Τα capital controls, τα e-shops και οι κίνδυνοι

Η υιοθέτηση του πλαστικού χρήματος ανεβάζει τον πήχη ασφαλείας

Γράφει ο
Νίκος Γεωργόπουλος,
MBA, CyRM. Cyber Risk Advisor

Card boom

Μετά την επιβολή των capital controls και των περιορισμών χρήσης φυσικού χρήματος αυξήθηκε ραγδαία η χρήση πλαστικού χρήματος (χρεωστικών και πιστωτικών καρτών) για τις αγορές αγαθών και πληρωμές οικονομικών υποχρεώσεων στα φυσικά σημεία πώλησης και στο ηλεκτρονικό επιχειρείν.

Ενδεικτικά ο αριθμός των καρτών που κυκλοφορούν αυξήθηκε αυτή την περίοδο κατά ένα περίπου εκατομμύριο.

Σύμφωνα με υπολογισμούς η Alpha Bank εξέδωσε περίπου 220.000 χρεωστικές κάρτες τον Ιούλιο, περισσότερες από όσες είχε εκδώσει συνολικά το 2014! Η Εθνική Τράπεζα εξέδωσε τις προηγούμενες τέσσερις εβδομάδες περισσότερες από 400.000 χρεωστικές κάρτες. Ενδεικτικό τούτου είναι ότι σύμφωνα με την Visa Europe, ο αριθμός των ενεργών χρεωστικών καρτών Visa στην Ελλάδα υπερδιπλασιάστηκε τον Ιούλιο σε σχέση με τους προηγούμενους μήνες. Μάλιστα τις δυο εβδομάδες που ακολούθησαν την επιβολή των capital controls οι συναλλαγών με κάρτες της ίδια εταιρείας αυξήθηκαν κατά 135%.

Οι πελάτες χρησιμοποιούν πλέον πλαστικό χρήμα για τις αγορές τους και οι έμποροι χρησιμοποιούν μηχανάκια POS ή e-POS για την διεκπεραίωση των συναλλαγών αυτών. Κατά την διαδικασία αγοράς (καλάθι αγορών) από e-shops κάθε πελάτης επιλέγει το προϊόν που θέλει να αγοράσει, συμπληρώνει προσωπικά του δεδομένα και χρησιμοποιεί πιστωτικές ή χρεωστικές κάρτες για την ολοκλήρωση της συναλλαγής.

Τα δεδομένα των συναλλαγών πλαστικού χρήματος αποτελούν στόχο κάθε κυβερνοεγκληματία γιατί μπορούν εύκολα να πουληθούν στην μαύρη αγορά.

Στον πίνακα που ακολουθεί φαίνονται οι τιμές πώλησης δεδομένων πιστωτικών καρτών ανάλογα με τα διαθέσιμα χαρακτηριστικά τους και την γεωγραφική περιοχή που έλαβε χώρα η κλοπή τους στη μαύρη αγορά του διαδικτύου. (*Πίνακας*)

Εάν δεδομένα πέσουν στα χέρια κυβερνοεγκληματιών και χρησιμοποιηθούν παράνομα τότε ο επιχειρηματίας ιδιοκτήτης μπορεί να αντιμετωπίσει έκτακτα έξοδα διαχείρισης του περιστατικού και αγωγές αποζημίωσης από τους πελάτες των οποίων χάθηκαν τα δεδομένα.

Για την αντιμετώπιση και διαχείριση περιστατικών παραβίασης συστημάτων, απώλειας δεδομένων και άρνησης παροχής

Πόσο πωλούνται στη "μαύρη αγορά" τα στοιχεία πιστωτικών καρτών ;								
	US		EU		CA, AU		Asia	
	Χωρίς PIN	Με PIN	Χωρίς PIN	Με PIN	Χωρίς PIN	Με PIN	Χωρίς PIN	Με PIN
Visa Classic	15	80	40	150	25	150	50	150
Master Card Standard		90		140		150		140
Visa Gold / Premier	25	100	45	160	30	160	55	150
Visa Platinum	30	110	50	170	35	170	60	170
Business Corporate	40	130	60	170	45	175	70	170
Master Card World		140						
AMEX	40		60		45		70	
AMEX Gold	70		90		75		100	
AMEX Platinum	150							

υπηρεσίας απαιτούνται να καλυφθούν άμεσα και έμμεσα κόστη όπως:

Άμεσα κόστη τα οποία περιλαμβάνουν, επαγγελματικές αμοιβές εξειδικευμένων συμβούλων διαχείρισης περιστατικών παραβάσης συστημάτων, πρόστιμα και έξοδα όπως:

