ΟΡΓΑΝΙΣΜΟΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Οδηγός κυβερνοασφάλειας για τις ΜΜΕ

12 ΒΗΜΑΤΑ

ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΗΣ ΕΠΙΧΕΙΡΗΣΗΣ ΣΑΣ

Η κρίση της πανδημίας COVID-19 έδειξε πόσο σημαντικό είναι το Διαδίκτυο και οι υπολογιστές εν γένει για τις ΜΜΕ. Για να συνεχίσουν επιτυχώς την επιχειρηματική τους δραστηριότητα κατά τη διάρκεια της πανδημίας, πολλές ΜΜΕ χρειάστηκε να λάβουν μέτρα επιχειρησιακής συνέχειας, όπως η χρήση υπηρεσιών υπολογιστικού νέφους, η βελτίωση των διαδικτυακών υπηρεσιών τους, η αναβάθμιση των διαδικτυακών τους τόπων και η παροχή δυνατότητας στο προσωπικό τους να εργάζεται εξ αποστάσεως.

Το παρόν φυλλάδιο συνιστά για τις ΜΜΕ έναν οδηγό 12 πρακτικών βημάτων υψηλού επιπέδου για το πώς μπορούν καλύτερα να διασφαλίσουν τα συστήματα και τις επιχειρηματικές τους δραστηριότητες. Πρόκειται για μια συνοδευτική δημοσίευση της λεπτομερέστερης έκθεσης του ENISA με τίτλο **«Κυβερνοασφάλεια για τις ΜΜΕ – Προκλήσεις και συστάσεις».**

1 ΑΝΑΠΤΥΞΤΕ ΜΙΑ ΦΙΛΟΣΟΦΙΑ ΚΑΛΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΠΡΟΒΕΙΤΕ ΣΤΗΝ ΑΝΑΘΕΣΗ ΔΙΑΧΕΙΡΙΣΤΙΚΗΣ ΕΥΘΥΝΗΣ

Η καλή κυβερνοασφάλεια αποτελεί κομβικό στοιχείο για την συνεχιζόμενη επιτυχία κάθε ΜΜΕ. Η ευθύνη για την κρίσιμη αυτή λειτουργία πρέπει να ανατίθεται σε κάποιον εντός της επιχείρησης, ο οποίος θα πρέπει να διασφαλίζει, για τους σκοπούς της κυβερνοασφάλειας, τους κατάλληλους πόρους, όπως χρόνος από το προσωπικό, αγορά λογισμικού, υπηρεσιών και υλικού κυβερνοασφάλειας, κατάρτιση του προσωπικού και ανάπτυξη αποτελεσματικών πολιτικών.

ΚΕΡΔΙΣΤΕ ΤΟ ΕΝΔΙΑΦΕΡΟΝ ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ

Ως διοίκηση, κερδίστε το ενδιαφέρον των εργαζομένων μέσω της αποτελεσματικής ενημέρωσής του σε θέματα κυβερνοασφάλειας, με πρωτοβουλίες που υποστηρίζουν ανοιχτά την κυβερνοασφάλεια, κατάλληλες εκπαιδεύσεις των εργαζομένων, καθώς και με τη γνωστοποίηση προς τους εργαζόμενους σαφών και συγκεκριμένων κανόνων που περιγράφονται μέσω των σχετικών πολιτικών κυβερνοασφάλειας.

ΔΗΜΟΣΙΕΥΣΤΕ ΚΑΝΟΝΕΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

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 ΤΠΕ 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.

ΔΙΕΝΕΡΓΕΙΤΕ ΕΛΕΓΧΟΥΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Τακτικοί έλεγχοι πρέπει να διενεργούνται μόνο από όσους διαθέτουν την κατάλληλη γνώση, τις δεξιότητες και την εμπειρία. Οι ελεγκτές θα πρέπει να είναι ανεξάρτητοι, είτε πρόκειται για εξωτερικούς αναδόχους είτε για εσωτερικό προσωπικό της ΜΜΕ, καθώς και ανεξάρτητοι από τις καθημερινές πράξεις της επιχείρησης στον τομέα της πληροφορικής.

