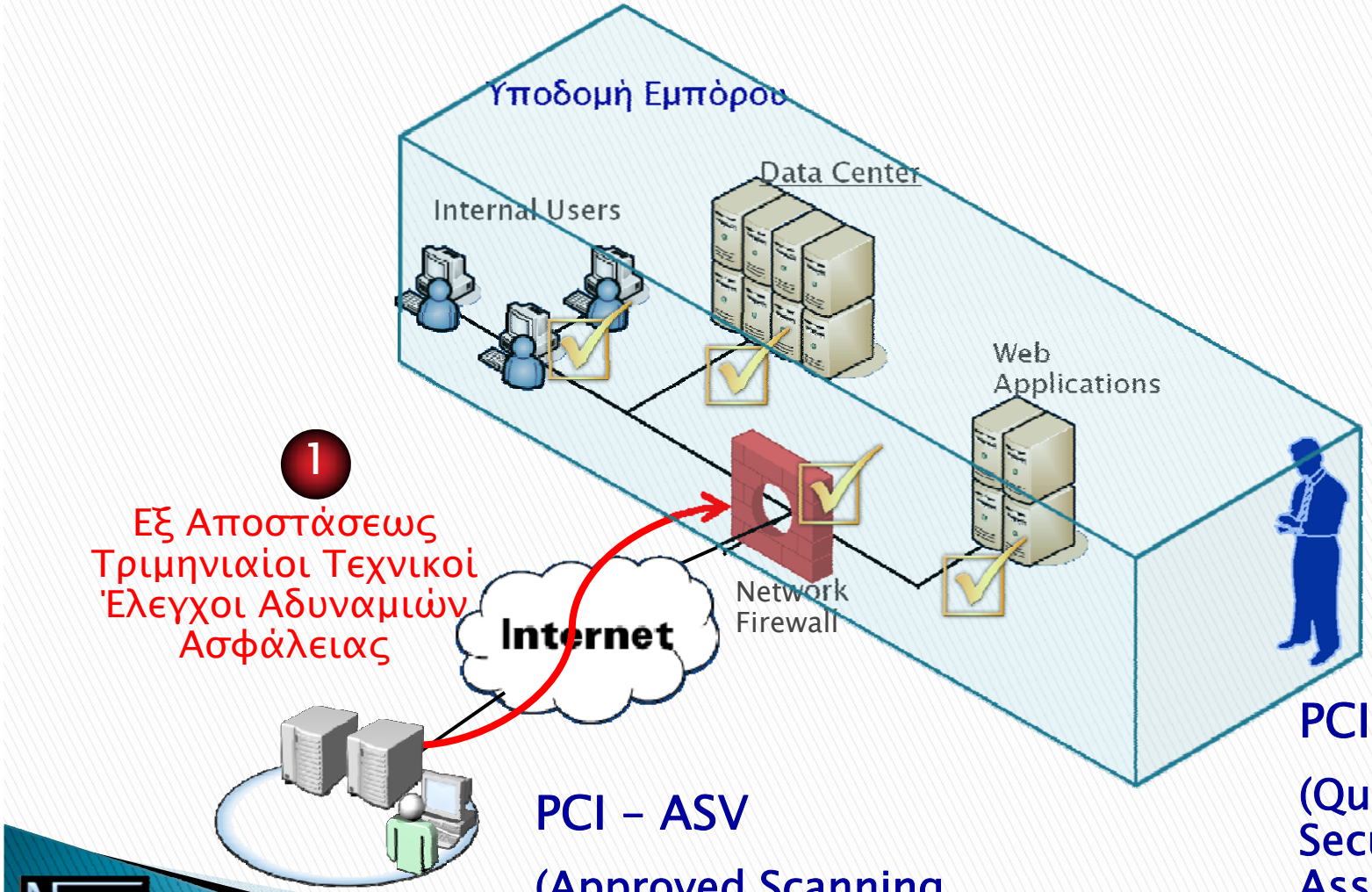



Παρότι το πρότυπο εστιάζει σε δεδομένα καρτών πληρωμής, η υλοποίηση των εν λόγω μηχανισμών προστασίας μπορεί να αυξήσει σημαντικά <u>το συνολικό επίπεδο ασφάλειας μιας επιχείρησης!</u>

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Αποδεκτές Μέθοδοι Επικύρωσης Συμμόρφωσης κατά PCI DSS




1

Εξ Αποστάσεως Τριμηνιαίοι Τεχνικοί Έλεγχοι Αδυναμιών Ασφάλειας

PCI – ASV

(Approved Scanning Vendor)

2

Ετήσιος Επιτόπιος Έλεγχος Συμμόρφωσης

(ή Αυτό-αξιολόγηση)

PCI – QSA

(Qualified Security Assessor)

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Επίπεδα Εμπορικών Επιχειρήσεων & Επικύρωση Συμμόρφωσης

| Επίπεδο | Περιγραφή | Επικύρωση Συμμόρφωσης |
|---|---|---|
| 1 | ▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών, με περισσότερες από **6.000.000 VISA/MasterCard ή 2.500.000 AMEX** συναλλαγές το χρόνο.<br>▪ **Επιχειρήσεις οι οποίες έχουν υποστεί διαρροή δεδομένων** καρτών.<br>▪ Εμπορικές επιχειρήσεις οι οποίες κατηγοριοποιούνται κατά την κρίση οποιασδήποτε εταιρίας πιστωτικών καρτών ως Επιπέδου 1. | ▪ Ετήσιος Επιτόπιος Έλεγχος Συμμόρφωσης από Πιστοποιημένο Αξιολογητή Ασφάλειας [**Qualified Security Assessor (QSA) Audit**]<br>▪ Τριμηνιαίοι Τεχνικοί Έλεγχοι Αδυναμιών Ασφάλειας από Πιστοποιημένο **ASV (Approved Scanning Vendor)** |
| 2 | ▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών, με **1.000.000 έως 6.000.000 VISA/MasterCard ή 50.000 έως 2.500.000 AMEX** συναλλαγές το χρόνο. | ▪ Συμπλήρωση Ερωτηματολογίου Αυτό-Αξιολόγησης PCI DSS Ετησίως<br>▪ Τριμηνιαίοι Τεχνικοί Έλεγχοι Αδυναμιών Ασφάλειας από Πιστοποιημένο ASV |
| 3 | ▪ Επιχειρήσεις με **20.000 έως 1.000.000 VISA/MasterCard** συναλλαγές μέσω καναλιών **ηλεκτρονικού εμπορίου** το χρόνο.<br>▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών, με **λιγότερες από 50.000 AMEX** συναλλαγές το χρόνο. | ▪ Συμπλήρωση Ερωτηματολογίου Αυτό-Αξιολόγησης PCI DSS Ετησίως<br>▪ Τριμηνιαίοι Τεχνικοί Έλεγχοι Αδυναμιών Ασφάλειας από Πιστοποιημένο ASV |
| 4 | ▪ Επιχειρήσεις με **λιγότερες από 20.000 VISA/MasterCard** συναλλαγές μέσω καναλιών **ηλεκτρονικού εμπορίου** το χρόνο.<br>▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών, με **λιγότερες από 1.000.000 VISA/MasterCard** συναλλαγές το χρόνο. | ▪ Συμπλήρωση Ερωτηματολογίου Αυτό-Αξιολόγησης PCI DSS Ετησίως<br>▪ Τριμηνιαίοι Τεχνικοί Έλεγχοι Αδυναμιών Ασφάλειας από Πιστοποιημένο ASV (προτεινόμενο) |

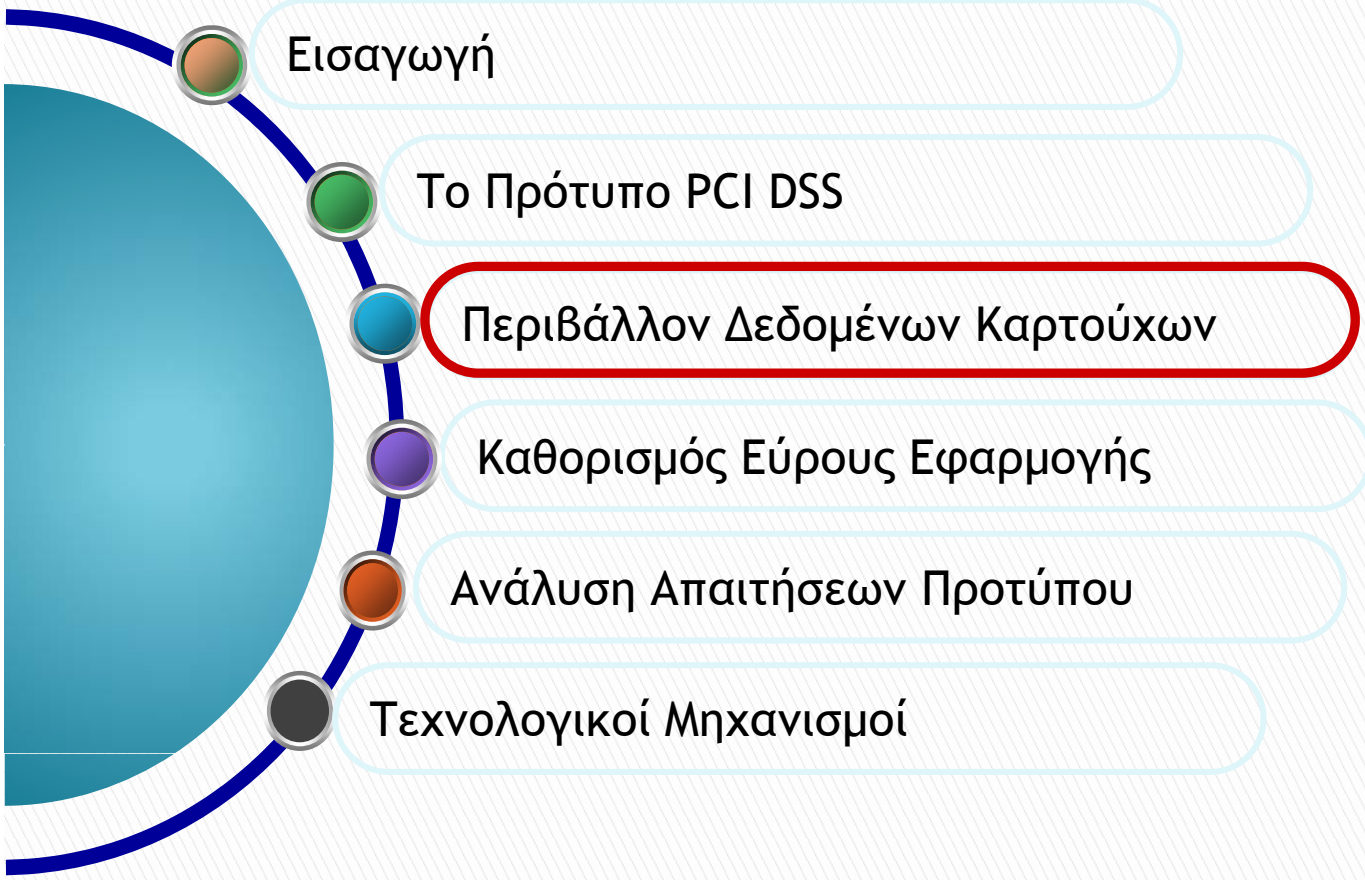
# Ενότητες του Προτύπου

- Εγκατάσταση και Συντήρηση Ασφαλούς Δικτύου
- Προστασία Δεδομένων Καρτούχων
- Συντήρηση Προγράμματος Διαχείρισης Αδυναμιών Ασφάλειας
- Υλοποίηση Ισχυρών Μέτρων Ελέγχου Πρόσβασης
- Περιοδική Παρακολούθηση και Έλεγχος Δικτύων
- Τήρηση Πολιτικής Ασφάλειας Πληροφοριών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

