«Γιατί η Εκπαίδευση στην Κυβερνοασφάλεια είναι Απαραίτητη για ΜΜΕ και Δημόσια Διοίκηση»

Σήμερα, το κυβερνοέγκλημα έχει γίνει μια όλο και πιο συνηθισμένη μορφή επίθεσης. Η CrowdStrike προειδοποιεί ότι μεταξύ 2023 και 2024 οι κυβερνοεπιθέσεις αυξήθηκαν κατά 75%. Αυτό μπορεί να οφείλεται στο πόσο εύκολα μπορούν να οργανωθούν (οι επιτιθέμενοι μπορούν να δρουν από το σπίτι χωρίς να χρειάζεται να ταξιδεύουν και με ελάχιστες γνώσεις πληροφορικής) ή στο πόσο γρήγορα μπορούν να πραγματοποιηθούν (συχνά με ένα απλό κλικ).

Οι κυβερνοεπιτιθέμενοι έχουν πολλούς στόχους, όμως ο βασικός είναι συνήθως το οικονομικό όφελος, το οποίο επιτυγχάνεται μέσω της ζημιάς ή της εκμετάλλευσης των δεδομένων που διαχειρίζονται οι οργανισμοί. Επιπλέον, οι περισσότερες κυβερνοεπιθέσεις προκύπτουν από ανθρώπινο λάθος: λανθασμένες ρυθμίσεις συστημάτων, άνοιγμα κακόβουλων email, χρήση αδύναμων κωδικών πρόσβασης, μεταξύ άλλων. Πρόσφατες μελέτες δείχνουν ότι το ανθρώπινο λάθος ευθύνεται για έως και το 95% των παραβιάσεων ασφάλειας στις εταιρείες.

Ένας τύπος επίθεσης που αυξάνεται σημαντικά είναι οι επιθέσεις που στοχεύουν στην εφοδιαστική αλυσίδα, οι οποίες εκμεταλλεύονται ευπάθειες σε προμηθευτές ή συνεργάτες για να αποκτήσουν πρόσβαση σε συστήματα. Για τον λόγο αυτό, η διαχείριση της κυβερνοασφάλειας στην εφοδιαστική αλυσίδα θα αποτελέσει μια αναπόφευκτη πρόκληση.

Λαμβάνοντας υπόψη όλα τα παραπάνω, θα μπορούσε κανείς να συμπεράνει ότι η ισχυρή προστασία και η σωστή εκπαίδευση στην κυβερνοασφάλεια μπορούν να αποτρέψουν ή να περιορίσουν τις ζημιές από τέτοιες επιθέσεις. Ωστόσο, εξακολουθούν να υπάρχουν οργανισμοί (τόσο μικρομεσαίες επιχειρήσεις όσο και δημόσιοι φορείς) που υστερούν, καθώς δεν διαθέτουν τα απαραίτητα μέτρα ασφάλειας για να αντιμετωπίσουν αυτές τις καθημερινές απειλές, οι οποίες γίνονται ολοένα και πιο δύσκολο να εντοπιστούν (κυρίως λόγω της χρήσης τεχνητής νοημοσύνης από τους επιτιθέμενους).

Οι μικρές επιχειρήσεις συχνά σκέφτονται: «Είμαστε μικροί, κανείς δεν θα μας επιτεθεί» ή «Δεν είμαστε τόσο σημαντικοί όσο οι μεγάλες εταιρείες». Όμως αυτό είναι απολύτως λανθασμένο. Πρέπει να έχουμε υπόψη ότι:

- Οι επιτιθέμενοι συχνά προτιμούν τις μικρές επιχειρήσεις επειδή έχουν συνήθως πιο αδύναμη προστασία και μικρότερη ικανότητα αντίδρασης, γεγονός που τις καθιστά ελκυστικούς στόχους.

- Η αντίληψη ότι «δεν είμαστε ενδιαφέροντες στόχοι» είναι λανθασμένη, καθώς οι ΜΜΕ διαθέτουν δεδομένα ιδιαίτερα πολύτιμα για τους επιτιθέμενους, όπως στοιχεία πελατών (αριθμούς ταυτότητας, τραπεζικούς λογαριασμούς, διευθύνσεις), τιμολόγια και πρόσβαση σε ηλεκτρονική τραπεζική.

- Ο αντίκτυπος μιας κυβερνοεπίθεσης σε μια ΜΜΕ είναι συχνά διπλάσιος σε σχέση με μια μεγάλη εταιρεία, λόγω των περιορισμένων πόρων. Σε ορισμένες περιπτώσεις, μια μόνο κυβερνοεπίθεση έχει αναγκάσει μικρές επιχειρήσεις να κλείσουν, εξαιτίας των καταστροφικών συνεπειών. Αντίθετα, οι μεγάλες εταιρείες είναι συνήθως καλύτερα εξοπλισμένες για να αντιμετωπίσουν τέτοια περιστατικά. Το Cybersecurity Magazine αναφέρει ότι το 83% των μικρομεσαίων επιχειρήσεων δεν είναι προετοιμασμένες να ανακάμψουν από την οικονομική ζημιά μιας κυβερνοεπίθεσης.

Για όλους αυτούς τους λόγους, η εκπαίδευση στην κυβερνοασφάλεια είναι απαραίτητη και ιδιαίτερα σημαντική. Προσφέρει οφέλη όπως:

- Μείωση των κυβερνοεπιθέσεων που προκαλούνται από ανθρώπινο λάθος (εργαζόμενοι).
- Ενίσχυση των μέτρων ασφάλειας απέναντι σε επιθέσεις.
- Δυνατότητα πρόβλεψης και ευκολότερου εντοπισμού απειλών.
- Βελτίωση της ικανότητας αντίδρασης κατά τη διάρκεια κυβερνοεπιθέσεων.
- Ενίσχυση καλών πρακτικών κυβερνοασφάλειας τόσο εντός όσο και εκτός του οργανισμού.
- Προστασία προσωπικών δεδομένων, καθώς και των δεδομένων πελατών και προμηθευτών.
- Ενίσχυση της εμπιστοσύνης του κοινού.

Εκπαιδευτείτε στην κυβερνοασφάλεια – Προστατεύστε την επιχείρησή σας.