ΝΑ ΘΥΜΟΣΑΣΤΕ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ

Δυνάμει του Γενικού Κανονισμού της ΕΕ για την Προστασία Δεδομένων[1], κάθε ΜΜΕ η οποία επεξεργάζεται ή αποθηκεύει προσωπικά δεδομένα που ανήκουν σε πολίτες της ΕΕ ή του ΕΟΧ πρέπει να διασφαλίζει την ύπαρξη κατάλληλων ελέγχων ασφάλειας για την προστασία των εν λόγω δεδομένων. Σε αυτούς περιλαμβάνεται και η διασφάλιση του ότι τρίτα μέρη που εργάζονται για λογαριασμό της ΜΜΕ εφαρμόζουν τα κατάλληλα μέτρα ασφάλειας.

1 Γενικός Κανονισμός για την Προστασία Δεδομένων https://ec.europa.eu/info/law/law-topic/data-protection_el

2

ΠΑΡΕΧΕΤΕ ΚΑΤΑΛΛΗΛΗ ΕΚΠΑΙΔΕΥΣΗ

Παρέχετε στο σύνολο των εργαζομένων τακτικές καταρτίσεις για την ευαισθητοποίησή τους ως προς την κυβερνοασφάλεια ώστε να διασφαλίζετε ότι μπορούν να αναγνωρίζουν και να αντιμετωπίζουν τις διάφορες απειλές κυβερνοασφάλειας. Οι καταρτίσεις αυτές πρέπει να προσαρμόζονται στις ΜΜΕ και να επικεντρώνονται σε καταστάσεις με πραγματικά περιστατικά.

Παρέχετε εξειδικευμένη κατάρτιση για την κυβερνοασφάλεια σε όσους έχουν αναλάβει τη διαχείρισή της στην επιχείρηση ώστε να διασφαλίζετε ότι διαθέτουν τις δεξιότητες και τις ικανότητες που απαιτούνται προκειμένου να κάνουν τη δουλειά τους.

3

ΔΙΑΣΦΑΛΙΖΕΤΕ ΤΗΝ ΑΠΟΤΕΛΕΣΜΑΤΙΚΗ ΔΙΑΧΕΙΡΙΣΗ ΤΡΙΤΩΝ

Να διασφαλίζετε την ενεργό διαχείριση όλων των πωλητών, ιδίως εκείνων που έχουν πρόσβαση σε ευαίσθητα δεδομένα και/ή συστήματα, καθώς και την επίτευξη των συμφωνημένων επιπέδων ασφάλειας. Θα πρέπει να προβλέπετε συμβατικές συμφωνίες για τη ρύθμιση του τρόπου με τον οποίο οι πωλητές πληρούν τις εν λόγω απαιτήσεις ασφάλειας.

4

ΑΝΑΠΤΥΞΤΕ ΕΝΑ ΣΧΕΔΙΟ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΣΥΜΒΑΝΤΩΝ

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.

5

ΑΣΦΑΛΙΣΤΕ ΤΗΝ ΠΡΟΣΒΑΣΗ ΣΤΑ ΣΥΣΤΗΜΑΤΑ

Ενθαρρύνετε όλους να χρησιμοποιούν μια μυστική φράση πρόσβασης, ένα σύνολο τουλάχιστον τριών τυχαίων κοινών λέξεων που συγκροτούν μια φράση, η οποία αφενός να απομνημονεύεται εύκολα και, αφετέρου, να διασφαλίζει την ασφάλεια. Εάν επιλέξετε έναν τυπικό μυστικό κωδικό:

- Φροντίστε να είναι μεγάλος, με μικρούς και κεφαλαίους χαρακτήρες, ενδεχομένως και με αριθμούς και ειδικούς χαρακτήρες.
- Αποφεύγετε προφανείς λέξεις, όπως «μυστικός κωδικός» και ακολουθίες γραμμάτων ή αριθμών, όπως «abc» ή αριθμούς όπως «123».
- Αποφεύγετε να χρησιμοποιείτε προσωπικά στοιχεία που μπορούν να βρεθούν στο Διαδίκτυο.

