Taiye Lambo
eFortresses

Η ασφάλεια περνάει μέσα από τη γνώση

Στην εποχή της πληροφορίας αλλά και των αυστηρών νομοθετικών ρυθμίσεων, η ασφάλεια των πληροφοριών αποτελεί πρωταρχικό ζητούμενο για τις εταιρείες. Και η επίτευξη αυτού του στόχου είναι κυρίως θέμα ανθρώπων, γνώσης και εκπαίδευσης, υποστηρίζει ο Taiye Lambo, Ιδρυτής και CTO της eFortresses

nw: Ποια θεωρείτε ότι είναι τα βασικότερα ζητήματα που αντιμετωπίζουν σήμερα οι εταιρείες σχετικά με την ασφάλεια των πληροφοριών;
Taiye Lambo: Δύο είναι τα βασικότερα ζητήματα που απασχολούν και επηρεάζουν τις σύγχρονες εταιρείες και οργανισμούς σχετικά με την ασφάλεια των πληροφοριών. Το πρώτο είναι ότι ζούμε στην εποχή της πληροφορίας. Αυτό σημαίνει ότι οι πληροφορίες αποτελούν για έναν οργανισμό το σημαντικότερο ίσως κεφάλαιο για τη λειτουργία του αλλά και ένα σημαντικό όπλο απέναντι στον ανταγωνισμό. Και η πληροφορία σήμερα κινδυνεύει. Οι εταιρείες αντιμετωπίζουν μεγάλες και σημαντικές απειλές. Παλιότερα λέγαμε ότι 'η γνώση είναι δύναμη'. Σήμερα 'η πληροφορία είναι δύναμη'. Ζούμε σε μια εποχή που πρέπει να διαχειριστούμε ένα τεράστιο όγκο πληροφοριών, ενώ ταυτόχρονα όλοι έχουμε πρόσβαση σε τόσο πολλές πληροφορίες από διαφορετικές πηγές και ποικίλα κανάλια (Internet, email κ.λπ). Για αυτό η πληροφορία έχει αποκτήσει ζωτική σημασία για τις εταιρείες σήμερα. Κατ' επέκταση η ασφάλεια της πληροφορίας έχει αναδειχτεί σε τεράστιο θέμα.
Το δεύτερο έχει να κάνει με την κανονιστική συμμόρφωση και το κόστος της επίτευξης της συμμόρφωσης, αλλά και το κόστος της μη συμμόρφωσης. Ποιες θα είναι οι επιδράσεις της συμμόρφωσης - σε επίπεδο κόστους, λειτουργιών κ.λπ. - αλλά και ποιες είναι οι πιθανές απώλειες της μη συμμόρφωσης. Όλα αυτά είναι ερωτήματα που πρέπει να απαντηθούν και να συνυπολογιστούν πριν οι εταιρείες αποφασίσουν σε ποιες ενέργειες θα προβούν.
Ο συνδυασμός αυτών των δύο έχει κάνει την ασφάλεια των πληροφοριών πάρα πολύ κρίσιμη σε όλο τον κόσμο.

nw: Είπατε ότι οι πληροφορίες κινδυνεύουν σήμερα. Από πού προέρχονται αυτοί οι κίνδυνοι; Πολλοί υποστηρίζουν ότι η μεγαλύτερη απειλή που πρέπει να αντιμετωπίσουν οι εταιρείες είναι από το εσωτερικό, καθώς η τεχνολογία επιτρέπει την καλή διασφάλιση των δικτύων. Συμφωνείτε;
T. Lambo: Νομίζω πως συμφωνώ. Η προσωπική μου άποψη είναι ότι σήμερα οι απειλές εκ των έσω είναι πιο σημαντικές. Δεν έχω κάποια στατιστική που να το υποστηρίζει αυτό, αλλά θεωρώ ότι οι εσωτερικές απειλές είναι πιο πιθανές, πιο σοβαρές και πιο δύσκολες να προληφθούν και να αποφευχθούν.
Με τις εξωτερικές απειλές το σημείο κλειδί είναι να καταφέρει κανείς να κρατήσει τους «κακούς» έξω από τα συστήματά του. Η πρόκληση με τις εσωτερικές απειλές είναι ότι πρέπει να εμπιστεύεσαι τους ανθρώπους σου. Πρέπει να εμπιστεύεσαι τους χρήστες σου, είτε είναι υπάλληλοι, είτε συνεργάτες. Και με το να τους εμπιστεύεσαι, βασικά τους δίνεις τα κλειδιά του βασιλείου. Μπορεί να μην τους δίνεις το κύριο κλειδί που ανοίγει όλες τις πόρτες του βασιλείου, αλλά πάλι τους εμπιστεύεσαι να έχουν πρόσβαση στην πληροφορία. Πρέπει λοιπόν να εμπιστεύεται μια εταιρεία τους χρήστες της αλλά και να τους ελέγχει.
Σε αυτό το πλαίσιο η πιο σημαντική παράμετρος είναι η ενημέρωση, η εκπαίδευση. Πρέπει να διασφαλίσει η εταιρεία ότι οι χρήστες γνωρίζουν τις απειλές, γνωρίζουν τους κινδύνους και πώς να τους αποφύγουν. Ένα από τα αγαπημένα μου μότο είναι ότι 'δεν μπορείς να νικήσεις τη βλακεία'. Το λογισμικό και η τεχνολογία δεν μπορούν να αντιμετωπίσουν τις ανόητες και απρόσεκτες ενέργειες των χρηστών. Υπάρχουν τεχνολογίες και εργαλεία που αντιμετωπίζουν τα τρωτά σημεία των συστημάτων, αλλά δεν έχει ανακαλυφθεί ακόμα λογισμικό για την ανοησία και την άγνοια.
Είναι σαφώς πολύ δύσκολο να αντιμετωπίσει μια εταιρεία όλους τους εσωτερικούς κινδύνους, αλλά μπορεί να προσπαθήσει να τους ελαχιστοποιήσει. Και η σωστή εκπαίδευση των χρηστών είναι ένα αποφασιστικό βήμα.

