

(Banker's Advertorial)



Ευ. Βασιλειάδου  
BESECURE

## Συμμόρφωση με το PCI DSS Αναγκαίο κακό ή αναγκαίο καλό;

Το Payment Card Industry Data Security Standard (PCI DSS) είναι ένα υποχρεωτικό προς εφαρμογή, διεθνές πρότυπο το οποίο απευθύνεται σε κάθε Οργανισμό ή Εταιρία που συμμετέχει σε μια αλυσίδα συναλλαγής.

Της Ευαγγελίας Βασιλειάδου, MSc Information Security, HISP, ISO27001 LA  
Information Security & Compliance Consultant, BESECURE

**Π**ιο συγκεκριμένα απευθύνεται σε Αποδέκτριες Τράπεζες, σε Εμπορους που παρέχουν υπηρεσίες χρηματοπιστωτικών συναλλαγών καθώς και σε Πάροχους Υπηρεσιών (συνήθως τρίτες οντότητες στις οποίες ανατίθενται μερικές από τις υπηρεσίες που προβλέπονται για την πραγματοποίηση των συναλλαγών). Το πρότυπο καθορίζει τις απαιτήσεις διασφάλισης των δεδομένων για την ολοκλήρωση συναλλαγών με τη χρήση πιστωτικών καρτών. Η επιβολή συμμόρφωσης με το πρότυπο απαιτείται από τους Οργανισμούς Πιστωτικών Καρτών, πιο συγκεκριμένα από τις VISA, MasterCard, American Express, Discover και JCB, ενώ η διαδικασία πιστοποίησης, η έκδοση και η εξέλιξη του προτύπου παρέχεται από τον ανεξάρτητο οργανισμό Payment Card Industry Security Standards Council.

Το PCI DSS εξετάζει την εφαρμογή σε περισσότερων των 200 μηχανισμών ελέγχου για την ασφάλεια των πληροφοριών σε επίπεδο διαχείρισης και σε επίπεδο δικτυακής και λειτουργικής ασφάλειας. Με την πλήρη εφαρμογή του προτύπου δημιουργείται μια σφαιρική ασπίδα προστασίας γύρω από κάθε διεργασία που αφορά την ολοκλήρωση μιας συναλλαγής.

### Απαιτούμενα μέτρα συμμόρφωσης

Σε ότι αφορά την προστασία του δικτύου, το πρότυπο απαιτεί την υλοποίηση συστημάτων firewall και θέτει αυστηρότερα από τα συνήθη μέτρα, για την προστασία των ασύρματων δικτύων. Ακόμα, απαιτεί τον περιοδικό έλεγχο διείσδυσης (penetration tests) τόσο σε επίπεδο δικτύου όσο και σε επίπεδο εφαρμογής. Παρόλο που μέσα από τις παραπάνω απαιτήσεις αποτρέπεται η πρόσβαση στα δεδομένα των πιστωτικών καρτών, ωστόσο αν η μεταφορά ή η αποθήκευσή τους δεν είναι κρυπτογραφημένη ο κίνδυνος μη εξουσιοδοτημένης πρόσβασης ή τροποποίησης παραμένει σε υψηλά επίπεδα. Για τον λόγο αυτό, το πρότυπο θέτει την χρήση της κρυπτογραφίας ως κρίσιμο, είτε κατά την αποθήκευση των δεδομένων είτε κατά την μεταφορά τους μέσω email. Το πρότυπο εστιάζοντας και σε διαχειρισιακές εκτός από τεχνολογικές απαιτήσεις, προσδιορίζει την ανάγκη δημιουργίας, διατήρησης και

κοινοποίησης στο προσωπικό, μιας πολιτικής ασφάλειας η οποία εξετάζει τα ζητήματα ασφάλειας πληροφοριών που απαιτούνται από το πρότυπο και προκύπτουν από την περιοδική διενέργεια μιας διαδικασίας για την Ανάλυση Επικινδυνότητας (risk assessment) του περιβάλλοντος μεταφοράς, επεξεργασίας ή αποθήκευσης των δεδομένων. Ακόμα, δίνεται ιδιαίτερη σημασία στην ενημέρωση και την εκπαίδευση του προσωπικού.