Και, είτε χρησιμοποιείτε μυστικές φράσεις ή μυστικούς κωδικούς

- Μην χρησιμοποιείτε παντού τους ίδιους.
- Μην τους κοινοποιείτε σε συναδέλφους.
- Φροντίζετε ώστε για την αναγνώριση χρήστη να απαιτούνται πολλαπλοί παράγοντες.
- Χρησιμοποιείτε ειδικό διαχειριστή μυστικών κωδικών.

6

ΑΣΦΑΛΕΙΣ ΣΥΣΚΕΥΕΣ

Η διατήρηση της ασφάλειας των συσκευών που προορίζονται για χρήση από το προσωπικό, είτε πρόκειται για τους επιτραπέζιους υπολογιστές τους είτε για φορητούς υπολογιστές, ταμπλέτες ή έξυπνα τηλέφωνα, αποτελεί βασικό βήμα ενός προγράμματος κυβερνοασφάλειας.

ΔΙΑΤΗΡΕΙΤΕ ΤΟ ΛΟΓΙΣΜΙΚΟ ΣΑΣ ΕΠΙΔΙΟΡΘΩΜΕΝΟ ΚΑΙ ΕΝΗΜΕΡΩΜΕΝΟ

Για καλύτερα αποτελέσματα, χρησιμοποιήστε μια κεντρική πλατφόρμα για τη διαχείριση των επιδιορθώσεων (patching). Συνιστάται ιδιαίτερα για τις ΜΜΕ:

- να ενημερώνουν τακτικά το λογισμικό τους.
- να ενεργοποιούν τις αυτόματες ενημερώσεις, όποτε αυτό είναι εφικτό.
- να εντοπίζουν λογισμικό και υλικό που απαιτεί χειροκίνητη ενημέρωση.
- να λαμβάνουν υπόψη κινητές συσκευές και συσκευές του Διαδικτύου των Πραγμάτων.

ANTI-VIRUS

Μια κεντρικά ελεγχόμενη λύση anti-virus πρέπει να εφαρμόζεται σε όλους τους τύπους συσκευών και να διατηρείται επικαιροποιημένη ώστε να διασφαλίζεται σταθερά η αποτελεσματικότητά της. Επίσης, μην εγκαθιστάτε πειρατικό λογισμικό διότι ενδέχεται να περιέχει κακόβουλο λογισμικό.

ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ ΕΡΓΑΛΕΙΑ ΠΡΟΣΤΑΣΙΑΣ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ ΚΑΙ ΔΙΑΔΙΚΤΥΟΥ

Χρησιμοποιήστε λύσεις για να αποκλείσετε τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου, τα ηλεκτρονικά μηνύματα που περιέχουν συνδέσμους προς κακόβουλες ιστοσελίδες, τα μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν κακόβουλα συνημμένα, όπως ιούς, και τα ηλεκτρονικά μηνύματα ηλεκτρονικού «ψαρέματος».

ΚΡΥΠΤΟΓΡΑΦΗΣΗ

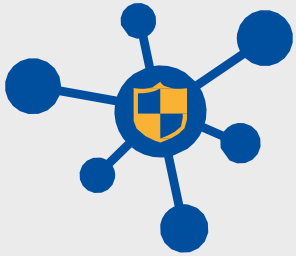
Προστατεύετε τα δεδομένα μέσω κρυπτογράφησης. Οι ΜΜΕ πρέπει να διασφαλίζουν την κρυπτογράφηση των δεδομένων που αποθηκεύονται σε κινητές συσκευές, όπως φορητοί υπολογιστές, έξυπνα τηλέφωνα και ταμπλέτες. Για τα δεδομένα που μεταφέρονται μέσω δημόσιων δικτύων, όπως τα ασύρματα δίκτυα ξενοδοχείων ή αεροδρομίων, πρέπει να διασφαλίζεται ότι τα δεδομένα κρυπτογραφούνται, είτε μέσω της χρήσης εικονικού ιδιωτικού δικτύου (VPN) είτε μέσω της πρόσβασης σε διαδικτυακούς τόπους βάσει ασφαλών συνδέσεων με τη χρήση του πρωτοκόλλου SSL/TLS. Διασφαλίζετε ότι και οι δικοί σας διαδικτυακοί τόποι χρησιμοποιούν την κατάλληλη τεχνολογία κρυπτογράφησης για την προστασία των δεδομένων των πελατών σας καθώς αυτά μεταφέρονται μέσω του Διαδικτύου.

