Νότης Ηλιόπουλος
Intelli Solutions S.A

Η ασφάλεια πληροφοριών στην εποχή της συνεχούς μείωσης των δαπανών

Το σημερινό επιχειρησιακό περιβάλλον διέπεται από μια συνεχή πίεση για μείωση του κόστους λειτουργίας. Πρώτος υποψήφιος η Πληροφορική και κατ' επέκταση οι δαπάνες που αφορούν στην ασφάλεια πληροφοριών

Σε εποχές που χαρακτηρίζονται από τη διαρκή προσπάθεια μείωσης του λειτουργικού κόστους, χρειάζεται να ιεραρχήσουμε τις ανάγκες μας και να αξιολογήσουμε καλύτερα τις επενδύσεις μας, ιδιαίτερα αυτές που αφορούν σε πολυδάπανες τεχνολογικού τύπου υποδομές. Σε δύσκολους καιρούς οικονομικής κρίσης, έχει αποδειχθεί ότι οι τα κρίσιμα εταιρικά δεδομένα αποτελούν τη λεία των απογοητευμένων εργαζομένων, καθώς και των οπορτουνιστών του εύκολου κέρδους.

Επιπρόσθετα, το κανονιστικό πλαίσιο δεν είναι χαλαρότερο και λιγότερο απαιτητικό λόγω οικονομικής κρίσης. Τέλος, η μείωση των επενδύσεων, γενικότερα στο χώρο της Πληροφορικής αυξάνει τον κίνδυνο εκμετάλλευσης απειλών ασφάλειας πληροφοριών λόγω της μείωσης των τεχνικών δικλείδων ασφάλειας.

Τι είναι αναγκαίο να υλοποιηθεί εσωτερικά

Η διαχείριση των κινδύνων ασφάλειας πληροφοριών είναι η ουσιαστικότερη διεργασία της ασφάλειας πληροφοριών και πρέπει να διενεργείται εσωτερικά στον Οργανισμό.

Επίσης, η επιβολή και ο έλεγχος υλοποίησης των μέτρων προστασίας, τόσο σε σχέση με την κανονιστική συμμόρφωση, όσο και σε σχέση με την προστασία από τους κινδύνους ασφάλειας, αποτελούν μέρος της εσωτερικής υλοποίησης. Η διαχείριση των συστατικών της ασφάλειας πληροφοριών, καθώς και η διαχείριση των κινδύνων είναι καθαρά εταιρική υπευθυνότητα. Οι επιμέρους διεργασίες που συγκροτούν τις παραπάνω διαδικασίες, μπορεί να αποτελέσουν μέρος υλοποίησης από εξωτερικούς συνεργάτες.

Μείωση λειτουργικού κόστους

Ο οικονομικότερος τρόπος διενέργειας των παραπάνω υπηρεσιών είναι η προμήθεια τους με τη μορφή συνεχούς ενοικιαζόμενης υπηρεσίας (security as a service). Η αποτελεσματική χρήση των υπηρεσιών SaaS (security as a service) δεν είναι δεδομένη μόνο με τη προμήθεια αυτών. Χρειάζεται προεργασία, συμμετοχή, έλεγχος και φυσικά θέληση να δουλέψουμε με έναν εξωτερικό συνεργάτη. Το κόστος των συγκεκριμένων υπηρεσιών και η φαινομενική κάλυψη των βασικών απαιτήσεων ασφάλειας πληροφοριών, είναι οι μόνοι προβλέψιμοι παράγοντες στη σχέση αυτή. Η αποτελεσματικότητα και η ποιότητα εξαρτάται, κυρίως, από την κατάλληλη προετοιμασία του Οργανισμού. Οι επιλογές πλέον είναι πολλές και με τη κατάλληλη προεργασία θα δούμε ότι υπάρχει προστιθέμενη αξία ειδικότερα σε υπηρεσίες πέρα των τετριμμένων. Τέτοιου είδους υπηρεσίες είναι οι ακόλουθες: • Υπηρεσίες αξιολόγησης κινδύνων, οι οποίες περιλαμβάνουν συνδυασμό αξιολόγησης κινδύνων, vulnerability assessment & penetration testing. Ο συνδυασμός και η συχνότητα διενέργειας είναι ανάλογος των αναγκών της κάθε εταιρείας. • Υπηρεσίες συμμόρφωσης, οι οποίες περιλαμβάνουν την αρχική ανάλυση απόκλισης από τις κανονιστικές και θεσμικές διατάξεις, τη διαμόρφωση του πλαισίου διαχείρισης, καθώς και τους τακτικούς ελέγχους τήρησης των θεσμικών διατάξεων και εφαρμογής του πλαισίου συμμόρφωσης. • Υποδομή και υπηρεσίες εγκατάστασης, συλλογής, παρακολούθησης και ανάλυσης log αρχείων. Η επιλογή των υπηρεσιών που θα διενεργηθούν, προκύπτουν από τη μελέτη των κινδύνων ασφάλειας πληροφοριών του Οργανισμού, η οποία θα βοηθήσει στην ιεράρχηση των αναγκών για υλοποίηση.

Αποτελεσματική επικοινωνία με τη Διοίκηση

Όσο και αν τα παραπάνω φαίνονται ή αξιολογούνται ως λογικά, δεν μπορεί να υλοποιηθούν εάν δε επικοινωνηθούν αποτελεσματικά με τη διοίκηση. Τις περισσότερες φορές η αιτία μη υλοποίησης αναγκαίων θεμάτων που αφορούν στην ασφάλεια πληροφοριών δεν έχει άμεση σχέση με την οικονομική ύφεση, αλλά με το τρόπο που επικοινωνούνται στην εκάστοτε Διοίκηση και ιδιαίτερα τα θέματα που αφορούν στις προτεραιότητες και ανάγκες υλοποίησης. Η πρωταρχική ενέργεια του Υπεύθυνου Ασφάλειας Πληροφοριών είναι να κατανοήσει τον τρόπο με τον οποίο λειτουργεί η εταιρεία, προκειμένου να πετύχει τους στόχους της.

Στη συνέχεια, πρέπει να αναγνωρίσει συνολικά τις πραγματικές ανάγκες όλου του Οργανισμού και να τις μετατρέψει σε συγκεκριμένες απαιτήσεις για λύσεις και υπηρεσίες που αφορούν στην ασφάλεια πληροφοριών. Οι απαιτήσεις κανονιστικής συμμόρφωσης, καθώς και η βούληση της Διοίκησης για το ανεκτό επίπεδο ανοχής του κινδύνου, είναι απαραίτητες γνώσεις. Εχοντας κατανοήσει τα παραπάνω, ο υπεύθυνος ασφάλειας πληροφοριών μπορεί να ιεραρχήσει τις ανάγκες του Οργανισμού και σε συνδυασμό με τα αποτελέσματα των αξιολογήσεων κινδύνων, να υποστηρίξει τις θέσεις του επαρκώς και να επιχειρηματολογήσει για αυτές με κάτι πέρα του γενικού κινδύνου που αντιμετωπίζουν όλες οι εταιρείες σε σχέση με την ασφάλεια πληροφοριών. **nw**

Ο **Νότης Ηλιόπουλος** είναι *Director of Technology* στην Intelli Solutions S.A