ΑΝΤΙΜΕΤΩΠΙΣΗ ΕΠΙΘΕΣΕΩΝ ΚΑΙ ΕΞΑΣΦΑΛΙΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΣΥΓΧΡΟΝΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

Η κυβερνοασφάλεια είναι πλέον θέμα στρατηγικής σημασίας για τις σύγχρονες επιχειρήσεις. Αυτό δικαιολογείται από τον αριθμό των κυβερνοεπιθέσεων, που αυξάνονται με εκπληκτικούς ρυθμούς, καθώς επίσης, από την πολυπλοκότητά τους.

Μια πρόσφατη μελέτη εκτιμά ότι επιθέσεις τύπου «Ransomware», που αποτελούν μια από τις πολλές μορφές κυβερνοεπιθέσεων, εκτελούνται κάθε 40 δευτερόλεπτα. Προβλέπει όμως ότι μέχρι το 2019 η συχνότητα τους θα μειωθεί στα 14''. Από οικονομικής άποψης, η παγκόσμια αγορά της κυβερνοασφάλειας αναμένεται να φτάσει τα €100 δισεκατομμύρια το 2018, τα €170 δισ. μέχρι το 2020 και ότι θα αναρριχηθεί στα €800 δισ. μέσα στα επόμενα πέντε χρόνια.
Από την άλλη μεριά αναμένεται ότι το κόστος των οικονομικών επιπτώσεων, που θα επιφέρει το κυβερνοέγκλημα στις επιχειρήσεις θα ξεπεράσει τα €500 δισεκατομμύρια το 2018.
Επιπλέον, βάσει της έκθεσης με τίτλο «Cyber Security Ventures», το συνολικό κόστος του κυβερνοεγκλήματος αναμένεται να ξεπεράσει τα $6 τρισεκατομμύρια δολάρια ετησίως μέχρι το 2021.
Οι εξελίξεις αυτές είναι αναμενόμενες, αν ληφθεί υπόψη πως η τεχνολογία διεισδύει όλο και περισσότερο στην καθημερινότητα των μέσων χρηστών, των οργανισμών και των επιχειρήσεων, ανεξαρτήτως των δραστηριοτήτων τους. Συνεπώς, κρίνεται αναγκαίο να υπάρχει ένα ολοκληρωμένο πλαίσιο ασφάλειας, το οποίο να βασίζεται σε διεθνείς πρακτικές, αλλά και να προσαρμόζεται στις ανάγκες και στις προτεραιότητες του εκάστοτε οργανισμού.

ΤΑ 5 ΒΗΜΑΤΑ ΑΣΦΑΛΕΙΑΣ
Ένα από τα διεθνή πρότυπα ασφάλειας, που συχνά επιλέγουν να ακολουθήσουν οι οργανισμοί, έχει εκδοθεί από τον οργανισμό NIST. Το πρότυπο αυτό περιλαμβάνει τα διακριτά βήματα, που πρέπει να γίνουν από έναν οργανισμό, ώστε να αντιμετωπιστεί ένα περιστατικό ασφάλειας. Συγκεκριμένα, τα βήματα αυτά περιλαμβάνουν:
1. Την αναγνώριση και αξιολόγηση των διαθέσιμων στοιχείων.
2. Την εφαρμογή κατάλληλων αντιμέτρων προστασίας.
3. Τον έγκαιρο εντοπισμό του περιστατικού.
4. Την αποδοτική αντιμετώπισή του.
5. Την ανάκαμψη από τις πιθανές επιπτώσεις του.
Αρχικά, πρέπει να καταγραφούν όλα τα στοιχεία που σχετίζονται με τον οργανισμό και τις κυβερνοαπειλές που ενδέχεται να αντιμετωπίσει. Η καταγραφή θα πρέπει να καλύπτει υλικά αγαθά, όπως είναι οι servers, οι υπολογιστές και στοιχεία του δικτύου (π.χ. δρομολογητές), τις ενδεχόμενες κυβερνοαπειλές, στις οποίες είναι εκτεθειμένος, καθώς και τις παραμέτρους που συνθέτουν το πλαίσιο κυβερνοασφάλειας του οργανισμού. Αφού εντοπιστούν όλα τα παραπάνω, θα πρέπει να υλοποιηθούν, βάσει των σχετικών προτεραιοτήτων, όλα τα αναγκαία μέτρα προστασίας του οργανισμού, όπως καθορίζονται από έγκυρες μεθοδολογίες (π.χ. ανάλυση επικινδυνότητας) και βέλτιστες πρακτικές ασφάλειας.
Στη συνέχεια, ο υπεύθυνος ασφάλειας πρέπει να επικεντρωθεί στο να επιλέξει και να υλοποιήσει ορθά τους μηχανισμούς ασφάλειας για τον εντοπισμό, την αντιμετώπιση και την ανάκαμψη από ένα πιθανό περιστατικό ασφάλειας. Σημειώνεται ότι όσο πιο αποδοτική είναι η προστασία απέναντι σε μία κυβερνοαπειλή τόσο ελαχιστοποιείται ή ακόμα και μηδενίζεται η επίπτωσή της στον οργανισμό. Συνεπώς, μόλις μία τέτοια απειλή λάβει χώρα, εάν εκτιμηθεί το μέγεθος της επίπτωσής της έγκαιρα και αποτελεσματικά, τότε ο οργανισμός θα είναι σε θέση να δημιουργήσει μία αρκετά ουσιαστική εικόνα για το απαιτούμενο επίπεδο προστασίας που θα πρέπει να εφαρμοστεί. Σημειώνεται πως τα δύο αυτά στοιχεία είναι αντιστρόφως ανάλογα μεταξύ τους, δεδομένου ότι η αύξηση του ενός συνεπάγεται μείωση του άλλου και αντίστροφα.

ΟΙ ΟΙΚΟΝΟΜΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ, ΠΟΥ ΘΑ ΕΠΙΦΕΡΕΙ ΤΟ ΚΥΒΕΡΝΟΕΓΚΛΗΜΑ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΑΝΑ ΤΟ ΠΑΓΚΟΣΜΙΟ, ΘΑ ΞΕΠΕΡΑΣΟΥΝ ΤΑ €500 ΔΙΣ. ΤΟ 2018

ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΕΦΑΡΜΟΓΗ
Τα βήματα που συνθέτουν το υπό αναφορά πρότυπο είναι συνδεδεμένα, με αποτέλεσμα η ελλιπής εφαρμογή των αρχικών βημάτων να επηρεάζει την αποτελεσματικότητα των ακολούθων και κατ' επέκταση ολόκληρου του πλαισίου. Για παράδειγμα, εάν ένα σύστημα δεν ληφθεί καν υπόψη στην αξιολόγηση του πρώτου βήματος, τότε υπάρχει μεγάλη πιθανότητα να μην εφαρμοστούν αντίμετρα για να το προστατεύσουν. Αντίστοιχα, αν οι υπάρχοντες μηχανισμοί αποτύχουν να αναγνωρίσουν ένα (πιθανό) περιστατικό ασφάλειας, τότε δεν είναι δυνατή η αποτελεσματική αντιμετώπισή του.
Όταν αναγνωριστούν αδυναμίες, ο οργανισμός θα πρέπει να επανεξετάσει όλα τα στάδια του πλαισίου ασφάλειας και να εντοπίσει τα σημεία που δεν εφαρμόστηκαν αποτελεσματικά. Σημειώνεται πως δεν είναι πάντα θέμα αμέλειας, καθώς ο οργανισμός είναι δυναμικός με πολλές αλλαγές σε διάφορα επίπεδα να εκτελούνται κατά την εφαρμογή του πλαισίου, π.χ. νέο σύστημα, διαδικασία, κτλ. Για τον λόγο αυτό, η εφαρμογή των παραπάνω βημάτων θα πρέπει να επανεξετάζεται σε τακτά χρονικά σημεία τόσο σε θεωρητικό επίπεδο όσο και σε πρακτικό (π.χ. δοκιμαστικά σενάρια περιστατικών ασφάλειας).

ΕΠΕΝΔΥΣΗ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ
Η επένδυση στην κυβερνοασφάλεια ενός οργανισμού τόσο σε χρόνο όσο και σε χρήμα είναι μία απαιτητική διαδικασία, που περιλαμβάνει αρκετές προκλήσεις, αλλά μπορεί να επιφέρει οφέλη και ανταγωνιστικό πλεονέκτημα. Ο κάθε οργανισμός θα πρέπει να εστιάσει στα ακόλουθα σημεία για τη θωράκισή του έναντι των κυβερνοαπειλών:
• Στο ανθρώπινο δυναμικό: Η κυβερνοασφάλεια θα πρέπει να αποτελεί υπόθεση όλων μέσα στον οργανισμό, από το Διοικητικό Συμβούλιο που θα καθορίσει τη στρατηγική μέχρι τον τελευταίο υπάλληλο που θα πρέπει να την ακολουθήσει. Σημαντική είναι η σύσταση μονάδας και ο διορισμός ατόμου υπεύθυνου για την ασφάλεια των πληροφοριών.
• Στα συστήματα και υποδομές: Οι οργανισμοί θα πρέπει να υιοθετήσουν συστήματα και να υλοποιήσουν υποδομές με βάση βέλτιστες πρακτικές και κατευθύνσεις, έχοντας ως στόχο την παρακολούθηση, την έγκαιρη αναγνώριση και την αποτελεσματική αντιμετώπιση των κυβερνοαπειλών.
• Στις διαδικασίες: Ένα πλαίσιο διαδικασιών θα πρέπει να σχεδιαστεί και να υλοποιηθεί, με στόχο να προωθεί την υιοθέτηση των απαιτούμενων μέτρων και μηχανισμών ασφαλείας κατά τη διεξαγωγή των εργασιών του οργανισμού.

Νίκος Τσάλης
Head of Information Security, Business Consulting Services

Η ΣΥΜΒΟΛΗ ΤΗΣ LOGICOM SOLUTIONS

Η Logicom Solutions βρίσκεται δίπλα στον κάθε οργανισμό για να συμβουλεύσει και να βοηθήσει στο σχεδιασμό, την ανάπτυξη και την υλοποίηση εξατομικευμένων και αποτελεσματικών πλαισίων διαχείρισης των κινδύνων που προκύπτουν από τις κυβερνοαπειλές. Με την παροχή ενός ολοκληρωμένου φάσματος υπηρεσιών και τεχνολογικών προϊόντων, που ξεκινούν από την αξιολόγηση μέσω υπηρεσιών «Penetration Testing» και τον καθορισμό πολιτικής και φθάνουν μέχρι και την υλοποίηση και εφαρμογή μηχανισμών κυβερνοασφάλειας, υποστηρίζουμε τον κάθε οργανισμό να λειτουργήσει σε ένα πιο ασφαλές και προστατευμένο περιβάλλον.

Στοιχεία Επικοινωνίας
Κεντρικά γραφεία: Λεωφ. Κέννεντυ 50, 1076 Λευκωσία | **Τηλέφωνο:** +357 22 551010
Φαξ: +357 22 660 969 | **E-mail:** solutions@logicom.net | **Ιστοσελίδα:** www.logicomsolutions.com.cy