ΕΦΑΡΜΟΣΤΕ ΣΥΣΤΗΜΑ ΔΙΑΧΕΙΡΙΣΗΣ ΤΩΝ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ

Όταν παρέχουν στο προσωπικό τους τη διευκόλυνση της εξ αποστάσεως εργασίας, πολλές ΜΜΕ επιτρέπουν στους εργαζομένους να χρησιμοποιούν τους δικούς τους φορητούς υπολογιστές, ταμπλέτες ή/και έξυπνα τηλέφωνα. Αυτό εγείρει διάφορους προβληματισμούς ως προς την ασφάλεια ευαίσθητων επιχειρηματικών δεδομένων που βρίσκονται αποθηκευμένα σε αυτές τις συσκευές. Ένας τρόπος διαχείρισης αυτού του κινδύνου είναι να χρησιμοποιείται μια λύση διαχείρισης κινητών συσκευών (MDM), η οποία επιτρέπει στις ΜΜΕ:

- να ελέγχουν ποιες συσκευές μπορούν να έχουν πρόσβαση στα συστήματα και στις υπηρεσίες τους.
- να διασφαλίζουν ότι η συσκευή έχει εγκατεστημένο ενημερωμένο λογισμικό anti-virus.
- να προσδιορίζουν εάν η συσκευή είναι κρυπτογραφημένη.
- να επιβεβαιώνουν εάν η συσκευή έχει εγκατεστημένες τις πλέον πρόσφατες επιδιορθώσεις λογισμικού.
- να επιβάλλουν τη προστασία της συσκευής μέσω της χρήσης κωδικού προσωπικού αριθμού αναγνώρισης ή/και μυστικού κωδικού.
- να διαγράφουν εξ αποστάσεως τυχόν δεδομένα της ΜΜΕ από τη συσκευή, εφόσον ο κάτοχός της δηλώσει απώλεια ή κλοπή, ή εφόσον η απασχόληση του κατόχου στην εκάστοτε ΜΜΕ πρόκειται να λήξει.

7 ΑΣΦΑΛΙΣΤΕ ΤΟ ΔΙΚΤΥΟ ΣΑΣ



ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ ΤΕΙΧΗ ΠΡΟΣΤΑΣΙΑΣ

Τα τείχη προστασίας διαχειρίζονται την κυκλοφορία των δεδομένων στην είσοδο και έξοδο ενός δικτύου και αποτελούν κρίσιμο εργαλείο για την προστασία των συστημάτων ΜΜΕ. Τα τείχη προστασίας πρέπει να εφαρμόζονται για την προστασία όλων των κρίσιμων συστημάτων, ιδίως για την προστασία των δικτύων των ΜΜΕ από το Διαδίκτυο.

ΕΠΑΝΕΞΕΤΑΖΕΤΕ ΤΙΣ ΛΥΣΕΙΣ ΕΞ ΑΠΟΣΤΑΣΕΩΣ ΠΡΟΣΒΑΣΗΣ

Οι ΜΜΕ θα πρέπει τακτικά να επανεξετάζουν τυχόν εργαλεία εξ αποστάσεως πρόσβασης ώστε να διασφαλίζουν ότι είναι ασφαλή. Ειδικότερα, θα πρέπει:

- να διασφαλίζουν ότι το σύνολο του λογισμικού για την εξ αποστάσεως πρόσβαση είναι δεόντως επιδιορθωμένο και ενημερωμένο.
- να περιορίζουν την εξ αποστάσεως πρόσβαση από ύποπτες γεωγραφικές τοποθεσίες ή από ορισμένες διευθύνσεις IP.
- να περιορίζουν την εξ αποστάσεως πρόσβαση του προσωπικού μόνο σε συστήματα και υπολογιστές που χρειάζονται για την εργασία τους.
- να επιβάλλουν τη χρήση ισχυρών μυστικών κωδικών για πρόσβαση εξ αποστάσεως και, όπου αυτό είναι εφικτό, να επιτρέπουν την αναγνώριση χρήστη μέσω πολλών παραγόντων.
- να διασφαλίζουν ότι οι λειτουργίες παρακολούθησης και παραγωγής προειδοποιήσεων είναι ενεργοποιημένες, ώστε να ενημερώνουν σχετικά με υποψίες επίθεσης ή ασυνήθιστη ύποπτη δραστηριότητα.

