ΚΥΠΡΙΑΚΟ
ΕΜΠΟΡΙΚΟ ΚΑΙ
ΒΙΟΜΗΧΑΝΙΚΟ
ΕΠΙΜΕΛΗΤΗΡΙΟ

26/05/22

Προς: Όλους τους ενδιαφερόμενους

Απο: Τμήμα Υπηρεσιών, Εμπορίου & Ψηφιοποίησης

**Θέμα: Οδηγός Κυβερνοασφάλειας για τις μικρομεσαίες επιχειρήσεις**

Κύριε/Κυρία,

Επιθυμούμε να σας ενημερώσουμε ότι ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA) έχει εκδώσει Οδηγό Κυβερνοασφάλειας για τις μικρομεσαίες επιχειρήσεις.

Ο Οδηγός περιλαμβάνει 12 πρακτικά βήματα μέσω των οποίων οι επιχειρήσεις μπορούν να προστατέψουν τα δίκτυα και τα συστήματα πληροφοριών τους.

Καθώς τα τελευταία χρόνια παρατηρείται ραγδαία ανάπτυξη των ψηφιακών τεχνολογιών και ενσωμάτωσή τους στις καθημερινές λειτουργίες των επιχειρήσεων, η ανάγκη για ανάληψη προληπτικών μέτρων για αξιολόγηση, αντιμετώπιση και διαχείριση των κινδύνων που διαρκώς εμφανίζονται, κρίνεται επιβεβλημένη.

Σας αποστέλλεται πιο κάτω η Ελληνική και Αγγλική έκδοση για δική σας μελέτη.

Με εκτίμηση,

Πόλυς Περατικός
Ανώτερος Λειτουργός

Λεωφ. Γρίβα Διγενή 38 & Δεληγιώργη 3, 1066, Τ.Θ 21455, 1509 Λευκωσία, Κύπρος
**T:** +357 22889800 **F:** +357 22669048 **E:** chamber@ccci.org.cy **W:** www.ccci.org.cy

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

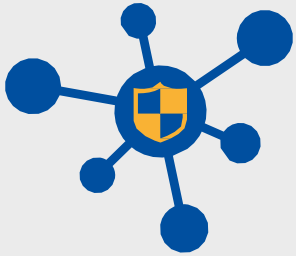
Προστατεύετε τα δεδομένα μέσω κρυπτογράφησης. Οι ΜΜΕ πρέπει να διασφαλίζουν την κρυπτογράφηση των δεδομένων που αποθηκεύονται σε κινητές συσκευές, όπως φορητοί υπολογιστές, έξυπνα τηλέφωνα και ταμπλέτες. Για τα δεδομένα που μεταφέρονται μέσω δημόσιων δικτύων, όπως τα ασύρματα δίκτυα ξενοδοχείων ή αεροδρομίων, 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

enisa

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Cybersecurity guide for SMEs

# 12 STEPS TO SECURING YOUR BUSINESS

The COVID-19 crisis showed how important the Internet and computers in general are for SMEs. In order to thrive in business during the pandemic many SMEs had to take business continuity measures, such as adopting to cloud services, improving their internet services, upgrading their websites and enabling staff to work remotely.

This leaflet provides SMEs with practical 12 high level steps on how to better secure their systems and their business. It is a companion publication to the more detailed ENISA report **"Cybersecurity for SMES – Challenges and Recommendations"**.

# 1 DEVELOP GOOD CYBERSECURITY CULTURE

## ASSIGN MANAGEMENT RESPONSIBILITY

Good cybersecurity is a key element in the ongoing success of any SME. Responsibility for this critical function should be assigned to someone within the organization who should ensure appropriate resources such as time from personnel, the purchasing of cybersecurity software, services and hardware, training for staff, and the development of effective policies are given to cybersecurity.

## GAIN EMPLOYEE BUY-IN

Gain employee buy-in through effective communication on cybersecurity from management, by management openly supporting cybersecurity initiatives, appropriate trainings delivered to employees, and providing employees with clear and specific rules outlined in cybersecurity policies.

