Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Οδηγός για την ασφάλεια στον κυβερνοχώρο για μικρές επιχειρήσεις

Πολυπλοκότητα περιεχομένου
ΑΠΛΗ ● ○ ○

cyber.gov.au

Εισαγωγή

Για μια μικρή επιχείρηση, ακόμη και ένα μικρό περιστατικό ασφάλειας στον κυβερνοχώρο μπορεί να έχει καταστροφικές επιπτώσεις. Αυτός ο οδηγός περιλαμβάνει βασικά μέτρα ασφαλείας που βοηθούν στην προστασία της επιχείρησής σας από κοινές απειλές για την ασφάλεια στον κυβερνοχώρο. Ως σημείο εκκίνησης, προτείνουμε τα ακόλουθα τρία μέτρα:

- **Ενεργοποίηση ελέγχου ταυτότητας πολλαπλών παραγόντων**
- **Ενημερώστε το λογισμικό σας**
- **Δημιουργήστε αντίγραφα ασφαλείας των πληροφοριών σας**

Αυτός ο οδηγός μπορεί να περιλαμβάνει μέτρα που δεν σχετίζονται με την επιχείρησή σας ή η επιχείρησή σας μπορεί να έχει πιο περίπλοκες ανάγκες. Μετά την ολοκλήρωση αυτού του οδηγού, συνιστούμε στις μικρές επιχειρήσεις να εφαρμόσουν το Επίπεδο Ωριμότητας Ενα από τα Βασικά Οκτώ. Εάν έχετε ερωτήσεις σχετικά με αυτήν τη συμβουλή ή την ασφάλεια στον κυβερνοχώρο γενικότερα, σας συνιστούμε να μιλήσετε με έναν επαγγελματία πληροφορικής ή έναν αξιόπιστο σύμβουλο.

Επισκεφτείτε το cyber.gov.au για να διαβάσετε τον πλήρη οδηγό μας, συμπεριλαμβανομένων των συμβουλών για κάθε μέτρο.

Πίνακας περιεχομένων

Απειλές για τις μικρές επιχειρήσεις

Μηνύματα απάτης

Οι απάτες είναι ένας συνηθισμένος τρόπος με τον οποίο οι κυβερνοεγκληματίες στοχεύουν μικρές επιχειρήσεις. Στόχος τους είναι να εξαπατήσουν εσάς ή το προσωπικό σας σε:

- αποστολή χρημάτων ή δωροκάρτας
- κάνοντας κλικ σε κακόβουλους συνδέσμους ή συνημμένα
- δίνοντας ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης.

Οι εγκληματίες του κυβερνοχώρου μπορεί να προσπαθήσουν να εξαπατήσουν την επιχείρησή σας μέσω email, μηνυμάτων κειμένου, τηλεφωνικών κλήσεων και μέσων κοινωνικής δικτύωσης. Συχνά προσποιούνται ότι είναι ένα άτομο ή ένας οργανισμός που εμπιστεύεστε.

Επιθέσεις ηλεκτρονικού ψαρέματος (phishing)

Ιδιαίτερη ανησυχία για τις μικρές επιχειρήσεις είναι οι **επιθέσεις phishing**. Αυτές οι απάτες συχνά περιέχουν έναν σύνδεσμο προς έναν ψεύτικο ιστότοπο όπου σας ενθαρρύνουν να συνδεθείτε σε έναν λογαριασμό ή να εισαγάγετε εμπιστευτικές λεπτομέρειες.

Οι επιθέσεις phishing συνήθως διακυβεύουν τους κωδικούς πρόσβασης του λογαριασμού σας. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν συχνά αυτή τη μέθοδο για να «κατακτήσουν» τους λογαριασμούς των μικρών επιχειρήσεων στα μέσα κοινωνικής δικτύωσης και να ζητήσουν λύτρα.

Τρόποι μετριασμού

Εάν ένα μήνυμα προέρχεται από μια γνωστή οντότητα και φαίνεται ύποπτο, να είστε προσεκτικοί. Επικοινωνήστε με το άτομο ή την επιχείρηση ξεχωριστά για να ελέγξετε εάν το μήνυμα είναι νόμιμο. Χρησιμοποιήστε τα στοιχεία επικοινωνίας που βρίσκετε μέσω μιας νόμιμης πηγής, για παράδειγμα, επισκεπτόμενοι τον επίσημο ιστότοπο της επιχείρησης και όχι αυτά που περιέχονται στο ύποπτο μήνυμα.

Μάθετε περισσότερα σχετικά με τον εντοπισμό απατών και επιθέσεων phishing με τους ακόλουθους πόρους:

- Αναγνωρίστε και καταγγείλετε απάτες
- Μάθετε πώς να αναγνωρίζετε απάτες phishing
- Ανίχνευση μηνυμάτων που έχουν σχεδιαστεί κοινωνικά.

Μελέτη περίπτωσης:

Μία υπάλληλος σε μια εταιρεία ταχυμεταφορών έλαβε ένα email από ένα από τα διοικητικά στελέχη της εταιρείας, που ζητούσε να αγοράσουν 6 προπληρωμένες πιστωτικές κάρτες MasterCard των $500. Το στέλεχος της είπε να το κρατήσει εμπιστευτικό καθώς οι κάρτες θα ήταν κουπόνια δώρου για τα μέλη του προσωπικού. Μετά την αγορά, ζητήθηκε από την υπάλληλο να φωτογραφίσει και τις δύο πλευρές των καρτών και να τις στείλει στο στέλεχος ως απόδειξη αγοράς.

Σύμφωνα με τις οδηγίες, η υπάλληλος πήγε σε ένα ταχυδρομείο και χρησιμοποίησε την προσωπική της πιστωτική κάρτα για να αγοράσει τις δωροκάρτες. Απάντησε στο email του στελέχους και έστειλε φωτογραφίες από τις δωροκάρτες ως απόδειξη.