> Το λογισμικό και η τεχνολογία δεν μπορούν να αντιμετωπίσουν τις ανόητες και απρόσεκτες ενέργειες των χρηστών

nw: Αν κάποιος σας ζητούσε μία συμβουλή για το ποιο είναι το σημαντικότερο πράγμα στην προσπάθεια για τη διασφάλιση των πληροφοριών, τι θα λέγατε;
T. Lambo: Η ενημέρωση, η γνώση, η εκπαίδευση. Η γνώση είναι δύναμη. Οι εταιρείες πρέπει να ενημερώσουν και να εφοδιάσουν με τις κατάλληλες γνώσεις το μέσο χρήστη τους για τους κινδύνους. Πιστεύω πραγματικά ότι όσο περισσότερο ενημερωμένος

είναι κανείς, όσο περισσότερα ξέρει, τόσο περισσότερο μπορεί να προστατευτεί απέναντι στις απειλές.

nw: Και το δεύτερο πιο σημαντικό;
T. Lambo: Η δέσμευση της διοίκησης σχετικά με τα ζητήματα της ασφάλειας. Οι εταιρείες - σε επίπεδο διοίκησης - πρέπει να αντιλαμβάνονται το Information Security πέρα από το IT και την τεχνολογία. Να το αντιμετωπίσουν ως ένα πραγματικά επιχειρηματικό πρόβλημα. Αυτό σημαίνει ότι πρέπει να αναπτύξουν και να υποστηρίξουν μία ολοκληρωμένη στρατηγική με συνέπεια και να διαθέσουν τους απαιτούμενους πόρους και χρήματα.

nw: Μπορούν οι επενδύσεις σε ασφάλεια να αξιοποιηθούν επιχειρηματικά και να αποκομίσουν οι εταιρείες ROI από αυτές;
T. Lambo: Απολύτως. Πιστεύω ότι η ασφάλεια μπορεί να αποτελέσει 'enabler' για το business. Μία εταιρεία μπορεί να χρησιμοποιήσει ένα καλό πρόγραμμα ασφάλειας ή να αξιοποιήσει ένα καλό περιβάλλον ασφάλειας σαν διαφοροποιητικό παράγοντα. Μπορεί οι επενδύσεις σε συστήματα, τεχνολογίες και υπηρεσίες ασφάλειας να μην έχουν ROI με την έννοια της δημιουργίας εσόδων - αν και σε αρκετές περιπτώσεις μπορεί να λειτουργήσουν και ως πηγή εσόδων - αλλά αποτελούν σίγουρα αποφασιστικό παράγοντα για τη διατήρηση εσόδων. Αν μια εταιρεία δεν είναι αρκετά ασφαλής, σίγουρα θα χάσει έσοδα. Αν είναι ασφαλής μπορεί να αυξήσει τα έσοδά της. Πρέπει να το δουν οι εταιρείες σαν πολιτική ασφάλισης (insurance). Επενδύεις σε ασφάλιση γιατί δεν θέλεις να πάρεις το ρίσκο να έχεις ένα τρωτό σημείο και να χάσεις χρήματα. Και όχι μόνο χρήματα. Μιλάμε για οικονομικές απώλειες αλλά και για απώλεια φήμης. Οπότε δεν είναι θέμα απόδοσης της επένδυσης, αλλά πολιτική ασφάλισης. Και αυτό είναι το κέρδος.

