Προετοιμασία και συμμόρφωση με το πρότυπο ασφάλειας δεδομένων καρτών PCI Data Security Standard

besecure
Managed E-Business Security™

Ιστότοπος πληροφοριών www.pcidsscompliance.eu

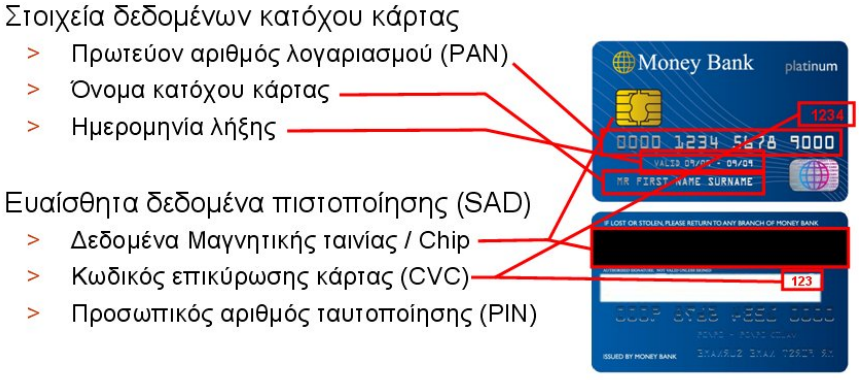
Σύμφωνα με σχετικές έρευνες σε περίπτωση συμβάντος παραβίασης ασφάλειας 49% των πελατών θεωρούν ότι ευθύνονται οι εμπορικές επιχειρήσεις & 3 στους 4 πελάτες δε θα προχωρήσουν σε αγορές ποτέ ξανά από τη συγκεκριμένη εμπορική επιχείρηση

Πηγή: Javelin Strategy and Research 2007

Η παραβίαση της ασφάλειας δεδομένων καρτούχων αποτελεί πλήγμα τόσο για τη φήμη των εμπόρων και όσο και για την εμπιστοσύνη των πελατών τους. Έρευνα που διεξήχθη από την Javelin Strategy & Research[1], έδειξε ότι η εικόνα που έχουν οι πελάτες για τη φήμη ενός εμπόρου σε επίπεδο προστασίας πληροφοριών λογαριασμών καρτών έχει άμεση σχέση με την προθυμία τους να τον επιλέξουν για τις αγορές τους. Μόλις το 22 τοις εκατό των ερωτηθέντων είπαν ότι πιθανότατα θα συνέχιζαν να κάνουν αγορές από έναν έμπορο αν μάθαιναν για περιστατικό παραβίασης δεδομένων που θα μπορούσε να διακυβεύσει τις πληροφορίες λογαριασμού της κάρτας τους, ενώ το 78 τοις εκατό είπε ότι πιθανότατα δεν θα διάλεγαν να κάνουν ξανά τις αγορές τους σε αυτόν. Εκτός από την απώλεια της πελατειακής πίστης, μια παραβίαση μπορεί να οδηγήσει σε αρνητική δημοσιότητα, σε πρόστιμα από τράπεζες ή κυβερνητικούς και ρυθμιστικούς φορείς, καθώς και σε εμπλοκή σε δικαστικούς αγώνες. Στην περίπτωση των μικρών επιχειρήσεων, το οικονομικό κόστος λήψης επανορθωτικών μέτρων σε περίπτωση παραβίασης μπορεί να είναι αρκετό για να οδηγήσει σε χρεοκοπία.

Γενικά για το πρότυπο ασφάλειας PCI DSS

Ο στόχος του PCI DSS είναι η προστασία των δεδομένων καρτούχων που επεξεργάζονται, αποθηκεύονται ή μεταδίδονται από τις εμπορικές επιχειρήσεις. Οι μηχανισμοί ασφάλειας και οι διαδικασίες που απαιτούνται από το πρότυπο, είναι ζωτικής σημασίας για την προστασία των δεδομένων καρτούχων που περιλαμβάνουν, μεταξύ άλλων, τον αριθμό λογαριασμού (Primary Account Number – PAN) ο οποίος βρίσκεται εκτυπωμένος στο μπροστινό μέρος της κάρτας πληρωμής. Οι εμπορικές επιχειρήσεις και οι πάροχοι υπηρεσιών που εμπλέκονται στη διαδικασία επεξεργασίας συναλλαγών με κάρτες πληρωμής, δεν πρέπει ποτέ να αποθηκεύουν ευαίσθητα δεδομένα αυθεντικοποίησης μετά το πέρας της διαδικασίας έγκρισης μιας συναλλαγής. Στα δεδομένα αυτά συμπεριλαμβάνονται ευαίσθητα δεδομένα τα οποία βρίσκονται εκτυπωμένα στην κάρτα ή είναι αποθηκευμένα στη μαγνητική ταινία ή στο chip της κάρτας, καθώς επίσης και το PIN που εισάγεται από τον κάτοχό της



[1] https://www.javelinstrategy.com/uploads/files/707.RP_DataBreaches&BuyerBehavior_Brochure.pdf