8 ΒΕΛΤΙΩΣΤΕ ΤΗ ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

Όπου φυλάσσονται σημαντικές πληροφορίες πρέπει να εφαρμόζονται κατάλληλοι φυσικοί έλεγχοι. Ένας εταιρικός φορητός υπολογιστής ή έξυπνο τηλέφωνο, για παράδειγμα, δεν πρέπει να αφήνονται χωρίς φύλαξη στο πίσω κάθισμα του αυτοκινήτου. Κάθε φορά που ένας χρήστης απομακρύνεται από τον υπολογιστή του, πρέπει να τον κλειδώνει. Διαφορετικά, φροντίζετε να ενεργοποιείτε τη λειτουργία αυτόματου κλειδώματος σε οποιαδήποτε συσκευή χρησιμοποιείτε για εταιρικούς σκοπούς. Τα ευαίσθητα εκτυπωμένα έγγραφα δεν πρέπει να αφήνονται χωρίς φύλαξη και, όταν δεν χρησιμοποιούνται, θα πρέπει να αποθηκεύονται με ασφαλή τρόπο.

9 ΕΞΑΣΦΑΛΙΣΤΕ ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ

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. Όσον αφορά τα αντίγραφα ασφαλείας, πρέπει να εφαρμόζονται οι ακόλουθοι κανόνες:

- τα αντίγραφα είναι τακτικά και παράγονται κάθε φορά που αυτό είναι εφικτό,
- τα αντίγραφα τηρούνται χωριστά από το περιβάλλον παραγωγής της ΜΜΕ,
- τα αντίγραφα είναι κρυπτογραφημένα, ειδικά εάν πρόκειται να μεταφερθούν μεταξύ τοποθεσιών,
- ελέγχεται η ικανότητα τακτικής ανάκτησης δεδομένων από τα αντίγραφα ασφαλείας. Ιδανικά, πρέπει να διενεργείται τακτικά δοκιμή πλήρους ανάκτησης, από την έναρξη μέχρι την ολοκλήρωσή της.

10

ΣΥΝΕΡΓΑΣΤΕΙΤΕ ΜΕ ΤΟ ΝΕΦΟΣ

Ενώ προσφέρουν πολλά πλεονεκτήματα, οι λύσεις που βασίζονται στο υπολογιστικό νέφος παρουσιάζουν κάποιους ιδιαίτερους κινδύνους, τους οποίους οι ΜΜΕ θα πρέπει να εξετάζουν προτού συνεργαστούν με πάροχο υπηρεσιών υπολογιστικού νέφους. Ο ENISA έχει δημοσιεύσει έναν «Οδηγό ασφάλειας υπολογιστικού νέφους για τις ΜΜΕ» [2], στον οποίο πρέπει να ανατρέχουν οι ΜΜΕ όταν μεταφέρουν δεδομένα τους στο νέφος.

Κατά την επιλογή παρόχου υπηρεσιών υπολογιστικού νέφους, οι ΜΜΕ πρέπει να διασφαλίζουν ότι αυτός δεν παραβιάζει τυχόν νόμους ή κανονισμούς μέσω της αποθήκευσης δεδομένων, ιδίως δεδομένων προσωπικού χαρακτήρα, εκτός ΕΕ/ΕΟΧ. Παραδείγματος χάριν, ο ΓΚΠΔ της ΕΕ προβλέπει ότι τα δεδομένα προσωπικού χαρακτήρα ατόμων που διαμένουν εντός ΕΕ/ΕΟΧ δεν αποθηκεύονται ούτε και διαβιβάζονται εκτός ΕΕ/ΕΟΧ παρά μόνο υπό πολύ ειδικές προϋποθέσεις.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 ΑΣΦΑΛΕΙΣ ΔΙΑΔΙΚΤΥΑΚΟΙ ΤΟΠΟΙ

