ΕΛΛΗΝΙΚΗ ΕΝΩΣΗ ΤΡΑΠΕΖΩΝ

# Η Πρωτοβουλία της ΕΕΤ για την υιοθέτηση του Προτύπου PCI DSS από τις Ελληνικές Επιχειρήσεις

Κων/νος Ταβλαρίδης

Διευθυντής ΕΕΤ

15 Σεπτεμβρίου 2009

# Ατζέντα

- Η σκοπιμότητα υλοποίησης του έργου
- Ο ρόλος της ΕΕΤ στο έργο
- Το Διεθνές Πρότυπο Ασφάλειας PCI DSS
- Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών
- Οφέλη συμμετοχής των επιχειρήσεων στο έργο

# Η σκοπιμότητα υλοποίησης του έργου 1/3

- Διαρκώς αυξανόμενα, διεθνώς αλλά και στην Ελλάδα, περιστατικά απάτης και οικονομικών εγκλημάτων με τη χρήση καρτών αλλά και την υποκλοπή στοιχείων μέσω του Διαδικτύου.

- Διαρκής αύξηση των συναλλαγών με κάρτες.

- Ανάγκη ενίσχυσης της εμπιστοσύνης του συναλλακτικού κοινού στη χρήση καρτών για αγορές αγαθών και υπηρεσιών.

- Συμβατικές υποχρεώσεις των τραπεζών που αποδέχονται συναλλαγές με κάρτες έναντι των διεθνών σχημάτων καρτών (VISA, MasterCard, κ.λπ.)

# Η σκοπιμότητα υλοποίησης του έργου 2/3

Αδυναμίες ασφάλειας μπορούν να εμφανιστούν σε όλη την αλυσίδα επεξεργασίας των πληρωμών με κάρτες:

- συσκευές POS,
- προσωπικοί Η/Υ ή διακομιστές (servers),
- ασύρματα σημεία πρόσβασης (hotspots),
- εφαρμογές για αγορές στο Web,
- συστήματα αποθήκευσης που βασίζονται στο χαρτί,
- διαβίβαση δεδομένων κατόχων καρτών στους φορείς παροχής υπηρεσιών (service providers).

**Επομένως, η χρήση αναγνωρισμένων διαδικασιών και τεχνολογιών ασφαλείας, για την αποφυγή υποκλοπής των δεδομένων κατόχων καρτών, αποτελεί επιτακτική ανάγκη.**

# Η σκοπιμότητα υλοποίησης του έργου 3/3

Η συμμόρφωση των επιχειρήσεων με το PCI DSS έχει ύψιστη σημασία τόσο για την ΕΕΤ, όσο και για τις τράπεζες μέλη της δεδομένου ότι:

- Οι τράπεζες μέλη της ΕΕΤ, που εκδίδουν και αποδέχονται κάρτες πληρωμών, καθώς και οι προς πιστοποίηση εμπορικές επιχειρήσεις εκπληρώνουν συμβατικές τους υποχρεώσεις που απορρέουν από τη συμμετοχή τους στα διεθνή σχήματα καρτών.
- Η ισχύουσα νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα επιβάλει η επεξεργασία των προσωπικών δεδομένων να είναι πάντοτε απόρρητη και να εκτελείται με πιστοποιημένες διαδικασίες ασφάλειας.
- Το οικονομικό κόστος και το κόστος φήμης σε περίπτωση υποκλοπής προσωπικών δεδομένων είναι πολύ μεγάλο.

# Ατζέντα

- Η σκοπιμότητα υλοποίησης του έργου
- Ο ρόλος της ΕΕΤ στο έργο
- Το Διεθνές Πρότυπο Ασφάλειας PCI DSS
- Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών
- Οφέλη συμμετοχής των επιχειρήσεων στο έργο

# Ο ρόλος της ΕΕΤ στο έργο 1/1

- Η ΕΕΤ στο πλαίσιο του καταστατικού της ρόλου και λαμβάνοντας υπόψη ότι θέματα ασφάλειας στα συστήματα και μέσα πληρωμών δεν συνιστούν πεδίο ανταγωνισμού μεταξύ των τραπεζών μελών της, ανέλαβε για λογαριασμό τους την επιλογή πιστοποιημένης από το PCI Security Standards Council (PCI SSC) εταιρείας για την εκτέλεση του έργου.

- Η ΕΕΤ συντονίζει τη διαδικασία υλοποίησης του έργου και μεσολαβεί όταν χρειάζεται ανάμεσα στις τράπεζες μέλη της που χρηματοδοτούν το διατραπεζικό έργο και στην ανάδοχο του έργου εταιρεία.