Μετά την επιστροφή της από το ταχυδρομείο, η υπάλληλος έδωσε τις φυσικές κάρτες στο στέλεχος - που δεν τις γνώριζε. Κατά τον έλεγχο, **όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου σχετικά με τις δωροκάρτες προέρχονταν από μια τυχαία διεύθυνση ηλεκτρονικού ταχυδρομείου και δεν προέρχονταν από τον νόμιμο λογαριασμό ηλεκτρονικού ταχυδρομείου του στελέχους. Ήταν μια απάτη.**

Επιθέσεις μέσω ηλεκτρονικού ταχυδρομείου

Εκτός από τις απάτες όπως το phishing, μια συνηθισμένη επίθεση ηλεκτρονικού ταχυδρομείου κατά μικρών επιχειρήσεων είναι ο **συμβιβασμός μέσω επαγγελματικού ηλεκτρονικού ταχυδρομείου** (BEC). Οι εγκληματίες μπορούν να παριστάνουν εκπροσώπους επιχειρήσεων χρησιμοποιώντας παραβιασμένους λογαριασμούς email ή με άλλα μέσα – όπως χρησιμοποιώντας ένα όνομα τομέα (domain name) που μοιάζει με το όνομα μιας πραγματικής επιχείρησης. Εκτός από την κλοπή πληροφοριών, ο στόχος αυτών των επιθέσεων είναι συνήθως να εξαπατήσουν τα θύματα για να στείλουν χρήματα σε έναν τραπεζικό λογαριασμό που λειτουργεί από τον απατεώνα.

Τρόποι μετριασμού

Η καλύτερη άμυνα ενάντια στις επιθέσεις ηλεκτρονικού ταχυδρομείου είναι η εκπαίδευση και η ευαισθητοποίηση των εργαζομένων σας. Βεβαιωθείτε ότι το προσωπικό σας γνωρίζει ότι πρέπει να είναι πάντα προσεκτικό με τα email σε σχέση με τα ακόλουθα:

- αιτήματα για πληρωμές, ειδικά εάν είναι επείγουσες ή εκπρόθεσμες
- αλλαγή τραπεζικών στοιχείων
- μια διεύθυνση email που δεν φαίνεται πολύ σωστή, όπως το όνομα τομέα που δεν ταιριάζει ακριβώς με το όνομα της εταιρείας του προμηθευτή.

Ενώ αυτές οι επιθέσεις μπορεί να είναι καταστροφικές, τα μέτρα μετριασμού είναι εύκολα και δεν κοστίζουν σχεδόν τίποτα. **Όταν το προσωπικό λαμβάνει τέτοια μηνύματα ηλεκτρονικού ταχυδρομείου, ο πιο αποτελεσματικός μετριασμός είναι να καλέσετε τον αποστολέα για να επιβεβαιώσετε ότι είναι νόμιμα.** Μην χρησιμοποιείτε τα στοιχεία επικοινωνίας που σας έχουν αποσταλεί, καθώς αυτά μπορεί να είναι δόλια. Εισαγάγετε μια επίσημη διαδικασία που πρέπει να ακολουθεί το προσωπικό όταν λαμβάνονται αιτήματα πληρωμής ή όταν αλλάζουν τα τραπεζικά στοιχεία.

Μάθετε να προστατεύετε την επιχείρησή σας από απάτες BEC και παραβιάσεις ηλεκτρονικού ταχυδρομείου με τους ακόλουθους πόρους:

- Συμβιβασμός επαγγελματικού ηλεκτρονικού ταχυδρομείου
- Προστατέψτε την επιχείρησή σας από απάτες και παραβιάσεις ηλεκτρονικού ταχυδρομείου
- Τι πρέπει να κάνετε εάν η επιχείρησή σας έχει γίνει στόχος απάτης ή παραβίασης μέσω ηλεκτρονικού ταχυδρομείου.

Μελέτη περίπτωσης:

Μια μικρή κατασκευαστική επιχείρηση έλαβε ένα email από τον προμηθευτή της που έλεγε ότι άλλαξαν τράπεζα. Ο προμηθευτής παρείχε νέα στοιχεία λογαριασμού για πληρωμές τιμολογίων. Επειδή το μήνυμα ηλεκτρονικού ταχυδρομείου φαινόταν νόμιμο, **η κατασκευαστική επιχείρηση δεν κάλεσε τον προμηθευτή για να επιβεβαιώσει την αλλαγή στα στοιχεία του τραπεζικού λογαριασμού.**

Η επιχείρηση πλήρωσε ένα τιμολόγιο από τον προμηθευτή για πάνω από $70.000. Την επόμενη μέρα, ένας άλλος υπάλληλος πλήρωσε κατά λάθος ξανά το ίδιο τιμολόγιο για ένα επιπλέον ποσό άνω των $70.000. Συνολικά, καταβλήθηκαν πάνω από $150.000 στον νέο τραπεζικό λογαριασμό.

Όταν η επιχείρηση τηλεφώνησε στον προμηθευτή της για να ρωτήσει εάν μπορούσε να επιστρέψει τα χρήματα της διπλής πληρωμής, ο προμηθευτής ενημέρωσε ότι αυτά τα τραπεζικά στοιχεία ήταν λανθασμένα. Αμέσως ξεκίνησε έρευνα και ο προμηθευτής ανακάλυψε ότι ένας από τους λογαριασμούς email τους είχε παραβιαστεί και έστελνε δόλια στοιχεία τραπεζικού λογαριασμού. **Δεν ανακτήθηκαν χρήματα.**

Κακόβουλο λογισμικό

Κακόβουλο λογισμικό (malware) είναι ένας γενικός όρος για λογισμικό που έχει σχεδιαστεί να προκαλεί βλάβη, όπως ransomware, ιούς, spyware και trojans. Το malware μπορεί:

- να κλέψει ή να κλειδώσει τα αρχεία στη συσκευή σας
- να κλέψει τους τραπεζικούς λογαριασμούς ή αριθμό πιστωτικής κάρτας σας
- να κλέψει τα ονόματα χρήστη ή κωδικούς πρόσβασης
- να πάρει τον έλεγχο ή να κατασκοπεύσει τον υπολογιστή σας.

Το malware μπορεί να σταματήσει τη σωστή λειτουργία της συσκευής σας, να διαγράψει ή να καταστρέψει τα αρχεία σας ή να επιτρέψει σε άλλους να έχουν πρόσβαση στις προσωπικές ή επιχειρηματικές πληροφορίες σας. Εάν η συσκευή σας έχει μολυνθεί με malware, μπορεί να είστε ευάλωτοι σε άλλες επιθέσεις. Το malware θα μπορούσε επίσης να εξαπλωθεί σε άλλες συσκευές του δικτύου σας.

