

πτέρνα των σύγχρονων επιχειρήσεων

αντίγραφο από το τμήμα marketing, στο οποίο και τα βρήκαν οι μελετητές της PricewaterhouseCoopers.

Υγεία

Χρησιμοποιώντας την ιδιότητα του “εξωτερικού συνεργάτη” απέκτησαν πρόσβαση σε 81 εκατ. αρχεία με ασφαλιστικά αιτήματα, ονόματα πελατών και αριθμούς Μητρώου Κοινωνικής Ασφάλισης μέσω αδύναμων κωδικών.

Λιανική

Εμφανιζόμενοι ως μέλη της ομάδας διαχείρισης αρχείων της εταιρίας, ζητήθηκε και δόθηκαν γνήσια αντίγραφα αιτήσεων για εργασία, τα οποία και περιελάμβαναν τους αριθμούς Μητρώου Κοινωνικής Ασφάλισης, ημερομηνίες γέννησης και άλλα.

Οι λόγοι για τους οποίους η κλοπή δεδομένων και ταυτότητας είναι ένα πρόβλημα που συνεχώς επιδεινώνεται.

1. Η κλοπή δεδομένων και ταυτότητας γίνεται από οργανωμένες ομάδες, που διαθέτουν εξελιγμένη τεχνολογία, με κύριο κίνητρο το οικονομικό όφελος
2. Τα σύγχρονα επιχειρηματικά μοντέλα βασίζονται σε παγκόσμια δίκτυα συνεργασίας που μοιράζονται ευαίσθητα δεδομένα με πολλές μεθόδους και το γεγονός αυτό πιθανόν αυξάνει τους κινδύνους
3. Τα μεγάλα κέρδη και οι πολύπλοκες τεχνικές κάνουν την κλοπή δεδομένων και ταυτότητας ακόμη πιο προσοδοφόρα, ευκολότερη στην υλοποίηση και δυσκολότερη στην ανίχνευση. Επιπλέον, οι αδύναμοι διεθνείς νόμοι/νομοθεσία δυσχεραίνουν την ποινική δίωξη των hackers
4. Η κλοπή της πνευματικής ιδιοκτησίας έχει συχνά αποτέλεσμα την παραποίηση των προϊόντων, η οποία αποτελεί επιπλέον πηγή εσόδων

5. Τα σύγχρονα μέτρα προστασίας εταιρικών δεδομένων είναι συχνά ανεπαρκή ως προς την ανίχνευση ή παρεμπόδιση δραστηριοτήτων hacking ή ηλεκτρονικής κατασκοπείας. Η προστασία των δεδομένων μοιάζει με κινούμενο στόχο: όσο εξελίσσεται η τεχνολογία τόσο αυξάνονται οι δυνατότητες προστασίας, αλλά και οι μέθοδοι κλοπής δεδομένων

6. Η συμμόρφωση με τα πρότυπα του κλάδου (π.χ. του PCI - κλάδου καρτών πληρωμής) ή με τα κανονιστικά πρότυπα (π.χ. Νόμοι περί προστασίας δεδομένων προσωπικού χαρακτήρα, Πράξη Διοικητή Τράπεζας της Ελλάδος 2577/ 9.3.2006, Sarbanes Oxley) μπορούν να δημιουργήσουν εσφαλμένη αίσθηση της ασφάλειας. Τα κανονιστικά πρότυπα έχουν πολύ συγκεκριμένα όρια και τα πιο ευαίσθητα δεδομένα μίας εταιρίας μπορεί να μην καλύπτονται από ένα συνηθισμένο πρότυπο.

Η φύση του εγκλήματος κάνει δύσκολη τη δίωξη. Η ανωνυμία της κλοπής δεδομένων και ταυτότητας, καθιστά το αδίκημα ελκυστικό, καθώς αυτός που διαπράττει το αδίκημα μπορεί να βρίσκεται χιλιόμετρα μακριά, σε άλλη χώρα, ή ακόμα και σε άλλη ήπειρο. Το μόνο που χρειάζεται είναι να έχει πρόσβαση σε έναν υπολογιστή. Η προστασία από

κλοπή ταυτότητας διαφέρει από χώρα σε χώρα και η κατοχυρωμένη διεθνώς προστασία της πνευματικής ιδιοκτησίας είναι ελλιπής, και πολλές φορές μη αποτελεσματική. Το γεγονός αυτό προκαλεί έκρηξη κλοπής και απάτης, από τη στιγμή που οι κακοποιοί λαμβάνουν μεγάλη αμοιβή χωρίς σημαντικό ρίσκο να συλληφθούν και να διωχθούν ποινικά.

