Ανδρέας Λάλος
BESECURE

Επένδυση στη διαφήμιση ή στην αποφυγή δυσφήμησης;

Κάθε οργανισμός έχει υποστεί το κόστος της απώλειας εμπιστευτικών πληροφοριών. Απλά δεν γνωρίζει ποια δεδομένα, πώς και πότε

Ακόμα και όταν το ανακαλύπτει προσπαθεί να περιορίσει την έκταση του συμβάντος ώστε να μην γνωστοποιηθεί σε πελάτες, σε συνεργάτες και στο ευρύ κοινό. Αλλά αν ο οργανισμός εμπίπτει στην εφαρμογή νόμων και κανονισμών ασφάλειας πληροφοριών τότε ο οργανισμός αποκτά δημοσιότητα με τον δύσκολο τρόπο. Και τα κακά νέα διαδίδονται γρήγορα! Ανεξαρτήτως αν οι πληροφορίες χάθηκαν λόγω λάθους ή κακόβουλων ενεργειών, το αποτέλεσμα για τον οργανισμό μπορεί να είναι καταστροφικό. Απώλεια οικονομικών πληροφοριών, στοιχείων πελατών, δεδομένων πνευματικής ιδιοκτησίας, επιχειρηματικών πλάνων ανάπτυξης, προσωπικών στοιχείων εργαζομένων, πληροφορίες σύνθεσης προϊόντων, πληροφορίες διαφημιστικής εκστρατείας, κυρώσεις μη συμμόρφωσης με σχετικές νομοθεσίες, και κανονισμούς, δυσμενής δημοσιότητα καθώς και απώλεια μελλοντικών εσόδων είναι ορισμένα από τα αποτελέσματα που δεν μπορεί να μετρηθεί επακριβώς το κόστος τους. Όπως επισημαίνεται σε αναφορά της Gartner, βιώνουμε επιδημία απώλειας δεδομένων, με δεκάδες εκατομμύρια αποδέκτες ενημερωτικών επιστολών για τη μη θελημένη αποκάλυψη προσωπικών τους δεδομένων. Σε παγκόσμια κλίμακα, μεγάλοι κυβερνητικοί, στρατιωτικοί και ιδιωτικοί οργανισμοί έχουν υποστεί το πλήγμα της απώλειας πληροφοριών αλλά και της δυσφήμισης λόγω υποχρεωτικής κοινοποίησης των συμβάντων ή μη δυνατότητας απόκρυψης αυτών και αδιαμφισβήτητα χιλιάδες άλλοι που δεν το κοινοποίησαν ποτέ. Με αυτά τα δεδομένα, εύλογα δημιουργείται η απορία πως είναι δυνατόν όταν επενδύονται και ειδικότερα σε μεγάλους οργανισμούς, τεράστια κονδύλια για την εφαρμογή μηχανισμών προστασίας υποδομών IT, πρόσληψη εξειδικευμένου ανθρώπινου δυναμικού διαχείρισης πληροφοριακών συστημάτων, εφαρμογή αυστηρών πολιτικών και διαδικασιών ασφάλειας πληροφοριών, να παρουσιάζονται με αυτή την συχνότητα τέτοια συμβάντα. Βασική αιτία είναι ότι οι επιχειρήσεις έχουν εστιάσει σε μέτρα προστασίας έναντι εξωτερικών απειλών, αδυνατώντας να αναγνωρίσουν ότι ο πραγματικός κίνδυνος ευρίσκεται εντός των τειχών. Οι επιχειρήσεις παραδοσιακά επένδυαν και επενδύουν σε τεχνολογικές λύσεις που θα εμποδίσουν τους κακόβουλους εισβολείς να εισέλθουν στο εταιρικό δίκτυο και θα αποτρέψουν την εκτέλεση κακόβουλων εισερχόμενων προγραμμάτων, όπως viruses, trojan horses, worms, logic bombs, malicious mobile code με τεχνολογίες όπως συστήματα anti virus, anti spam, firewalls, intrusion prevention systems κ.α.

Κενά ασφάλειας

Αυτή η προσέγγιση όμως στην προστασία των εταιρικών πληροφοριών, έχει δημιουργήσει κενά ασφάλειας σε εσωτερικές απειλές είτε αυτές είναι κακόβουλες ή από λάθος με αποτέλεσμα σημαντικές απώλειες πληροφοριών να οφείλονται σε εσωτερικούς χρήστες. Γεγονός που επίσης επιβεβαιώνετε και με την έρευνα CSI/FBI Computer Crime and Security Survey 2006, όπου ένα αξιοσημείωτο ποσοστό 68% των ερωτηθέντων ανέφερε ότι κατέγραψαν σημαντικές απώλειες εκ των έσω.

Για την προστασία των πληροφοριών από εσωτερικές απειλές οι επιχειρήσεις υιοθετούν κυρίως τεχνολογίες όπως identity management systems, access control systems, data encryption οι οποίες όμως παρέχουν προστασία μόνο έναντι μη εξουσιοδοτημένων εσωτερικών χρηστών. Τα μέτρα αυτά δεν αποτρέπουν την απώλεια πληροφοριών από πιστοποιημένους χρήστες στους οποίους έχει δοθεί πρόσβαση στην πληροφορία. Και η διαρροή ή μη θελημένη απώλεια αυτών των πληροφοριών μπορεί να πραγματοποιηθεί μέσω ηλεκτρονικής αλληλογραφίας, δημοσίευσης στο διαδίκτυο, μεταφοράς μέσω USB disk keys, μεταφοράς σε κάρτες αποθήκευσης κινητών τηλεφώνων, κάρτες αποθήκευσης ψηφιακών καμερών, μέσω ασύρματων δικτύων, μέσω εκτύπωσης, μέσω p2p τεχνολογιών όπως Skype, MSN Messenger, Yahoo Messenger κλπ. Η απώλεια πληροφοριών από «έμπιστους» χρήστες είναι υπαρκτό πρόβλημα και τα δημοσιεύματα του τύπου συνεχώς πληθαίνουν.

Νέες τεχνολογίες ασφάλειας

Για τον σκοπό αυτό έχουν αναπτυχθεί νέες τεχνολογίες Data Loss Prevention (DLP) που επιτρέπουν στους οργανισμούς την εφαρμογή των εταιρικών πολιτικών ασφάλειας, την εποπτεία και αναφορά συμβάντων και την αποτροπή αυτών. Οι τεχνολογίες DLP βασίζονται σε αναγνώριση ακολουθίας δεδομένων (pattern analysis - πιστωτικές κάρτες, τραπεζικοί λογαριασμοί, ταυτότητες κλπ), σε αναγνώριση περιεχομένου (content analysis) λόγω χαρακτηρισμού του ως εμπιστευτικού, απόρρητου, κοινού κλπ, ή και λόγω θέσης αποθήκευσης στο εταιρικό δίκτυο. Παρέχουν προστασία σε πολλαπλά επίπεδα όπως σε επίπεδο δικτύου και σε επίπεδο σταθμών εργασίας χρηστών επιτρέποντας τον έλεγχο, την αναφορά και την αποτροπή απώλειας αυτών όπως μέσω εκτύπωσης, πρόσβασης μη εξουσιοδοτημένων εφαρμογών, μεταφοράς μέσω δικτύων (email, web, p2p, wired & wireless), καθώς επίσης θωρακίζουν τις πληροφορίες έναντι αντιγραφής τους σε μεταφέρσιμα αποθηκευτικά μέσα όπως USB Keys, CDs/DVDs, iPods, Bluetooth devices). **nw**

Ο **Ανδρέας Λάλος** είναι *Professional Services Manager* της BESECURE