### Ποιοι υποχρεούνται σε συμμόρφωση

Οι Οργανισμοί Πιστωτικών Καρτών επιβάλλουν τη συμμόρφωση με το πρότυπο μόνο στις Αποδέκτριες Τράπεζες, με τις αντίστοιχες κυρώσεις. Ωστόσο αυτό δε σημαίνει πως η αλυσίδα συναλλαγών αρχίζει και τελειώνει στις Τράπεζες. Κάθε Έμπορος ο οποίος παρέχει τη δυνατότητα πληρωμών με πιστωτικές κάρτες είναι κρίκος της αλυσίδας αυτής, όπως και κάθε τρίτη οντότητα στην οποία αναθέτονται υπηρεσίες αποθήκευσης, μεταφοράς ή επεξεργασίας των δεδομένων πιστωτικών καρτών. Κατά συνέπεια, οι αποδέκτριες τράπεζες οφείλουν να παρουσιάζουν την πιστοποιημένη συμμόρφωσή τους με το PCI DSS και να επιβάλλουν με τη σειρά τους τη συμμόρφωση στους Έμπορους αλλά και τους πάροχους υπηρεσιών, που αναφέρονται σε αυτές. Πρέπει να αναφερθεί πως η χρήση Πάροχων Υπηρεσιών για τις υπηρεσίες μεταφοράς, επεξεργασίας και αποθήκευσης των δεδομένων πιστωτικών καρτών είναι η συνήθης πρακτική από τις Τράπεζες αλλά και από τους Έμπορους. Το λάθος που πολλές φορές γίνεται εδώ είναι να θεωρηθεί πως από τη στιγμή που τα δεδομένα δεν μεταφέρονται, δεν επεξεργάζονται ή δεν αποθηκεύονται στην περίμετρο της Τράπεζας ή του Έμπορου, τότε αυτοί δεν υποχρεούνται να συμμορφωθούν με το πρότυπο. Εφόσον είναι κρίκοι στην αλυσίδα συναλλαγής, η συμμόρφωση επιβάλλεται. Εκκωρώντας την διαχείριση των παραπάνω υπηρεσιών πετυχαίνεται ο περιορισμός του πεδίου εφαρμογής του προτύπου, και κατά συνέπεια απαιτείται μικρότερος προϋπολογισμός για την συμμόρφωση, αλλά όχι η πλήρης κατάργηση της ιδιότητας τους στην αλυσίδα συναλλαγής. Όσο μικρό κι αν είναι το πεδίο εφαρμογής πρέπει να είναι συμμορφούμενο με τις απαιτήσεις το πρότυπου.

### Επιπτώσεις μη συμμόρφωσης

Καθώς η συμμόρφωση με το πρότυπο είναι υποχρεωτική, η μη συμμόρφωση επιβάλλει κυρώσεις. Πιο συγκεκριμένα, οι Οργανισμοί Πιστωτικών Καρτών μπορούν να επιβάλλουν στην Αποδέκτρια Τράπεζα την αύξηση εισφορών σε κάθε διενέργεια συναλλαγής, την αναστολή της ικανότητας να παρέχουν υπηρεσίες συναλλαγής με πιστωτικές κάρτες από τον Οργανισμό που επιβάλλει το πρόστιμο, καθώς και την καταβολή πρόστιμο μεγάου οικονομικού μεγέθους. Παρόλο που αυτά είναι τα άμεσα έξοδα από τις κυρώσεις ενός μη συμμορφούμενου Οργανισμού ή εταιρίας, μέσα από έρευνα της Forrester Research, τα έμμεσα έξοδα που προκύπτουν με την παραβίαση των δεδομένων πιστωτικών καρτών, κυμαίνονται από \$90 έως \$305 ανά εγγραφή (record).

**Figure 1** The Cost Of A Breach, Broken Out For Three Sample Companies

Category	Description	Cost per record		
		Company A: Low-profile breach in a nonregulated industry	Company B: Low-profile breach in a regulated industry	Company C: High-profile breach in a highly regulated industry
Discovery, notification, and response	Outside legal counsel, mail notification, calls, call center, and discounted product offers	\$50	\$50	\$50
Lost employee productivity	Employees diverted from other tasks	\$20	\$25	\$30
Opportunity cost	Customer churn and difficulty in getting new customers	\$20	\$50	\$100
Regulatory fines	FTC, PCI, SOX	\$0	\$25	\$60
Restitution	Civil courts may ask to put this money aside in case breaches are discovered.	\$0	\$0	\$30
Additional security and audit requirements	The security and audit requirements levied as a result of a breach	\$0	\$5	\$10
Other liabilities	Credit card replacement costs. Civil penalties if specific fraud can be traced to the breach.	\$0	\$0	\$25
<b>Total cost per record</b>		<b>\$90</b>	<b>\$155</b>	<b>\$305</b>

Source: Forrester Research, Inc.