Συνέπειες

Οι πιθανές αρνητικές επιπτώσεις της κλοπής δεδομένων και ταυτότητας είναι τεράστιες. Σε περίπτωση τέτοιου περιστατικού, οι εταιρίες πρέπει να περιμένουν άμεσες αρνητικές επιπτώσεις στα οικονομικά στοιχεία τους, ως αποτέλεσμα των ερευνών, των νομικών εξόδων, των υπηρεσιών παρακολούθησης της πίστωσης των θυμάτων, της χορήγησης εκ νέου των πιστωτικών καρτών, των κυβερνητικών προστίμων και των ρυθμιστικών ποινών. Οι εταιρίες μπορεί, επίσης, να αντιμετωπίσουν σημαντικές αρνητικές επιπτώσεις στη φήμη τους, αρνητική δημοσιότητα, απώλεια πελατών, εσόδων, καθώς και της εμπιστοσύνης των πελατών τους. Όταν η κλοπή δεδομένων και ταυτότητας αφορά δεδομένα πελατών, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα μπορεί να επιβάλει διοικητικές κυρώσεις στον καταγγελλόμενο, εφόσον κρίνει, ότι αυτό απαιτείται ή να παραπέμψει την υπόθεση στον αρμόδιο Εισαγγελέα.

Η προστασία από κλοπή ταυτότητας διαφέρει από χώρα σε χώρα. Το γεγονός αυτό προκαλεί έκρηξη κλοπής και απάτης, από τη στιγμή που οι κακοποιοί λαμβάνουν μεγάλη αμοιβή χωρίς σημαντικό ρίσκο να συλληφθούν και να διωχθούν ποινικά.

χρηματικές απώλειες ή ακόμα και νητικές βλάβες

- Οι υπάλληλοι και τα δίκτυα συνεργασίας είναι οι πιο συνηθισμένες πηγές διαρροής δεδομένων
- Οι κίνδυνοι είναι πραγματικοί και σημαντικοί και σε αυτούς περιλαμβάνονται η έκθεση σε κίνδυνο των εταιρικών συστημάτων πληροφορικής, οι αγωγές πελατών, η απώλεια της αξιοπιστίας στην εταιρία και πελατών, τα πρόστιμα, καθώς και η επιβολή νέων ρυθμιστικών πλαισίων
- Η προστασία των ευαίσθητων δεδομένων αποτελεί ένα ζήτημα που αφορά ολόκληρη την επιχείρηση και όχι μόνο την πληροφορική και πρέπει να αντιμετωπίζεται σε επίπεδο Διευθύνοντος Συμβούλου.

Λύσεις

Η παγκόσμια δραστηριοποίηση έχει κάνει τις εταιρίες πιο ευάλωτες σε κλοπή δεδομένων και ταυτότητας, καθώς ο διανομημένος χαρακτήρας των δεδομένων με συνεργάτες έχει αυξήσει τις πιθανότητες για απώλεια, εσφαλμένη χρήση ή έκθεση σε κίνδυνο. Η παραδοσιακή άποψη είναι, ότι τα δεδομένα είναι περιορισμένα εντός της επιχείρησης και ότι εξασφαλίζοντας το κατάλληλο firewall (τείχος προστασίας) και προστατεύοντας την περίμετρο, μπορεί κανείς να έχει όλη την απαραίτητη προστασία. Τα πράγματα όμως έχουν αλλάξει. Τα δεδομένα μπορούν εύκολα να μεταφερθούν και να αντιγραφούν. Αν και ο χώρος φύλαξης (Data Center) και οι servers μπορούν να προσφέρουν υψηλότερο επίπεδο ασφάλειας δεδομένων, η επικράτηση των φορητών συσκευών - όπως φορητοί ηλεκτρονικοί υπολογιστές, PDAs και plug-in drives - είναι λιγότερο ασφαλή και αυξάνουν τον κίνδυνο κλοπής.