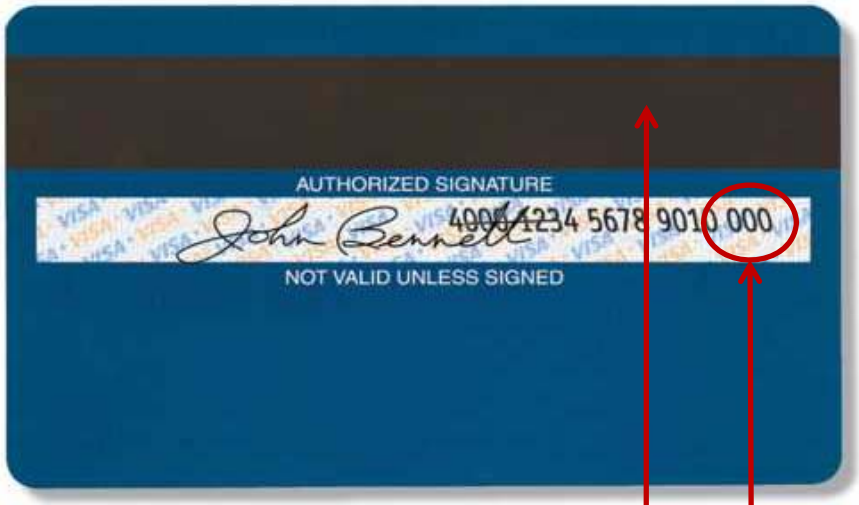
# Ατζέντα




encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Τύποι Δεδομένων


PAN: Μοναδικός αριθμός κάρτας πληρωμών που προσδιορίζει τον εκδότη της κάρτας και το συγκεκριμένο λογαριασμό του καρτούχου

CVV2:τριψήφιος κωδικός

Chip

Ημερομηνία Λήξης

Δεδομένα Μαγνητικής Ταινίας (track data): Δεδομένα που έχουν κωδικοποιηθεί στη μαγνητική ταινία ή στο chip και χρησιμοποιούνται π.χ. για την πιστοποίηση της ταυτότητας του κατόχου κατά τη διάρκεια της συναλλαγής

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Τύποι Δεδομένων & Απαιτήσεις Ασφάλειας

| | Τύπος Δεδομένων | Επιτρέπεται η αποθήκευσή του; | Απαιτείται η προστασία του; | Απαιτείται κρυπτογρ; (Απ. 3.4) |
|---|---|---|---|---|
| Δεδομένα Καρτούχων | PAN | Ναι | Ναι | Ναι |
| | Όνομα Καρτούχου* | Ναι | Ναι* | Όχι |
| | Service Code* | Ναι | Ναι* | Όχι |
| | Ημερομηνία Λήξης* | Ναι | Ναι* | Όχι |
| Ευαίσθητα Δεδομένα Αυθεντικοποίησης** | Full Magnetic Stripe | Όχι | M/E | M/E |
| | CVC2/CVV2/CID | Όχι | M/E | M/E |
| | PIN / PIN Block | Όχι | M/E | M/E |

M/E Μη Εφαρμόσιμο.

* Πρέπει να προστατεύονται αν είναι αποθηκευμένοι σε συνδυασμό με το PAN. Η προστασία αυτή πρέπει να είναι εναρμονισμένη με τις απαιτήσεις του προτύπου για τη γενική προστασία του περιβάλλοντος καρτούχων.

** Δεν επιτρέπεται να αποθηκεύονται μετά την έγκριση της συναλλαγής, ακόμα κι αν είναι κρυπτογραφημένα.

Απ. 3.4 Το PAN πρέπει να είναι μη αναγνώσιμο (π.χ. μέσω χρήσης one-way hash functions, truncation, ισχυρή κρυπτογράφηση).

encode
Information Risk Management

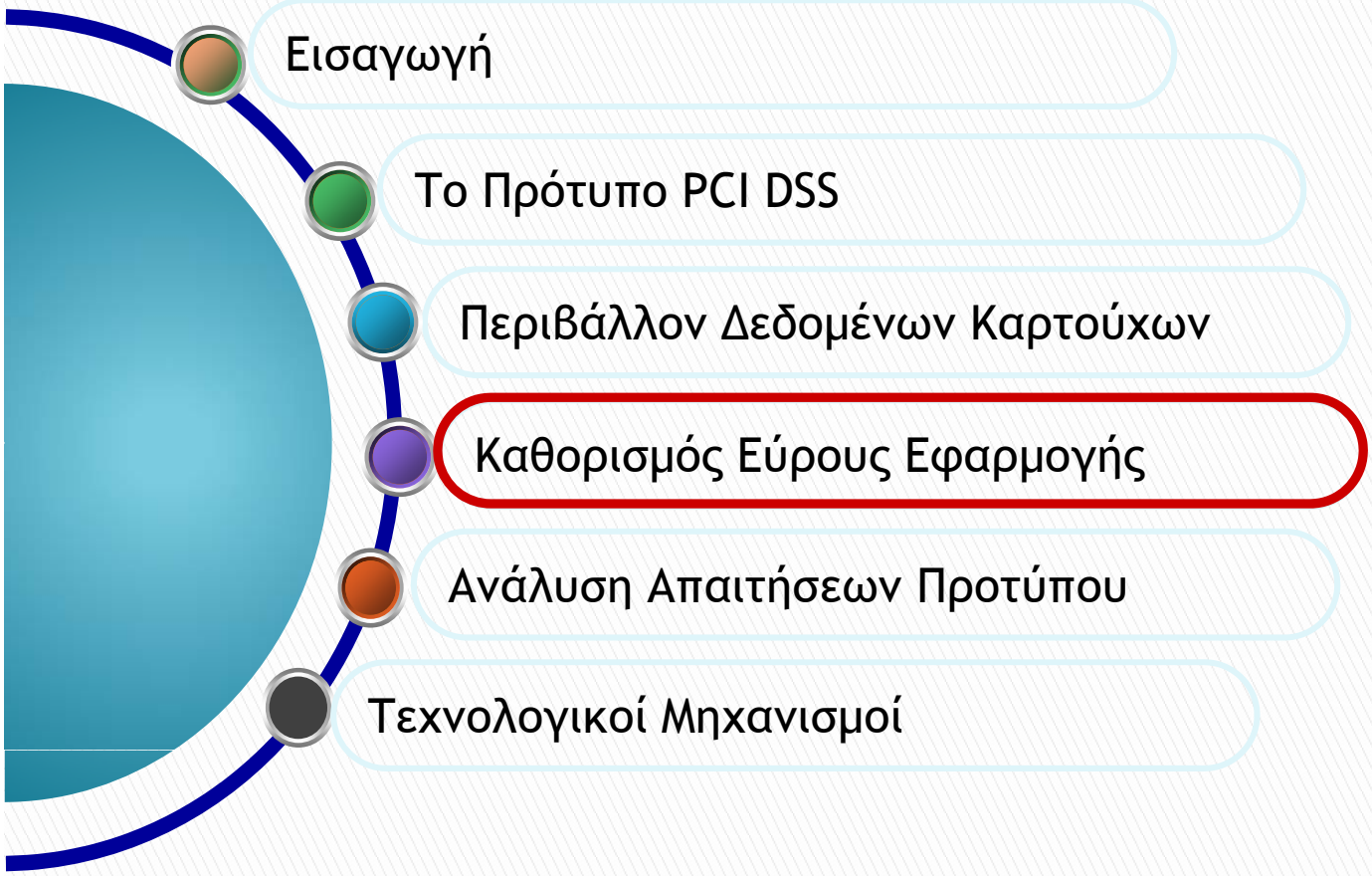
ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Περιβάλλον Δεδομένων Καρτούχων

- Αποτελεί τμήμα του δικτύου στο οποίο βρίσκονται δεδομένα καρτούχων, ή ευαίσθητα δεδομένα αυθεντικοποίησης

- Όλα τα συστήματα τα οποία συμπεριλαμβάνονται στο ή συνδέονται άμεσα με το περιβάλλον δεδομένων καρτούχων πρέπει να συμπεριληφθούν στο εύρος εφαρμογής του προτύπου, π.χ.:
  - Δικτυακές συσκευές, όπως firewalls, switches, routers, wireless access points και άλλες συσκευές ασφάλειας (π.χ. IDSs)
  - Servers, όπως Mainframes, Web, Database, Authentication, Mail, Proxy, Domain Name Service (DNS)
  - Εφαρμογές: όλες οι εμπορικές εφαρμογές ή / και οι εφαρμογές που έχουν αναπτυχθεί εσωτερικά

# Ατζέντα




encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Καθορισμός Εύρους Εφαρμογής…

- Το στάδιο του καθορισμού εύρους εφαρμογής (scoping) είναι ιδιαίτερης σημασίας
  - επιτρέπει στην εμπορική επιχείρηση, σε συνεργασία με την εταιρία QSA, να εντοπίσει επακριβώς εντός του περιβάλλοντός της, τα σημεία στα οποία αποθηκεύονται, επεξεργάζονται ή / και μεταδίδονται δεδομένα καρτούχων
  - επηρεάζει άμεσα την πληρότητα αλλά και τη διάρκεια που απαιτείται για την διαδικασία πιστοποίησης μιας εμπορικής επιχείρησης κατά το πρότυπο PCI DSS

# ...Καθορισμός Εύρους Εφαρμογής

- Συχνά ερωτήματα που δημιουργούνται:
  - Περιλαμβάνονται και τα έντυπα στο εύρος εφαρμογής του προτύπου;
  - Ποια συστήματα και διαδικασίες πρέπει να συμμορφώνονται με τις απαιτήσεις του προτύπου;
  - Υπάρχει τρόπος να περιοριστεί το εύρος πιστοποίησης διαχωρίζοντας αυτά τα συστήματα;
  - Τι ισχύει για τα συστήματα εκείνα η ευθύνη λειτουργίας των οποίων έχει ανατεθεί (outsource) σε παρόχους υπηρεσιών, όπως για παράδειγμα σε εταιρίες επεξεργασίας καρτών πληρωμής;

# Γενικές Κατευθύνσεις …

- Πλήρης κατανόηση των επιχειρηματικών αναγκών και των διαδικασιών αναφορικά με την αποθήκευση, την επεξεργασία και την μετάδοση των δεδομένων καρτούχων

- Προσδιορισμός του κύκλου ζωής διαχείρισης των δεδομένων καρτούχων (Cardholder Data Lifecycle Management) μέσω της καταγραφής και της ανάλυσης των παρακάτω:
  - Τρόποι συναλλαγής των καρτούχων με την εμπορική επιχείρηση σε θέματα πληρωμών με κάρτες
  - Επιχειρηματικές διαδικασίες (τεκμηριωμένες ή μη) που αφορούν στη διαχείριση των δεδομένων καρτούχων
  - Εμπλεκόμενα πληροφοριακά συστήματα
  - Προσωπικό της εμπορικής επιχείρησης ή τρίτων με φυσική, ή ηλεκτρονική πρόσβαση στα δεδομένα καρτούχων

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# ...Γενικές Κατευθύνσεις

- Κατανόηση & αποτύπωση των ροών δεδομένων και διαδικασιών που σχετίζονται με τα δεδομένα καρτούχων
  - σημεία του περιβάλλοντος (φυσικά και / ή ηλεκτρονικά) στα οποία υπάρχουν δεδομένα καρτούχων,
  - άτομα τα οποία έχουν πρόσβαση στα δεδομένα
  - επιχειρηματικές διαδικασίες που συνδέονται με την επεξεργασία, την αποθήκευση και την μετάδοση των δεδομένων καρτούχων

- Συνεισφορά διαφόρων μελών του οργανισμού
  - επιχειρηματικοί ιδιοκτήτες εφαρμογών
  - τεχνικοί υπεύθυνοι εφαρμογών,
  - χρήστες εφαρμογών,
  - Διεύθυνση Πληροφορικής,
  - Διεύθυνση Φυσικής Ασφάλειας κ.ά.