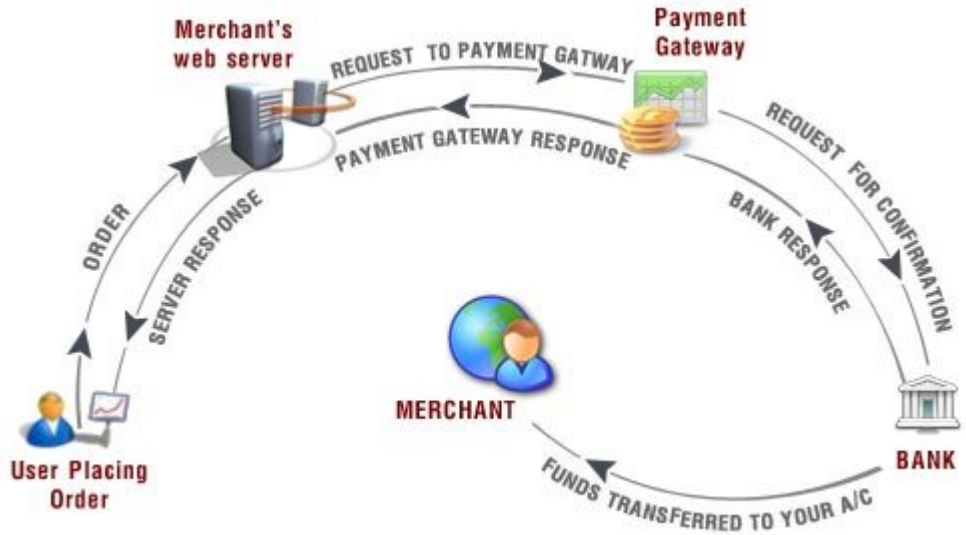
Σύμφωνα με έρευνα της Forrester "The State of PCI Compliance[2]" που διεξήχθει σε επιχειρήσεις στις Η.Π.Α. και στην Ευρώπη αποκαλύπτει πρακτικές που μπορούν να θέσουν σε κίνδυνο τα δεδομένα των καρτούχων. Συγκεκριμένα :

- 81% των επιχειρήσεων αποθηκεύουν του αριθμούς καρτών πληρωμής,
- 73% των επιχειρήσεων αποθηκεύουν τις ημερομηνίες λήξης των καρτών πληρωμής,
- 71% των επιχειρήσεων αποθηκεύουν τους κωδικούς επικύρωσης των καρτών πληρωμής,
- 57% των επιχειρήσεων αποθηκεύουν τα δεδομένα της μαγνητικής ταινίας των καρτών πληρωμής,

16% των επιχειρήσεων αποθηκεύουν άλλα προσωπικά δεδομένα.

Αδυναμίες (ή αλλιώς ευπάθειες) που σχετίζονται με τις εμπορικές επιχειρήσεις μπορούν να εμφανιστούν σχεδόν οπουδήποτε στην αλυσίδα επεξεργασίας των πληρωμών με κάρτες, συμπεριλαμβανομένων των συσκευών POS, των προσωπικών Η/Υ και διακομιστών, των ασύρματων σημείων πρόσβασης (hotspots) ή των εφαρμογών για αγορές στο web, των συστημάτων αποθήκευσης που βασίζονται στο χαρτί και στην διαβίβαση δεδομένων καρτούχων στους παρόχους υπηρεσιών (credit cards service providers).

Αδυναμίες μπορεί να υπάρξουν ακόμη και στα συστήματα που χρησιμοποιούνται από τους παρόχους υπηρεσιών και τις τράπεζες (acquirers), εκείνα δηλαδή τα χρηματοπιστωτικά ιδρύματα που είναι υπεύθυνα για την έναρξη και τη διατήρηση επιχειρηματικών σχέσεων με τις εμπορικές επιχειρήσεις που δέχονται κάρτες πληρωμών. Η συμμόρφωση με το Πρότυπο Ασφάλειας Δεδομένων PCI DSS μετριάζει τις ευπάθειες και κατά συνέπεια ενισχύει το συνολικό επίπεδο προστασίας δεδομένων των καρτούχων.



[2] http://www.rsa.com/solutions/PCI/ar/RSA_AR_State_of_PCI_Compliance.pdf

Τα Πρότυπα Ασφάλειας PCI

Τα Πρότυπα Ασφάλειας PCI αποτελούν τεχνικές και λειτουργικές απαιτήσεις που καθορίζονται από το Συμβούλιο Προτύπων Ασφάλειας - PCI Council και έχουν ως σκοπό την προστασία των δεδομένων των καρτούχων. Τα πρότυπα ισχύουν για όλους τους οργανισμούς που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα καρτούχων και παρέχουν καθοδήγηση σε προγραμματιστές λογισμικού και κατασκευαστές εφαρμογών και συσκευών που χρησιμοποιούνται σε τέτοιου είδους συναλλαγές. Το Συμβούλιο είναι αρμόδιο για τη διαχείριση των προτύπων ασφάλειας, ενώ η συμμόρφωση με το σύνολο των προτύπων PCI επιβάλλεται από τα ιδρυτικά μέλη του Συμβουλίου, δηλαδή την American Express, τη Discover Financial Services, τη JCB,τη MasteCard Worldwide και τη Visa Inc. Το Συμβούλιο Προτύπων Ασφάλειας - PCI Council έχει καθορίσει τα ακόλουθα πρότυπα ασφάλειας :

Πρότυπο Ασφάλειας Δεδομένων (PCI DSS)

Το PCI DSS ισχύει για όλες τις οντότητες που αποθηκεύουν, επεξεργάζονται, και / ή μεταδίδουν δεδομένα των καρτούχων. Καλύπτει τα τεχνικά και λειτουργικά τμήματα των συστημάτων που περιλαμβάνονται ή συνδέονται με τα δεδομένα των καρτούχων. Εάν μια εμπορική επιχείρηση δέχεται ή επεξεργάζεται κάρτες πληρωμών, τότε πρέπει να συμμορφωθεί με τις απαιτήσεις του Προτύπου PCI DSS.