- αμοιβές εξειδικευμένου δικηγόρου
- υπηρεσίες ειδικών ψηφιακης εγκληματολογίας
- υπηρεσίες δημοσίων σχέσεων και επικοινωνίας
- υπηρεσίες τηλεφωνικού κέντρου
- credit monitoring παρακολούθηση συναλλαγών πιστωτικών καρτών
- έξοδα αντικατάστασης στοιχείων ενεργητικού όπως αντικατάσταση της πιστωτικής κάρτας του πελάτη και αντικατάσταση υλικού hardware ή software κ.λπ.
- πρόστιμα για μη τήρηση της νομοθεσίας περί προσωπικών δεδομένων
- έξοδα για την επίτευξη επιχειρησιακής συνέχειας

Έμμεσα κόστη μπορεί να είναι ακόμα πιο σημαντικά, συμπεριλαμβανομένων:

- μείωση της φήμης της εταιρείας
- την πτώση των εσόδων
- χαμένων επιχειρηματικών ευκαιριών
- απώλειας πελατών
- απώλειας συνεργατών
- αύξηση των αμοιβών των υπηρεσιών τρίτων παρόχων
- κόστη εκπαίδευσης και ευαισθητοποίησης σε θέματα ασφάλειας πληροφοριών του ανθρώπινου δυναμικού της εταιρείας
- καθώς και πρόσθετα επαναλαμβανόμενα έξοδα για ελέγχους ασφάλειας.

Δυστυχώς, πολλά από αυτά τα κόστη είναι απρογραμμάτιστα και μπορούν να έχουν αρνητική επίπτωση στην ρευστότητα και τις ταμειακές ροές μιας επιχείρησης.

Σύμφωνα με τα στοιχεία της έρευνας "Global Corporate IT Security Risks 2014" έδειξαν ότι ο παγκόσμιος μέσος όρος του κόστους ενός περιστατικού ασφάλειας, για μία μικρομεσαία επιχείρηση, μπορεί να φτάσει τα $47.000. Στη Δυτική Ευρώπη, το ποσό αυτό διαμορφώνεται στα $55.000.

Στο κόστος αυτό περιλαμβάνεται η απώλεια επιχειρηματικών ευκαιριών, η πρόσληψη εξωτερικού συνεργάτη Πληροφορικής για τη διόρθωση του προβλήματος και - ενδεχομένως - η αγορά νέου εξοπλισμού. Εν τω μεταξύ, σύμφωνα με εκπροσώπους εταιρειών απ' όλο τον κόσμο, το μέσο κόστος ενός περιστατικού ασφάλειας δεδομένων ήταν $720.000 για μια μεγάλη εταιρεία.

Το κόστος πάντως δεν είναι μόνο οικονομικό. Το 57% των συμβάντων απώλειας δεδομένων είχε αρνητικό αντίκτυπο στη συνολική λειτουργία της επιχείρησης. Επίσης, πάνω από τα μισά περιστατικά απώλειας δεδομένων (56%) έχουν αρνητικό αντίκτυπο στη φήμη και την αξιοπιστία μιας εταιρείας. Όπως προκύπτει από την έρευνα, το 61% των ερωτηθέντων αντιμετώπισε προβλήματα με ιούς, worms, Trojans και άλλα είδη κακόβουλου λογισμικού.

Η ασφάλιση Cyber Insurance ως εργαλείο διαχείρισης κινδύνου και αποτελεσματικής διαχείρισης περιστατικών απώλειας δεδομένων πελατών.

Λαμβάνοντας υπόψη ότι δεν μπορούμε να εξαλείψουμε την πιθανότητα πραγματοποίησης συμβάντων θα πρέπει να μπορούμε να διαχειριστούμε αποτελεσματικά περιστατικά απώλειας δεδομένων και εμπιστευτικών πληροφοριών.

Κάθε εταιρία για να διαχειριστεί αποτελεσματικά αυτά τα περιστατικά θα πρέπει να έχει πρόσβαση σε ειδικούς: δικηγόρους , επικοινωνιολόγους, δημοσίων σχέσεων και ψηφιακούς εγκληματολόγους. Μετά τον εντοπισμό του περιστατικού θα πρέπει να δρομολογηθεί η διαδικασία διαχείρισής του και αντιμετώπισής του.

Η ασφάλιση Cyber Insurance προσφέρει εκτός από την κάλυψη των χρηματοοικονομικών επιπτώσεων της εταιρίας και πρόσβαση σε ομάδες ειδικών οι οποίες έχουν αντιμετωπίσει πλήθος περιστατικών. Η πρόσβαση σε ομάδες ειδικών μπορεί να βοηθήσει και να ελαχιστοποιήσει την οικονομική καταστροφή και τη βλάβη της φήμης που μπορεί να συντελεστεί σε σύντομο χρονικό διάστημα.