ΟΔΗΓΟΣ
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΓΙΑ ΤΙΣ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ (ΜΜΕ)

Παρακάτω θα βρείτε βέλτιστες πρακτικές πρόληψης για την καλύτερη προστασία των πληροφοριών και συστημάτων των ΜΜΕ

1. Αναπτύξτε πολιτικές ασφάλειας και κανόνες για την κυβερνοασφάλεια

Σαφείς και συγκεκριμένοι κανόνες πρέπει να περιγράφονται συνοπτικά στις πολιτικές κυβερνοασφάλειας για τους εργαζόμενους, ώστε να γνωρίζουν πώς πρέπει να συμπεριφέρονται όταν χρησιμοποιούν το περιβάλλον, τον εξοπλισμό και τις υπηρεσίες της επιχείρησης. Αυτές οι πολιτικές θα πρέπει επίσης να υπογραμμίζουν τις συνέπειες που θα μπορούσε να αντιμετωπίσει ένας εργαζόμενος εάν δεν συμμορφώνεται με αυτές. Οι πολιτικές πρέπει να επανεξετάζονται και να επικαιροποιούνται τακτικά.

2. Επενδύστε στην εκπαίδευση των εργαζομένων

Παρέχετε στο σύνολο των εργαζομένων τακτικές καταρτίσεις για την ευαισθητοποίησή τους ως προς την κυβερνοασφάλεια. Το κλειδί για να λειτουργήσει η ασφάλεια στον κυβερνοχώρο είναι να διασφαλίσετε ότι οι εργαζόμενοι σας είναι καλά εκπαιδευμένοι και εφαρμόζουν με συνέπεια τις καλές πρακτικές ασφάλειας. Μερικές φορές, ένα λάθος από έναν ακατάλληλα εκπαιδευμένο εργαζόμενο μπορεί να προκαλέσει την κατάρρευση ολόκληρου του συστήματος ασφαλείας.

3. Αναπτύξτε ένα σχέδιο αντιμετώπισης συμβάντων

Αναπτύξτε ένα επίσημο σχέδιο αντιμετώπισης συμβάντων, το οποίο περιέχει σαφείς οδηγίες, ρόλους και αρμοδιότητες με την κατάλληλη τεκμηρίωση, ώστε να διασφαλίζεται ότι η αντιμετώπιση κάθε συμβάντος γίνεται έγκαιρα με επαγγελματικό και αποτελεσματικό τρόπο. Για την ταχεία αντιμετώπιση των απειλών ασφάλειας, διερευνήστε εργαλεία που θα μπορούσαν να παρακολουθούν και να παράγουν προειδοποιήσεις όταν εκδηλώνονται ύποπτες δραστηριότητες ή παραβιάσεις ασφάλειας.

4. Χρησιμοποιείτε anti-virus και anti-malware λογισμικά

Εφόσον είστε συνδεδεμένοι στο διαδίκτυο, είναι αδύνατο να έχετε πλήρη προστασία από κακόβουλα λογισμικά. Ωστόσο, μπορείτε να μειώσετε σημαντικά την ευπάθειά σας διασφαλίζοντας ότι έχετε εγκατεστημένα στους υπολογιστές προγράμματα προστασίας από ιούς, όπως μια κεντρικά ελεγχόμενη λύση anti-virus η οποία να εφαρμόζεται σε όλους τους τύπους συσκευών και να διατηρείται επικαιροποιημένη, ώστε να διασφαλίζεται σταθερά η αποτελεσματικότητά της.

5. Διατηρήστε τα λογισμικά σας ενημερωμένα

Οι εταιρείες λογισμικών παρέχουν συνήθως ενημερώσεις λογισμικού για να προσθέσουν νέες δυνατότητες, να διορθώσουν γνωστά σφάλματα και να αναβαθμίσουν την ασφάλεια. Πάντα να ενημερώνετε στην πιο πρόσφατη έκδοση του λογισμικού σας για να προστατεύεστε από νέες ή υπάρχουσες ευπάθειες ασφαλείας. Μην αγνοείτε τις ενημερώσεις.

6. Δημιουργήστε αντίγραφα ασφαλείας σημαντικών δεδομένων (backup)

Για να παρέχεται η δυνατότητα ανάκτησης σημαντικών πληροφοριών, πρέπει να τηρούνται αντίγραφα ασφαλείας, τα οποία αποτελούν αποτελεσματική μέθοδο ανάκτησης από καταστροφές όπως, π.χ. επίθεση με σκοπό την αποκόμιση λύτρων (ransomware). Όσον αφορά τα αντίγραφα ασφαλείας, πρέπει να εφαρμόζονται οι ακόλουθοι κανόνες:

- Τα αντίγραφα να είναι τακτικά.
- Τα αντίγραφα να διατηρούνται χωριστά από το περιβάλλον της ΜΜΕ.

7. Ασφαλίστε το δίκτυό σας – υλοποίηση πολυεπίπεδης άμυνας

- Χρησιμοποιείτε τείχη προστασίας (firewall) που διαχειρίζονται την κυκλοφορία των δεδομένων στην είσοδο και έξοδο ενός δικτύου και αποτελούν κρίσιμο εργαλείο για την προστασία των συστημάτων των ΜΜΕ.
- Κατατμήστε το δίκτυο σε χρήστες και συσκευές.

8. Διαχείριση λογαριασμών και έλεγχος πρόσβασης

Η πρόσβαση σε πληροφορίες και συστήματα θα πρέπει να γίνεται βάσει ρόλων και καθηκόντων. Ο κωδικός ασφάλειας του κάθε χρήστη να χαρακτηρίζεται από ένα επαρκές επίπεδο δυσκολίας, για να μην αποτελέσει τον αδύναμο κρίκο σε περίπτωση επίθεσης. Να γίνεται χρήση ισχυρών κωδικών πρόσβασης σύμφωνα με τις πολιτικές ασφαλείας της επιχείρησης, καθώς και η εφαρμογή της τακτικής αλλαγής τους (συστήνεται κάθε 90 μέρες).

9. Χρήση εικονικού ιδιωτικού δικτύου

Τα εικονικά ιδιωτικά δίκτυα (VPN) παρέχουν έναν εξαιρετικό τρόπο για τους εργαζόμενους να έχουν ασφαλή πρόσβαση σε απομακρυσμένους πόρους από πολλές τοποθεσίες, συνδέοντας δύο ιδιωτικά δίκτυα με ασφάλεια μέσω διαδικτύου.

10. Συνεργαστείτε με έναν white hat hacker

Δεν είναι όλοι οι χάκερ κακοί. Μερικοί χάκερ εκθέτουν κινδύνους για την ασφάλεια, ώστε να βοηθήσουν άλλους να βελτιώσουν την κυβερνοασφάλειά τους, κρατώντας τους ενήμερους για ελαττώματα ασφαλείας και διορθώνοντάς τα. Αυτοί οι χάκερ είναι γνωστοί ως χάκερ «λευκού καπέλου» ή «penetration testers» οι οποίοι μπορούν να σας βοηθήσουν να βρείτε κινδύνους/ευπάθειες στο δίκτυο της επιχείρησής σας.

ΥΦΥΠΟΥΡΓΕΙΟ ΕΡΕΥΝΑΣ, ΚΑΙΝΟΤΟΜΙΑΣ ΚΑΙ ΨΗΦΙΑΚΗΣ ΠΟΛΙΤΙΚΗΣ
ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας
ΓΡΑΦΕΙΟ ΤΥΠΟΥ ΚΑΙ ΠΛΗΡΟΦΟΡΙΩΝ