Πρότυπο Συσκευών εισαγωγής PIN (PIN Transaction Security – PCI PTS)

Το Πρότυπο Συσκευών Εισαγωγής PIN (Personal Identification Number) απευθύνεται σε κατασκευαστές που προδιαγράφουν και υλοποιούν τόσο τα χαρακτηριστικά συσκευών όσο και τη διαχείριση τερματικών εισαγωγής προσωπικού αριθμού αναγνώρισης που χρησιμοποιούνται για οικονομικές συναλλαγές με κάρτες πληρωμών. Οι εμπορικές επιχειρήσεις πρέπει να χρησιμοποιούν συσκευές εισαγωγής PIN που έχουν ελεγχθεί και εγκριθεί από το Συμβούλιο Προτύπων Ασφάλειας PCI. Οι συσκευές που έχουν εγκριθεί από το Συμβούλιο παρατίθενται στην ακόλουθη ιστοσελίδα:
www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

Το κόστος ενός συμβάντος παραβίασης ασφάλειας κυμαίνεται από $90 έως $305 ανά εγγραφή (record)

Πηγή Forrester Research “Calculating The Cost Of A Security Breach”

Πρότυπο Ασφάλειας Εφαρμογών Πληρωμών (PCI PA – DSS)

Το Πρότυπο Ασφάλειας Εφαρμογών Πληρωμών απευθύνεται σε προγραμματιστές και σε integrators εφαρμογών πληρωμών οι οποίες αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα καρτούχων ως τμήμα της έγκρισης ή της εκκαθάρισης της συναλλαγής, και εφόσον οι εφαρμογές αυτές πωλούνται, διανέμονται ή χορηγούνται μέσω άδειας σε τρίτους. Οι περισσότεροι οργανισμοί καρτών ενθαρρύνουν τις εμπορικές επιχειρήσεις να χρησιμοποιούν εφαρμογές πληρωμών που ελέγχονται και εγκρίνονται από το Συμβούλιο Προτύπων Ασφάλειας PCI. Οι εφαρμογές πληρωμών που έχουν επικυρωθεί από το Συμβούλιο παρατίθενται στην ακόλουθη ιστοσελίδα:

www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php

Επιπτώσεις μη συμμόρφωσης

Καθώς η συμμόρφωση με το πρότυπο είναι υποχρεωτική, η μη συμμόρφωση επιβάλει 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 πρόστιμου μεγάλου οικονομικού μεγέθους. Παρόλο που αυτά είναι τα άμεσα έξοδα από τις κυρώσεις ενός μη συμμορφούμενου Οργανισμού ή εταιρίας, μέσα από έρευνα της Forrester Research “Calculating The Cost Of A Security Breach[3]”, τα έμμεσα έξοδα που προκύπτουν με την παραβίαση των δεδομένων πιστωτικών καρτών, κυμαίνονται από $90 έως $305 ανά εγγραφή. Ενδεικτικά, η VISA, μπορεί να επιβάλει ανλά συμβάν παραβίασης ασφάλειας δεδομένων καρτούχων, πρόστιμο έως και $ 500.000[4]

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). Τα άμεσα κόστη που πληρώθηκαν στην VISA με συμβιβασμό, ανήλθαν στα 40 εκατομμύρια δολάρια[5].

Οφέλη Συμμόρφωσης

Η συμμόρφωση με το πρότυπο εξασφαλίζει σημαντικά οφέλη στην επιχείρηση που το εφαρμόζει.

- Διασφάλιση δημόσιας εικόνας / φήμης της επιχείρησης
- Διασφάλιση των μετόχων της επιχείρησης
- Ενίσχυση της εμπιστοσύνης πελατών
- Αποφυγή αρνητικής δημοσιότητας

[3] http://www.forrester.com/rb/Research/calculating_cost_of_security_breach/q/id/42082/t/2
[4] http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html
[5] http://corporate.visa.com/media-center/press-releases/press748.jsp

- Βελτίωση συνολικού επιπέδου ασφάλειας/ Μείωση κινδύνων:
- Βελτιστοποίηση εσωτερικών διαδικασιών
- Βελτιστοποίηση τεχνολογιών ασφάλειας
- Αποφυγή οικονομικών επιβαρύνσεων / κυρώσεων
- Διατήρηση δυνατότητας αποδοχής συναλλαγών με πιστωτικές κάρτες
- Αποφυγή δαπανών έρευνας ηλεκτρονικού εγκλήματος & νομικών εξόδων (σε περίπτωση περιστατικού διακύβευσης)
- Κάλυψη συναφών απαιτήσεων συμμόρφωσης διαφορετικών προτύπων / κανονιστικών απαιτήσεων (π.χ. SOX, ΑΔΑΕ, ISO27001)