Η συσκευή σας μπορεί να μολυνθεί από malware με διάφορους τρόπους, όπως:

- ανατρέχοντας σε ιστότοπους που έχουν μολυνθεί από κακόβουλο λογισμικό
- μέσω λήψης μολυσμένων αρχείων ή λογισμικού από το διαδίκτυο
- ανοίγοντας μολυσμένα συνημμένα αρχεία σε email.

Κακόβουλο λογισμικό που ζητά λύτρα (Ransomware)

Το Ransomware είναι ένας κοινός και επικίνδυνος τύπος κακόβουλου λογισμικού. Λειτουργεί κλειδώνοντας ή κρυπτογραφώντας τα αρχεία σας, ώστε να μην μπορείτε πλέον να έχετε πρόσβαση σε αυτά. Απαιτούνται λύτρα, συνήθως με τη μορφή κρυπτονομίσματος, για την αποκατάσταση της πρόσβασης στα αρχεία. Οι εγκληματίες του κυβερνοχώρου ενδέχεται επίσης να απειλήσουν να δημοσιεύσουν ή να πουλήσουν δεδομένα στο διαδίκτυο, εκτός εάν καταβληθούν λύτρα.

Τρόποι μετριασμού

Ενώ το λογισμικό προστασίας από ιούς ή ασφάλειας μπορεί να σας προστατεύσει από κακόβουλο λογισμικό, κανένα λογισμικό δεν είναι 100% αποτελεσματικό. Το προσωπικό πρέπει να είναι σε εγρήγορση με τα email, τους ιστότοπους και τις λήψεις αρχείων και να ενημερώνει τακτικά τις συσκευές του για να παραμένουν ασφαλείς.

Δείτε τους παρακάτω πόρους για περισσότερες πληροφορίες σχετικά με την προστασία της επιχείρησής σας από ransomware:

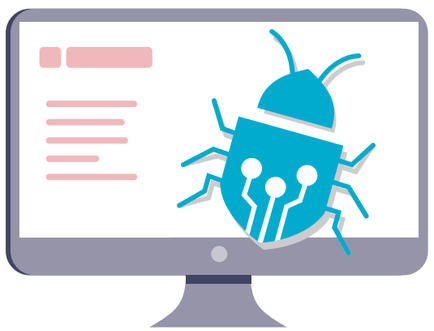
- Ransomware
- Προστατευτείτε από επιθέσεις ransomware
- Τι πρέπει να κάνετε εάν σας ζητούν λύτρα.

Μελέτη περίπτωσης:

Οι υπάλληλοι ενός καταστήματος ανταλλακτικών αυτοκινήτων ήρθαν στη δουλειά ένα πρωί και δεν μπόρεσαν να εκκινήσουν τον υπολογιστή διακομιστή τους. Όταν ο πάροχος πληροφορικής τους απόκτησε πρόσβαση στον διακομιστή, βρήκαν ένα παράθυρο ανοιχτό που έλεγε ότι όλα τα δεδομένα του υπολογιστή είχαν κρυπτογραφηθεί. Το σημείωμα απαιτούσε να πληρώσουν λύτρα σε bitcoin για να ξεκλειδώσουν τα αρχεία.

Υπήρχε μια μονάδα αντιγράφου ασφαλείας συνδεδεμένη στον υπολογιστή, η οποία ήταν επίσης κρυπτογραφημένη. Προσπάθησαν να συνδέσουν περισσότερες μονάδες αντιγράφων ασφαλείας, αλλά τα αρχεία κρυπτογραφήθηκαν αυτόματα μέσα σε δευτερόλεπτα. **Απέτυχαν να καταργήσουν το ransomware πριν επιχειρήσουν να ανακτήσουν τα δεδομένα τους και έχασαν κάθε αρχείο αντιγράφου ασφαλείας που είχαν.**

Η μόνη επιλογή που απέμενε ήταν να επαναφέρουν τις εργοστασιακές ρυθμίσεις του διακομιστή και να ξεκινήσουν εκ νέου με ένα νέο σύστημα. Η επιχείρησή τους έχασε δεδομένα πολλών ετών και έπρεπε να ξεκινήσει από την αρχή.



Ασφαλίστε τους λογαριασμούς σας

Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) καθιστά πιο δύσκολη την πρόσβαση των εγκληματιών του κυβερνοχώρου στους λογαριασμούς σας.

Το MFA προσθέτει άλλο ένα επίπεδο ασφάλειας στον λογαριασμό σας. Είναι ένας από τους πιο αποτελεσματικούς τρόπους για να προστατεύσετε τους λογαριασμούς σας από κάποιον να αποκτήσει πρόσβαση, επομένως θα πρέπει να τον χρησιμοποιείτε όπου είναι δυνατόν. Όποιος συνδεθεί στον λογαριασμό σας θα πρέπει να παράσχει κάτι άλλο εκτός από το όνομα χρήστη και τον κωδικό πρόσβασής σας. Αυτό θα μπορούσε να είναι ένας μοναδικός κωδικός από ένα μήνυμα κειμένου ή μια εφαρμογή ελέγχου ταυτότητας. Για περισσότερες πληροφορίες, διαβάστε τις συμβουλές μας για το MFA, που διατίθεται στη διεύθυνση **cyber.gov.au/mfa**.

✓ **Ενεργοποιήστε το MFA όπου είναι δυνατόν, ξεκινώντας από τους πιο σημαντικούς λογαριασμούς σας.**

Εφαρμογή ελέγχων πρόσβασης

Ο περιορισμός της πρόσβασης των χρηστών μπορεί να περιορίσει τη ζημιά που προκαλείται από ένα περιστατικό ασφάλειας στον κυβερνοχώρο.

Ο έλεγχος πρόσβασης είναι ένας τρόπος περιορισμού της πρόσβασης σε ορισμένα αρχεία και συστήματα. Συνήθως, το προσωπικό δεν απαιτεί πλήρη πρόσβαση σε όλα τα δεδομένα, τους λογαριασμούς και τα συστήματα μιας επιχείρησης. Θα πρέπει να τους επιτρέπεται να έχουν πρόσβαση μόνο σε ό,τι χρειάζονται για να ασκήσουν τα καθήκοντά τους.