## PUBLISH CYBERSECURITY POLICIES

Clear and specific rules should be outlined in cybersecurity policies for employees on how they are expected to behave when using the company's ICT environment, equipment and services. These policies should also highlight the consequences an employee could face should they not adhere to the policies. The policies need to be regularly reviewed and updated.

## CONDUCT CYBERSECURITY AUDITS

Regular audits should be carried out by those with the appropriate knowledge, skills and experience. Auditors should be independent, be it an outside contractor or internal to the SME and independent of daily IT operations.

## REMEMBER DATA PROTECTION

Under the EU General Data Protection Regulation[1] any SMEs that process or store personal data belonging to EU/EEA residents need to ensure that appropriate security controls are in place to protect that data. This includes ensuring that any third parties working on behalf of the SME have appropriate security measures in place.

1 General Data Protection Regulation https://ec.europa.eu/info/law/law-topic/data-protection_en

2

# PROVIDE APPROPRIATE TRAINING

Provide regular cybersecurity awareness trainings for all employees to ensure they can recognize and deal with the various cybersecurity threats. These trainings should be tailored for SME's and focus on real-life situations.

Provide specialized cybersecurity training for those responsible for managing cybersecurity within the business to ensure they will have the skills and competencies required to do their job.

3

# ENSURE EFFECTIVE THIRD PARTY MANAGEMENT

Ensure that all vendors, particularly those with access to sensitive data and/or systems, are actively managed and meet agreed levels of security. Contractual agreements should be in place to regulate how vendors meet those security requirements.

# 4

# DEVELOP AN INCIDENT RESPONSE PLAN

Develop a formal incident response plan, which contains clear guidelines, roles and responsibilities documented to ensure that all security incidents are responded to in a timely, professional and appropriate manner. To respond quickly to security threats, investigate tools that could monitor and create alerts when suspicious activity or security breaches are occurring.

# 5 SECURE ACCESS TO SYSTEMS

Encourage everyone to use a passphrase, a collection of at least three random common words combined into a phrase that provide a very good combination of memorability and security. If you opt for a typical password:

- Make it long, with lower and upper case characters, possibly also numbers and special characters.
- Avoid obvious, such as “password”, sequences of letters or numbers like “abc”, numbers like “123”.
- Avoid using personal info that can be found online.

And whether you use passphrases or passwords

- Do not reuse them elsewhere.
- Do not share them with colleagues.
- Enable Multi-Factor Authentication.
- Use a dedicated password manager.


# 6 SECURE DEVICES

Keeping the devices staff use, be their desktop PCs, laptops, tablets, or smartphones, secure is a key step in a cybersecurity program.

## KEEP SOFTWARE PATCHED AND UP TO DATE

Ideally using a centralized platform to manage patching. It is highly recommended for SMEs to:

- Regularly update all of their software.
- Turn on automatic updates whenever possible.
- Identify software and hardware that requires manual updates.
- Take into account mobile and IoT devices.

## ANTI-VIRUS

A centrally managed anti-virus solution should be implemented on all types of devices and kept up-to-date in order to ensure its continuous effectiveness. Also, do not install pirated software as it may contain malware.

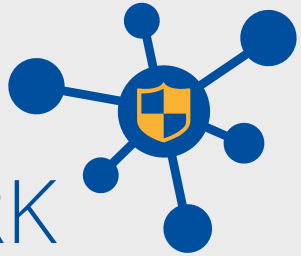
## EMPLOY EMAIL AND WEB PROTECTION TOOLS

Employ solutions to block spam emails, email-containing links to malicious websites, emails containing malicious attachments such as viruses, and phishing emails.

## ENCRYPTION

Protect data by encrypting it. SMEs should ensure the data stored on mobile devices such as laptops, smartphones, and tables are encrypted. For data transferred over public networks, such as hotel or airport WiFi networks, ensure that data is encrypted, either by employing a Virtual Private Network (VPN) or accessing websites over secure connections using SSL/TLS protocol. Ensure their own websites are employing suitable encryption technology to protect client data as it travels over the Internet.