Απαιτήσεις Προτύπου Ασφάλειας Δεδομένων (PCI DSS)

Το πρότυπο PCI DSS αποτελείται από 6 βασικούς στόχους καθένας από τους οποίους έχει συγκεκριμένες απαιτήσεις, οι οποίες ανέρχονται συνολικά σε δώδεκα. Καθεμία από τις 12 απαιτήσεις έχει συγκεκριμένη λογική και μπορεί να αναλυθεί περαιτέρω σε υπο-απαιτήσεις. Οι ενότητες καλύπτουν ένα ευρύ φάσμα μηχανισμών ασφαλείας που άπτονται διοικητικών θεμάτων (πολιτικές και διαδικασίες), θεμάτων φυσικής ασφάλειας καθώς και τεχνικών θεμάτων (passwords, κρυπτογράφηση δεδομένων, κτλ).

Στόχοι	**Απαιτήσεις**
Εγκατάσταση και Συντήρηση Ασφαλούς Δικτύου	1. Εγκατάσταση και συντήρηση firewalls για την προστασία των δεδομένων των καρτούχων 2. Αποφυγή χρήσης προκαθορισμένων από τους κατασκευαστές κωδικών πρόσβασης και ρυθμίσεων ασφάλειας
Προστασία Δεδομένων Καρτούχων	3. Προστασία αποθηκευμένων δεδομένων καρτούχων 4. Κρυπτογράφηση δεδομένων καρτούχων κατά τη μετάδοσή τους σε ανοικτά, δημόσια δίκτυα
Συντήρηση Προγράμματος Διαχείρισης Αδυναμιών Ασφάλειας	5. Χρήση και περιοδική ενημέρωση λογισμικού προστασίας από κακόβουλο λογισμικό (anti-virus) 6. Ανάπτυξη και συντήρηση ασφαλών συστημάτων και εφαρμογών
Υλοποίηση Ισχυρών Μέτρων Ελέγχου Πρόσβασης	7. Περιορισμός πρόσβασης στα δεδομένα των 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
Περιοδική Παρακολούθηση και Έλεγχος Δικτύων	10. Εντοπισμός και παρακολούθηση οποιασδήποτε πρόσβασης σε δικτυακούς πόρους 11. Περιοδικός έλεγχος συστημάτων και διαδικασιών ασφάλειας
Τήρηση Πολιτικής Ασφάλειας Πληροφοριών	12. Τήρηση πολιτικής ασφάλειας πληροφοριών

Επίτευξη Συμμόρφωσης με το PCI DSS

Οι εμπορικές επιχειρήσεις και οι οργανισμοί που αποθηκεύουν, επεξεργάζονται και μεταδίδουν δεδομένα καρτούχων πρέπει να συμμορφώνονται με το PCI DSS. Ενώ το Συμβούλιο είναι υπεύθυνο για τη διαχείριση των προτύπων ασφάλειας δεδομένων, κάθε οργανισμός καρτών διατηρεί ξεχωριστά το δικό του πρόγραμμα επιβολής της συμμόρφωσης. Κάθε οργανισμός καρτών έχει ορίσει ειδικές απαιτήσεις που αφορούν τόσο στον τρόπο επικύρωσης της συμμόρφωσης, όπως είναι για παράδειγμα οι διατάξεις που αφορούν στη διαδικασία αυτό - αξιολόγησης έναντι της χρήσης Πιστοποιημένων Αξιολογητών Ασφάλειας (QSAs).

Ανάλογα με τη διαβάθμιση ή το επίπεδο επικινδυνότητας του κάθε οργανισμού, όπως αυτό καθορίζεται από τους οργανισμούς καρτών, η μέθοδος για την επικύρωση της συμμόρφωσης και του τρόπου υποβολής των αναφορών συμμόρφωσης στα χρηματοπιστωτικά ιδρύματα, συνήθως ακολουθεί την παρακάτω σειρά βημάτων:

- Ανάλυση Εύρους Εφαρμογής PCI DSS (PCI DSS Scooping) - προσδιορισμός των συστημάτων που καλύπτονται από το PCI DSS.
- Δειγματοληψία (Sampling) – έλεγχος συμμόρφωσης υποσυνόλου των συστημάτων που ανήκουν στο εύρος εφαρμογής.
- Αντισταθμιστικά Μέτρα (Compensating Controls) – επικύρωση των αντισταθμιστικών μέτρων από τον Πιστοποιημένο Αξιολογητή Ασφάλειας.
- Υποβολή Αναφορών (Reporting) - Ο αξιολογητής και / ή η εμπορική επιχείρηση / οργανισμός υποβάλει τις απαιτούμενες αναφορές

Διευκρινήσεις – Ο αξιολογητής και / ή η εμπορική επιχείρηση / οργανισμός διευκρινίζει / ενημερώνει τις αναφορές που έχει υποβάλλει (εφόσον ενδείκνυται) κατόπιν αιτήματος των τραπεζών.

