Κυβερνοασφάλεια στην ψηφιακή εποχή

- *Στο μέλλον όλο και περισσότεροι οργανισμοί θα επηρεαστούν από κυβερνοεπιθέσεις*
- *Η επίτευξη «ψηφιακής ανθεκτικότητας» απαιτεί την εμπλοκή όλων μέσα στον οργανισμό*

Η ψηφιακή επανάσταση συνεχίζει να μεταλλάσσει την καθημερινότητά μας. Αυτό θέτει την καινοτομία και την ανάπτυξη στο επίκεντρο της επιχειρηματικής ατζέντας του κάθε CEO και Διοικητικού Συμβουλίου παγκοσμίως. Τα επιχειρηματικά μοντέλα γίνονται πιο ψηφιακά, οι επιχειρήσεις λειτουργούν 24/7, ενώ παράλληλα οι διαδικασίες τρέχουν σε αληθινό χρόνο με τον όγκο των δεδομένων που παράγονται να γίνεται όλο και μεγαλύτερος. Αυτό βέβαια αφήνει τους οργανισμούς πιο ευάλωτους στην απειλή των κυβερνοεπιθέσεων αυξάνοντας σημαντικά την επιφάνεια που μπορεί να εκμεταλλευτεί ένας πιθανός επιτιθέμενος.

Μέχρι πρότινος, μεγάλες επιχειρήσεις, κυρίως του χρηματοοικονομικού τομέα, καθώς και κυβερνήσεις ήταν οι αποκλειστικοί στόχοι αυτών των επιθέσεων. Όχι πλέον. Τα πρόσφατα περιστατικά (2017) «ransomware», «WannaCry» και «NotPetya» επηρέασαν τη λειτουργία επιχειρήσεων, μικρών και μεγάλων, που δραστηριοποιούνται σε ένα μεγάλο εύρος επιχειρηματικών τομέων. Στο πρώτο μισό του 2018, η ανεύρεση των τρωτών σημείων, «Meltdown» και «Spectre», σε τσιπ υπολογιστών απέδειξε ότι πλέον σημαντικοί κίνδυνοι στον κυβερνοχώρο δεν εμφανίζονται μόνο στο επίπεδο του λογισμικού αλλά και σε υλισμικό («hardware»).

Το 2018 υπήρχαν περισσότεροι κυβερνοεγκληματίες στη λίστα των καταζητούμενων του FBI από οποιαδήποτε άλλη χρονιά

Παράλληλα, αξίζει να σημειωθεί πως το 2018 υπήρχαν περισσότεροι κυβερνοεγκληματίες στη λίστα των καταζητούμενων του FBI από οποιαδήποτε άλλη χρονιά. Συνεπώς, αυτοί οι παράγοντες αναδεικνύουν την ανάγκη προς λήψη αποτελεσματικών μέτρων κυβερνοασφάλειας, αφού όλο και περισσότεροι οργανισμοί θα επηρεαστούν από πιθανές κυβερνοεπιθέσεις στο εγγύς μέλλον.

Μία πρόσφατη μελέτη της Accenture δείχνει ότι η κυβερνοασφάλεια είναι πλέον στρατηγικής σημασίας για τις Γενικές Διευθύνσεις και τα Διοικητικά Συμβούλια των επιχειρήσεων. Αναγνωρίζεται πλέον το μέγεθος της ζημιάς που μπορεί να επιφέρει μια επικείμενη κυβερνοεπίθεση σε έναν οργανισμό, τόσο από οικονομικής απόψεως όσο και στην υστεροφημία του. Είναι όμως εμφανές το γεγονός ότι υπάρχουν ακόμα πολλά που πρέπει να γίνουν για να θεωρηθεί ότι οι οργανισμοί είναι κατάλληλα προετοιμασμένοι για να αντιμετωπίσουν αποτελεσματικά τους ελλοχεύοντες κινδύνους στον κυβερνοχώρο.

Η αλόγιστη και χωρίς σχεδιασμό επένδυση πόρων στην κυβερνοασφάλεια σίγουρα δεν αποτελεί λύση στο πρόβλημα. Η κυβερνοασφάλεια δεν είναι μια περιοχή η οποία μπορεί να αναπτυχθεί μεμονωμένα ή χωρίς να λαμβάνει υπόψη το ευρύτερο επιχειρηματικό και τεχνολογικό πλαίσιο του οργανισμού. Αντιθέτως, η κυβερνοασφάλεια πρέπει να είναι ενσωματωμένη σε αυτά.