Ο περιορισμός της πρόσβασης θα συμβάλει στον περιορισμό της ζημίας που προκαλείται από ένα περιστατικό ασφάλειας στον κυβερνοχώρο. Για παράδειγμα, εάν ο υπολογιστής ενός μέλους του προσωπικού έχει μολυνθεί με ransomware, με τους κατάλληλους ελέγχους πρόσβασης μπορεί να επηρεάσει μόνο έναν μικρό αριθμό αρχείων και όχι ολόκληρη την επιχείρηση.

✓ **Βεβαιωθείτε ότι κάθε χρήστης έχει πρόσβαση μόνο σε αυτό που χρειάζεται για τον ρόλο του.**

Χρησιμοποιήστε ισχυρούς κωδικούς πρόσβασης ή φράσεις πρόσβασης

Προστατέψτε τους λογαριασμούς σας από εγκληματίες στον κυβερνοχώρο με έναν ασφαλή κωδικό πρόσβασης ή φράση πρόσβασης.

Πολλές μικρές επιχειρήσεις αντιμετωπίζουν επιθέσεις στον κυβερνοχώρο ως αποτέλεσμα κακών συνηθειών με τους κωδικούς πρόσβασης. Για παράδειγμα, η επαναχρησιμοποίηση του ίδιου κωδικού πρόσβασης σε πολλούς λογαριασμούς. Μπορείτε να χρησιμοποιήσετε τόσο διαχειριστές κωδικών πρόσβασης όσο και φράσεις πρόσβασης για να δημιουργήσετε ισχυρούς κωδικούς πρόσβασης.

Ένας **διαχειριστής κωδικών πρόσβασης** λειτουργεί σαν εικονικό χρηματοκιβώτιο για τους κωδικούς πρόσβασής σας. Μπορείτε να τον χρησιμοποιήσετε για να δημιουργήσετε και να αποθηκεύσετε ισχυρούς, **μοναδικούς** κωδικούς πρόσβασης για κάθε έναν από τους λογαριασμούς σας. Εάν έχετε πολλούς λογαριασμούς, αυτό αφαιρεί το βάρος της απομνημόνευσης μοναδικών κωδικών πρόσβασης. Δεν χρειάζεται να θυμάστε τους κωδικούς πρόσβασης ή τους λογαριασμούς στους οποίους ανήκουν, καθώς όλα καταγράφονται στον διαχειριστή κωδικών πρόσβασης.

Για λογαριασμούς στους οποίους συνδέεστε τακτικά ή που διαφορετικά δεν θέλετε να αποθηκεύσετε σε διαχειριστή κωδικών πρόσβασης, εξετάστε το ενδεχόμενο να χρησιμοποιήσετε μια φράση πρόσβασης ως κωδικό πρόσβασής σας. Οι φράσεις πρόσβασης είναι ένας συνδυασμός τυχαίων λέξεων, για παράδειγμα «crystal onion clay pretzel». Είναι χρήσιμες όταν θέλετε έναν ασφαλή κωδικό πρόσβασης που είναι εύκολο να θυμάστε. Χρησιμοποιήστε έναν τυχαίο συνδυασμό τεσσάρων ή περισσότερων λέξεων και διατηρήστε τον μοναδικό – **μην επαναχρησιμοποιήσετε μια φράση πρόσβασης** σε πολλούς λογαριασμούς. Για περισσότερες πληροφορίες, διαβάστε τις συμβουλές μας σχετικά με τις φράσεις πρόσβασης και τους διαχειριστές κωδικών πρόσβασης, που είναι διαθέσιμες στη διεύθυνση **cyber.gov.au/passphrases**.

✓ **Χρησιμοποιήστε έναν διαχειριστή κωδικών πρόσβασης για να δημιουργήσετε και να αποθηκεύσετε μοναδικούς κωδικούς πρόσβασης για κάθε έναν από τους σημαντικούς λογαριασμούς σας.**

Διαχείριση κοινόχρηστων λογαριασμών

Η κοινή χρήση λογαριασμών μπορεί να θέσει σε κίνδυνο την ασφάλεια και καθιστά δύσκολη την παρακολούθηση κακόβουλης δραστηριότητας.

Σε μια μικρή επιχείρηση, μπορεί να υπάρχουν βάσιμοι λόγοι για τους οποίους το προσωπικό πρέπει να μοιράζεται λογαριασμούς, αλλά θα πρέπει να αποφεύγεται όσο το δυνατόν περισσότερο. Όταν πολλά άτομα χρησιμοποιούν τον ίδιο λογαριασμό, μπορεί να είναι δύσκολο να παρακολουθήσετε τη δραστηριότητα σε έναν συγκεκριμένο υπάλληλο και ακόμη πιο δύσκολο να παρακολουθήσετε τους εγκληματίες του κυβερνοχώρου που εισβάλλουν. Εάν δεν αλλάξετε τον κωδικό πρόσβασης, οι εργαζόμενοι θα μπορούσαν επίσης να συνεχίσουν να έχουν πρόσβαση σε λογαριασμούς ακόμα και μετά την αποχώρησή τους από την επιχείρηση.

✓ **Περιορίστε τη χρήση κοινόχρηστων λογαριασμών και ασφαλίστε οποιονδήποτε χρησιμοποιείται στην επιχείρησή σας.**

Προστατέψτε τις συσκευές και τις πληροφορίες σας

Ενημερώστε το λογισμικό σας

Το να διατηρείτε το λογισμικό σας ενημερωμένο είναι ένας από τους καλύτερους τρόπους για να προστατεύετε την επιχείρησή σας από μια επίθεση στον κυβερνοχώρο.