Προγράμματα Συμμόρφωσης Οργανισμών καρτών

Συγκεκριμένες ερωτήσεις που αφορούν στα επίπεδα επικύρωσης συμμόρφωσης πρέπει να απευθύνονται προς τα χρηματοπιστωτικά ιδρύματα. Μόνο τα χρηματοπιστωτικά ιδρύματα μπορούν να ορίσουν το επίπεδο επικύρωσης των εμπορικών επιχειρήσεων. Παρακάτω παρατίθενται σύνδεσμοι στα προγράμματα συμμόρφωσης των οργανισμών καρτών:

- American Express: www.americanexpress.com/datasecurity
- Discover: www.discovernetwork.com/fraudsecurity/disc.html
- JCB: www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide: www.mastercard.com/sdp
- Visa Inc: www.visa.com/cisp
- Visa Europe: www.visaeurope.com/ais

Ορισμός Επίπεδων Εμπόρων σύμφωνα με την VISA

Όλοι οι έμποροι εμπίπτουν σε ένα από τα τέσσερα επίπεδα εμπόρων με βάση τον όγκο των συναλλαγών VISA για μια περίοδο 12 μηνών συμπεριλαμβανομένων των πιστωτικών, χρεωστικών και προπληρωμένων καρτών. Εκτός από την τήρηση του PCI DSS, η επικύρωση της συμμόρφωσης απαιτείται για Επίπεδο 1, Επίπεδο 2 και Επίπεδο 3 εμπόρους, και μπορεί να απαιτηθεί για εμπόρους Επιπέδου 4. Το PCI DSS ορίζει ότι όλοι οι έμποροι που έχουν πρόσβαση σε δημόσια δίκτυα, μέσω δημόσιων διευθύνσεων IP πρέπει να διενεργούν τριμηνιαίους εξωτερικούς ελέγχους δικτύου, προκειμένου να είναι συμμορφούμενοι ως προς τις απαιτήσεις του προτύπου. Οι αποδέκτριες τράπεζες μπορεί να απαιτηθεί να υποβάλουν επίσης τις τριμηνιαίες εκθέσεις εξωτερικών ελέγχων ή / και των ερωτηματολογίων των εμπόρων ορισμένων ως Επίπεδο 4.

Επίπεδο Εμπόρου	Κριτήρια	Επιτόπιος Έλεγχος Συμμόρφωσης	Υποβολή Ερωτηματολογίου Αυτό - Αξιολόγησης	Δικτυακός Έλεγχος Ασφάλειας Αδυναμιών
Επίπεδο 1	▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών με περισσότερες από 6.000.000 VISA συναλλαγές το χρόνο. ▪ Επιχειρήσεις οι οποίες έχουν υποστεί διαρροή δεδομένων καρτών.	Απαιτείται Ετησίως από Πιστοποιημένο Αξιολογητή Ασφάλειας (QSA)	Δεν απαιτείται	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV
Επίπεδο 2	Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών με 1.000.000 έως 6.000.000 VISA συναλλαγές το χρόνο	Δεν απαιτείται	Απαιτείται Ετησίως	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV
Επίπεδο 3	Επιχειρήσεις με 20.000 έως 1.000.000 VISA συναλλαγές μέσω καναλιών ηλεκτρονικού εμπορίου το χρόνο.	Δεν απαιτείται	Απαιτείται Ετησίως	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV
Επίπεδο 4	▪ Επιχειρήσεις με λιγότερες από 20.000 VISA συναλλαγές μέσω καναλιών ηλεκτρονικού εμπορίου το χρόνο. ▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών με λιγότερες από 1.000.000 VISA συναλλαγές το χρόνο	Δεν απαιτείται	Απαιτείται Ετησίως σύμφωνα με την πολιτική των αποδεκτριών τραπεζών	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV σύμφωνα με την πολιτική των αποδεκτριών τραπεζών

Ορισμός Επίπεδων Εμπόρων σύμφωνα με την Mastercard

Ακολούθως παρουσιάζονται οι απαιτήσεις συμμόρφωσης των 4 επιπέδων εμπόρων που διενεργούν συναλλαγές με κάρτες Mastercard ως ορίζονται από το πρόγραμμα Site Data Protection (SDP) της MasterCard.

Επίπεδο Εμπόρου	Κριτήρια	Επιτόπιος Έλεγχος Συμμόρφωσης	Υποβολή Ερωτηματο-λογίου Αυτό - Αξιολόγησης	Δικτυακός Έλεγχος Ασφάλειας Αδυναμιών
Επίπεδο 1	▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών με περισσότερες από 6.000.000 MasterCard και Maestro συναλλαγές το χρόνο ▪ Επιχειρήσεις οι οποίες έχουν υποστεί διαρροή δεδομένων καρτών. ▪ Εμπορικές επιχειρήσεις οι οποίες κατηγοριοποιούνται κατά την κρίση των Mastercard & VISA ως Επιπέδου 1	Απαιτείται Ετησίως από Πιστοποιημένο Αξιολογητή Ασφάλειας (QSA)	Δεν απαιτείται	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV
Επίπεδο 2	▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών με 1.000.000 έως 6.000.000 MasterCard και Maestro συναλλαγές το χρόνο ▪ Εμπορικές επιχειρήσεις οι οποίες κατηγοριοποιούνται κατά την κρίση της VISA ως Επιπέδου 2.	Δεν απαιτείται	Απαιτείται Ετησίως	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV
Επίπεδο 3	▪ Επιχειρήσεις με 20.000 έως 1.000.000 MasterCard και Maestro συναλλαγές μέσω καναλιών ηλεκτρονικού εμπορίου το χρόνο. ▪ Εμπορικές επιχειρήσεις οι οποίες κατηγοριοποιούνται κατά την κρίση της VISA ως Επιπέδου 3.	Δεν απαιτείται	Απαιτείται Ετησίως	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV
Επίπεδο 4	▪ Επιχειρήσεις με λιγότερες από 20.000 MasterCard και Maestro συναλλαγές μέσω καναλιών ηλεκτρονικού εμπορίου το χρόνο. ▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών με λιγότερες από 1.000.000 MasterCard και Maestro συναλλαγές συναλλαγές το χρόνο	Δεν απαιτείται	Απαιτείται Ετησίως	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV

Ορισμός Επίπεδων Εμπόρων σύμφωνα με την American Express

Ακολούθως παρουσιάζονται οι απαιτήσεις συμμόρφωσης των 3 επιπέδων εμπόρων που διενεργούν συναλλαγές με κάρτες American Express

Επίπεδο Εμπόρου	Κριτήρια	Επιτόπιος Έλεγχος Συμμόρφωσης	Υποβολή Ερωτηματο-λογίου Αυτό - Αξιολόγησης	Δικτυακός Έλεγχος Ασφάλειας Αδυναμιών
Επίπεδο 1	▪ Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών με περισσότερες από 2.500.000 AMEX συναλλαγές το χρόνο ▪ Επιχειρήσεις οι οποίες έχουν υποστεί διαρροή δεδομένων καρτών. ▪ Εμπορικές επιχειρήσεις οι οποίες κατηγοριοποιούνται κατά την κρίση της American Express ως Επιπέδου 1.	Απαιτείται Ετησίως από Πιστοποιημένο Αξιολογητή Ασφάλειας (QSA)	Δεν απαιτείται	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV
Επίπεδο 2	Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών με 50.000 έως 2.500.000 AMEX συναλλαγές το χρόνο	Δεν απαιτείται	Απαιτείται Ετησίως	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV
Επίπεδο 3	Επιχειρήσεις, ανεξαρτήτως καναλιού πληρωμών με λιγότερες από 50.000 AMEX συναλλαγές το χρόνο	Δεν απαιτείται	Απαιτείται Ετησίως[6]	Απαιτείται τριμηνιαία από Πιστοποιημένο ASV[7]

[6] Οι έμποροι Επιπέδου 3 δεν χρειάζεται να υποβάλλουν έγγραφα τεκμηρίωσης, αλλά πρέπει να συμμορφώνονται με τις απαιτήσεις του προτύπου PCI DSS

[7] Οι έμποροι Επιπέδου 3 δεν χρειάζεται να υποβάλλουν έγγραφα τεκμηρίωσης, αλλά πρέπει να συμμορφώνονται με τις απαιτήσεις του προτύπου PCI DSS

Ερωτηματολόγιο Αυτό – Αξιολόγησης

Οι εμπορικές επιχειρήσεις και οι πάροχοι υπηρεσιών που δεν απαιτείται να προβούν σε επιτόπιες αξιολογήσεις για τη συμμόρφωσή τους με το πρότυπο PCI DSS πρέπει να συμπληρώσουν το Ερωτηματολόγιο Αυτό – Αξιολόγησης (Self Assessment Questionnaire – SAQ) το οποίο αποτελεί ένα εργαλείο αυτό – επικύρωσης της συμμόρφωσής τους. Για το λόγο αυτό, έχουν προσδιοριστεί διαφορετικά είδη ερωτηματολογίων αυτό – αξιολόγησης που απευθύνονται σε διαφορετικούς τύπους επιχειρηματικών δραστηριοτήτων. Ο τύπος επικύρωσης του SAQ δεν συνδέεται με τη διαβάθμιση ή το επίπεδο επικινδυνότητας της εμπορικής επιχείρησης. Περισσότερες λεπτομέρειες είναι διαθέσιμες ακολούθως:

Περιγραφή	SAQ
Στην κατηγορία αυτή συμπεριλαμβάνονται εμπορικές επιχειρήσεις που δέχονται συναλλαγές χωρίς φυσική παρουσία της κάρτας (Card – Not – Present – ηλεκτρονικό εμπόριο, ταχυδρομικά, τηλεφωνικά) και εμπορικές επιχειρήσεις που έχουν αναθέσει τη διαχείριση των δεδομένων καρτούχων σε τρίτους. Στην κατηγορία αυτή δεν συμπεριλαμβάνονται εμπορικές επιχειρήσεις οι οποίες συναλλάσσονται με τους πελάτες τους πρόσωπο με πρόσωπο	A
Στην κατηγορία αυτή συμπεριλαμβάνονται εμπορικές επιχειρήσεις οι οποίες χρησιμοποιούν συσκευές χειροκίνητης καταγραφής των στοιχείων των πιστωτικών καρτών (imprint) και δεν αποθηκεύουν δεδομένα καρτούχων σε ηλεκτρονική μορφή ή αυτόνομα dial – up τερματικά (POS) και δεν αποθηκεύουν σε ηλεκτρονική μορφή δεδομένα καρτούχων	B
Στην κατηγορία αυτή συμπεριλαμβάνονται εμπορικές επιχειρήσεις που χρησιμοποιούν μόνο web-based εικονικά τερματικά και δεν αποθηκεύουν σε ηλεκτρονική μορφή δεδομένα καρτούχων	C-VT
Στην κατηγορία αυτή συμπεριλαμβάνονται εμπορικές επιχειρήσεις που χρησιμοποιούν συστήματα εφαρμογών πληρωμής που συνδέονται στο Διαδίκτυο και δεν αποθηκεύουν δεδομένα καρτούχων	C
Όλες οι υπόλοιπες εμπορικές επιχειρήσεις (που δεν συμπεριλαμβάνονται στις παραπάνω κατηγορίες) και όλοι οι πάροχοι υπηρεσιών που επιλέγονται από τους οργανισμούς καρτών για να συμπληρώσουν το SAQ	D