Είναι εξαιρετικά σημαντικό οι ΜΜΕ να διασφαλίζουν ότι οι διαδικτυακοί τους τόποι παραμετροποιούνται και διατηρούνται ασφαλείς, καθώς και ότι όλα τα δεδομένα προσωπικού χαρακτήρα ή οικονομικά στοιχεία, όπως στοιχεία πιστωτικών καρτών, προστατεύονται δεόντως. Αυτό συνεπάγεται τη διενέργεια τακτικών δοκιμών ασφαλείας των διαδικτυακών τους τόπων ώστε να διαπιστώνονται τυχόν αδυναμίες ως προς την ασφάλεια, καθώς και τη διενέργεια τακτικών αξιολογήσεων ώστε να διασφαλίζεται ότι οι διαδικτυακοί τόποι διατηρούνται και επικαιροποιούνται σωστά.

12 ΖΗΤΑΤΕ ΚΑΙ ΑΝΤΑΛΛΑΣΣΕΤΕ ΠΛΗΡΟΦΟΡΙΕΣ

Ένα αποτελεσματικό εργαλείο στον αγώνα κατά του κυβερνοεγκλήματος είναι η ανταλλαγή πληροφοριών. Η ανταλλαγή πληροφοριών όσον αφορά το κυβερνοέγκλημα είναι ιδιαίτερα σημαντική για τις ΜΜΕ προκειμένου αυτές να κατανοούν καλύτερα τους κινδύνους με τους οποίους βρίσκονται αντιμέτωπες. Επιχειρήσεις που μαθαίνουν από άλλες επιχειρήσεις σχετικά με τις προκλήσεις της κυβερνοασφάλειας και τους τρόπους με τους οποίους αυτές αντιμετωπίστηκαν έχουν περισσότερες πιθανότητες να λάβουν μέτρα για την ασφάλιση των συστημάτων τους απ' ό,τι εάν μάθαιναν για τέτοια περιστατικά από αναφορές του κλάδου τους ή από έρευνες με θέμα την κυβερνοασφάλεια.

ΟΡΓΑΝΙΣΜΟΣ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

ΠΛΗΡΟΦΟΡΙΕΣ ΓΙΑ ΤΟΝ ENISA

Ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια, ENISA, είναι ο οργανισμός της Ένωσης που αποσκοπεί να διασφαλίσει υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ευρώπη. Ο Ευρωπαϊκός Οργανισμός για την Κυβερνοασφάλεια, που ιδρύθηκε το 2004 και ενισχύθηκε από την Πράξη της ΕΕ για την ασφάλεια στον κυβερνοχώρο, συμβάλλει στη χάραξη της πολιτικής της ΕΕ στον τομέα του κυβερνοχώρου, ενισχύει την αξιοπιστία των προϊόντων, υπηρεσιών και διαδικασιών ΤΠΕ με συστήματα πιστοποίησης της κυβερνοασφάλειας, συνεργάζεται με κράτη μέλη και φορείς της ΕΕ και βοηθά την Ευρώπη να προετοιμαστεί για τις μελλοντικές προκλήσεις στον κυβερνοχώρο. Μέσω της ανταλλαγής γνώσεων, της ανάπτυξης ικανοτήτων και της αύξησης της εγρήγορσης, ο Οργανισμός συνεργάζεται με τους βασικούς ενδιαφερόμενους φορείς για την ενίσχυση της εμπιστοσύνης στη συνδεδεμένη οικονομία, την υποστήριξη της ανθεκτικότητας των υποδομών της Ένωσης και, τελικά, τη διατήρηση της ψηφιακής ασφάλειας για την κοινωνία και τους πολίτες της Ευρώπης. Για περισσότερες πληροφορίες επισκεφθείτε τη διεύθυνση www.enisa.europa.eu.

ENISA

Οργανισμός της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

Γραφείο Αθηνών
Εθνικής Αντιστάσεως 72 και
Αγαμέμνονος 14
Χαλάνδρι, 15231, Αττική,
Ελλάδα

Γραφείο Ηρακλείου
Νικολάου Πλαστήρα 95
700 13 Βασιλικά Βουτών
Ηράκλειο, Ελλάδα

enisa.europa.eu