Εμπειρικά, οι οργανισμοί οι οποίοι διαθέτουν ένα ολοκληρωμένο και αποτελεσματικό πλαίσιο κυβερνοασφάλειας είναι αυτοί που υιοθετούν ένα πρόγραμμα «ψηφιακής ανθεκτικότητας». Αυτό σημαίνει ότι σχεδιάζουν τις επιχειρηματικές τους διαδικασίες και την τεχνολογική τους υποδομή και συστήματα με τρόπο που διευκολύνει την προστασία κρίσιμων πληροφοριών, την υλοποίηση ισχυρών δικλείδων κυβερνοασφάλειας και την εφαρμογή αποτελεσματικού πλάνου αντιμετώπισης κυβερνοεπιθέσεων.

Βέλτιστες πρακτικές

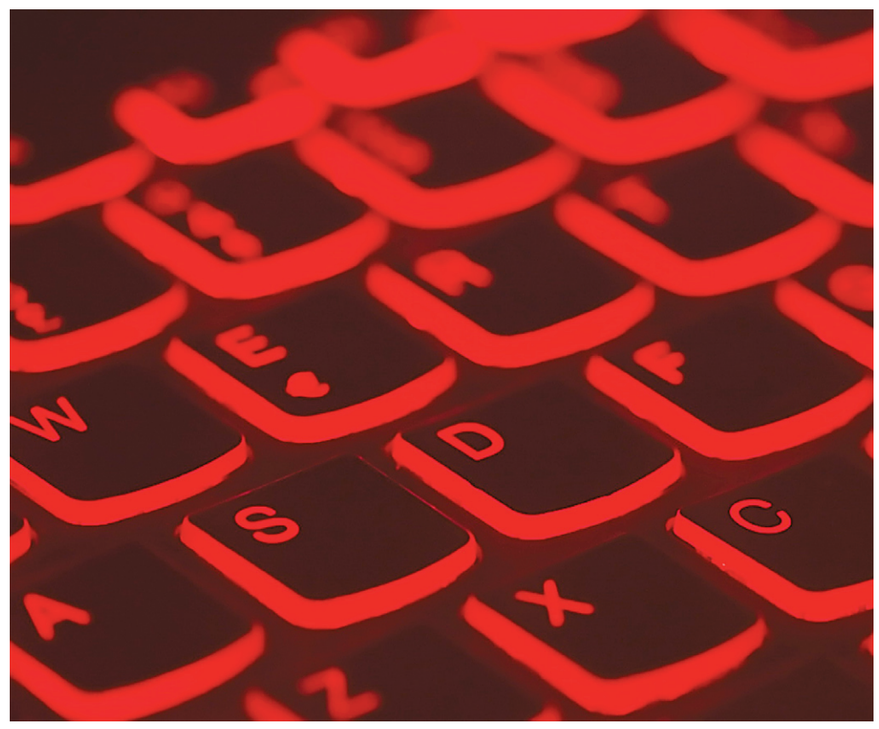
Οι ακόλουθες καλές πρακτικές, όπως αυτές αναγνωρίζονται από διεθνείς οίκους και αρχές ασφαλείας, είναι καίριες στην επίτευξη ενός σωστού και ολοκληρωμένου προγράμματος ψηφιακής ανθεκτικότητας:

1 Ενσωμάτωση της κυβερνοασφάλειας στις διαδικασίες διαχείρισης και διακυβέρνησης του οργανισμού. Ο κυβερνοκίνδυνος είναι ένα πολύπλοκο, μη οικονομικής φύσεως θέμα το οποίο μπορεί να έχει σημαντική αρνητική επίδραση στην κερδοφορία και στην υστεροφημία του οργανισμού. Γι' αυτό τον λόγο οι εταιρείες πρέπει να ενσωματώσουν μέτρα προστασίας εναντίον του συγκεκριμένου κινδύνου μέσα στις καθημερινές επιχειρηματικές τους διαδικασίες. Επιπλέον, είναι σημαντικό να αναγάγουν την κυβερνοασφάλεια σε στρατηγικής σημασίας θέμα, το οποίο θα είναι παράγοντας που αξιολογείται σοβαρά στο πλαίσιο λήψης στρατηγικών αποφάσεων από τις Διευθύνσεις και τα Διοικητικά Συμβούλια.