Χαρακτηριστικό παράδειγμα μη συμμορφούμενης εταιρίας που υπέστη παραβίαση και υποκλοπή των δεδομένων των κατόχων πιστωτικών καρτών αποτελεί η TJX, της οποίας ο αριθμός των δεδομένων που υποκλάπηκαν υπερβαίνει τα 45 εκατομμύρια. Η παραβίαση έγινε με την εκμετάλλευση των αδυναμιών του πρωτοκόλλου κρυπτογράφησης WEP, ώστε να μπορέσουν να εισβάλουν στο εσωτερικό δίκτυο της εταιρίας μέσω ασύρματης πρόσβασης. Σύμφωνα με την έρευνα της Forrester Research, και υπολογίζοντας το κόστος των \$305 για κάθε αρχείο που έχει υποκλαπεί, η TJX μέχρι να κλείσει η υπόθεση θα έχει πληρώσει πάνω από 100 εκατομμύρια δολάρια (χωρίς τους συμβιβασμούς). Μέχρι σήμερα, και με συμβιβασμό, γνωστοποιήθηκε πως η VISA τους επέβαλλε 40 εκατομμύρια δολάρια.

### Διαδικασία Πιστοποίησης

Η διαδικασία πιστοποίησης συμμόρφωσης με το PCI DSS διαφέρει, ανάλογα με τα χαρακτηριστικά του προς συμμόρφωση Οργανισμού ή Εταιρίας. Έτσι για τις Αποδέκτριες Τράπεζες τους Πάροχους Υπηρεσιών αλλά και τους Έμπορους με πολύ μεγάλο αριθμό συναλλαγών

το χρόνο απαιτείται επιτόπιος έλεγχος κάθε χρόνο, από Qualified Security Assessors καθώς και απομακρυσμένους ελέγχους μη εξουσιοδοτημένης διείσδυσης στο δίκτυο για εύρεση αδυναμιών, από Approved Scanning Vendors, 4 φορές το χρόνο. Σε ότι αφορά τους Έμπορους που δεν ανήκουν στην παραπάνω κατηγορία, απαιτείται η διενέργεια ετησίων ελέγχους μη εξουσιοδοτημένης διείσδυσης στο δίκτυο τους για εύρεση αδυναμιών, από Approved Scanning Vendors, και η αποστολή μιας έκθεσης της απόκλισής τους από την πλήρη συμμόρφωση με πρότυπο, στον εκάστοτε Οργανισμό Πιστωτικών Καρτών καθώς και στο PCI Security Standards Council.

### Υπηρεσίες Συμμόρφωσης από την BESECURE

Η BESECURE δραστηριοποιείται στην παροχή ολοκληρωμένων λύσεων και υπηρεσιών ασφάλειας και διαχείρισης κινδύνου πληροφοριών και παρέχει μια ολιστική προσέγγιση στην ασφάλεια πληροφοριών και την συμμόρφωση ενός Οργανισμού ή μιας Εταιρίας. Για την πλήρη εφαρμογή των απαιτήσεων του πρότυπου PCI DSS, η BESECURE παρέχει συμβουλευτικές υπηρεσίες και λύσεις από την μελέτη μέχρι την πιστοποίηση. Ειδικότερα παρέχονται υπηρεσίες και λύσεις που αφορούν

- Την Εκπόνηση Μελετών Επικινδυνότητας και Προσδιορισμού Απαιτήσεων Ασφάλειας
- Την Ανάπτυξη Πολιτικών και Διαδικασιών για την Διαχείριση της Ασφάλειας Πληροφοριών
- Τον Σχεδιασμό και Ανάπτυξη Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών
- Την Διενέργεια Ελέγχων Συμμόρφωσης βάσει των απαιτήσεων του προτύπου
- Την Διενέργεια Τεχνικών Ελέγχων Ασφάλειας και Δοκιμών Διείσδυσης σε πληροφοριακά συστήματα και δίκτυα δεδομένων και επικοινωνιών
- Την Εκπαίδευση στην Ασφάλεια Πληροφοριών
- Την εγκατάσταση και παραμετροποίηση λύσεων firewalls και ασύρματων δικτυακών υποδομών
- Την παροχή λύσεων κρυπτογράφησης και προστασίας διαρροής πληροφοριών

Η BESECURE σε συνεργασία με το HISP Institute, πραγματοποιεί το Πιστοποιήσιμο Σεμινάριο HISP (Holistic Information Security Practitioner) που παρέχει πρακτική γνώση εφαρμογής βέλτιστων πρακτικών Διαχείρισης Ασφάλειας Πληροφοριών, Ελέγχου Συστημάτων Πληροφορικής και Συμμόρφωσης με κανονισμούς και νομοθεσίες. Το 3ο HISP Certification Training Course, διοργανώνεται από την BESECURE, στις 20-24 Οκτωβρίου στην Αθήνα (περισσότερες πληροφορίες [www.hispcertification.com](http://www.hispcertification.com))



**BESECURE**  
 Λ. Συγγρού 19,  
 117 43 Αθήνα  
 Τηλ. 210 330 7 440  
 Fax 210 330 7 441  
 info@besecure.gr  
 www.besecure.eu