# 7 SECURE YOUR NETWORK



## IMPLEMENT MOBILE DEVICE MANAGEMENT

When facilitating staff to work remotely many SMEs allow staff to use their own laptops, tablet and/or smartphones. This introduces several security concerns about sensitive business data stored on those devices. One way to manage this risk is to employ a Mobile Device Management (MDM) solution, allowing SMEs to:

- Control what devices are allowed to access its systems and services.
- Ensure the device has up to date anti-virus software installed.
- Determine if the device is encrypted.
- Confirm if the device has up to date software patches installed.
- Enforce the device is protected by a PIN and/or a password.
- Remotely wipe any SME data from the device should the device owner report it lost or stolen, or if the device owner's employment was to end with the SME.

## EMPLOY FIREWALLS

Firewalls manage the traffic that enters and leaves a network and are a critical tool in protecting SMEs systems. Firewalls should be deployed to protect all critical systems, in particular a firewall should be employed to protect the SME's network from the Internet.

## REVIEW REMOTE ACCESS SOLUTIONS

SMEs should regularly review any remote access tools to ensure they are secure, particularly:

- Ensure all remote access software is patched and up date.
- Restrict remote access from suspicious geographical locations or certain IP addresses.
- Restrict staff remote access only to the systems and computers they need for their work.
- Enforce strong passwords for remote access and where possible enable multi-factor authentication.
- Ensure monitoring and alerting is enabled to warn of suspected attacks or unusual suspicious activity.

# 8 IMPROVE PHYSICAL SECURITY

Appropriate physical controls should be employed wherever important information resides. A company laptop or a smartphone, for instance, should not be left unattended in the back seat of a car. Anytime a user walks away from their computer they should lock it. Otherwise, enable auto-lock function on any device used for business purposes. Sensitive printed documents should also not be left unattended and when not in use, securely stored away.

# 9 SECURE BACKUPS

To enable the recovery of key formation, backups should be maintained as they are an effective way to recover from disasters such as a ransomware attack. The following backup rules should apply:

- backup is regular and automated whenever possible,
- backup is held separately from the SME's production environment,
- backups are encrypted, especially if they are going to be moved between locations,
- the ability to regularly restore data from the backups is tested. Ideally, a regular test of a full restore from start to finish should be done.

# 10

# ENGAGE WITH THE CLOUD

While offering many advantages, cloud based solutions do present some unique risks, which SMEs should consider before engaging with a cloud provider. ENISA have published a "Cloud Security Guide for SMEs"[2] which SMEs should refer to when migrating to the cloud.

When selecting a cloud provider, SME should ensure it does not breach any laws or regulations by storing data, especially personal data, outside of the EU/EEA. For example, the EU GDPR requires that personal data of residents within the EU/EEA is not stored or transmitted outside of the EU/EEA unless under very specific conditions.

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


# 11 SECURE ONLINE SITES

It is essential that SMEs ensure that their online websites are configured and maintained in a secure manner and that any personal data or financial details, such as credit card data, is appropriately protected. This will entail running regular security tests against the websites to identify any potential security weaknesses and conducting regular reviews to ensure the site is maintained and updated properly.

# 12 SEEK AND SHARE INFORMATION

An effective tool in the fight against cybercrime is the sharing of information. The sharing of information in relation to cybercrime is key to SMEs to better understand the risks they face. Firms that hear about cybersecurity challenges, and how those challenges were overcome, from their peers will more likely take steps to secure their systems than if they were to hear similar details from industry reports or from cybersecurity surveys.

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

**ABOUT ENISA**

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. For more information, visit www.enisa.europa.eu.

**ENISA**
European Union Agency for Cybersecurity

**Athens Office**
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki, Greece

**Heraklion Office**
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Greece

enisa.europa.eu