Οι ενημερώσεις μπορούν να διορθώσουν ελαττώματα ασφαλείας στο λειτουργικό σας σύστημα και σε άλλο λογισμικό, έτσι ώστε να είναι πιο δύσκολο για έναν κυβερνοεγκληματία να εισβάλει. Νέα ελαττώματα ανακαλύπτονται συνεχώς, γι' αυτό μην αγνοείτε τα μηνύματα για ενημέρωση. Η τακτική ενημέρωση του λογισμικού σας θα μειώσει την πιθανότητα να χρησιμοποιήσει ένας κυβερνοεγκληματίας μια γνωστή αδυναμία για να εγκαταστήσει κακόβουλο λογισμικό ή να χακάρει τη συσκευή σας. Εάν χρειάζεστε βοήθεια, το ACSC έχει δημοσιεύσει οδηγίες σχετικά με τις ενημερώσεις.

Εάν η συσκευή ή το λογισμικό σας είναι πολύ παλιό, τότε ενδέχεται να μην είναι διαθέσιμες οι ενημερώσεις. Εάν ο κατασκευαστής έχει σταματήσει να υποστηρίζει το προϊόν με ενημερώσεις, θα πρέπει να εξετάσετε το ενδεχόμενο αναβάθμισης σε νεότερο προϊόν για να παραμείνετε ασφαλείς. Παραδείγματα συστημάτων που δεν λαμβάνουν πλέον σημαντικές ενημερώσεις είναι το **iPhone 7** και το **Microsoft Windows 7**.

Για περισσότερες πληροφορίες, διαβάστε τις οδηγίες μας για ενημερώσεις, που διατίθενται στη διεύθυνση **cyber.gov.au/updates**.

✓ **Ενεργοποιήστε τις αυτόματες ενημερώσεις για τις συσκευές και το λογισμικό σας.**

Χρησιμοποιήστε λογισμικό ασφαλείας

Λογισμικό ασφαλείας, όπως προστασία από ιούς και ransomware, μπορεί να βοηθήσει στην προστασία των συσκευών σας.

Χρησιμοποιήστε λογισμικό ασφαλείας για να εντοπίσετε και να αφαιρέσετε κακόβουλο λογισμικό από τις συσκευές σας. Το λογισμικό προστασίας από ιούς μπορεί να ρυθμιστεί ώστε να σαρώνει τακτικά για ύποπτα αρχεία και προγράμματα. Όταν εντοπιστεί μια απειλή, θα λάβετε μια ειδοποίηση και το ύποπτο αρχείο θα τεθεί σε καραντίνα ή θα αφαιρεθεί.

Πολλές μικρές επιχειρήσεις μπορούν να **χρησιμοποιήσουν την Ασφάλεια των Windows** για να προστατευθούν από ιούς και κακόβουλο λογισμικό. Η Ασφάλεια των Windows είναι ενσωματωμένη σε συσκευές Windows 10 και Windows 11 και περιλαμβάνει δωρεάν προστασία από ιούς και απειλές. Μπορείτε επίσης να τη χρησιμοποιήσετε για να ενεργοποιήσετε τις λειτουργίες προστασίας από ransomware στη συσκευή σας.

Για εναλλακτικά προϊόντα και επιλογές, διαβάστε τις συμβουλές μας για το λογισμικό προστασίας από ιούς, αναζητώντας *antivirus* στο cyber.gov.au.

✓ **Ρυθμίστε το λογισμικό ασφαλείας για να ολοκληρώνετε τακτικές σαρώσεις στις συσκευές σας.**

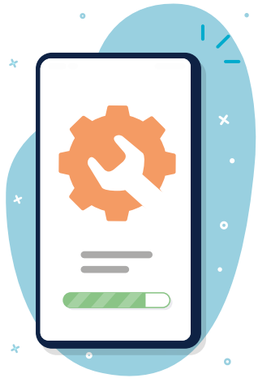
Δημιουργήστε αντίγραφα ασφαλείας των πληροφοριών σας

Τα τακτικά αντίγραφα ασφαλείας μπορούν να σας βοηθήσουν να ανακτήσετε τις πληροφορίες σας εάν χαθούν ή παραβιαστούν.

Η δημιουργία αντιγράφων ασφαλείας σημαντικών πληροφοριών θα πρέπει να είναι μια τακτική ή αυτόματη πρακτική στην επιχείρησή σας. Χωρίς κανονικό αντίγραφο ασφαλείας, θα μπορούσε να είναι αδύνατο να ανακτήσετε τις πληροφορίες σας μετά από μια επίθεση στον κυβερνοχώρο.

Υπάρχουν πολλές μέθοδοι και προϊόντα που θα μπορούσατε να χρησιμοποιήσετε για να δημιουργήσετε αντίγραφα ασφαλείας των πληροφοριών σας. Για λεπτομερείς συμβουλές σχετικά με τη δημιουργία αντιγράφων ασφαλείας της επιχείρησής σας, διαβάστε τις συμβουλές μας για δημιουργία αντιγράφων ασφαλείας, που είναι διαθέσιμες στη διεύθυνση **cyber.gov.au/backups**. Η καλύτερη επιλογή θα διαφέρει για κάθε επιχείρηση, επομένως μιλήστε με έναν επαγγελματία πληροφορικής εάν δεν είστε σίγουροι.

✓ **Δημιουργήστε και εφαρμόστε ένα σχέδιο για να δημιουργείτε τακτικά αντίγραφα ασφαλείας των πληροφοριών σας.**



Ασφαλίστε το δίκτυό σας και τις εξωτερικές υπηρεσίες σας

Προστατέψτε την επιχείρησή σας από επίθεση στον κυβερνοχώρο με την αντιμετώπιση πιθανών τρωτών σημείων του δικτύου σας.

Οι συσκευές και οι υπηρεσίες στο δίκτυό σας μπορούν να αποτελέσουν πρωταρχικό στόχο για εγκληματίες του κυβερνοχώρου. Πολλά από αυτά τα συστήματα μπορεί να είναι πολύπλοκα στην ασφάλεια, γι' αυτό συζητήστε τις παρακάτω συστάσεις με έναν επαγγελματία πληροφορικής.