2 Προτεραιοποίηση των πληροφοριών που συλλέγονται και κρατούνται ανάλογα με τη σημαντικότητά τους και καταγραφή των σχετικών με αυτές κινδύνων. Στις πλείστες επιχειρήσεις μεγάλο ποσοστό των πληροφοριών που κρατούνται, σε διάφορα συστήματα, δεν είναι «mission critical». Οι επιχειρήσεις θα πρέπει να καταγράψουν τις πληροφορίες που συλλέγονται, να αξιολογήσουν τη σημαντικότητά τους και να αναγνωρίσουν πού αυτές αποθηκεύονται, σε ποια συστήματα και βάσεις δεδομένων. Παράλληλα θα πρέπει να αναγνωρίσουν και να αξιολογήσουν τους κυβερνοκινδύνους στους οποίους αυτές οι πληροφορίες είναι εκτεθειμένες. Οι προσπάθειές τους θα πρέπει να εστιάζουν στην προστασία των πιο σημαντικών για τη λειτουργία του οργανισμού πληροφοριών. Αυτό μπορεί να βοηθήσει να βελτιώσουν την επένδυση στην κυβερνοασφάλεια, κάνοντάς την πιο στοχευμένη, μειώνοντας τις δαπάνες τους σε σημαντικό βαθμό.

3 Ενδυνάμωση των μέτρων προστασίας από κυβερνοεπιθέσεις σε σχέση με τα ζωτικής σημασίας περιουσιακά στοιχεία του οργανισμού. Η εφαρμογή των ίδιων μέτρων κυβερνοασφάλειας για όλα τα στοιχεία ενεργητικού του οργανισμού δημιουργεί επιπλέον επιβάρυνση τόσο οικονομική όσο και σε ανθρώπινους πόρους. Τα ζωτικής σημασίας περιουσιακά στοιχεία πρέπει να προστατεύονται καλύτερα από τα λιγότερο σημαντικά. Οι έλεγχοι θα πρέπει να υπερβαίνουν τις τυπικές επιλογές, όπως η κρυπτογράφηση και να συμπεριλαμβάνουν διαδικασίες ταυτοποίησης, υιοθέτησης δικαιωμάτων πρόσβασης, πρόληψης απώλειας δεδομένων («data loss prevention»), διαχείρισης ψηφιακών δικαιωμάτων («digital-rights management»), ανίχνευσης εισβολών («intrusion detection») και πλαίσιο σχεδιασμού και υλοποίησης διορθωτικών ενεργειών («patching»).

> *Όσο εξελίσσεται και εξαπλώνεται η τεχνολογία τόσο περισσότερο αυξάνονται οι κυβερνοαπειλές για τις επιχειρήσεις*



4 Εμπλοκή όλων των υπαλλήλων. Ο κάθε υπάλληλος έχει ένα σημαντικό ρόλο να διαδραματίσει στην προστασία του οργανισμού στον κυβερνοχώρο. Για παράδειγμα, η όποια ανταλλαγή ευαίσθητων πληροφοριών θα πρέπει να γίνεται μέσω ασφαλών καναλιών και όχι καναλιών που αφήνουν τον οργανισμό εκτεθειμένο, όπως το ηλεκτρονικό ταχυδρομείο. Συνεπώς, οι καμπάνιες ηλεκτρονικού «ψαρέματος» (phishing), η τακτική εκπαίδευση και ενημέρωση όσο και οι πρακτικές ασκήσεις κυβερνοασφάλειας επιτρέπουν στους υπαλλήλους να συνειδητοποιήσουν τους κινδύνους που ελλοχεύουν και πώς μπορούν να τους μετριάσουν αποτελεσματικά, υιοθετώντας συγκεκριμένες βέλτιστες πρακτικές.

5 Ανάπτυξη και αποτελεσματική ενσωμάτωση χαρακτηριστικών ασφαλείας στα συστήματα πληροφορικής του οργανισμού. Οι οργανισμοί θα πρέπει να αναπτύσσουν αποτελεσματικά μέτρα κυβερνοασφάλειας στον πυρήνα των πληροφοριακών τους συστημάτων και υποδομών, ακριβώς όπως τα θεμέλια τοποθετούνται πριν την ανάπτυξη μίας οικοδομής. Οι υπεύθυνοι για την ανάπτυξη λογισμικού στον οργανισμό πρέπει να διαθέτουν τα απαραίτητα εργαλεία για να αναπτύξουν εφαρμογές που είναι λιγότερο ευάλωτες στους πιθανούς επιτιθέμενους. Οι εταιρείες θα πρέπει επίσης να αναπτύσσουν και να «ρυθμίζουν» τα συστήματα πληροφορικής τους με τρόπους που μειώνουν την έκθεση σε κυβερνοκινδύνους.