Μόλις τα δεδομένα διαμοιραστούν, όλες οι συσκευές που έχουν πρόσβαση σε αυτά είναι πιθανές πηγές απώλειας ασφάλειας. Επίσης, μέσω των συνεργασιών με τρίτους, οι οποίες απαιτούν την ανταλλα-



γή δεδομένων, αναγκαστικά βασίζομαστε στα δικά τους πρότυπα προστασίας δεδομένων, που πολλές φορές δεν είναι επαρκή, εκθέτοντας έτσι τα δεδομένα σε μεγαλύτερο κίνδυνο. Ένα δυσάρεστο γεγονός είναι ότι τα περισσότερα εταιρικά μέτρα προστασίας δεδομένων εστιάζουν στη συμμόρφωση και είναι ανεπαρκή σε σύγκριση με τις σύγχρονες έξυπνες - πολύπλοκες απειλές. Με λίγα λόγια, η συμμόρφωση είναι απλά το ελάχιστο επίπεδο προστασίας δεδομένων που απαιτείται. Παρόλο που προσφέρει ένα "δίχτυ ασφαλείας", μια διασφάλιση, στην ουσία παραμένει ένα δίχτυ με τις αναμενόμενες απώλειες. Εστιάζοντας στους κινδύνους και στην έκθεση των κινδύνων παρά αποκλειστικά στη συμμόρφωση, οι εταιρίες μπορούν να αυξήσουν το επίπεδο προστασίας δεδομένων τους στο σημείο που είναι αναγκαίο.

Τι πρέπει να λάβουν υπόψη οι διοικήσεις των εταιριών για την προστασία των δεδομένων τους

- Πού βρίσκονται τα πιο ευαίσθητα δεδομένα της επιχείρησης και ποιοι έχει πρόσβαση σε αυτά
- Ποιοι κανονισμοί και πρότυπα αρμόζουν στα δεδομένα τους
- Αν έχουν αποτελέσει στο παρελθόν στόχο κλοπής δεδομένων και ταυτότητας.
- Αν η επικοινωνία και η ανταλλαγή δε-

δομένων θέτει τα δεδομένα σε κίνδυνο

- Αν οι υπάλληλοι, πελάτες και συνεργάτες της επιχείρησης κατανοούν το ρόλο τους, όσον αφορά στην προστασία ευαίσθητων δεδομένων
- Αν τα μέτρα που έχουν λάβει παρέχουν ολοκληρωμένη προστασία στα δεδομένα, ακόμη και στις φορητές συσκευές.

Μία αποτελεσματική προσέγγιση για την καταπολέμηση και τον περιορισμό του ρίσκου λόγω κλοπής δεδομένων και ταυτότητας πρέπει να περιλαμβάνει τα ακόλουθα:

- Ανάπτυξη και υλοποίηση ενός λεπτομερούς σχεδίου προστασίας δεδομένων
- Προσδιορισμός και ταξινόμηση δεδομένων ανάλογα με το πόσο σημαντικά είναι και τον κίνδυνο σε περίπτωση περιστατικού ασφαλείας. Να γνωρίζει κανείς που αποθηκεύονται και πού μεταφέρονται
- Κατανόηση των απειλών που διατρέχουν τα δεδομένα και η επιχείρηση
- Υλοποίηση των δυνατοτήτων ολοκληρωμένης προστασίας, που αφορούν τα ευαίσθητα δεδομένα της επιχείρησης
- Δοκιμή και έλεγχος των δυνατοτήτων προστασίας. Συχνή παρακολούθηση και ενημέρωση ανάλογα με τις ανάγκες της επιχείρησης
- Διαδικασίας αντιμετώπισης συμβάντος, όπως π.χ. σε περίπτωση κλοπής ή απώλειας δεδομένων.

Η ισχυρή προστασία δεδομένων προσφέρει μεγαλύτερη ελευθερία για την εκμετάλλευση των ευκαιριών

Η κατάλληλη στρατηγική προστασίας δεδομένων μπορεί να αποτελέσει ανταγωνιστικό πλεονέκτημα μιας επιχείρησης, καθώς και να συμβάλει στην ελαχιστοποίηση του κινδύνου, τόσο όσον αφορά στα οικονομικά, όσο και στη φήμη της. Το πιο σημαντικό όμως είναι, ότι οι επιχειρηματίες που έχουν εμπιστοσύνη στην προστασία των δεδομένων τους, έχουν την ελευθερία να επικεντρωθούν στην ενίσχυση των επιχειρηματικών τους δραστηριοτήτων. ⓘ