nw: Μιλήστε μας λίγο για το HISP (Holistic Information Security Practitioner) Certification Course. Τι περιλαμβάνει;
T. Lambo: Πρόκειται για ένα ολιστικό πρόγραμμα εκπαίδευσης και πιστοποίησης που παρέχει πρακτική γνώση εφαρμογής βέλτιστων πρακτικών Διαχείρισης Ασφάλειας Πληροφοριών, Ελέγχου Συστημάτων Πληροφορικής και Συμμόρφωσης με κανονισμούς και νομοθεσίες. Η εκπαίδευση καλύπτει τη συσχέτιση του ISO/IEC 17799:2005 με το COBIT, το COSO και το ITIL, και εξηγεί τη μεθοδολογία ταύτισης πολλαπλών κανονισμών και απαιτήσεων όπως Sarbanes Oxley Act, EU Data Protection Act, VISA PCI Data Security κα. στο διεθνώς αναγνωρισμένο κώδικα πρακτικής για τη Διαχείριση της Ασφάλειας Πληροφοριών ISO/IEC 17799:2005.

nw: Γιατί μια εταιρεία να επενδύσει/ πληρώσει ώστε τα στελέχη της να παρακολουθήσει το HISP course και να πιστοποιηθεί σε αυτό;
T. Lambo: Όπως είπα προηγουμένως, το κλειδί στα θέματα της ασφάλειας είναι η γνώση. Μέσα από αυτό το σεμινάριο οι υπάλληλοι και οι συνεργάτες μιας εταιρείας θα μάθουν πώς να ακολουθήσουν μία ολοκληρωμένη, πολύπλευρη και ενοποιημένη προσέγγιση για την ασφάλεια των πληροφοριών και την κανονιστική συμμόρφωση. Και αυτό είναι πολύ σημαντικό γιατί μόνο μέσα από μια ολιστική προσέγγιση μπορεί μια εταιρεία να επιτύχει υψηλά επίπεδα ασφάλειας, συμμόρφωση προς τα ολοένα αυστηρότερα νομοθετικά πλαίσια, αλλά και σημαντικά άλλα οφέλη, όπως η μείωση των δαπανών. Μία περισσότερο στρατηγική προσέγγιση αυτών των ζητημάτων προσφέρει σημαντική μείωση του κόστους.

» Οι εταιρείες πρέπει να διασφαλίσουν ότι οι χρήστες τους γνωρίζουν τις απειλές, γνωρίζουν τους κινδύνους και πώς να τους αποφύγουν «

nw: Σε ποιους κλάδους και σε τι εταιρείες απευθύνεται το HISP; Ποια είναι τα πλεονεκτήματα που θα αποκομίσει μια εταιρεία;
T. Lambo: Σε οποιαδήποτε εταιρεία, σε οποιοδήποτε κλάδο και αν δραστηριοποιείται, η οποία καλείται να προστατεύσει πολύτιμα δεδομένα αλλά και να ανταποκριθεί σε κανονιστικά πλαίσια και νομοθετικές ρυθμίσεις. Η ανάγκη για αποτελεσματική προστασία των δεδομένων είναι ανεξάρτητη από το μέγεθος μιας εταιρείας ή την αγορά μέσα στην οποία επιχειρεί. Η ολιστική προσέγγιση που προτείνεται περιγράφει την ενοποίηση των διεθνών προτύπων και των κανονιστικών πλαισίων και νομοθετικών ρυθμίσεων που σχετίζονται με το Information Security & Privacy και εστιάζει κυρίως στους ανθρώπους και τις διαδικασίες και δευτερευόντως στην τεχνολογία. Η ασφάλεια άλλωστε είναι πρώτα από όλα ζήτημα ανθρώπων και διαδικασιών που απαιτεί ολοκληρωμένη στρατηγική προσέγγιση.

nw: Ποιος είναι ο σκοπός του Holistic Information Security Practitioner (HISP) Institute (HISPI) ;
T. Lambo: Το Ινστιτούτο Holistic Information Security Practitioner είναι ένας ανεξάρτητος οργανισμός πιστοποίησης, που αποτελείται από εθελοντές πραγματικούς επαγγελματίες (practitioners) της ασφάλειας των πληροφοριών, όπως Chief Information Security Officers (CISO), Information Security Officers (CSO), Technology Risk Managers, αναλυτές ασφάλειας κ.λπ., στελέχη μεγάλων εταιρειών και οργανισμών.
Στόχος του HISPI είναι να προωθήσει μία ολιστική προσέγγιση για τη διαχείριση της ασφάλειας των πληροφοριών, παρέχοντας εκπαίδευση και ευκαιρίες πιστοποίησης σε information security, assurance και governance. **nw**