- **Ασφαλίστε τους διακομιστές σας**: Εάν χρησιμοποιείτε NAS ή άλλο διακομιστή στο σπίτι ή την επιχείρησή σας, φροντίστε ιδιαίτερα να τον ασφαλίσετε. Αυτές οι συσκευές αποτελούν κοινούς στόχους για εγκληματίες του κυβερνοχώρου, επειδή συχνά αποθηκεύουν σημαντικά αρχεία ή εκτελούν σημαντικές λειτουργίες. Απαιτούνται πολλές στρατηγικές μετριασμού για την προστασία αυτών των συσκευών. Για παράδειγμα, είναι σημαντικό να διασφαλίζετε ότι οποιοσδήποτε διακομιστής ή συσκευές NAS ενημερώνονται τακτικά. Οι λογαριασμοί διαχείρισης θα πρέπει να προστατεύονται με ισχυρή φράση πρόσβασης ή έλεγχο ταυτότητας πολλαπλών παραγόντων.
- **Ελαχιστοποίηση του αποτυπώματος που βλέπει προς τα έξω**: Ελέγξτε και ασφαλίστε τυχόν υπηρεσίες που εκτίθενται στο διαδίκτυο στο δίκτυό σας. Αυτό μπορεί να περιλαμβάνει υπηρεσίες Απομακρυσμένης Επιφάνειας εργασίας, Κοινής χρήσης αρχείων, διαδικτυακού ταχυδρομείου Webmail και απομακρυσμένης διαχείρισης.
- **Μετεγκατάσταση σε υπηρεσίες cloud:** Εξετάστε το ενδεχόμενο να χρησιμοποιήσετε διαδικτυακές ή υπηρεσίες cloud που προσφέρουν ενσωματωμένη ασφάλεια, αντί να διαχειρίζεστε τη δική σας. Για παράδειγμα, χρησιμοποιήστε διαδικτυακές υπηρεσίες για πράγματα όπως το ηλεκτρονικό ταχυδρομείο ή τη φιλοξενία ιστοτόπων αντί να εκτελείτε και να ασφαλίζετε μόνοι σας αυτές τις υπηρεσίες.
- **Βελτιώστε την ασφάλεια του δρομολογητή σας:** Ακολουθήστε τις οδηγίες μας σχετικά με τους τρόπους ασφάλειας του δρομολογητή σας, συμπεριλαμβανομένης της ενημέρωσης των προεπιλεγμένων κωδικών πρόσβασης, της ενεργοποίησης του «Guest» Wi-Fi για πελάτες ή επισκέπτες και της χρήσης των ισχυρότερων πρωτοκόλλων κρυπτογράφησης. Αναζητήστε *router* στο **cyber.gov.au** για περισσότερες πληροφορίες.
- **Κατανοήστε την αλυσίδα εφοδιασμού στον κυβερνοχώρο:** Οι σύγχρονες επιχειρήσεις συχνά αναθέτουν πολλαπλές υπηρεσίες σε τρίτους. Για παράδειγμα, χρησιμοποιώντας έναν διαχειριζόμενο πάροχο υπηρεσιών για τη συντήρηση των συστημάτων πληροφορικής του. Ζητήματα ασφάλειας με αυτές τις υπηρεσίες ή παρόχους θα μπορούσαν να έχουν σημαντικό αντίκτυπο στην επιχείρησή σας. Για λεπτομερείς συμβουλές σχετικά με τη διαχείριση κινδύνου της αλυσίδας εφοδιασμού στον κυβερνοχώρο, διαβάστε την Καθοδήγηση για την αλυσίδα εφοδιασμού στον κυβερνοχώρο στο **cyber.gov.au**.

✓ **Μιλήστε με έναν επαγγελματία πληροφορικής σχετικά με τρόπους προστασίας του δικτύου σας.**

Βελτιώστε την ασφάλεια του ιστότοπού σας

Οι ιστότοποι αποτελούν πρωταρχικό στόχο για επιθέσεις στον κυβερνοχώρο.

Προστατέψτε τον ιστότοπό σας από την παραβίαση ακολουθώντας ορισμένα βασικά μέτρα ασφαλείας:

- ασφαλίστε τη σύνδεση στον ιστότοπό σας με έλεγχο ταυτότητας πολλαπλών παραγόντων ή ισχυρό κωδικό πρόσβασης
- ενημερώνετε τακτικά τα συστήματα διαχείρισης περιεχομένου και τις προσθήκες του ιστότοπού σας
- δημιουργήστε αντίγραφα ασφαλείας του ιστότοπού σας τακτικά, ώστε να μπορείτε να τον επαναφέρετε μετά από μια επίθεση στον κυβερνοχώρο.

Το ACSC διαθέτει πρόσθετους πόρους για τους κατόχους ιστότοπων. Αναζητήστε αυτούς τους πόρους στο **cyber.gov.au**:

- Γρήγορες νίκες για τον ιστότοπό σας
- Εφαρμογή πιστοποιητικών, TLS, HTTPS και ευκαιριακών TLS
- Ασφάλεια συστήματος ονομάτων τομέα για κατόχους τομέων
- Προετοιμασία και απόκριση σε επιθέσεις άρνησης υπηρεσίας

✓ **Διαβάστε τους πόρους ACSC για την ασφάλεια του ιστότοπου.**

Επαναφέρετε τις συσκευές σας πριν τις πουλήσετε ή τις απορρίψετε

Άγνωστοι μπορούν να έχουν πρόσβαση στα δεδομένα των παλιών συσκευών σας.

Εάν δεν πετάξετε τις συσκευές σας με ασφάλεια, οι εγκληματίες του κυβερνοχώρου θα μπορούσαν να έχουν πρόσβαση στις πληροφορίες που περιέχονται σε αυτές. Αυτό θα μπορούσε να περιλαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου, αρχεία και άλλα επιχειρηματικά δεδομένα. Αφαιρέστε όλες τις πληροφορίες από τις συσκευές της επιχείρησής σας πριν τις πουλήσετε, τις ανταλλάξετε ή τις πετάξετε. Για παράδειγμα, κάνοντας επαναφορά εργοστασιακών ρυθμίσεων. Αυτό θα βοηθήσει να διαγράψετε τυχόν πληροφορίες και να επαναφέρετε τη συσκευή στις αρχικές της ρυθμίσεις.

Για συμβουλές σχετικά με την επαναφορά των συσκευών σας, διαβάστε τις οδηγίες μας σχετικά με τον τρόπο ασφαλούς απόρριψης της συσκευής σας. Αναζητήστε *dispose* στο **cyber.gov.au**.