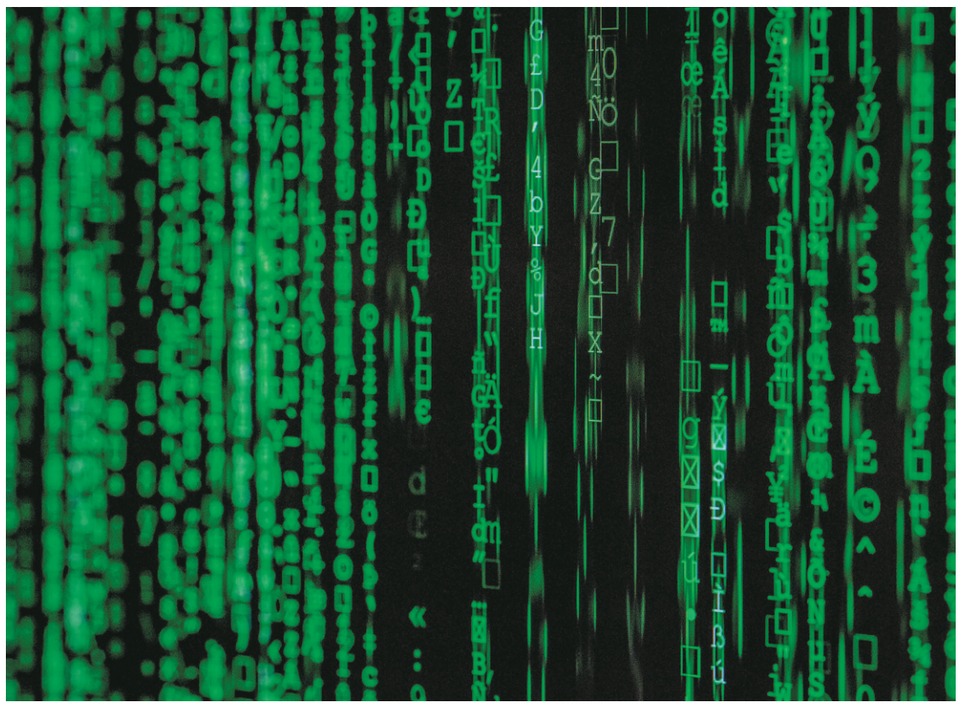
6 Χρήση πρακτικών «ενεργητικής άμυνας» για την προστασία έναντι των εισβολέων. Αργά ή γρήγορα η κάθε επιχείρηση θα δεχτεί κάποιου είδους κυβερνοεπίθεση. Οι εταιρείες μπορούν να προστατευτούν από τους «hackers», πιο αποτελεσματικά, αν αντιληφθούν πώς συμπεριφέρονται. Οι κορυφαίες εταιρείες στον κόσμο χρησιμοποιούν πλέον αναλύσεις μεγάλων δεδομένων («big data analytics») για τον εντοπισμό δεικτών ή ενδείξεων που ενδέχεται να υποδηλώνουν επικείμενη επίθεση, όπως για παράδειγμα οι προσπάθειες σύνδεσης σε δίκτυα από ασυνήθιστες τοποθεσίες. Διατηρούν επίσης ενημερωμένες πληροφορίες σχετικά με τις ικανότητες και τις προθέσεις των εγκληματιών του κυβερνοχώρου – και μερικές φορές ακόμη και την ταυτότητά τους.

7 Προγραμματισμός και αξιολόγηση μέτρων αντιμετώπισης σε περιστατικά κυβερνοεπιθέσεων. Γνωρίζοντας ότι η πιθανότητα κυβερνοεπίθεσης είναι πλέον μεγάλη, οι εταιρείες πρέπει να καταρτίσουν πλάνο αντιμετώπισης αυτών. Μετά την ολοκλήρωση του σχεδιασμού και εφαρμογής των σχεδίων αντιμετώπισης τέτοιων περιστατικών, οι εταιρείες πρέπει να τα αξιολογούν σε τακτά χρονικά διαστήματα, με τεχνικές προσομοίωσης τέτοιων καταστάσεων για να είναι όσο πιο κοντά στην πραγματικότητα γίνεται. Βάσει ερευνών, οι ρεαλιστικές προσομοιώσεις αυξάνουν την ψηφιακή ανθεκτικότητα των οργανισμών.