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

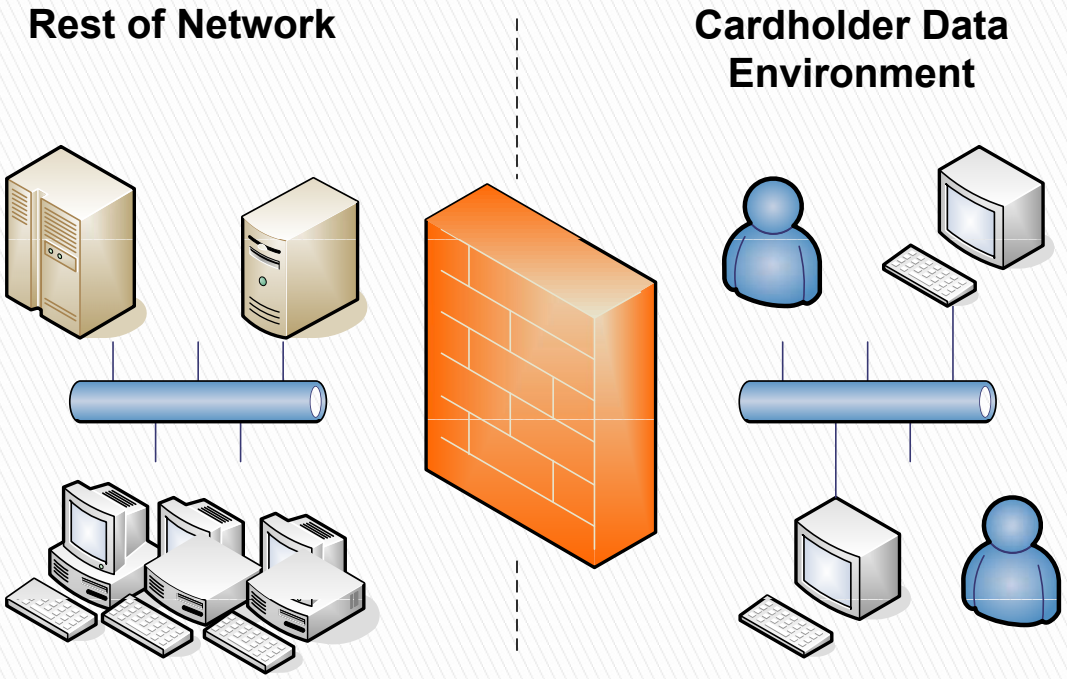
# Μέθοδοι Περιορισμού του Εύρους Εφαρμογής

- Ο επαρκής δικτυακός διαχωρισμός (network segmentation) μπορεί να μειώσει αισθητά το εύρος του περιβάλλοντος δικτύου που πρέπει να ελεγχθεί ώστε να πιστοποιηθεί

- Απομόνωση συστημάτων που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα καρτούχων, μέσω
  - Συστημάτων firewall
  - Διαμόρφωσης VLANs με ACLs
  - Διαμόρφωσης logical partitions κ.ά.

- Οι μηχανισμοί διαχωρισμού πρέπει να αξιολογούνται ως προς την αποτελεσματικότητά τους από QSA, προκειμένου να μειωθεί το απαιτούμενο εύρος πιστοποίησης

# Παραδείγματα Περιορισμού του Εύρους Εφαρμογής

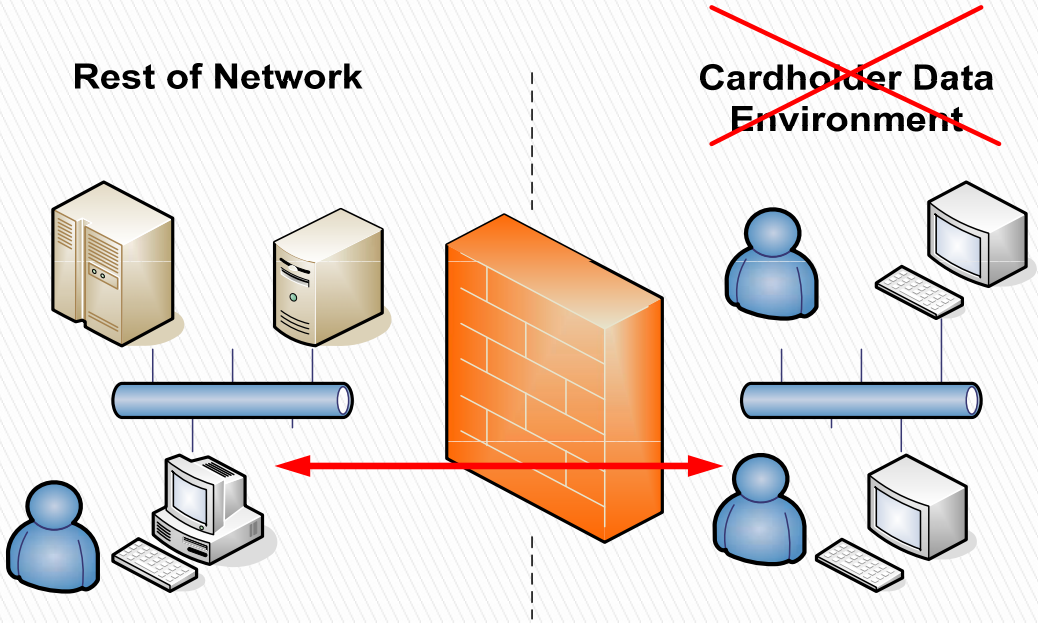



- Αν το υπόλοιπο δίκτυο είναι διαχωρισμένο από το περιβάλλον δεδομένων καρτούχων, μέσω ενός firewall, που δεν επιτρέπει την επικοινωνία του ενός δικτύου με το CDE, τότε το πρώτο εξαιρείται από το πεδίο εφαρμογής

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# ...Παραδείγματα Περιορισμού Εύρους




- Αν ένας σταθμός εργασίας από το υπόλοιπο δίκτυο μπορεί να αποκτήσει πρόσβαση σε δεδομένα καρτούχων, ώστε να προσχωρήσει σε επεξεργασία, μετάδοση ή αποθήκευση, τότε θεωρείται ότι βρίσκεται εντός του εύρους εφαρμογής
- Αν ο σταθμός εργασίας βρίσκεται εντός εύρους εφαρμογής, όλα τα άλλα συστατικά μέρη του δικτύου τα οποία δεν είναι διαχωρισμένα από το PC, θεωρείται ότι βρίσκονται εντός του εύρους εφαρμογής

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Ατζέντα

- Εισαγωγή
- Το Πρότυπο PCI DSS
- Περιβάλλον Δεδομένων Καρτούχων
- Καθορισμός Εύρους Εφαρμογής
- Ανάλυση Απαιτήσεων Προτύπου
- Τεχνολογικοί Μηχανισμοί

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Απαιτήσεις του Προτύπου


1. Εγκατάσταση και συντήρηση firewalls για την προστασία των δεδομένων των καρτούχων

2. Αποφυγή χρήσης προκαθορισμένων από τους κατασκευαστές κωδικών πρόσβασης και ρυθμίσεων ασφάλειας

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Εγκατάσταση & Συντήρηση Firewalls

- Ανάπτυξη προτύπου ρυθμίσεων firewall & Router:
  - Επίσημη διαδικασία έγκρισης και ελέγχου όλων των εξωτερικών δικτυακών συνδέσεων και αλλαγών στις ρυθμίσεις του firewall
  - Ενημερωμένο διάγραμμα δικτύου με τις συνδέσεις με δεδομένα καρτούχων, συμπεριλαμβανομένων και των ασύρματων δικτύων
  - Ύπαρξη firewall σε κάθε διαδικτυακή σύνδεση και μεταξύ των DMZs και του εσωτερικού δικτύου
  - Περιγραφή ρόλων και καθηκόντων για τη λογική διαχείριση των δικτυακών στοιχείων (network components)
  - Καταγεγραμμένη λίστα των δικτυακών υπηρεσιών και των θυρών που είναι απαραίτητες για την ορθή λειτουργία των συστημάτων

# Εγκατάσταση & Συντήρηση Firewalls

- Αιτιολόγηση και τεκμηρίωση χρήσης για κάθε πρωτόκολλο (π.χ. HTTP, SSL, SSH κλπ.)
- Αιτιολόγηση και τεκμηρίωση των μηχανισμών προστασίας που εφαρμόζονται για κάθε πρωτόκολλο το οποίο ενδέχεται να έχει ιστορικά κενά ασφάλειας (π.χ. FTP) και επιτρέπεται η μετάδοση του
- Επισκόπηση των κανόνων (rule sets) των firewall και των router σε εξαμηνιαία βάση

# Εγκατάσταση & Συντήρηση Firewalls

- Δημιουργία ρυθμίσεων firewall που να απαγορεύει όλη την επικοινωνία από μη έμπιστα δίκτυα και servers, εκτός από τα απαραίτητα πρωτόκολλα για το περιβάλλον δεδομένων καρτούχων
- Ρύθμιση firewall ώστε να περιορίζονται οι συνδέσεις μεταξύ servers, που μπορούν να προσπελαστούν δημόσια, και οποιουδήποτε συστήματος που αποθηκεύει στοιχεία καρτούχων, συμπεριλαμβανομένων και όλων των συνδέσεων από ασύρματα δίκτυα
- Απαγόρευση απευθείας πρόσβασης μεταξύ εξωτερικών δημόσιων δικτύων (π.χ. Internet) και οποιουδήποτε μέρους των συστημάτων τα οποία αποθηκεύουν δεδομένα καρτούχων (π.χ. βάσεις δεδομένων)
- Υλοποίηση 'IP Masquerading' για την αποφυγή γνωστοποίησης εσωτερικών διευθύνσεων της επιχείρησης

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Αποφυγή Χρήσης Προκαθορισμένων Ρυθμίσεων Ασφάλειας

- Αλλαγή προκαθορισμένων από τους κατασκευαστές ρυθμίσεων πριν την εγκατάστασή τους στο δίκτυο (π.χ. συνθηματικά, SNMP community strings και απαλοιφή των μη απαραίτητων λογαριασμών)
  - κλειδιά WEP, SSID, κωδικοί πρόσβασης, SNMP community strings
  - απενεργοποίηση εκπομπής SSID , ενεργοποίηση τεχνολογιών κρυπτογράφησης και αυθεντικοποίησης (WPA, WPA2)
- Κρυπτογράφηση της δικτυακής επικοινωνίας που χρησιμοποιείται για την εκτός-κονσόλας πρόσβαση των διαχειριστών στα συστήματα του CDE

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Αποφυγή Χρήσης Προκαθορισμένων Ρυθμίσεων Ασφάλειας

- Ανάπτυξη προτύπων ενίσχυσης του επιπέδου ασφάλειας πληροφοριών
  - Αντιμετώπιση γνωστών αδυναμιών ασφάλειας
  - Υλοποίηση μόνο μιας κύριας λειτουργίας σε κάθε server (π.χ. web servers, database servers, DNS)
  - Απενεργοποίηση μη απαραίτητων και μη ασφαλών υπηρεσιών & πρωτοκόλλων
  - Διαμόρφωση παραμέτρων ασφάλειας συστήματος ώστε να ελαχιστοποιείται η δυνατότητα μη αποδεκτής χρήσης
  - Απενεργοποίηση περιττών λειτουργιών (π.χ. scripts, drivers, υποσυστήματα, συστήματα αρχείων) και περιττών Web servers

# Απαιτήσεις του Προτύπου


3 Προστασία αποθηκευμένων δεδομένων καρτούχων

4 Κρυπτογράφηση δεδομένων καρτούχων κατά τη μετάδοσή τους σε ανοικτά, δημόσια δίκτυα

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Προστασία Αποθηκευμένων Δεδομένων Καρτούχων

- Αποθήκευση μόνο των απαραίτητων δεδομένων καρτούχων

- Ανάπτυξη πολιτικής διατήρησης και καταστροφής δεδομένων
  - καθορίζει τον όγκο των αποθηκευμένων δεδομένων
  - την περίοδο τήρησης βάσει επιχειρηματικών / νομικών ή/και κανονιστικών απαιτήσεων

- Απαγόρευση αποθήκευσης ευαίσθητων δεδομένων αυθεντικοποίησης μετά την έγκριση (ακόμη και αν είναι κρυπτογραφημένα)

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Προστασία Αποθηκευμένων Δεδομένων Καρτούχων