Απαιτήσεις PCI DSS **σύμφωνα με την κατηγορία** SAQ

Σύμφωνα με την κατηγορία ερωτηματολογίου αυτό αξιολόγησης που εμπίπτουν οι έμποροι, πρέπει να συμμορφώνονται με συγκεκριμένες απαιτήσεις του προτύπου

Στόχοι PCI DSS	**Περιγραφή των απαιτήσεων**	SAQ A	SAQ B	SAQ C-VT	SAQ C	SAQ D
1	Εγκατάσταση και συντήρηση firewalls για την προστασία των δεδομένων των καρτούχων	✘	✘	✓	✓	✓
2	Αποφυγή χρήσης προκαθορισμένων από τους κατασκευαστές κωδικών πρόσβασης και ρυθμίσεων ασφάλειας	✘	✘	✓	✓	✓
3	Προστασία αποθηκευμένων δεδομένων καρτούχων	✘	✘	✓	✓	✓
4	Κρυπτογράφηση δεδομένων καρτούχων κατά τη μετάδοσή τους σε ανοικτά, δημόσια δίκτυα	✘	✘	✓	✓	✓
5	Χρήση και περιοδική ενημέρωση λογισμικού προστασίας από κακόβουλο λογισμικό (anti-virus)	✘	✘	✓	✓	✓
6	Ανάπτυξη και συντήρηση ασφαλών συστημάτων και εφαρμογών	✘	✘	✓	✓	✓
7	Περιορισμός πρόσβασης στα δεδομένα των 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	✓	✓	✓	✓	✓
10	Εντοπισμός και παρακολούθηση οποιασδήποτε πρόσβασης σε δικτυακούς πόρους	✘	✘	✘	✘	✓
11	Περιοδικός έλεγχος συστημάτων και διαδικασιών ασφάλειας	✘	✘	✘	✓	✓
12	Τήρηση πολιτικής ασφάλειας πληροφοριών	✓	✓	✓	✓	✓

Υπηρεσίες και λύσεις της BESECURE **σχετικά με το πρότυπο** PCI

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

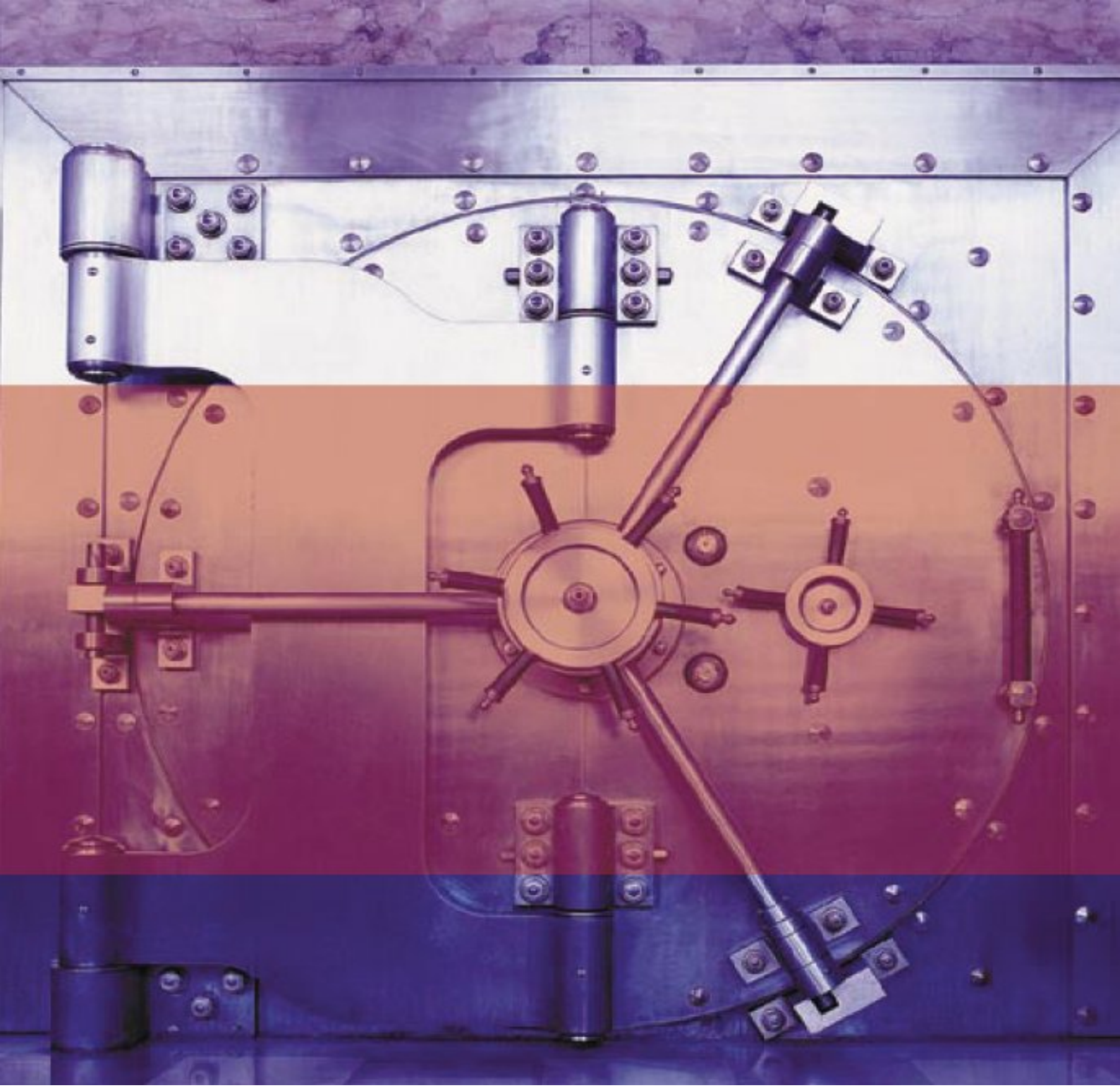
- Την Εκπόνηση Μελετών Επικινδυνότητας και Προσδιορισμού Απαιτήσεων Ασφάλειας
- Την Ανάπτυξη Πολιτικών και Διαδικασιών για την Διαχείριση της Ασφάλειας Πληροφοριών
- Τον Σχεδιασμό και Ανάπτυξη Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών
- Την Διενέργεια Ελέγχων Συμμόρφωσης βάση των απαιτήσεων του προτύπου
- 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 ασφάλειας για όλο το εύρος απαιτήσεων του προτύπου

Επιπρόσθετα η BESECURE σε συνεργασία με το HISP Institute, πραγματοποιεί το Πιστοποιήσιμο Σεμινάριο HISP (Holistic Information Security Practitioner[8]) που παρέχει πρακτική γνώση εφαρμογής βέλτιστων πρακτικών Διαχείρισης Ασφάλειας Πληροφοριών, Ελέγχου Συστημάτων Πληροφορικής και Συμμόρφωσης με κανονισμούς και νομοθεσίες.

Σχετικά με την BESECURE

Η BESECURE καλύπτει όλο το φάσμα των υπηρεσιών και λύσεων που σχετίζονται με την ασφάλεια των πληροφορικών συστημάτων και την εφαρμογή συστημάτων διαχείρισης ασφάλειας πληροφοριών. Οι υπηρεσίες και λύσεις ασφάλειας πληροφοριών που παρέχονται έχουν αναπτυχθεί και καλύπτουν όλες τις φάσεις του κύκλου ζωής της ασφάλειας πληροφοριών όπως τον ορίζουμε στην BESECURE. Ενδεικτικές υπηρεσίες αφορούν : Εκπόνησης Μελετών Επικινδυνότητας και Προσδιορισμού Απαιτήσεων Ασφάλειας, Υπηρεσίες Σχεδιασμού Αρχιτεκτονικής Ασφάλειας Πληροφορικής Υποδομής, Σχεδιασμού και Ανάπτυξη Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών βάση προτύπου ISO/IEC 27001:2005, Υπηρεσίες Διαχείρισης & Παρακολούθησης Υποδομών Ασφαλείας, Υπηρεσίες Έλεγχου & Πιστοποίησης Ασφάλειας βάση διεθνών προτύπων και βέλτιστων πρακτικών, Διενέργειας Τεχνικών Ελέγχων Ασφάλειας και Δοκιμών Διείσδυσης σε πληροφορικά συστήματα και δίκτυα δεδομένων και επικοινωνιών και Υπηρεσίες εκπαίδευσης στην Ασφάλεια Πληροφοριών. Η BESECURE, στα πλαίσια των εκπαιδευτικών υπηρεσιών που παρέχει, έχει συνάψει στρατηγικές συνεργασίες για τη διεξαγωγή αναγνωρισμένων σεμιναρίων που θέτουν τις κατάλληλες βάσεις για την ανάπτυξη Συστημάτων Διαχείρισης Ασφάλειας Πληροφοριών που θα υποστηρίξουν τις απαιτήσεις Εταιρικής Διακυβέρνησης & Διακυβέρνησης Ασφάλειας των εταιρειών επιτρέποντας την υγιή ανάπτυξή τους και τη συμμόρφωσή τους με πρότυπα, κανονισμούς και νομοθεσίες που υπόκεινται.

[8] http://www.hispcertification.com/



besecure
Managed E-Business Security™

TÜV AUSTRIA HELLAS
EN ISO 27001:2005
No. : 0808012

DIN EN ISO 9001:2008

19, Syggrou Ave.
GR - 117 43, Athens, Greece,
Tel.: +30 210 330 7 440
Fax: +30 210 330 7 441

e-mail: info@besecuregroup.com
web: www.besecuregroup.com

131, Gladstonos Street
Kermia Court, 3317 Limassol – Cuprus,
Tel. +357 25 376 800
Fax: +357 25 376 799