Ομάδα Κυβερνοασφάλειας, Τμήμα Συμβουλευτικών Υπηρεσιών, Logicom Solutions

Η ομάδα παροχής συμβουλευτικών υπηρεσιών κυβερνοασφάλειας της Logicom Solutions αντιλαμβάνεται πλήρως την ανάγκη των επιχειρήσεων να προστατευτούν επαρκώς από τον κίνδυνο κυβερνοεπιθέσεων που καλούνται να αντιμετωπίσουν. Παράλληλα, οι άριστα καταρτισμένοι επαγγελματίες που απαρτίζουν την ομάδα, αναγνωρίζουν ότι η ασφάλεια στον κυβερνοχώρο αφορά τη σωστή και συντονισμένη διαχείριση του κινδύνου αφού δεν είναι πάντα εφικτή η πλήρης εξάλειψή του η οποία μπορεί να συνεπάγει περιορισμό των επιχειρηματικών δραστηριοτήτων ή και της ανταγωνιστικότητάς του οργανισμού.

Με γνώμονα τις ανάγκες και το βαθμό ωριμότητας του πλαισίου κυβερνοασφάλειας του κάθε οργανισμού, η ομάδα της Logicom Solutions μπορεί να παρέχει και να υποστηρίξει τις εξατομικευμένες υπηρεσίες που χρειάζεται ο κάθε οργανισμός για την επίτευξη των επιχειρηματικών του στόχων με την καλύτερη δυνατή προστασία απέναντι στους κινδύνους που ελλοχεύουν. Οι πιστοποιημένοι από διεθνείς οργανισμούς επαγγελματίες μας (ISC2, ISACA, Offensive Security) μπορούν να βοηθήσουν στον καθορισμό των στρατηγικών και πολιτικών ασφάλειας πληροφοριών, στην εφαρμογή της απαιτούμενης διακυβέρνησης κυβερνοασφάλειας και στην πρακτική υλοποίηση των κατάλληλων μέτρων αντιμετώπισης περιστατικών. Παράλληλα, η ομάδα μας υποστηρίζει τον σχεδιασμό και υλοποίηση του απαραίτητου πλαισίου κυβερνοασφάλειας του οργανισμού, που αποτελεί ένα από τα βασικά συστατικά ανάπτυξής του. Από την παροχή υπηρεσιών «Penetration Testing» και «Vulnerability Assessment» μέχρι και την εφαρμογή εργαλείων και υποδομής κυβερνοασφάλειας, η Logicom Solutions είναι δίπλα σε κάθε οργανισμό για μια πιο ασφαλή πορεία στον κυβερνοχώρο.



Εξειδικευμένες ομάδες κατά των απειλών

Οι επιχειρήσεις είναι πλέον αναγκασμένες να προστατεύσουν τις πιο σημαντικές πληροφορίες που διαθέτουν, διατηρώντας παράλληλα την ευκολία και ευελιξία της καθημερινής τους λειτουργίας. Η επίτευξη «ψηφιακής ανθεκτικότητας» απαιτεί την εμπλοκή όλων μέσα στον οργανισμό. Η παρακολούθηση από το Διοικητικό Συμβούλιο και την Ανώτερη Διεύθυνση είναι απαραίτητη για να διασφαλιστεί η πληρότητα και αποτελεσματικότητα του προγράμματος κυβερνοασφάλειας ενός οργανισμού. Οι εξειδικευμένες ομάδες κυβερνοασφάλειας πρέπει να διατηρούν μια εμπεριστατωμένη και ενημερωμένη κατανόηση των απειλών που αντιμετωπίζουν οι εταιρείες τους και να σχεδιάζουν ολοκληρωμένα συστήματα άμυνας για την αντιμετώπισή τους. Παράλληλα, τόσο το τμήμα πληροφορικής όσο και η κάθε επιχειρηματική μονάδα του οργανισμού θα πρέπει να αναγνωρίσουν τους κινδύνους στους οποίους είναι εκτεθειμένες και να ενσωματώσουν κατάλληλα πρωτόκολλα και δικλίδες ασφαλείας στις καθημερινές τους διαδικασίες, σε συντονισμό πάντα με την ομάδα κυβερνοασφάλειας του οργανισμού.

Είναι πλέον ευρέως αποδεκτό ότι όσο εξελίσσεται και εξαπλώνεται η τεχνολογία τόσο περισσότερο αυξάνονται οι κυβερνοαπειλές για τις επιχειρήσεις. Η κυβερνοασφάλεια είναι υπόθεση όλων μέσα στον οργανισμό και η ολοκληρωμένη αντιμετώπιση των κινδύνων είναι αναγκαία επένδυση για την κάθε επιχείρηση, η οποία μπορεί να υποστηρίξει την ανάπτυξή της και την κερδοφορία της.