- **Οι επιχειρήσεις θα πρέπει να απευθύνονται στις συνεργαζόμενες με αυτές τράπεζες, καθώς και στην ανάδοχο του έργου εταιρεία για ερωτήματα, διευκρινίσεις και τυχόν προβλήματα και όχι στην Ένωση.**

# Ατζέντα

- Η σκοπιμότητα υλοποίησης του έργου
- Ο ρόλος της ΕΕΤ στο έργο
- Το Διεθνές Πρότυπο Ασφάλειας PCI DSS
- Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών
- Οφέλη συμμετοχής των επιχειρήσεων στο έργο

# Το διεθνές πρότυπο ασφάλειας PCI DSS 1/2

- Το 2004 συστήθηκε το PCI SSC με ιδρυτικά μέλη τις American Express, Discover Financial Services, JCB, MasterCard Worldwide και Visa International
- Ανεξάρτητος οργανισμός προτύπων ο οποίος έχει, σε παγκόσμιο επίπεδο, τη συνολική εποπτεία της ανάπτυξης και διαχείρισης των Προτύπων Ασφάλειας του Payment Card Industry (PCI)
- Το Συμβούλιο εκδίδει το Πρότυπο Ασφάλειας Δεδομένων (PCI DSS), το οποίο περιείχε τις ελάχιστες απαιτήσεις ασφάλειας που πρέπει να πληρούνται ως προς την επεξεργασία, μετάδοση και αποθήκευση δεδομένων καρτών πληρωμής
- Στόχος των διεθνών σχημάτων καρτών είναι να διευκολυνθεί η ευρεία υιοθέτηση μέτρων σε παγκόσμια βάση ώστε να αμβλυνθούν οι αναδυόμενοι κίνδυνοι στην ασφάλεια των συναλλαγών με κάρτες

# Το διεθνές πρότυπο ασφάλειας PCI DSS 2/2

- Τα κριτήρια επιλογής των 131 επιχειρήσεων :

  1. Ο ετήσιος όγκος των συναλλαγών με κάρτες VISA & MASTERCARD
  2. Ο τύπος συναλλαγών με κάρτες (π.χ. Μέσω ηλεκτρονικού εμπορίου)

- Τα 4 επίπεδα κατανομής των επιλεγμένων επιχειρήσεων:

  1. Επίπεδο 1ο: αφορά επιχειρήσεις που διεκπεραιώνουν άνω των 6 εκατομμυρίων συναλλαγών με κάρτες σε ετήσια βάση συμπεριλαμβανομένου του ηλεκτρονικού εμπορίου (6 στις 131 επιχειρήσεις)
  2. Επίπεδο 2ο: εντάσσονται οι επιχειρήσεις με 1 έως 6 εκατομμύρια συναλλαγές με κάρτες σε ετήσια βάση (25 στις 131 επιχειρήσεις)
  3. Επίπεδο 3ο: εντάσσονται οι επιχειρήσεις με 20.000 έως 1 εκατομμύριο συναλλαγές με κάρτες, μέσω του ηλεκτρονικού εμπορίου, σε ετήσια βάση (25 στις 131 επιχειρήσεις)
  4. Επίπεδο 4ο: εντάσσονται όλες οι υπόλοιπες επιχειρήσεις που διεκπεραιώνουν γενικά συναλλαγές με κάρτες (75 στις 131 επιχειρήσεις)

# Ατζέντα

- Η σκοπιμότητα υλοποίησης του έργου
- Ο ρόλος της ΕΕΤ στο έργο
- Το Διεθνές Πρότυπο Ασφάλειας PCI DSS
- Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών
- Οφέλη συμμετοχής των επιχειρήσεων στο έργο

# Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών 1/6

- Οι άμεσοι στόχοι του έργου:
  - η πιστοποίηση συμμόρφωσης των επιλεγμένων 131 εμπορικών επιχειρήσεων που αποδέχονται συναλλαγές με κάρτες με το πρότυπο ασφαλείας PCI DSS
  - η διατήρηση της πιστοποίησης συμμόρφωσης των επιχειρήσεων

- Οι έμμεσοι στόχοι του έργου:
  - η ενίσχυση της εμπιστοσύνης των επιχειρήσεων και του συναλλακτικού κοινού στη χρήση καρτών πληρωμής

# Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών 2/6

- **Ο ειδικότερος ρόλος της ΕΕΤ** :
  - Ευθύνη διαχείρισης του έργου για λογαριασμό των μελών της
  - Συνδρομή στην αντιμετώπιση τυχόν προβλημάτων που θα προκύψουν κατά την εκτέλεση του έργου μέσω της συγκρότησης μόνιμης διατραπεζικής ομάδας για την παρακολούθηση του έργου
  - Κάλυψη του κόστους το οποίο αφορά σε μια σειρά απαιτήσεων του προτύπου PCI DSS που άλλως θα καλούνταν να πληρώσουν οι ίδιες προς πιστοποίηση επιχειρήσεις

# Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών 3/6

- **Ο ρόλος των τραπεζών** :
  - Ενημέρωση των συνεργαζόμενων με αυτές επιχειρήσεων για τη σκοπιμότητα και τη σημασία υλοποίησης του έργου
  - Στήριξη των τεχνικών ομάδων έργου που θα συγκροτηθούν από τις προς πιστοποίηση επιχειρήσεις κατά την διαδικασία υλοποίησης του έργου
  - Συνεργασία με την ανάδοχο του έργου εταιρεία για την αντιμετώπιση τυχόν προβλημάτων που θα ανακύψουν κατά την εκτέλεση του έργου

# Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών 4/6

- **Ο ρόλος της αναδόχου εταιρείας** :
  - Θα ενημερώσει και εκπαιδεύσει το προσωπικό των επιχειρήσεων στις ανάγκες του προτύπου
  - Θα ελέγξει τα συστήματα της επιχείρησης που συνδέονται με τη διαχείριση των συναλλαγών καρτών για τυχόν ελλείψεις και αδυναμίες
  - Θα υποδείξει τις τυχόν ελλείψεις που εντοπίζει κατά τη διάρκεια των ελέγχων στις επιχειρήσεις. Οι επιχειρήσεις έχουν την απόλυτη ευχέρεια επιλογής εταιρείας στην οποία θα αναθέσουν την κάλυψη των ενδεχόμενων ελλείψεων

# Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών 5/6

- Θα υποστηρίζει τις τεχνικές ομάδες έργου των προς πιστοποίηση επιχειρήσεων και θα συνδράμει στην αντιμετώπιση τυχόν προβλημάτων κατά τη διαδικασία υλοποίησης του έργου

- Θα προβεί στην έκδοση πιστοποιητικού συμμόρφωσης της επιχείρησης με το πρότυπο

# Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών 6/6

- **Ο ρόλος των προς πιστοποίηση επιχειρήσεων** :
  - Καθορισμός υπευθύνου ή συγκρότηση ομάδας έργου που θα συνεργάζεται με την ανάδοχο εταιρεία καθ' όλη τη διάρκεια του έργου
  - Επικοινωνία με τις συνεργαζόμενες τράπεζες για την υποβολή ερωτημάτων, την παροχή διευκρινίσεων και διευθέτηση τυχόν προβλημάτων που θα ανακύψουν κατά τη διαδικασία υλοποίησης του έργου
  - Κάλυψη των ενδεχόμενων ελλείψεων που θα τους υποδείξει η ανάδοχος του έργου εταιρεία μετά την ολοκλήρωση των απαιτούμενων ελέγχων στα συστήματά τους

# Ατζέντα

- Η σκοπιμότητα υλοποίησης του έργου
- Ο ρόλος της ΕΕΤ στο έργο
- Το Διεθνές Πρότυπο Ασφάλειας PCI DSS
- Στόχοι του έργου και ρόλος των εμπλεκόμενων μερών
- Οφέλη συμμετοχής των επιχειρήσεων στο έργο

# Οφέλη συμμετοχής των επιχειρήσεων στο έργο 1/2

1. Ενίσχυση της εμπιστοσύνης της πελατείας σας. Σύμφωνα με σχετικές έρευνες σε περίπτωση συμβάντος παραβίασης ασφάλειας*:
   - 49% των πελατών θεωρούν ότι ευθύνονται οι εμπορικές επιχειρήσεις
   - 3 στους 4 πελάτες δε θα προχωρήσουν σε αγορές ποτέ ξανά από τη συγκεκριμένη εμπορική επιχείρηση

2. Περιορισμός απάτης και συναφών οικονομικών απωλειών

3. Αποφυγή αρνητικής δημοσιότητας

*Πηγή: Javelin Strategy and Research 2007

# Οφέλη συμμετοχής των επιχειρήσεων στο έργο 2/2

4. Αποφυγή επιπρόσθετων κανονιστικών ελέγχων

5. Για τις παρεχόμενες υπηρεσίες του έργου από την ανάδοχο εταιρεία δεν θα υπάρξει καμία οικονομική επιβάρυνση

6. Μη συμμόρφωση της επιχείρησης μπορεί να οδηγήσει σε προβλήματα στις σχέσεις της εταιρείας με την τράπεζα με την οποία συνεργάζεται και ενδεχομένως στην απώλεια της δυνατότητας αποδοχής συναλλαγών με κάρτες πληρωμών

Ευχαριστούμε για το χρόνο σας