✓ **Επαναφέρετε τις εργοστασιακές ρυθμίσεις στις συσκευές της επιχείρησής σας πριν τις πουλήσετε ή τις απορρίψετε.**

Διατηρήστε τις συσκευές σας κλειδωμένες και φυσικά ασφαλείς

Ο περιορισμός της πρόσβασης στις συσκευές της επιχείρησής σας θα μειώσει τις ευκαιρίες για κακόβουλη δραστηριότητα.

Ο περιορισμός της φυσικής πρόσβασης στις συσκευές της επιχείρησής σας είναι ένας απλός τρόπος για να αποτρέψετε την κλοπή δεδομένων ή άλλη κακόβουλη δραστηριότητα. Οι επαγγελματικές συσκευές δεν θα πρέπει να φυλάσσονται εκεί όπου θα μπορούσε να έχει πρόσβαση μη εξουσιοδοτημένο προσωπικό ή μέλη του κοινού.

Χρησιμοποιήστε στοιχεία ελέγχου ασφαλείας για την περαιτέρω προστασία των επαγγελματικών σας συσκευών. Τουλάχιστον, θα πρέπει να κλειδώνονται με φράση πρόσβασης, PIN ή βιομετρικά στοιχεία. Βεβαιωθείτε ότι αυτές οι συσκευές έχουν ρυθμιστεί να κλειδώνουν αυτόματα μετά από μια σύντομη περίοδο αδράνειας.

✓ **Διαμορφώστε τις συσκευές ώστε να κλειδώνουν αυτόματα μετά από σύντομο χρονικό διάστημα αδράνειας.**

Προστατέψτε τα δεδομένα της επιχείρησής σας

Τα δεδομένα που κατέχει η επιχείρησή σας αποτελούν ελκυστικό στόχο για εγκληματίες στον κυβερνοχώρο.

Οι παραβιάσεις δεδομένων αυξάνονται – μην αφήσετε την επιχείρησή σας να πέσει θύμα. Είναι σημαντικό να κατανοήσετε ποια δεδομένα διαθέτει η επιχείρησή σας και σε ποιες τοποθεσίες. Μόλις το καταλάβετε, χρησιμοποιήστε τις συστάσεις σε αυτόν τον οδηγό για να προστατεύσετε τα δεδομένα σας από την πρόσβαση των κυβερνοεγκληματιών. Ορισμένες μικρές επιχειρήσεις ενδέχεται επίσης να έχουν πρόσθετες υποχρεώσεις βάσει της νομοθεσίας.

- **Ενοποιήστε τα δεδομένα της επιχείρησής σας.** Μπορεί να έχετε αποθηκευμένα δεδομένα σε πολλές συσκευές ή υπηρεσίες. Όταν τα δεδομένα είναι αποκεντρωμένα, αυξάνεται ο αριθμός των συστημάτων που πρέπει να διατηρήσετε ασφαλή και να δημιουργήσετε αντίγραφα ασφαλείας. Πολλά συστήματα μπορούν επίσης να δημιουργήσουν περισσότερες ευκαιρίες για επίθεση από έναν κυβερνοεγκληματία. Όπου είναι δυνατόν, αποθηκεύστε τα δεδομένα της επιχείρησής σας σε μια κεντρική τοποθεσία που είναι ασφαλής και δημιουργείται τακτικά αντίγραφα ασφαλείας. Η συγκέντρωση των δεδομένων σας μπορεί να δημιουργήσει μεγαλύτερη παραβίαση εάν τα συστήματά σας παραβιαστούν, επομένως βεβαιωθείτε ότι αυτή η κεντρική τοποθεσία προστατεύεται επαρκώς με ασφαλείς διαμορφώσεις και περιορισμένη πρόσβαση. Μιλήστε με έναν επαγγελματία πληροφορικής ή ασφάλειας στον κυβερνοχώρο για συμβουλές.
- **Γνωρίστε τις υποχρεώσεις σας για την προστασία των δεδομένων.** Ορισμένες μικρές επιχειρήσεις ενδέχεται να έχουν νομικές υποχρεώσεις για τον χειρισμό των προσωπικών πληροφοριών που συλλέγουν. Διαβάστε τον οδηγό για μικρές επιχειρήσεις του Γραφείου του Αυστραλού Επιτρόπου Πληροφοριών (Office of the Australian Information Commissioner) για να μάθετε περισσότερα. Ο οδηγός είναι διαθέσιμος στη διεύθυνση **oaic.gov.au**. Συμβουλευτείτε έναν επαγγελματία νομικό εάν δεν είστε σίγουροι.

✓ **Κατανοήστε τα δεδομένα που κατέχει η επιχείρησή σας και τις ευθύνες σας για την προστασία της.**

Προετοιμάστε το προσωπικό σας

Εκπαιδεύστε τους εργαζομένους

Οι υπάλληλοι με καλές πρακτικές ασφάλειας στον κυβερνοχώρο είναι η πρώτη γραμμή άμυνάς σας ενάντια στις επιθέσεις στον κυβερνοχώρο.

Οι υπάλληλοί σας θα πρέπει να έχουν επίγνωση της ασφάλειας στον κυβερνοχώρο, συμπεριλαμβανομένων των ακόλουθων θεμάτων:

- κοινές απειλές για την ασφάλεια στον κυβερνοχώρο, όπως ο συμβιβασμός των επαγγελματικών email και το ransomware
- προστατευτικά μέτρα, συμπεριλαμβανομένων ισχυρών κωδικών πρόσβασης ή φράσεων πρόσβασης, MFA και ενημερώσεων λογισμικού
- πώς να εντοπίσουν απάτες και επιθέσεις phishing
- πολιτικές για τη συγκεκριμένη επιχείρηση (για παράδειγμα, οι διαδικασίες για την αναφορά ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου ή για την επιβεβαίωση της αυθεντικότητας τιμολογίων πριν από την πληρωμή)
- τι να κάνουν σε περίπτωση έκτακτης ανάγκης.