- Ευαίσθητα δεδομένα αυθεντικοποίησης:
  - Απαγόρευση αποθήκευσης πλήρους περιεχομένου των δεδομένων που περιέχονται σε κάθε ίχνος της μαγνητικής ταινίας / chip
  - Απαγόρευση αποθήκευσης της αριθμητικής τιμής επικύρωσης των καρτών (CVV2, CVC2, CID)
  - Απαγόρευση αποθήκευσης του αριθμού PIN ή του PIN block

# Προστασία Αποθηκευμένων Δεδομένων Καρτούχων

- Απόκρυψη (masking) του PAN
- Αποθήκευση PAN σε μη αναγνώσιμη μορφή σε οποιοδήποτε μέσο
  - φορητά ψηφιακά μέσα μεταφοράς
  - σε αντίγραφα ασφαλείας,
  - σε αρχεία καταγραφής (Logs)
    - (hash functions – hashed indexes)
    - Αποκοπή πληροφορίας(truncation)
    - Index tokens και pads
    - Ισχυρή κρυπτογράφηση και εφαρμογή διαδικασίας διαχείρισης κρυπτογραφικών κλειδιών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Προστασία Αποθηκευμένων Δεδομένων Καρτούχων

- Πλήρης καταγραφή και υλοποίηση της διαδικασίας διαχείρισης κρυπτογραφικών κλειδιών τα οποία χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων καρτούχων. Η διαδικασία πρέπει να περιλαμβάνει τα ακόλουθα:
  - Δημιουργία ισχυρών κλειδιών
  - Ασφαλή διακίνηση κλειδιών
  - Ασφαλή αποθήκευση κλειδιών
  - Περιοδικές αλλαγές κλειδιών
  - Καταστροφή παλαιών κλειδιών
  - Διαχωρισμός γνώσης και υλοποίηση διπλού ελέγχου (dual control) των κλειδιών
  - …

# Κρυπτογράφηση Δεδομένων Καρτούχων

- Χρήση ισχυρών πρωτοκόλλων ασφαλείας και αλγορίθμων κρυπτογράφησης (SSL, TLS, IPSEC, AES, 3DES κλπ.) κατά τη μετάδοσή των δεδομένων σε ανοικτά, δημόσια δίκτυα (Internet, 802.11x, GSM, GPRS)
  - Για την μετάδοση δεδομένων μέσω ασύρματων δικτύων απαιτείται κρυπτογράφηση με χρήση τεχνολογιών προστασίας όπως
    - WPA ή WPA2,
    - IPSEC VPN ή SSL/TLS.
  - Δεν επιτρέπεται η χρήση του πρωτοκόλλου WEP σε νέες εγκαταστάσεις ασύρματων δικτύων έπειτα από τις 31 Μαρτίου 2009
  - Δεν επιτρέπεται η χρήση του πρωτοκόλλου WEP σε υφιστάμενες εγκαταστάσεις ασύρματων δικτύων έπειτα από τις 30 Ιουνίου 2010

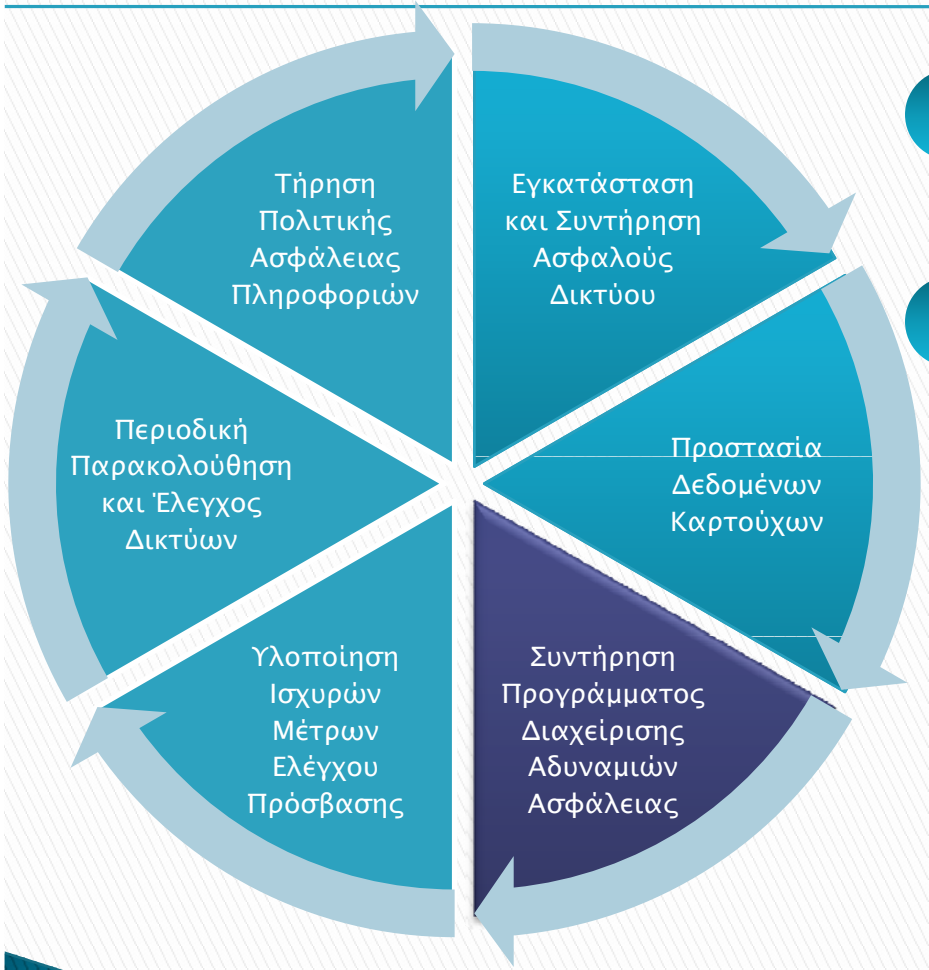
encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Κρυπτογράφηση Δεδομένων Καρτούχων

- Σε περίπτωση χρήσης WEP,
  - Χρήση κλειδιού ελαχίστου μήκους 104-bit
  - Μήκος IV 24-bit.
  - Περιορισμός της πρόσβασης βάσει διευθύνσεων MAC
  - Περιοδική αλλαγή κλειδιών (WEP key rotation)
  - Χρήση επιπρόσθετων μηχανισμών κρυπτογράφησης (π.χ. SSL, IPSec κλπ.)
- Απαγόρευση αποστολής μη κρυπτογραφημένων PAN μέσω email, Chat, IRC κλπ.

# Απαιτήσεις του Προτύπου




5 Χρήση και περιοδική ενημέρωση λογισμικού προστασίας από κακόβουλο λογισμικό (anti-virus)

6 Ανάπτυξη και συντήρηση ασφαλών συστημάτων και εφαρμογών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Χρήση & Περιοδική Ενημέρωση anti-virus

- Εγκατάσταση προγραμμάτων anti-virus σε όλα τα συστήματα τα οποία «προσβάλλονται» συνήθως από ιούς (Windows Servers / PCs)
  - Επιβεβαίωση ότι τα προγράμματα anti-virus είναι ικανά να εντοπίσουν, να απομακρύνουν και να προστατεύσουν από όλες τις μορφές γνωστού κακόβουλου λογισμικού, συμπεριλαμβανομένου Spyware και Adware

- Επιβεβαίωση ότι όλοι οι μηχανισμοί anti-virus είναι ενημερωμένοι, ενεργοί και παράγουν αρχεία καταγραφής (logs)

# Ανάπτυξη & Συντήρηση ασφαλών Συστημάτων & Εφαρμογών

- Σε όλα τα συστατικά του συστήματος και στο λογισμικό είναι εγκατεστημένα όλα τα τελευταία πακέτα διόρθωσης αδυναμιών ασφάλειας (security patches)
- Διαδικασία αναγνώρισης νέων ευπαθειών ασφάλειας πληροφοριών
- Ενημέρωση των προτύπων ώστε να συμπεριλαμβάνουν όλα τα τελευταία θέματα ευπαθειών ασφάλειας πληροφοριών
- Η ανάπτυξη εφαρμογών θα πρέπει να βασίζεται σε βέλτιστες πρακτικές ασφάλειας κατά την ανάπτυξη λογισμικού

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Ανάπτυξη & Συντήρηση ασφαλών Συστημάτων & Εφαρμογών

- Εφαρμογή διαδικασιών διαχείρισης μεταβολών σε όλες τις αλλαγές ρυθμίσεων στα συστήματα και στο λογισμικό

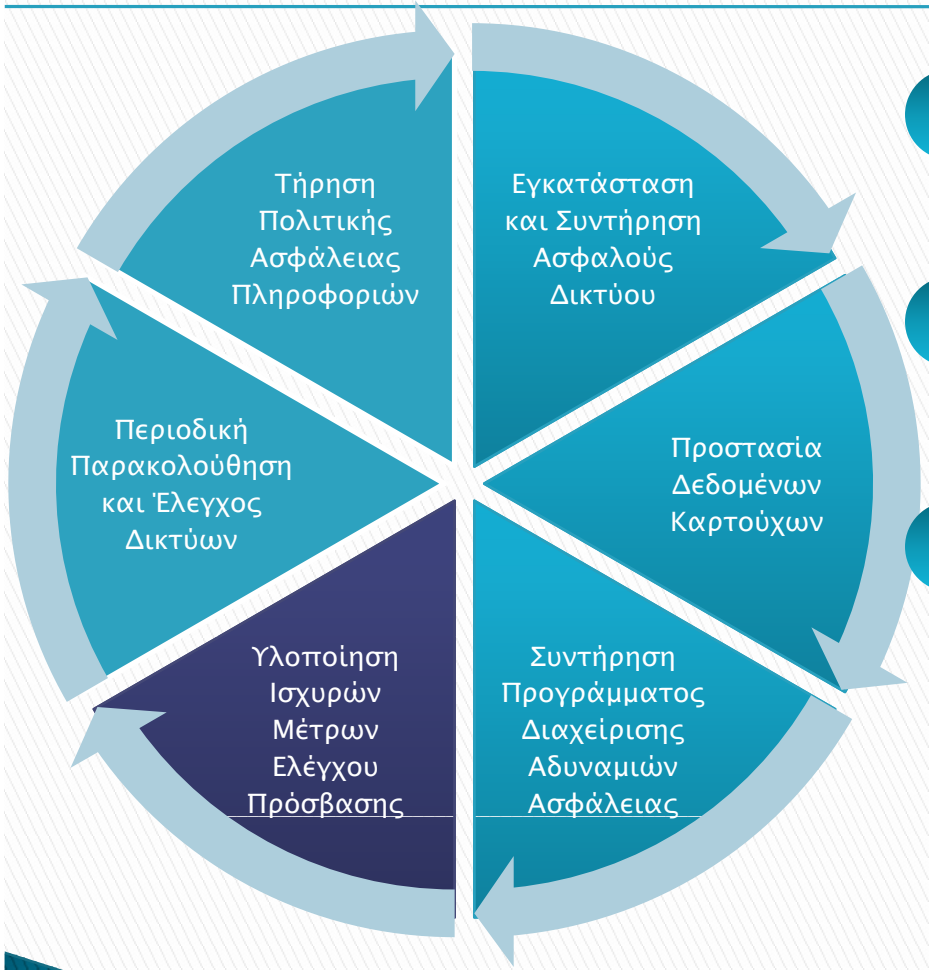
- Ανάπτυξη διαδικτυακών εφαρμογών σύμφωνα με οδηγίες ασφαλούς προγραμματισμού,
  - Έλεγχος του κώδικα με σκοπό την αναγνώριση ευπαθειών στον κώδικα
  - Προληπτική αντιμετώπιση εμφάνισης λαθών στον κώδικα

- Επιβεβαίωση ότι οι εφαρμογές web, προστατεύονται από γνωστές μορφές διακύβευσης της ασφάλειας τους μέσω,
  - ελέγχου του κώδικα από πάροχο υπηρεσιών ασφάλειας
  - εγκατάστασης web application firewall

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Απαιτήσεις του Προτύπου




7 Περιορισμός πρόσβασης στα δεδομένα καρτούχων βάσει επιχειρηματικής ανάγκης γνώσης (need-to-know)

8 Απόδοση μοναδικής ταυτότητας χρήστη σε κάθε πρόσωπο με πρόσβαση σε υπολογιστικά συστήματα

9 Περιορισμός φυσικής πρόσβασης στα δεδομένα καρτούχων

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Περιορισμός Πρόσβασης Βάσει Επιχειρηματικής Ανάγκης Γνώσης

- Περιορισμός πρόσβασης στους πόρους των υπολογιστικών συστημάτων και στις πληροφορίες των κατόχων καρτών μόνο στο προσωπικό που απαιτείται για την ολοκλήρωση της εργασία του

- Εγκαθίδρυση μηχανισμού για συστήματα με πολλαπλούς χρήστες ο οποίος περιορίζει την πρόσβαση βάσει ανάγκης γνώσης του κάθε χρήστη
  - Η απαιτούμενη τακτική προϋποθέτει την εφαρμογή της αρχής καθολικής απαγόρευσης της πρόσβασης (default deny)

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Απόδοση Μοναδικής Ταυτότητας Χρήστη

- Αυθεντικοποίηση χρηστών μέσω μοναδικής ταυτότητας χρήστη πριν την απόκτηση πρόσβασης στα συστατικά των συστημάτων ή στα στοιχεία καρτούχων

- Υλοποίηση μεθόδων αυθεντικοποίησης χρηστών:
  - Κωδικός πρόσβασης
  - Tokens (SecureID, ψηφιακά πιστοποιητικά κλπ.)
  - Βιομετρικά συστήματα

- Υλοποίηση αυθεντικοποίησης δύο παραγόντων για απομακρυσμένη πρόσβαση στο CDE
  - RADIUS, TACACS με tokens
  - SSL/TLS ή IPSEC VPN με ξεχωριστά πιστοποιητικά κλπ.

# Απόδοση Μοναδικής Ταυτότητας Χρήστη

- Κρυπτογράφηση όλων συνθηματικών κατά την μετάδοση και την αποθήκευσή τους σε όλα τα συστατικά του συστήματος

- Διασφάλιση αυθεντικοποίησης και διαχείρισης συνθηματικών για τους απλούς χρήστες και τους διαχειριστές των συστημάτων του CDE, σύμφωνα με επίσημες και καταγεγραμμένες διαδικασίες διαχείρισης της πρόσβασης των χρηστών / διαχειριστών και διαχείρισης συνθηματικών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Περιορισμός Φυσικής Πρόσβασης

- Χρήση κατάλληλων ελεγκτικών μηχανισμών φυσικής πρόσβασης στα συστήματα τα οποία αποθηκεύουν, επεξεργάζονται και μεταδίδουν στοιχεία καρτούχων
- Ανάπτυξη διαδικασιών οι οποίες υποστηρίζουν τη διάκριση μεταξύ υπαλλήλων και επισκεπτών, ειδικότερα σε περιοχές στις οποίες υπάρχει πρόσβαση σε πληροφορίες που αφορούν στους καρτούχους.
- Χρήση αρχείου καταγραφής επισκεπτών
- Αποθήκευση των αντιγράφων ασφάλειας σε ασφαλή τοποθεσία
- Φυσική προστασία των έγγραφων και ηλεκτρονικών μέσων αποθήκευσης τα οποία περιέχουν δεδομένα καρτούχων.

# Περιορισμός Φυσικής Πρόσβασης

- Διενέργεια αυστηρού έλεγχου στην εσωτερική ή εξωτερική διανομή οποιουδήποτε τύπου μέσων, τα οποία περιέχουν δεδομένα καρτούχων
- Υλοποίηση διαδικασιών που διασφαλίζουν ότι έχει δοθεί έγκρισης της «διοίκησης» πριν τη μετακίνηση οποιουδήποτε μέσου από μια ασφαλή τοποθεσία
- Διενέργεια αυστηρού έλεγχου των μεθόδων αποθήκευσης και της προσβασιμότητας των μέσων, που περιέχουν δεδομένα καρτούχων
- Ασφαλής καταστροφή των μέσων που περιέχουν δεδομένα καρτούχων, έπειτα από την απόσυρση τους

# Απαιτήσεις του Προτύπου


10 Εντοπισμός και παρακολούθηση οποιασδήποτε πρόσβασης σε δικτυακούς πόρους

11 Περιοδικός έλεγχος συστημάτων και διαδικασιών ασφάλειας

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Εντοπισμός & Παρακολούθηση Πρόσβασης σε Δικτυακούς Πόρους

- Καθιέρωση διαδικασίας για τον καθορισμό των προσβάσεων των χρηστών στα συστήματα του CDE
- Αυτοματοποιημένη καταγραφή των ενεργειών των χρηστών για όλα τα συστατικά του συστήματος
- Καταγραφή για κάθε συστατικό του συστήματος :
  - ταυτοποίηση χρηστών
  - είδος γεγονότων
  - ημερομηνία και ώρα
  - ένδειξη επιτυχίας ή αποτυχίας
  - προέλευση του γεγονότος
  - ταυτότητα ή το όνομα των δεδομένων, του συστατικού του συστήματος, ή των πόρων που επηρεάστηκαν

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Εντοπισμός & Παρακολούθηση Πρόσβασης σε Δικτυακούς Πόρους

- Συγχρονισμός των ρολογιών σε όλα τα συστήματα του CDE
- Προστασία των αρχείων καταγραφής ενεργειών των χρηστών ώστε να μην είναι δυνατή η τροποποίησή τους
- Ημερήσια επισκόπηση όλων των αρχείων καταγραφής των συστημάτων του CDE
- Διατήρηση ιστορικού αρχείων καταγραφής τουλάχιστον για ένα έτος, με τα αρχεία των τελευταίων τριών μηνών να είναι άμεσα διαθέσιμα για ανάλυση

# Περιοδικός Έλεγχος Συστημάτων & Διαδικασιών Ασφάλειας

- Διενέργεια έλεγχου εντοπισμού wireless access points μέσω
  - Συστήματος εντοπισμού ασύρματων δικτύων (wireless analyzer) ή
  - ασύρματου IDS/IPS
- Διενέργεια ελέγχου εντοπισμού ευπαθειών στο εσωτερικό και στο εξωτερικό δίκτυο (από ASV) τουλάχιστον ανά τρίμηνο και έπειτα από κάθε σημαντική αλλαγή στο δίκτυο
- Διενέργεια ελέγχων εισβολής τουλάχιστον μία φορά το χρόνο και έπειτα από κάθε σημαντική αναβάθμιση στην υποδομή ή στις εφαρμογές ή μετατροπές
  - Έλεγχοι εισβολής στο επίπεδο δικτύου (Network Layer)
  - Έλεγχοι εισβολής στο επίπεδο εφαρμογής (Application Layer)

# Περιοδικός Έλεγχος Συστημάτων & Διαδικασιών Ασφάλειας

- Χρήση συστημάτων ανίχνευσης / αποτροπής εισβολών, για την παρακολούθηση των επικοινωνιών. Οι μηχανισμοί ανίχνευσης και αποτροπής εισβολών θα πρέπει να διατηρούνται ενημερωμένοι

- Εγκατάσταση λογισμικού παρακολούθησης της ακεραιότητας των αρχείων για την ενημέρωση του αρμόδιου προσωπικού σε περιπτώσεις μη εξουσιοδοτημένων αλλαγών στα κρίσιμα αρχεία ή στα περιεχόμενα του συστήματος

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Απαιτήσεις του Προτύπου


12 Τήρηση πολιτικής ασφάλειας πληροφοριών

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Τήρηση Πολιτικής Ασφάλειας Πληροφοριών

- Ανάπτυξη, έκδοση, συντήρηση και επικοινωνία πολιτικής ασφάλειας πληροφοριών
- Ανάπτυξη διαδικασιών ασφάλειας (π.χ. διαδικασίες συντήρησης λογαριασμών χρηστών, διαδικασίες επανεξέτασης αρχείων καταγραφής κτλ.)
- Ανάπτυξη πολιτικών χρήσης κρίσιμων τεχνολογιών (laptops, PDAs, e-mail, Internet, κτλ)
- Διαβεβαίωση ότι οι πολιτικές και διαδικασίες ασφαλείας καθορίζουν σαφώς τις υποχρεώσεις ασφάλειας πληροφοριών για όλους τους εργαζόμενους και τους εξωτερικούς συνεργάτες
- Ανάθεση σε ένα συγκεκριμένο άτομο ή ομάδα, των αρμοδιοτήτων διαχείρισης ασφάλειας πληροφοριών (information security management)

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

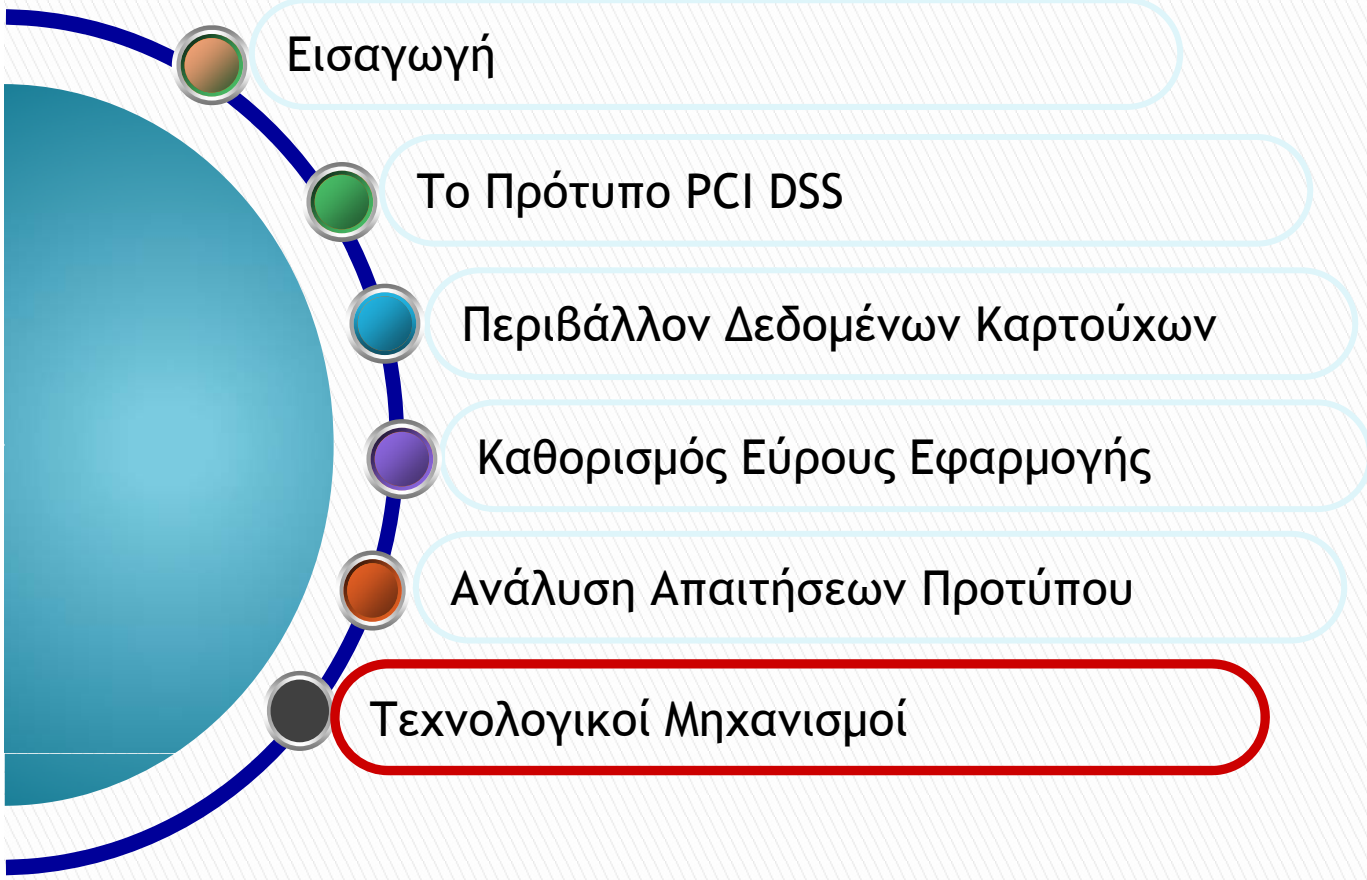
# Τήρηση Πολιτικής Ασφάλειας Πληροφοριών

- Υλοποίηση προγράμματος επιμόρφωσης χρηστών σε θέματα ασφάλειας
- Έλεγχος υποψήφιων για πρόσληψη υπαλλήλων
- Υλοποίηση σχεδίου αντιμετώπισης περιστατικών ασφάλειας

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Ατζέντα




encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Πρακτικές & Τεχνολογικοί Μηχανισμοί

- Δικτυακός διαχωρισμός & συστήματα Firewalls
- Κρυπτογράφηση επικοινωνιών (VPN Connections)
- Μηχανισμοί ανίχνευσης & καταστολής εισβολών (IDS/IPS) σε επίπεδο Δικτύου
- Μηχανισμοί προστασίας Web εφαρμογών & βάσεων δεδομένων
- Μηχανισμοί ασφάλειας περιεχομένου
- Υποδομή ελέγχου τροποποιήσεων και συμμόρφωσης (Integrity & Compliance)

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Πρακτικές & Τεχνολογικοί Μηχανισμοί

- Υποδομή ασφαλούς διαχείρισης συνθηματικών (Password Infrastructure)
- Μηχανισμοί ισχυρής αυθεντικοποίησης
- Υποδομή αντιμετώπισης κακόβουλου λογισμικού (Antivirus – Antispyware)
- Μηχανισμοί ασφάλειας τερματικών (Endpoint Security)
- Υποδομή προστασίας διαρροής δεδομένων (Data Leak Prevention)
- Υποδομή διαχείρισης περιστατικών ασφαλείας (Security Event Management)
- Υποδομή διαχείρισης αδυναμιών (Threat & Vulnerability Management Infrastructure)

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Δικτυακός Διαχωρισμός & Συστήματα Firewalls…

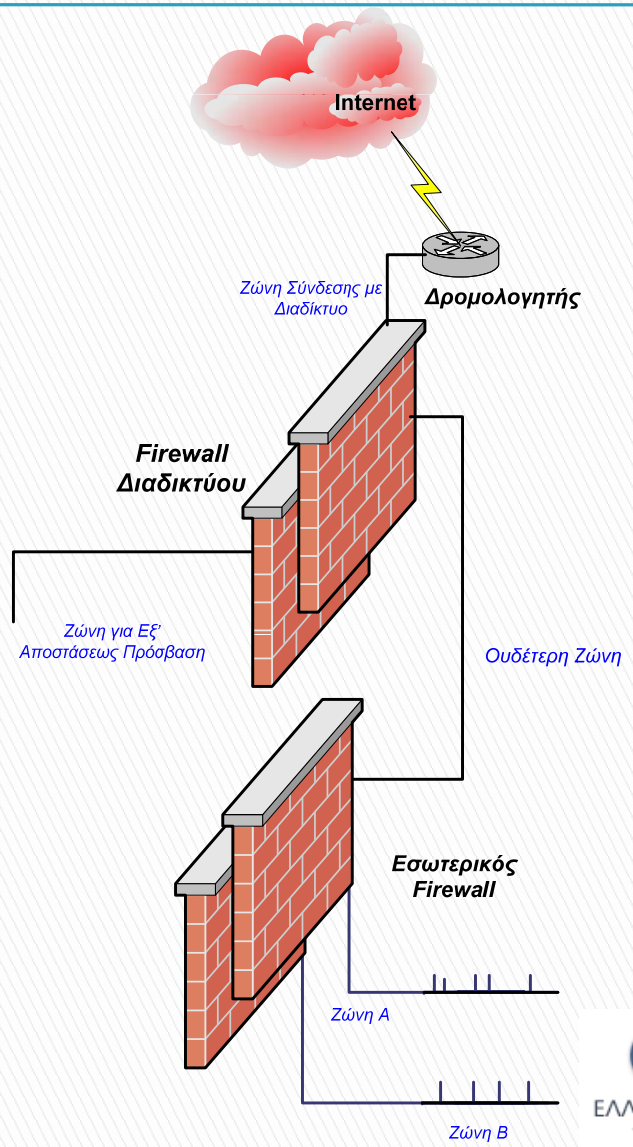
- Διαχωρισμός εσωτερικού δικτύου σε επίπεδο:
  - Υποδομών
  - Συστημάτων και εφαρμογών
- Βασικά Κριτήρια:
  - λειτουργικός ρόλος του συστήματος ή της υποδομής
  - Κρισιμότητα
  - προφίλ επικινδυνότητας
  - απαιτούμενες επικοινωνίες με άλλα συστήματα ή υποδομές
  - οποιοσδήποτε άλλος παράγοντας μπορεί να επηρεάσει την ασφάλεια της εταιρικής υποδομής

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# ...Δικτυακός Διαχωρισμός & Συστήματα Firewalls

- Επιτυγχάνεται κυρίως με την υλοποίηση συστημάτων firewalls
  - Σε επίπεδο συστημάτων και εφαρμογών ο διαχωρισμός του εταιρικού δικτύου πραγματοποιείται με τη δημιουργία των κατάλληλων προστατευμένων δικτυακών ζωνών (firewall zones/DMZs), και
  - τη χρήση τεχνικών Private VLANs οι οποίες επιτυγχάνουν τη δικτυακή απομόνωση των συστημάτων σε Layer 2




encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Κρυπτογράφηση Επικοινωνιών (VPN Connections)…

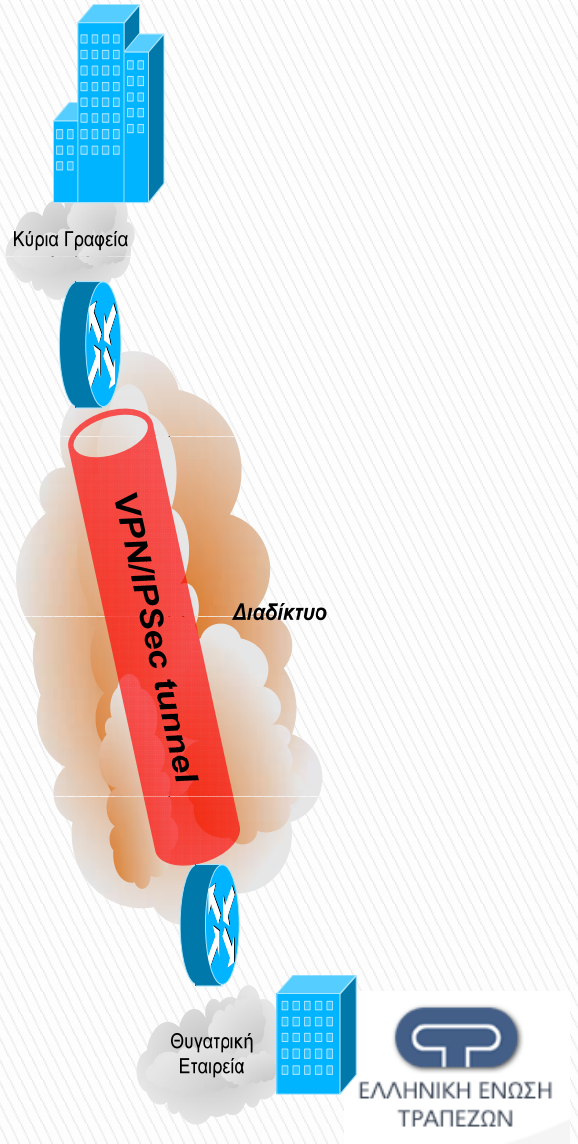
- Η κρυπτογράφηση των επικοινωνιών διασφαλίζει την εμπιστευτικότητα και ακεραιότητα των δεδομένων τα οποία διακινούνται μέσω μη έμπιστων δικτύων (π.χ. Internet)

- Η δημιουργία κρυπτογραφημένων καναλιών επικοινωνίας βασίζεται στην τεχνολογία VPN και υλοποιείται με
  - περιμετρικά συστήματα ασφαλείας (Internet/Extranet Firewalls)
  - εξειδικευμένες συσκευές (SSL Gateways και VPN concentrators)

# ...Κρυπτογράφηση Επικοινωνιών (VPN Connections)

- Μέσω VPN συνδέσεων επιτυγχάνεται η:
  - ασφαλής διασύνδεση δυο απομακρυσμένων μερών (δικτύων, συστημάτων ή χρηστών) μέσω Internet/Extranet κλπ.
  - εμπιστευτικότητα και ακεραιότητα των δεδομένων που διακινούνται μεταξύ αυτών

- Οι πιο συνηθισμένες μέθοδοι για υλοποίηση κρυπτογραφημένων VPN συνδέσεων είναι τα πρωτόκολλα
  - IPSec, και
  - Secure Socket Layer (SSL)




encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

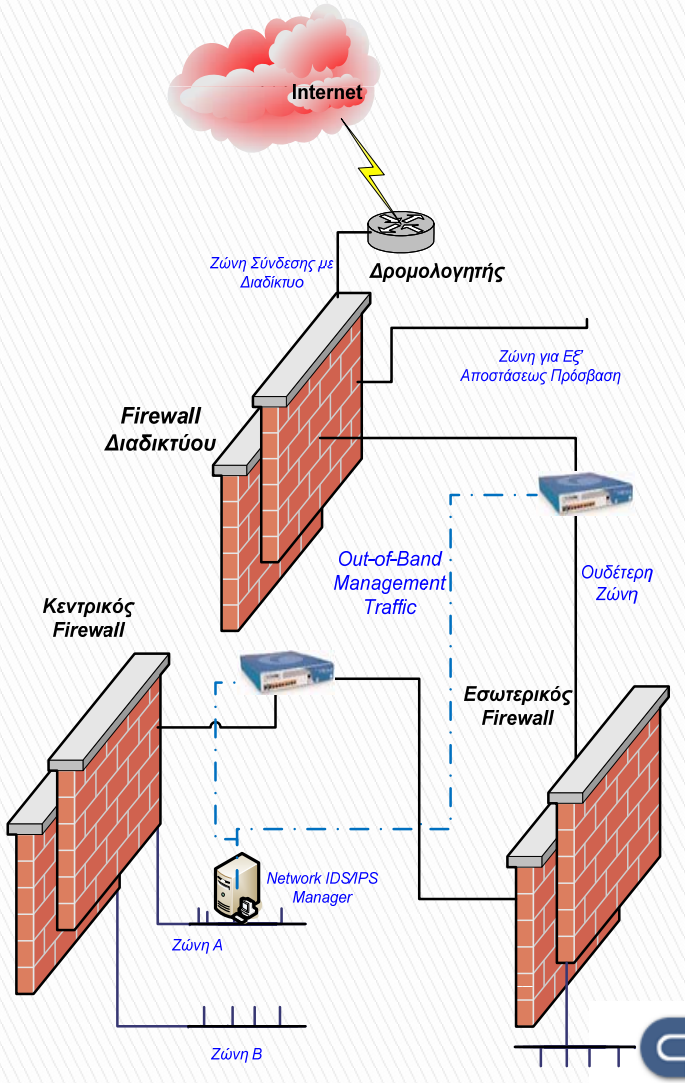
# Μηχανισμοί Ανίχνευσης & Καταστολής Εισβολών σε Επίπεδο Δικτύου…

- IDS/IPS: Το σύνολο των τεχνικών που ακολουθούνται για την ανίχνευση & την αποτροπή εισβολής σε ένα πληροφοριακό σύστημα ή δίκτυο

- Η ανίχνευση μίας εισβολής ή αποτροπής μπορεί να υλοποιηθεί με τη βοήθεια κάποιου εξειδικευμένου συστήματος ασφάλειας (σύστημα ανίχνευσης & αποτροπής εισβολών), το οποίο εξετάζει την δικτυακή κίνηση για στοιχεία παραβίασης (pattern matching)

# Μηχανισμοί Ανίχνευσης & Καταστολής Εισβολών σε Επίπεδο Δικτύου

- Pattern Matching:
  - Χρήση βάσης δεδομένων γνωστών επιθέσεων και αδυναμιών η οποία ανανεώνεται ανά τακτά χρονικά διαστήματα, γεγονός που καθιστούν δυνατή την αποτροπή γνωστών επιθέσεων, προτού αυτές εισέλθουν στο εσωτερικό δίκτυο




encode
Information Risk Management

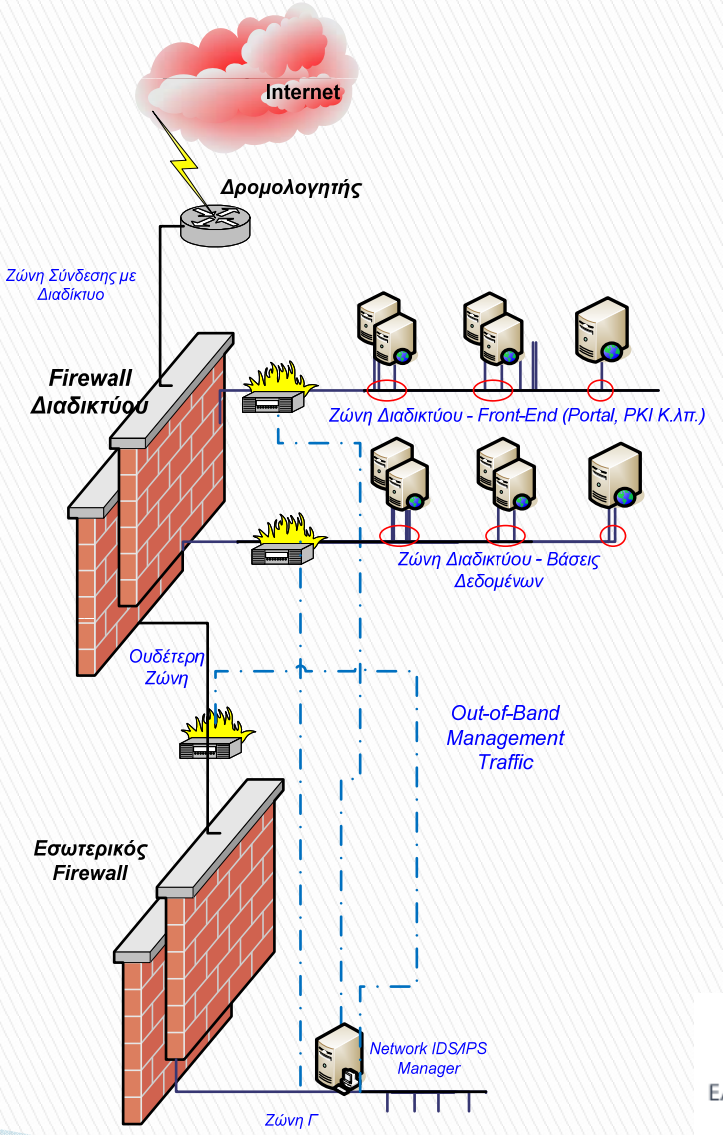
ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Μηχανισμοί Προστασίας Web Εφαρμογών & Βάσεων Δεδομένων…

- Εγκαθίστανται ανάμεσα στις εφαρμογές και στα υπόλοιπα πληροφοριακά συστήματα ώστε να
  - εξετάζουν την εισερχόμενη και την εξερχόμενη κίνηση τους σε επίπεδο εφαρμογών
  - εφαρμόζουν προκαθορισμένες ή/και επιλεγμένες πολιτικές ασφαλείας
  - παρέχουν εξελιγμένες δυνατότητες έγκαιρης ανίχνευσης και καταστολής (IDS/IPS) γνωστών και μη γνωστών (zero-day attack) επιθέσεων καλύπτοντας ειδικά και σε μεγαλύτερο βάθος την ασφάλεια των web εφαρμογών και βάσεων δεδομένων

# ...Μηχανισμοί Προστασίας Web Εφαρμογών & Βάσεων Δεδομένων

- Δημιουργία «προφίλ» αποδεκτής χρήσης εφαρμογών:
  - ολοκληρωμένη προστασία συστημάτων ελέγχοντας τη συμμόρφωση των web ή sql requests που κατευθύνονται προς το σύστημα σύμφωνα με γνωστές και άγνωστες μεθόδους παραβίασης




encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Μηχανισμοί Ασφάλειας Περιεχομένου…

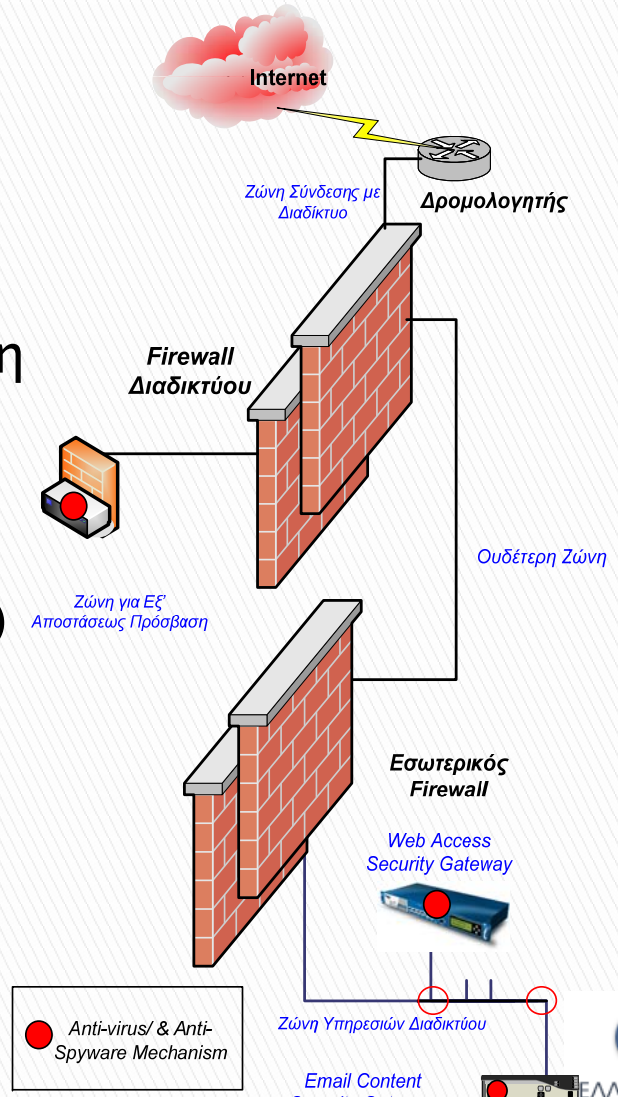
- Παρέχουν προστασία σε απειλές, οι οποίες μπορεί να εισέλθουν στο εταιρικό δίκτυο μέσω του διακινούμενου περιεχομένου των διαδικτυακών υπηρεσιών, όπως
  - e-mail (SMTP),
  - web (HTTP)
  - FTP
- Βασικές λειτουργίες :
  - Web/FTP Content Security
  - Mail Content Filtering

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# ...Μηχανισμοί Ασφάλειας Περιεχομένου

- Έλεγχος πρόσβασης σε επίπεδο δικτυακών τόπων, βάσει λίστας επιτρεπόμενων / μη επιτρεπόμενων URLs η οποία ενημερώνεται καθημερινά
- Έλεγχος περιεχομένου για ύπαρξη κακόβουλου λογισμικού
- Έλεγχος του περιεχομένου για ύπαρξη κακόβουλου Mobile Code (π.χ. ActiveX, Java, Javascripts κτλ.)
- MIME filtering (επιτρέποντας συγκεκριμένα MIME types)
- Εφαρμογή πολιτικών ασφάλειας ανά χρήστη ή ομάδα χρηστών




encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Υποδομή Ελέγχου Τροποποιήσεων και Συμμόρφωσης

- Δημιουργία «προφίλ» της υφιστάμενης λειτουργίας των κρίσιμων πληροφοριακών συστημάτων, ώστε να διασφαλιστεί ότι
  - ότι οποιαδήποτε τροποποίηση του λογισμικού και των ρυθμίσεων τους διενεργείται από εξουσιοδοτημένο προσωπικό και με τρόπο που δεν υποβαθμίζει το υφιστάμενο επίπεδο ασφαλείας
  - η συμμόρφωση με τις απαιτήσεις του προτύπου PCI-DSS (ή και άλλων προτύπων ασφαλείας) μέσω περιοδικών αυτοματοποιημένων ελέγχων των παραμέτρων ασφαλείας των συστημάτων

# Υποδομή Ασφαλούς Διαχείρισης Συνθηματικών

- Διαχείριση συνθηματικών: δημιουργία, γνωστοποίησή τους στο εξουσιοδοτημένο προσωπικό, μετάδοση, τροποποίηση, αποθήκευση

- Η υποδομή «υιοθετεί» τον «κύκλο ζωής» του συνόλου των συνθηματικών:
  - τα συγκεντρώνει σε ένα «θωρακισμένο» λογικό χώρο όπου κρυπτογραφούνται, και
  - προσπελαύνονται μόνο από εξουσιοδοτημένο προσωπικό ή / και τις εφαρμογές

- Η υποδομή αυτοματοποιεί τη χειροκίνητη διαχείριση των συνθηματικών ενώ ταυτόχρονα την περιβάλλει με ισχυρούς μηχανισμούς ασφάλειας

encode
Information Risk Management

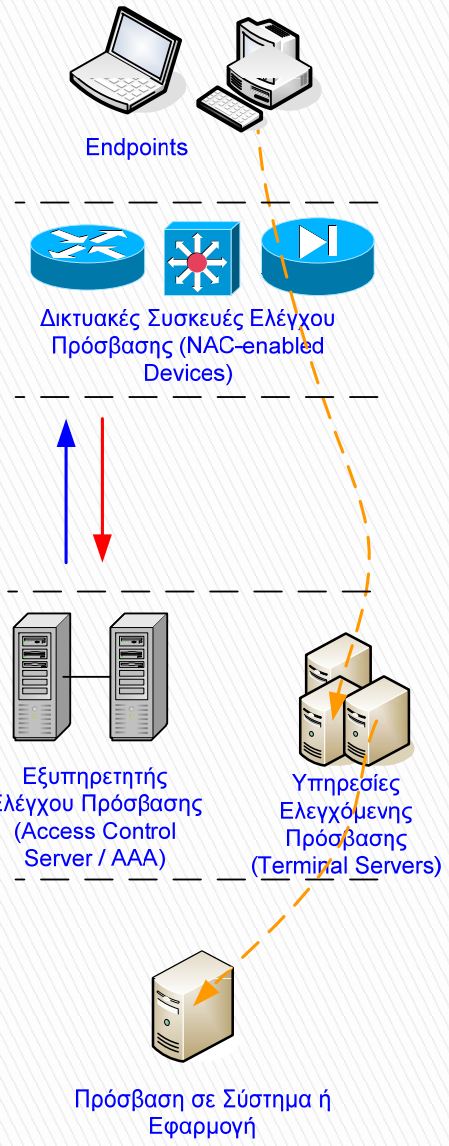
ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Μηχανισμοί Ισχυρής Αυθεντικοποίησης…

- Πιστοποίηση ταυτότητας χρήστη μέσω κατάλληλων μηχανισμών «αναγνώρισης» και «πιστοποίησης ή αυθεντικοποίησης» με :
  - Συστήματα (AAA) αυθεντικοποίησης, εξουσιοδότησης και απόδοσης ευθυνών (authentication – authorization – accountability), όπως: RADIUS ή TACACS.
  - Συστήματα firewalls
  - Εξειδικευμένες συσκευές (π.χ. SSL-VPN Gateways),
  - Συστήματα υπηρεσιών ελεγχόμενης πρόσβασης (terminal servers)
  - RBAC συστήματα πρόσβασης βάσει ρόλων, όπως: Microsoft Active Directory, Microsoft SQL Server, Oracle DBMS, κλπ.
  - …

# ...Μηχανισμοί Ισχυρής Αυθεντικοποίησης

- Ενδεικτικοί μηχανισμοί ισχυρής αυθεντικοποίησης:
  - Ψηφιακά Πιστοποιητικά (εγκατεστημένα στο PC του χρήστη ή σε USB token) σε συνδυασμό με προσωπικό κωδικό πρόσβασης
  - One-Time-Passwords σε συνδυασμό με προσωπικό κωδικό πρόσβασης (PIN)



# Υποδομή Αντιμετώπισης Κακόβουλου Λογισμικού

- Ελέγχει το περιεχόμενο των μεταδιδόμενων δεδομένων (π.χ. μέσω διαδικτύου ή μέσω ηλεκτρονικού ταχυδρομείου) κυρίως για την ανίχνευση κακόβουλου λογισμικού (ιούς υπολογιστών, επιβλαβή κώδικα κ.λπ.)

- Έχουν κατασταλτικό χαρακτήρα και βασίζονται σε
  - κριτήρια καταγεγραμμένης συμπεριφοράς (signature based) και
  - ιδιαίτερων στοιχείων που χαρακτηρίζουν το εκάστοτε κακόβουλο λογισμικό (π.χ. ιό)

- Ενημερώνονται τακτικά με νέα χαρακτηριστικά (signatures)

# Μηχανισμοί Ασφάλειας Τερματικών (Endpoint Security)

- Προστατεύουν το εταιρικό δίκτυο από επιθέσεις που έχουν ως αρχικό στόχο τα τερματικά χρηστών

- Βασικές λειτουργίες
  - Έλεγχος πρόσβασης και επικοινωνιών σε επίπεδο δικτύου (Personal firewalls)
  - Έλεγχος πρόσβασης σε επίπεδο εφαρμογών (πχ. ποιες εφαρμογές επιτρέπεται να αποκτούν πρόσβαση στο δίκτυο)
  - Καταστολή εισβολών σε επίπεδο τερματικών (Host IPS)
  - Εφαρμογή πολιτικής ελέγχου πρόσβασης στο εταιρικό δίκτυο (NAC – network admission control)

# Υποδομή Προστασίας Διαρροής Δεδομένων (DLP Infrastructure)…

- Σκοπός της υλοποίησης υποδομής προστασίας διαρροής δεδομένων είναι η αποτελεσματική προστασία των κρίσιμων εταιρικών δεδομένων από κινδύνους και απειλές όπως η μη εξουσιοδοτημένη πρόσβαση, χρήση ή διαρροή δεδομένων, προερχόμενες από τους εξουσιοδοτημένους χρήστες του εσωτερικού δικτύου του οργανισμού ή από μη εξουσιοδοτημένους χρήστες γενικά

- Παρέχουν συνεχή παρακολούθηση, καταγραφή και έλεγχο της χρήσης των εταιρικών δεδομένων

# ...Υποδομή Προστασίας Διαρροής Δεδομένων (DLP Infrastructure)

- Καταγράφουν κάθε ενέργεια του χρήστη σχετικά με την πρόσβαση ή χρήση κρίσιμων εταιρικών δεδομένων και εφαρμόζουν σε πραγματικό χρόνο τους απαραίτητους κανόνες πρόσβασης διασφαλίζοντας τη νόμιμη χρήση των δεδομένων βάσει της υπάρχουσας πολιτικής ασφάλειας

- Προστασία από:
  - αντιγραφή δεδομένων σε CD ή USB memory stick,
  - εκτύπωση,
  - δικτυακή μεταφορά,
  - αποστολή μέσω ηλεκτρονικής αλληλογραφίας κ.α.

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

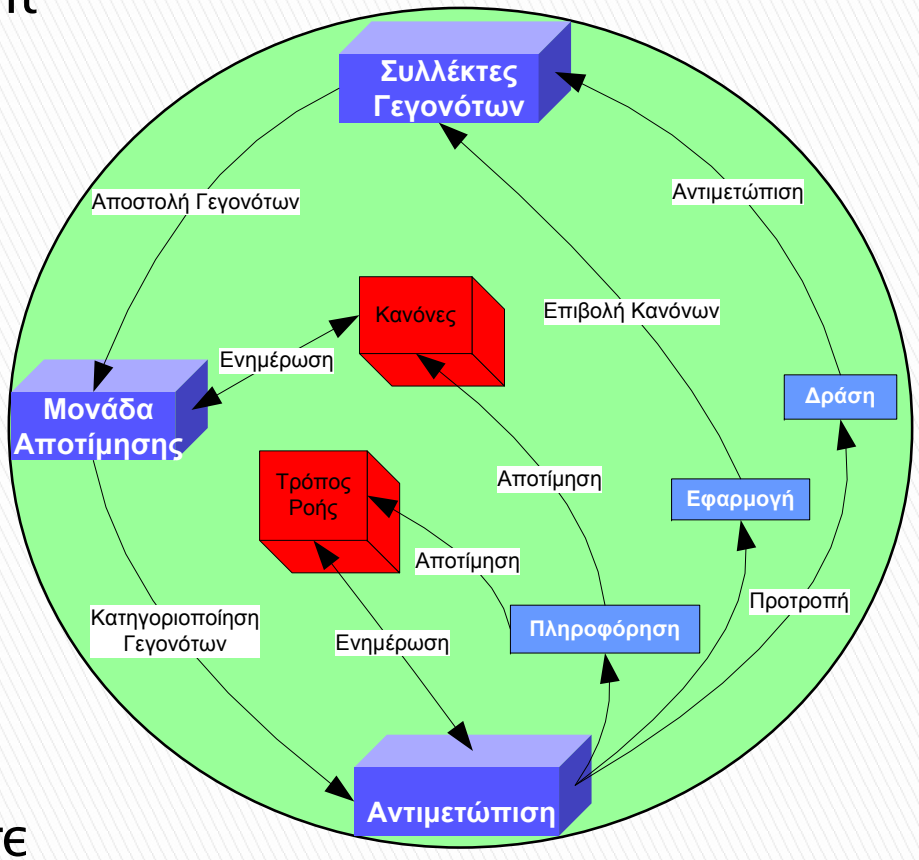
# Υποδομή Διαχείρισης Περιστατικών Ασφαλείας (Security Event Management)…

- Στόχος της είναι να:
  - συλλέγει security event data από όλα τα κρίσιμα συστήματα του οργανισμού
  - φιλτράρει, έτσι ώστε να μειώνονται οι λάθος συναγερμοί και ο όγκος τους, και
  - τα συνδυάζει βάσει συγκεκριμένων κανόνων

- Θα πρέπει να επιφέρει τις μικρότερες δυνατές επιπτώσεις στην απόδοση των συστημάτων και των δικτύων και να προσφέρει αποτελεσματική παρακολούθηση και ανάλυση των διαφόρων περιστατικών ασφάλειας

# ...Υποδομή Διαχείρισης Περιστατικών Ασφαλείας (Security Event Management)

- Εναρμόνιση γεγονότων (event harmonization),
- Συσχετισμός (correlation),
- Άθροιση (aggregation),
- Συγχώνευση (consolidation),
- Απεικόνιση (visualization),
- Έγκαιρη αντιμετώπιση περιστατικών ασφάλειας (incident response),
- Αναφορές γεγονότων (event reporting)
- Αναφορές σχετικά με τη συμμόρφωση (compliance) σε κανονισμούς ή σε πολιτικές.




**Ροή γεγονότων σε ένα σύστημα διαχείρισης γεγονότων ασφάλειας**

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Υποδομή Διαχείρισης Αδυναμιών (Threat & Vulnerability Management Infrastructure)

- Διασφαλίζεται
  - ο έγκαιρος εντοπισμός, η καταγραφή και η ανάλυση των υφιστάμενων ευπαθειών των πληροφοριακών συστημάτων και των δικτυακών υποδομών
  - η ανάλυση των συσχετιζόμενων παραγόντων απειλής
- Περιοδικότητα & αυτοματοποίηση
- Πλήθος προτάσεων διορθωτικών ενεργειών:
  - εφαρμογή διορθωτικού λογισμικού
  - εγκατάσταση επιπρόσθετων μέτρων ασφαλείας
  - τροποποίηση των υφιστάμενων κανόνων σε συστήματα ασφάλειας κλπ

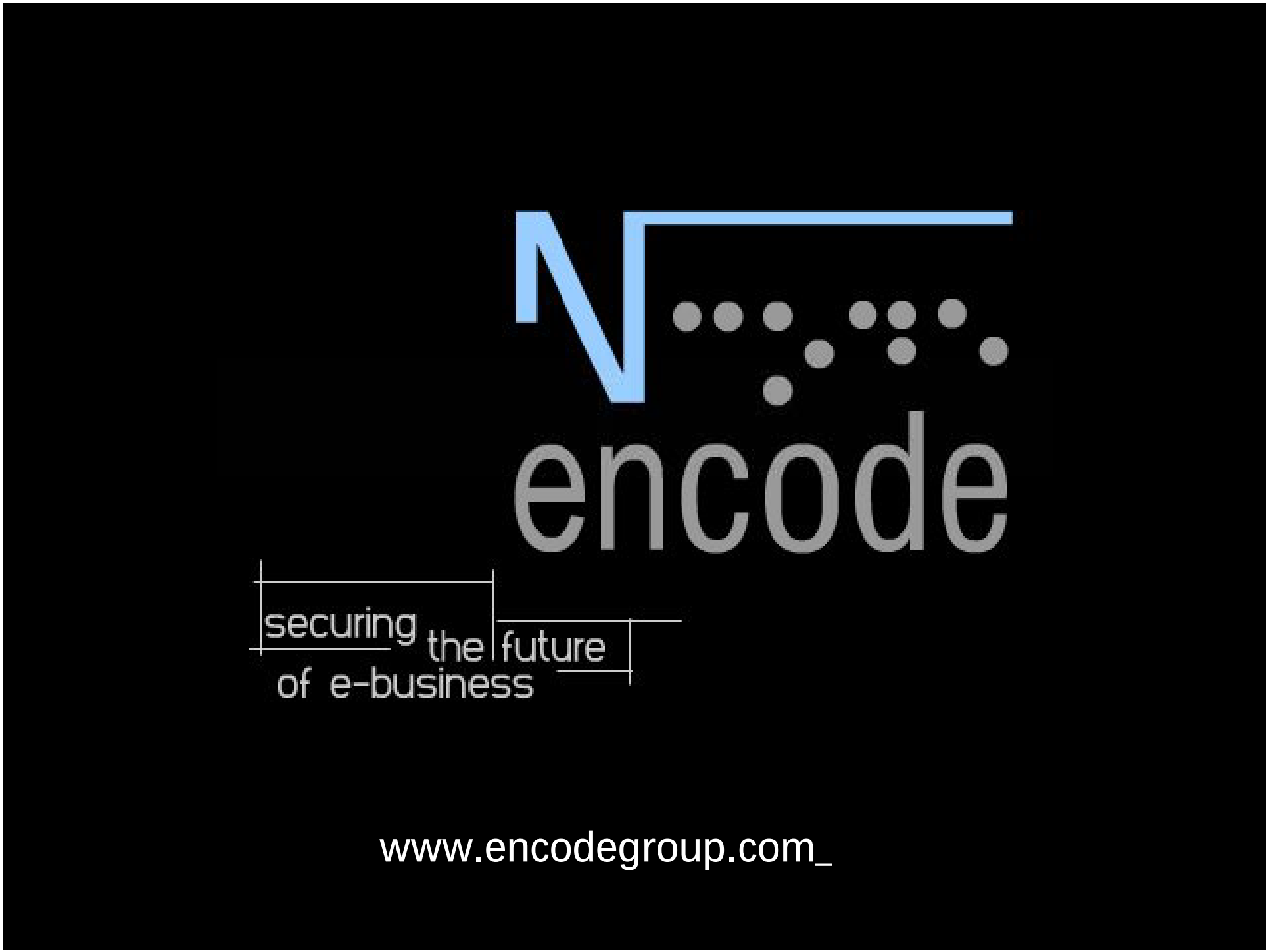
encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

Ευχαριστούμε για το χρόνο σας

encode
Information Risk Management

ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ
ΤΡΑΠΕΖΩΝ


encode
securing the future
of e-business
www.encodegroup.com_