Issue

Γιατί τα **e-shop** χρειάζονται ασφάλιση **cyber insurance!**

Φθορές σε ιστοσελίδες και διαδικτυακά καταστήματα πώλησης προϊόντων (e-shop) προκαλούν επιτήδειοι, έναντι αμοιβής τους από ανταγωνιστές των εταιρειών που πλήττονται, καθώς αποκτούν πρόσβαση σε κωδικούς πιστωτικών καρτών τρίτων ατόμων και στοιχεία διαδικτυακών πληρωμών.

350.000 η ζημιά ελληνικού e-shop λόγω κυβερνοεπίθεσης. Το δικό σας είναι ασφαλισμένο;

Αρχικά η Δίωξη Ηλεκτρονικού Εγκλήματος διερευνούσε υπόθεση που αφορούσε σε διαδικτυακή επίθεση σε βάρος διαδικτυακού φαρμακείου, που διήρκησε πέραν του ενός χρόνου, με αποτέλεσμα να προκληθεί στην επιχείρηση συνολική ζημιά ύψους 350.000 ευρώ. Οι διαδικτυακές αυτές επιθέσεις σε βάρος του φαρμακείου ήταν τύπου μαζικής άρνησης παροχής υπηρεσιών **(Distributed Denial of Service-DDoS)** και ήταν ιδιαιτέρως σφοδρές, καθώς κατά καιρούς χρησιμοποιήθηκαν ηλεκτρονικοί υπολογιστές «φαντάσματα» που προκαλούσαν 70.000.000 επισκέψεις ημερησίως στο εν λόγω ηλεκτρονικό κατάστημα, καθιστώντας το έτσι μη λειτουργικό. Η ανάλυση των ηλεκτρονικών ιχνών μέσω των οποίων έγιναν οι διαδικτυακές αυτές επιθέσεις συνεχίζεται, σε συνεργασία με τις εμπλεκόμενες χώρες του εξωτερικού, για τον εντοπισμό και την ταυτοποίηση προσώπων που ενεργούσαν οργανωμένα σε βάρος διαδικτυακών επιχειρήσεων, «εκτελώντας» συμβόλαια από ανταγωνίστριες εταιρείες, με σκοπό να αποκομίζουν αμοιβές για τους ψηφιακούς βανδαλισμούς που έκαναν. Εκτος από την περίπτωση άρνησης παροχής υπηρεσίας τα Eshops κινδυνεύουν με απώλεια δεδομένων των πελατών τους. Ας δούμε λίγο την διαδικασία αγοράς κατα την διάρκεια της οποίας ο 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 αυτά αποτελούν στόχο κάθε κυβερνοεγκληματία γιατί μπορούν εύκολα να πουληθούν στην μαύρη αγορά. Εάν δεδομένα που χρησιμοποιούν οι πελάτες για την αγορά προϊόντων πέσουν στα χέρια κυβερνοεγκληματιών και χρησιμοποιηθούν παράνομα τότε ο επιχειρηματίας ιδιοκτήτης του e shop μπορεί να αντιμετωπίσει αγωγές αποζημίωσης από αυτούς και από τις συνεργαζόμενες εταιρίες διαχείρισης πιστωτικών και χρεωστικών καρτών. Για την αντιμετώπιση και διαχείριση περιστατικών παραβίασης συστημάτων, απώλειας δεδομένων και άρνησης παροχής υπηρεσίας απαιτούνται να καλυφθούν άμεσο και έμμεσο κόστος όπως: **Άμεσο κόστος** το οποίο περιλαμβάνει, επαγγελματικές αμοιβές εξειδικευμένων συμβούλων διαχείρισης περιστατικών παράβασης συστημάτων, πρόστιμα και έξοδα όπως:


Νίκος Γεωργόπουλος, *MBA, CyRM.*
Cyber Risk Advisor , www.cyberinsurancegreece.com
CROMAR Coverholder at LLOYD´S

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

Έμμεσο κόστος μπορεί να είναι ακόμα πιο σημαντικά πράγματα, 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**. Τα κόστη πάντως δεν είναι μόνο οικονομικά.

- 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**.

Τι προσφέρει η ασφάλιση

Τα κύρια στοιχεία της ασφάλισης Cyber Insurance είναι:

- **Αστική Ευθύνη** έναντι τρίτων οι οποίοι υπέστησαν ζημιά λόγω απώλειας των προσωπικών τους δεδομένων από την εταιρία στην οποία τα είχαν δώσει
- **Ανταπόκριση** - Έξοδα και Υπηρεσίες διαχείρισης περιστατικών παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών
- **Διακοπή Εργασιών** - Κάλυψη για απώλεια εσόδων λόγω διακοπής της επιχειρηματικής δραστηριότητας από περιστατικά παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών
- **Κυβερνοεκβιασμός** - Κάλυψη για διαχείριση περιστατικών εκβιασμού από απειλές που μπορεί να βλάψουν ένα δίκτυο ή να οδηγήσουν σε διαρροή εμπιστευτικών πληροφοριών

Λαμβάνοντας υπόψη τις συνθήκες της αγοράς η **Cromar** σχεδίασε την λύση Cyber Secure Solution η οποία υποστηρίζεται από την αγορά των Lloyds. Πιο συγκεκριμένα μέσω της λύσης **Cyber Secure Solution** διαθέτει στην ελληνική αγορά σε συνεργασία με τους Beazley μία από τις καλύτερες ασφαλιστικές λύσεις διαχείρισης περιστατικών απώλειας εμπιστευτικών πληροφοριών και προσωπικών δεδομένων παγκοσμίως το "Beazley Global Breach Solution". Το "Beazley Global Breach Solution" αποτελεί μια συνολική λύση αποτελεσματικής διαχείρισης των κινδύνων παραβίασης συστημάτων και απώλειας δεδομένων και επιτρέπει στις επιχειρήσεις να διαχειριστούν την αυξανόμενη ευθύνη τους λόγω της διαχείρισης μεγάλου όγκου δεδομένων των πελατών τους, καθώς και να μετριάσουν τον κίνδυνο να θιγεί η εταιρική φήμη από πιθανή παραβίαση συστημάτων και απώλειας των δεδομένων αυτών. Το "Beazley Global Breach Solution" προσφέρει εκτός από τις χρηματικές αποζημιώσεις πρόσβαση στην Ομάδα Διαχείρισης Περιστατικών του η οποία έχει αντιμετωπίσει άνω των 3.000 περιστατικών παγκοσμίως και έχει βραβευθεί από την Advisen ως η καλύτερη ομάδα διαχείρισης για το 2014. ITSecurity