Ο ιστότοπος ACSC διαθέτει πόρους για τα περισσότερα από αυτά τα θέματα στη διεύθυνση cyber.gov.au/learn. Μπορείτε να εξετάσετε άλλους τρόπους εκπαίδευσης των υπαλλήλων σας, για παράδειγμα με ένα επίσημο μάθημα ή εσωτερική εκπαίδευση. Όπως κι αν αποφασίσετε, να θυμάστε ότι η εκπαίδευση στον κυβερνοχώρο δεν είναι εφάπαξ απαίτηση και θα πρέπει να ανανεώνεται περιοδικά.

✓ **Καθορίστε πώς θα διδάσκεται η ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο στην επιχείρησή σας.**

Κάντε ένα σχέδιο έκτακτης ανάγκης

Ένα σχέδιο έκτακτης ανάγκης θα μπορούσε να μειώσει τον αντίκτυπο μιας κυβερνοεπίθεσης στην επιχείρησή σας.

Όταν απαντάτε σε ένα περιστατικό ασφάλειας στον κυβερνοχώρο, το κάθε λεπτό μετράει. Έχοντας ένα σχέδιο έκτακτης ανάγκης σημαίνει ότι το προσωπικό σας μπορεί να αφιερώσει λιγότερο χρόνο για να καταλάβει τι πρέπει να κάνει και περισσότερο χρόνο για να αναλάβει δράση.

Λάβετε υπόψη τις ακόλουθες ερωτήσεις κατά τη δημιουργία του σχεδίου έκτακτης ανάγκης:

- Ποια είναι η διαδικασία για το προσωπικό σας να αναφέρει πιθανά περιστατικά ασφάλειας του κυβερνοχώρου;
- Με ποιον επικοινωνείτε για βοήθεια; Για παράδειγμα, με επαγγελματίες πληροφορικής και την τράπεζά σας.
- Πώς θα κοινοποιηθεί το περιστατικό στο προσωπικό, τους ενδιαφερόμενους ή τους πελάτες σας;
- Πώς θα διαχειριστείτε την επιχειρηματική δραστηριότητα ως συνήθως, εάν κάποια κρίσιμα συστήματα είναι εκτός σύνδεσης;

Βεβαιωθείτε ότι το προσωπικό σας είναι εξοικειωμένο με το σχέδιο έκτακτης ανάγκης, συμπεριλαμβανομένων τυχόν ρόλων ή ευθυνών που μπορεί να έχει. Διατηρήστε ένα έντυπο αντίγραφο του σχεδίου σε περίπτωση που τα συστήματά σας είναι εκτός σύνδεσης όταν το χρειάζεστε.

✓ **Δημιουργήστε ένα σχέδιο έκτακτης ανάγκης για περιστατικά ασφάλειας στον κυβερνοχώρο.**

Μείνετε ενημερωμένοι

Γίνετε συνεργάτης του ACSC για να λαμβάνετε τις πιο πρόσφατες πληροφορίες από το ACSC.

Μείνετε ενημερωμένοι για τις πιο πρόσφατες απειλές και ευπάθειες στον κυβερνοχώρο με το να γίνετε συνεργάτης του ACSC. Αυτή η υπηρεσία θα σας στέλνει μηνιαία ενημερωτικά δελτία και ειδοποιήσεις όταν εντοπιστεί μια νέα απειλή στον κυβερνοχώρο.

Η ασφάλεια στον κυβερνοχώρο είναι ένας ταχέως εξελισσόμενος τομέας. Οι κυβερνοεγκληματίες εκμεταλλεύονται ενεργά τις ευπάθειες μέσα σε λίγα λεπτά από την ανακάλυψή τους. Η ενημέρωση για το τοπίο της ασφάλειας στον κυβερνοχώρο θα βοηθήσει την επιχείρησή σας να κατανοήσει τις απειλές που είναι πιθανό να αντιμετωπίσει και πώς να προστατευτεί από αυτές.

✓ **Καταχωρίστε την επιχείρησή σας στο Πρόγραμμα Συνεργασίας ACSC.**

Αποποίηση ευθυνών

Το περιεχόμενο του παρόντος οδηγού είναι γενικού χαρακτήρα και δεν θα πρέπει να θεωρηθεί ως νομική συμβουλή ή ως βάση για βοήθεια σε οποιαδήποτε ιδιαίτερη περίσταση ή κατάσταση έκτακτης ανάγκης. Σε κάθε σημαντικό θέμα, θα πρέπει να ζητάτε την κατάλληλη ανεξάρτητη επαγγελματική συμβουλή σχετικά με τις δικές σας περιστάσεις.

Η Κοινοπολιτεία δεν αναλαμβάνει καμία ευθύνη ή υποχρέωση για οποιαδήποτε ζημιά, απώλεια ή δαπάνη που προκύπτει από την επίκληση των πληροφοριών που περιέχονται σε αυτόν τον οδηγό.

Πνευματικά δικαιώματα

© Κοινοπολιτεία της Αυστραλίας 2023

Με εξαίρεση το Εθνόσημο και εκτός εάν αναφέρεται διαφορετικά, όλο το υλικό που παρουσιάζεται στην παρούσα δημοσίευση υπόκειται στην άδεια Creative Commons Attribution 4.0 International (www.creativecommons.org/licenses).

Προς αποφυγή αμφιβολιών, αυτό σημαίνει ότι αυτή η άδεια ισχύει μόνο για το υλικό το οποίο περιέχεται στο παρόν έγγραφο.

Οι λεπτομέρειες των σχετικών προϋποθέσεων της άδειας είναι διαθέσιμες στον ιστότοπο του Creative Commons, όπως και ο πλήρης νομικός κώδικας για την άδεια CC BY 4.0 (www.creativecommons.org/licenses).

Χρήση του Εθνόσημου

Οι όροι υπό τους οποίους μπορεί να χρησιμοποιηθεί το Εθνόσημο αναφέρονται λεπτομερώς στον ιστότοπο του Υπουργείου του Πρωθυπουργού και του Υπουργικού Συμβουλίου (www.pmc.gov.au/government/commonwealth-coat-arms).

Για περισσότερες πληροφορίες ή για να αναφέρετε ένα περιστατικό ασφάλειας στον κυβερνοχώρο, επικοινωνήστε μαζί μας:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Αυτός ο αριθμός είναι διαθέσιμος για χρήση μόνο εντός της Αυστραλίας.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre