Digital Skills & Jobs Platform

Μικρές Επιχειρήσεις Μεγάλες Άμυνες

Ο ΟΔΗΓΟΣ ΣΑΣ ΠΡΟΣ ΜΙΑ ΚΥΒΕΡΝΟ-ΑΝΘΕΚΤΙΚΟΤΗΤΑ

ΕΓΧΕΙΡΙΔΙΟ ΓΙΑ ΜΙΚΡΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

ΔΗΜΙΟΥΡΓΗΘΗΚΕ ΑΠΟ ΤΗΝ SQUAD 2025

Συμμετοχή

Gustavo Frega

Ο Gustavo Frega είναι Διευθυντής Ακαδημαϊκής Στρατηγικής και Επιχειρηματικών Συνεργασιών για την περιοχή EMEA στην ISACA.

Καταξιωμένος μηχανικός υπολογιστών, πέρασε πάνω από δύο δεκαετίες συνδέοντας βιομηχανίες, ιδέες και ανθρώπους στους τομείς της κυβερνοασφάλειας, της πληροφορικής και των τηλεπικοινωνιών.
Έχοντας συνεργαστεί με εταιρείες όπως η Apple, η Orange και η Vodafone, τώρα επικεντρώνεται στη δημιουργία συνεργασιών με ακαδημαϊκά ιδρύματα σε όλη την περιοχή EMEA, συμβάλλοντας στη διαμόρφωση των δεξιοτήτων και των ευκαιριών της επόμενης γενιάς ψηφιακών ηγετών.
Δημιούργησε μοντέλα B2B υψηλού αντίκτυπου, επιτυγχάνοντας σταθερά μετρήσιμα αποτελέσματα και προωθώντας παράλληλα τη βιώσιμη ανάπτυξη και τις μακροχρόνιες συνεργασίες.

Manuel Avramescu

Ο M. Avramescu είναι πιστοποιημένος επαγγελματίας στον τομέα της κυβερνοασφάλειας (CC) από το ISC2 και διευθυντής πολιτικής της ΕΕ στο ISC2.

Διαθέτει εκτεταμένη εμπειρία στον τομέα της νομοθεσίας της ΕΕ για την κυβερνοασφάλεια και της πολιτικής για τις ψηφιακές δεξιότητες, με περισσότερα από 20 χρόνια εμπειρίας σε ευρωπαϊκές δημόσιες υποθέσεις, δημόσια διοίκηση και συμβουλευτικούς ρόλους για την προώθηση της καινοτομίας και της συνεργασίας των ενδιαφερόμενων μερών.

Roberto Garrone

Ο Roberto Garrone είναι ερευνητής στον τομέα της τεχνητής νοημοσύνης και της υπολογιστικής μοντελοποίησης και ανεξάρτητος σύμβουλος πληροφορικής που υποστηρίζει μικρομεσαίες και μικρές επιχειρήσεις σε θέματα ψηφιοποίησης, αυτοματοποίησης και ετοιμότητας στον τομέα της κυβερνοασφάλειας.

Meagan Tudge

Ανώτερο διευθυντικό στέλεχος (EMEA) στο πρόγραμμα «Securing the Human» του SANS Institute), μία από τις κορυφαίες εταιρείες εκπαίδευσης στον τομέα της κυβερνοασφάλειας.

Υποστηρίζει την αποστολή της ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο από μια απλή διαδικασία συμμόρφωσης σε μια συνήθεια με επίκεντρο τον άνθρωπο. Πιστεύει ότι η ασφάλεια αφορά τόσο τα τείχη προστασίας και την τεχνολογία, όσο και τη διαμόρφωση συμπεριφορών, την ευαισθητοποίηση και την ενδυνάμωση των ανθρώπων ώστε να κάνουν καθημερινά σοφές ψηφιακές επιλογές.

Tony O'Keefe

Διευθυντής για την περιοχή EMEA (SANS Institute), υπεύθυνος για την υποστήριξη των πελατών του SANS σε ολόκληρη την ηπειρωτική Ευρώπη.

Αυτό περιλαμβάνει τη συνεργασία του με κυβερνήσεις, στρατιωτικές υπηρεσίες, το NATO και την ΕΕ για την υποστήριξη της ανάπτυξης δεξιοτήτων στον τομέα της ασφάλειας των πληροφοριών.
Με περισσότερα από 15 χρόνια στο SANS Institute, ήταν υπεύθυνος για ορισμένα από τα μεγαλύτερα προγράμματά του SANS στην ΕΕ, όπως η ανάπτυξη Ακαδημιών Κυβερνοασφάλειας.
Έχει συνεργαστεί εκτενώς με την ΕΕ σε πρωτοβουλίες υψηλού επιπέδου για την υποστήριξη της ανάπτυξης δεξιοτήτων στον κυβερνοχώρο, καθώς και με την ENISA για την ανάπτυξη και την εφαρμογή του νέου Ευρωπαϊκού Πλαισίου Δεξιοτήτων στον Κυβερνοχώρο (ECSF).
Έχει επίσης εργαστεί στη Μελέτη για το Παγκόσμιο Εργατικό Δυναμικό στον Κυβερνοχώρο του Ινστιτούτου SANS.

Πριν ενταχθεί στο SANS Institute, εργάστηκε για 15 χρόνια σε κυβερνητικούς θώκους, με πάνω από 10 στις Ηνωμένες Πολιτείες σε εταιρείες τεχνολογίας, όπως η Apple, η Google και η Amazon.

Κατέχει επίσης την πιστοποίηση GSTRT GIAC.

Δράση Σήμερα, Ασφάλεια Αύριο

Η κυβερνοασφάλεια αποτελεί πλέον μέρος της ορθής διαχείρισης των επιχειρήσεων — δεν είναι απλά μια τεχνική λεπτομέρεια. Κάθε ενέργεια έχει σημασία: η ενημέρωση των συστημάτων, η επαλήθευση των μηνυμάτων, η εκπαίδευση του προσωπικού και η προστασία των δεδομένων δημιουργούν πραγματική ανθεκτικότητα. Εφαρμόζοντας ακόμη και μερικά από τα βήματα αυτού του εγχειριδίου, οι πολύ μικρές και μικρές επιχειρήσεις μπορούν να μειώσουν τους κινδύνους, να ενισχύσουν την εμπιστοσύνη των πελατών και να αποκτήσουν ένα διαρκές ανταγωνιστικό πλεονέκτημα: **ξεκινήστε σήμερα, ενεργήστε με συνέπεια και κάντε την ασφάλεια μια κοινή συνήθεια σε όλη την ομάδα σας** — γιατί όταν μια μικρή επιχείρηση γίνεται ισχυρότερη, ολόκληρη η κοινότητα γίνεται ασφαλέστερη.

Σχετικά με το Εγχειρίδιο

Στη σημερινή ψηφιακή οικονομία, ακόμη και οι μικρότερες επιχειρήσεις αντιμετωπίζουν διαρκώς αυξανόμενους κινδύνους στον τομέα της κυβερνοασφάλειας. Από το phishing και την κλοπή δεδομένων έως τις αναδυόμενες απάτες που βασίζονται στην τεχνητή νοημοσύνη, κάθε οργάνωση μπορεί εν δυνάμει να αποτελέσει στόχο. Αυτό το εγχειρίδιο έχει σχεδιαστεί ειδικά για **πολύ μικρές και μικρές επιχειρήσεις**, προκειμένου να τις βοηθήσει **να κατανοήσουν, να ιεραρχήσουν και να εφαρμόσουν τα πιο κρίσιμα μέτρα κυβερνοασφάλειας**, χωρίς να απαιτείται βαθιά τεχνική εμπειρογνωμοσύνη ή μεγάλοι προϋπολογισμοί.

Η δομή ακολουθεί μια **σταδιακή, προοδευτική προσέγγιση**, βασισμένη σε πραγματικά πλαίσια ΜμΕ και υποστηριζόμενη από τις γνώσεις της ENISA σχετικά με το τοπίο των απειλών. Κάθε ενότητα είναι προσαρμοσμένη στους βασικούς ενδιαφερόμενους — από ιδιοκτήτες επιχειρήσεων και ειδικούς πληροφορικής έως οικονομικές υπηρεσίες και εξωτερικούς συμβούλους — εξασφαλίζοντας ότι κάθε ρόλος γνωρίζει τι πρέπει να κάνει, γιατί είναι σημαντικό να το κάνει και πώς να ξεκινήσει.

Θα βρείτε επίσης **έτοιμα προς χρήση εργαλεία**, όπως γρήγορες λίστες ελέγχου, πρότυπα αντιμετώπισης περιστατικών και σύντομους πρακτικούς οδηγούς για την ευαισθητοποίηση, τη μείωση των κινδύνων και τη βελτίωση της ανθεκτικότητας σε ολόκληρη την οργάνωσή σας.

Ο στόχος είναι απλός: **να καταστεί η κυβερνοασφάλεια εφικτή, πρακτική και βιώσιμη για τις επιχειρήσεις** εκείνες που τροφοδοτούν τις κοινότητες και τις οικονομίες μας.

Οι τυπικοί ενδιαφερόμενοι - επωφελούμενοι από αυτό το εγχειρίδιο είναι:

1. Ιδιοκτήτες μικρών επιχειρήσεων - Διευθύνοντες σύμβουλοι

- **Ρόλος:** Εποπτεύουν όλη την επιχείρηση - λαμβάνουν τις σχετικές με την τεχνολογία αποφάσεις.
- **Απαιτήσεις:** Επιχειρησιακή συνέχεια, φήμη και εμπιστοσύνη των πελατών στοιχεία που ενισχύει η κυβερνοασφάλεια. Αναζήτηση οικονομικά αποδοτικών στρατηγικών ασφάλειας.
- **Προκλήσεις:** Περιορισμένος χρόνος, προϋπολογισμός και τεχνικές γνώσεις.

2. Διευθυντές IT - Τεχνικό προσωπικό

- **Ρόλος**: Διαχειρίζονται IT υποδομή και υποστήριξη, συχνά μόνοι ή ως μέλοι μιας μικρής ομάδας.
- **Απαιτήσεις**: Πρακτικά, εφαρμόσιμα μέτρα για την ασφάλεια δικτύων, συσκευών και δεδομένων με περιορισμένα εργαλεία/προσωπικό.
- **Προκλήσεις**: Εξισορρόπηση ασφάλειας με λειτουργικές απαιτήσεις και περιορισμένους πόρους.

3. Επιχειρησιακοί Δ/ντές - Δ/ντές Διοικητικού

- **Ρόλος**: Διαχειρίζονται εσωτερικές διαδικασίες, ανθρώπινο δυναμικό, προμήθειες τεχνολογίας.
- **Απαιτήσεις**: Κουλτούρα εργαζομένων, ασφάλεια στον κυβερνοχώρο, εφαρμογή ορθών πρακτικών.
- **Προκλήσεις**: Η κυβερνοασφάλεια ως τμήμα της εργασίας.

4. Μη-τεχνικό προσωπικό - Υπάλληλοι

- **Ρόλος**: Συχνοί χρήστες ηλεκτρονικού ταχυδρομείου, κοινοποίησης αρχείων - εφαρμογών.
- **Απαιτήσεις**: Απλές οδηγίες για τον εντοπισμό απειλών (π.χ. phishing), την ασφάλεια των κωδικών πρόσβασης και την αναφορά περιστατικών.
- **Προκλήσεις**: Έλλειψη ευαισθητοποίησης και εκπαίδευσης σε θέματα κυβερνοασφάλειας.

5. Οικονομικές Υπηρεσίες & Έλεγχος

- **Ρόλος**: Διαχείριση ευαίσθητων δεδομένων, οικονομικών αρχείων - συμμόρφωση με GDPR κ.ά.
- **Απαιτήσεις**: Κατανόηση επιπτώσεων κυβερνοαπειλών στην προστασία των δεδομένων και τρόποι μετριασμού κινδύνων.
- **Προκλήσεις**: Διασφάλιση συμμόρφωσης χωρίς εξειδικευμένες ομάδες νομικών / ασφάλειας.

6. Εξωτερ. Σύμβουλοι - Ελεύθεροι Επαγγελματίες

- **Ρόλος**: Έμπιστοι σύμβουλοι με μερική απασχόληση ή βάσει έργου (π.χ. σύμβουλοι πληροφορικής κ.λπ). Συχνά υποστηρίζουν πολλές επιχειρήσεις.
- **Ανάγκες**: Συνοπτικό πλαίσιο για αξιολόγηση και προτάσεις βελτίωσης στον τομέα της κυβερνοασφάλειας σε διαφορετικούς πελάτες.
- **Προκλήσεις**: Χρειάζονται καθοδήγηση - οι πρακτικές τους να είναι σύμφωνες με πρότυπα ΕΕ - απαιτήσεις συμμόρφωσης.

Δράση Βήμα-Βήμα

Digital Skills & Jobs Platform

Η Φιλοσοφία πίσω από τις βήμα-προς-βήμα ενέργειες

Τα παρακάτω βήματα περιγράφουν μια προληπτική προσέγγιση μείωσης του κινδύνου για μικρές και πολύ μικρές επιχειρήσεις. Αντί να δοθεί έμφαση στη συνέχιση της επιχειρηματικής δραστηριότητας — η οποία αφορά τον τρόπο λειτουργίας κατά τη διάρκεια ή μετά από ένα συμβάν — **επικεντρωνόμαστε στη μείωση της πιθανότητας και του αντίκτυπου των απειλών στον κυβερνοχώρο πριν αυτές συμβούν**. Κάθε βήμα στοχεύει σε μια κατηγορία κινδύνου και αποφεύγει εκ των υστέρων διορθωτικά μέτρα. Η προσέγγιση είναι ρεαλιστική: μικρές ενέργειες που εφαρμόζονται με συνέπεια, μπορούν συλλογικά να μειώσουν την έκθεση στις πιο κοινές κυβερνοεπιθέσεις σε ΜμΕ.

7 Βήματα προς την Κυβερνο-Ανθεκτικότητα

01 **Αναγνωρίστε & Ιεραρχήστε τους Κινδύνους**
Βασική ευαισθητοποίηση σχετικά με επιβλαβή στοιχεία του ψηφιακού κόσμου.

02 **Μειώστε τα Ανθρώπινα Λάθη**
Περιορίστε τη μεγαλύτερη πηγή παραβιάσεων: τους ανθρώπους.

03 **Θωρακίστε την Πρόσβαση και την Αυθεντικοποίηση**
Αποτρέψτε μη εξουσιοδοτημένη είσοδο και υποκλοπή διαπιστευτηρίων.

04 **Διατηρήστε την Καλή Λειτουργία του Συστήματος**
Διορθώστε γνωστές ευπάθειες πριν τις εκμεταλλευτούν οι επιτιθέμενοι.

05 **Προστατέψτε τα Δεδομένα (Αποθήκευση & Μεταφορά)**
Αποτρέψτε τη διαρροή δεδομένων και τη μη εξουσιοδοτημένη πρόσβαση.

06 **Πρωτόκολλα Ανίχνευσης & Έγκαιρης Αντίδρασης**
Ανίχνευση ύποπτης συμπεριφοράς σε πρώιμο, έγκαιρα αποτρεπτικό στάδιο.

07 **Επικυρώστε και ελέγξτε τακτικά**
Διατηρήστε ενημερωμένες τις άμυνες σε ένα εξελισσόμενο τοπίο απειλών.

Αυτές οι ενέργειες συνιστούν **μια προοδευτική διαδικασία για τους μικρούς οργανισμούς** προς την προληπτική ελαχιστοποιήση των κίνδυνων και την προώθηση μιας κουλτούρας κυβερνοασφάλειας χωρίς προηγμένη τεχνογνωσία ή μεγάλους προϋπολογισμούς. Κάθε βήμα ευθυγραμμίζεται με τις **οδηγίες της ENISA για τις ΜμΕ** και τις αρχές διαχείρισης κινδύνων (**στο πλαίσιο της Οδηγίας NIS2**). Η έμφαση δίνεται στη μείωση της έκθεσης σε κοινές απειλές, όπως το phishing, η υποκλοπή διαπιστευτηρίων ή οι ευπάθειες λογισμικού, μέσω της ενίσχυσης της ευαισθητοποίησης, του ελέγχου πρόσβασης και της υγειούς λειτουργίας των συστημάτων.

01 Αναγνωρίστε & Ιεραρχήστε τους Κινδύνους

Στόχος: Να αποκτήσετε βασικές γνώσεις για τα πιθανά επιβλαβή προς την επιχείρησή σας στοιχεία αναφορικά με τον ψηφιακό κόσμο.
Εστίαση: Κατανόηση της ευπάθειας, όχι απλός σχεδιασμός ανάκαμψης από ένα συμβάν.
Γιατί: Η μείωση του κινδύνου ξεκινά με την ευαισθητοποίηση — όχι με την τεχνολογία. Μια μικρή επιχείρηση δεν μπορεί να προστατευθεί από τα πάντα, αλλά μπορεί να προστατεύσει τα πιο κρίσιμα στοιχεία.

Βασικές Ενέργειες	Προσδοκώμενο Αποτέλεσμα	Εργαλεία / Πόροι
Αναγνωρίστε τα μέσα μείζονος σημασίας (συσκευές, e-mails, δεδομένα, ιστότοποι, συστήματα πληρωμών).	Μάθετε τι να προστατεύετε κατά προτεραιότητα.	Εργαλείο Αυτοαξιολόγησης ΜμΕ της ENISA, πρότυπα CIS Controls 1–2
Σημειώστε τις κύριες ψηφιακές απειλές (phishing, ransomware, κλοπή συσκευών, αδύναμοι κωδικοί πρόσβασης).	Ευαισθητοποίηση σχετικά με τους συνήθεις κινδύνους.	Συνόψεις από το ‘Περιβάλλον Απειλών για τις ΜμΕ’ από την ENISA
Χαρτογραφήστε ποιος χρησιμοποιεί τι και πώς (υπάλληλοι, προμηθευτές, πάροχοι υπηρεσιών cloud)	Αναγνωρίστε ποιος μπορεί να αποτελέσει απειλή.	Απλό φύλλο Excel “Στοιχεία Επιχείρησης - Μέσα & Πρόσβαση”

02 Μειώστε τα Ανθρώπινα Λάθη (Ευαισθητοποίηση & Αλλαγή κουλτούρας)

Στόχος: Περιορισμός της μεγαλύτερης πηγής παραβιάσεων — αυτής των ανθρώπων.
Εστίαση: Εκπαίδευση, συνήθειες και κουλτούρα.
Γιατί: το 80-90% των περιστατικών κυβερνοασφάλειας στις ΜμΕ προέρχονται από ενέργειες των χρηστών (κλικ σε συνδέσμους, επαναχρησιμοποίηση κωδικών πρόσβασης). Η ενημέρωση μειώνει άμεσα αυτόν τον κίνδυνο.

Βασικές Ενέργειες	Προσδοκώμενο Αποτέλεσμα	Εργαλεία / Πόροι
Διοργανώστε ενημερωτικές συνεδρίες διάρκειας 1 ώρας δύο φορές το χρόνο.	Το προσωπικό **να μπορεί να αναγνωρίζει** τις προσπάθειες ηλεκτρονικού ψαρέματος ή απάτης.	Εκπαίδευση ‘Cybersecurity Awareness’ της ENISA
Χρησιμοποιήστε παραδείγματα πλαστών τιμολογίων ή ηλεκτρονικών μηνυμάτων phishing.	Έγκαιρη ανίχνευση μηχανισμών χειραγώγησης.	Δωρεάν προσομοιωτές ηλεκτρονικού ψαρέματος ‘phising’ (KnowBe4, PhishTest)
Δημιουργήστε μια μίνι πολιτική με τίτλο «Σκεφτείτε πριν κάνετε κλικ» (1 σελίδα).	Λιγότερες τυχαίες λήψεις (downloads) ή διαρροές διαπιστευτηρίων.	Αφίσα ή ψηφιακό memo εντός όλης της επιχείρησης

03 Θωρακίστε την Πρόσβαση και την Αυθεντικοποίηση

Στόχος: Να προλάβετε μη εξουσιοδοτημένη πρόσβαση και υποκλοπή διαπιστευτηρίων.
Εστίαση: Να μειώσετε την πιθανότητας εισβολής, όχι να ανακάμπτετε από αυτήν.
Γιατί: Η παραβίαση της ταυτότητας είναι η ευκολότερη και η πιο συνήθης εισβολή. Η ενισχυμένη πρόσβαση είναι το πιο αποδοτικό και οικονομικό μέτρο μετριασμού των απειλών.

Βασικές Ενέργειες	Προσδοκώμενο Αποτέλεσμα	Εργαλεία / Πόροι
Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς πρόσβασης και ενεργοποιήστε τον **MFA (Multi-Factor Authentication - Έλεγχος Ταυτότητας Πολλαπλών Παραγόντων)** για όλους τους λογαριασμούς cloud/email.	Οι λογαριασμοί παραμένουν ασφαλείς ακόμη και σε περίπτωση διαρροής κωδικών πρόσβασης	Google Authenticator, Authy
Κατάργηση πεπαλαιωμένων ή ανενεργών λογαριασμών χρηστών.	Μειωμένη έκθεση σε επίθεση.	Φύλλο ελέγχου πρόσβασης
Εφαρμογή της **αρχής «ελάχιστων προνομίων»** – παραχώρηση πρόσβασης μόνο σε ό,τι είναι απαραίτητο.	Περιορισμένος αντίκτυπος σε περίπτωση παραβίασης.	Ενσωματωμένες ρυθμίσεις ρόλων στο Google Workspace / Microsoft 365

04 Διατηρήστε την Καλή Λειτουργία του Συστήματος (Επιδιόρθωση, Προστασία, Απλοποίηση)

Στόχος: Να ‘σφραγίζετε’ γνωστές ευπάθειες πριν τις εκμεταλλευτούν οι επιτιθέμενοι.
Εστίαση: Να αποτρέψετε την έκθεση, όχι τον χρόνο κατά τη διάρκεια των επιθέσεων.
Γιατί: Τα συστήματα χωρίς ενημερώσεις και τα ξεπερασμένα plugins ευθύνονται για τις περισσότερες παραβιάσεις σε **μικρομεσαίες επιχειρήσεις**. Η προληπτική συντήρηση μειώνει την πιθανότητα παραβίασης **κατά ~60–70%**.

Βασικές Ενέργειες	Προσδοκώμενο Αποτέλεσμα	Εργαλεία / Πόροι
Ενεργοποιήστε τις **αυτόματες ενημερώσεις** για όλες τις συσκευές και το λογισμικό (**μόνο** για ενημερώσεις **ΑΣΦΑΛΕΙΑΣ**)	Οι γνωστές ευπάθειες εξαλείφονται γρήγορα.	Ρυθμίσεις ενημέρωσης λειτουργικού συστήματος
Εγκαταστήστε/συντηρήστε προγράμματα προστασίας από ιούς και τείχη προστασίας.	Έγκαιρη ανίχνευση κακόβουλων αρχείων.	Microsoft Defender, Avast Free
Αφαιρέστε το παρωχημένο λογισμικό και τα αχρησιμοποίητα πρόσθετα.	Μειωμένοι δίαυλοι επίθεσης.	Περιοδικός έλεγχος αποθεμάτων.

Χρησιμοποιείτε τις αυτόματες ενημερώσεις μόνο για ενημερώσεις ασφαλείας. Έτσι αποφεύγονται ανώφελες αλλαγές σε εφαρμογές και λειτουργικά συστήματα, οι οποίες ενδέχεται να περιορίσουν ήδη απαραίτητες στους χρήστες λειτουργίες.
Διαβάζετε πάντα τις τεχνικές σημειώσεις (εφόσον διαθέσιμες) που εξηγούν τους εισαγόμενους από τις ενημερώσεις ασφαλείας λειτουργικούς περιορισμούς, ώστε να ενημερώνετε τους χρήστες για αυτούς.
Αποφεύγετε **πάντα τις γενικές αυτόματες ενημερώσεις** για λειτουργικά συστήματα και μεγάλες εφαρμογές (SAP, Oracle, MSSql, Office). Προτιμήστε τα service packs.
Παραμείνετε στην τελευταία έκδοση: όσο παλαιότερη τόσο καλύτερη (εκτός από συγκεκριμένες περιπτώσεις που συνήθως διαχειρίζεται ο προμηθευτής του λογισμικού).

05 Προστατέψτε τα Δεδομένα (κατά την Αποθήκευση & τη Μεταφορά)

Στόχος: Πρόληψη διαρροών δεδομένων και μη εξουσιοδοτημένης πρόσβασης.
Εστίαση: Περιορισμός των επιπτώσεων σε περίπτωση παραβίασης.
Γιατί: Η κρυπτογράφηση και ο έλεγχος πρόσβασης ελαχιστοποιούν τις ζημίες, ακόμη και αν οι εισβολείς εισέλθουν στο σύστημα — βασικός παράγοντας για τον περιορισμό του αντικτύπου.

Βασικές Ενέργειες	Προσδοκώμενο Αποτέλεσμα	Εργαλεία / Πόροι
Κρυπτογραφήστε ευαίσθητα δεδομένα και συσκευές.	Τα υποκλεμμένα δεδομένα καθίστανται μη αναγνώσιμα.	BitLocker, VeraCrypt
Εφαρμόστε έλεγχο πρόσβασης σε κοινόχρηστους φακέλους.	Αποτρέψτε την υπερβολική έκθεση των δεδομένων των πελατών.	Ρυθμίσεις κοινής χρήσης στο Cloud

06 Καθιέρωση πρωτοκόλλων ανίχνευσης & έγκαιρης αντίδρασης

Στόχος: Έγκαιρη ανίχνευση ύποπτης συμπεριφοράς προς αποτροπή επιθέσεων πριν αυτές κλιμακωθούν.
Εστίαση: Γρήγορη ανάσχεση και αναφορά, όχι επαναφορά των λειτουργιών της επιχείρησης.
Γιατί: Η έγκαιρη ανίχνευση ελαχιστοποιεί τις ζημίες. Πολλές μικρές επιχειρήσεις χάνουν δεδομένα, επειδή κανείς δεν παρατηρεί τα πρώιμα προειδοποιητικά σημάδια.

Βασικές Ενέργειες	Προσδοκώμενο Αποτέλεσμα	Εργαλεία / Πόροι
Παρατηρήστε ασυνήθιστες **προσπάθειες σύνδεσης** ή μεταφορές **μεγάλων αρχείων**	Γρήγορος εντοπισμός παραβιάσεων.	Ενσωματωμένα αρχεία καταγραφής δραστηριότητας λογαριασμού.
Ορίστε μια απλή ‘λίστα ελέγχου περιστατικών’ (**ποιον να καλέσετε, τι να αποσυνδέσετε**).	Ταχύτερος περιορισμός των ζητημάτων.	Πρότυπο σχεδίου αντίδρασης μιας (1) σελίδας.
Εκπαιδεύστε το προσωπικό να **αναφέρει** αμέσως τυχόν αποκλίσεις.	Μειωμένος χρόνος παραμονής (κατά τη διάρκεια επίθεσης).	Κοινόχρηστο σημείο ειδοποιήσεων Slack/WhatsApp.

07 Επικυρώστε και ελέγξτε τακτικά

Στόχος: Διατηρείστε τους αμυντικούς μηχανισμούς ενημερωμένους, καθώς το τοπίο των απειλών εξελίσσεται.
Εστίαση: Συνεχής προληπτική βελτίωση.
Γιατί: Η μείωση του κινδύνου είναι δυναμική — οι μικρές, τακτικές ενημερώσεις είναι πιο αποτελεσματικές από τις μείζονες ενημερώσεις που γίνονται κάθε λίγα χρόνια.

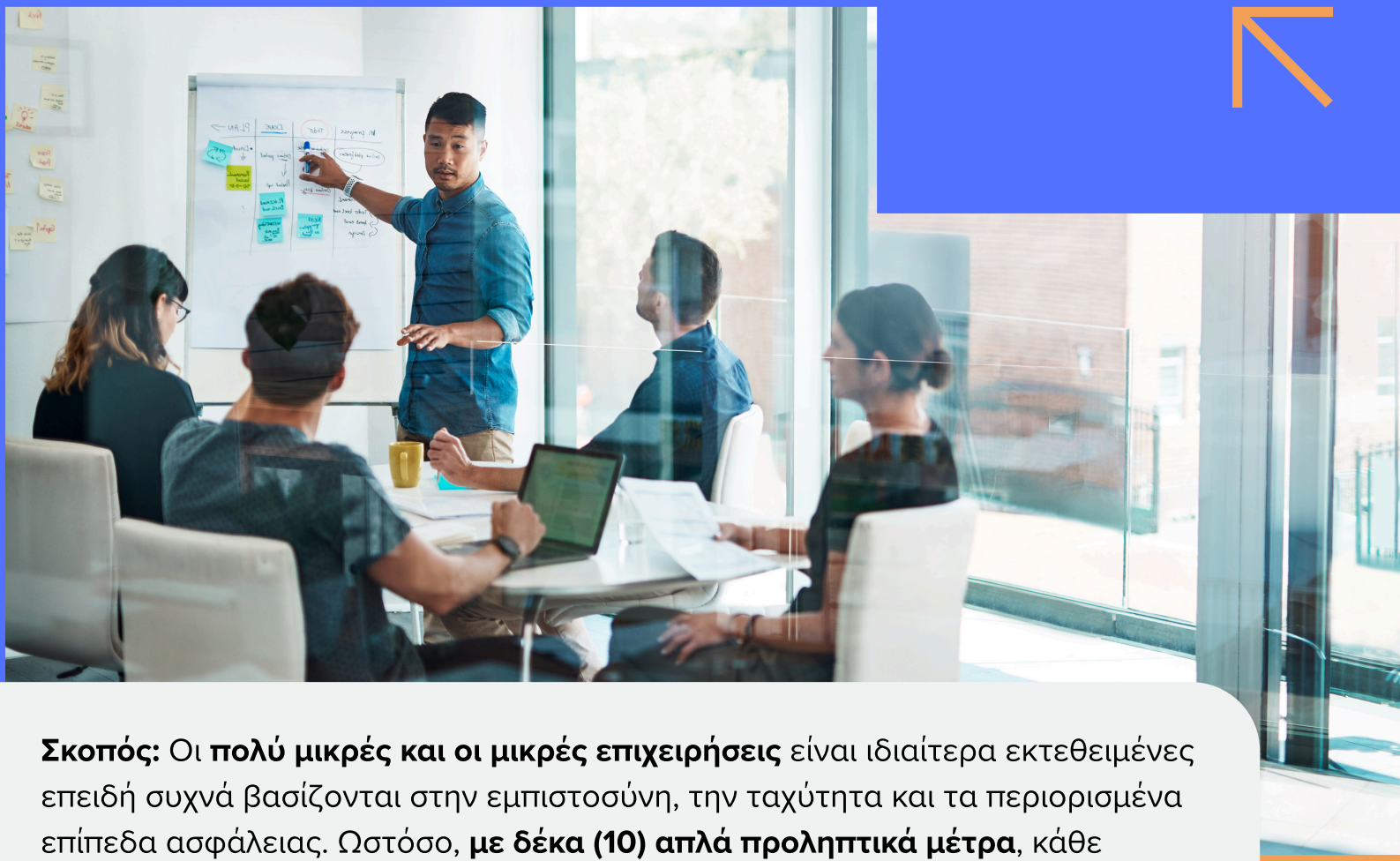
Βασικές Ενέργειες	Προσδοκώμενο Αποτέλεσμα	Εργαλεία / Πόροι
Εκτελέστε **τριμηνιαίες** μικρο-ενημερώσεις των λιστών ελέγχου.	Ενημερωμένη ευαισθητοποίηση της κατάστασης ασφάλειας.	Εσωτερικό υπολογιστικό φύλλο, 'Αξιολόγηση ΜμΕ' από την ENISA.
Ελέγξτε **ετησίως** την πρόσβαση και τις συμβάσεις των **προμηθευτών**.	Πρόληψη κληρονομημένων από προμηθευτές κινδύνων.	Ερωτηματολόγιο προμηθευτή.
Διεξάγετε **προσομοιώσεις** phishing ή προσομοιώσεις περιστατικών.	Δοκιμή της ικανότητας αντίδρασης των εργαζομένων.	Δωρεάν διαδικτυακά εργαλεία.

Παράδειγμα: Τριμηνιαίος Κύκλος Βελτίωσης

- Επανεξέταση περιστατικών και συμμόρφωσης βάσει ενός καταλόγου ελέγχου.
- Ενημέρωση κωδικών πρόσβασης, αντιγράφων ασφαλείας και εκπαίδευσης.
- Σύγκριση των KPIs με τους στόχους.
- Ανταμοιβή προσωπικού που εντοπίζει/αναφέρει έγκαιρα τις απειλές.

Digital Skills & Jobs Platform

Ιδιαίτερη Έμφαση:
Οι ενισχυμένες από την Τεχνητή Νοημοσύνη απάτες θα απειλήσουν την Επιχείρησή σας:
‘10 Γρήγορες Μέθοδοι Προστασίας που κάθε Μικρή Επιχείρηση πρέπει να εφαρμόσει άμεσα’



Σκοπός: Οι **πολύ μικρές και οι μικρές επιχειρήσεις** είναι ιδιαίτερα εκτεθειμένες επειδή συχνά βασίζονται στην εμπιστοσύνη, την ταχύτητα και τα περιορισμένα επίπεδα ασφάλειας. Ωστόσο, **με δέκα (10) απλά προληπτικά μέτρα**, κάθε επιχείρηση μπορεί να μειώσει δραματικά τον κίνδυνο των **ενισχυμένων από την ΤΝ επιθέσεων**. Ο οδηγός αυτός αναφέρεται σε ανοικτό εκπαιδευτικό υλικό από το **Center for Cyber Safety & Education** *και το πρόγραμμά του* ***Cybersecurity Health Check***, το οποίο βοηθά τις μικρές επιχειρήσεις και τις ΜΚΟ να αξιολογήσουν και να ενισχύσουν τη θέση τους στον κυβερνοχώρο.

Ιδιαίτερη Έμφαση: *Οι ενισχυμένες από την Τεχνητή Νοημοσύνη απάτες θα απειλήσουν την Επιχείρησή σας:* 10 Γρήγορες Μέθοδοι Προστασίας που κάθε Μικρή Επιχείρηση πρέπει να εφαρμόσει άμεσα

1. Εκπαιδεύστε Την Ομάδα Σας (ακόμα και αν αποτελείται μόνο από 2 άτομα)
Γιατί έχει σημασία: Τα ανθρώπινα λάθη παραμένουν η υπ' αριθμόν ένα αιτία των περιστατικών.
Δράση: Παρέχετε σύντομες, ρεαλιστικές ενημερωτικές συνεδρίες σχετικά με τις τακτικές ηλεκτρονικού ψαρέματος 'phising' και κοινωνικής χειραγώγησης. Δείξτε παραδείγματα πλαστών τιμολογίων ή επειγόντων μηνυμάτων πληρωμής. Εξηγήστε τα **«παρόμοια» domain** (π.χ. @supply-co.com έναντι @supplyco.com). Ενθαρρύνετε τη συνήθεια «παύση και επαλήθευση» πριν από την ανταπόκριση σε επείγοντα ή απροσδόκητα αιτήματα.
Πόροι: Εργαλειοθήκη ENISA AR-in-a-Box — δωρεάν ενημερωτικό υλικό, κουίζ και πρότυπα εκστρατείας.

2. Χρησιμοποιείτε Παντού 'Έλεγχο Ταυτότητας Πολλών Παραγόντων' (Multi-Factor Authentication - MFA)
Γιατί έχει σημασία: Ο έλεγχος αυτός διακόπτει τις περισσότερες υποκλοπές λογαριασμών ακόμη και αν οι κωδικοί πρόσβασης παραβιάζονται.
Δράση: Ενεργοποιήστε τον σε όλες τις υπηρεσίες email, τραπεζικών συναλλαγών, cloud. Προτιμήστε την επαλήθευση μέσω εφαρμογής ή βιομετρικών στοιχείων αντί για SMS, όπου αυτό είναι δυνατόν.
Πόροι: ISC2 Insight – 'Έλεγχος ταυτότητας πολλών παραγόντων: Ενίσχυση της ψηφιακής ασφάλειας'.

3. Σκεφτείτε Πριν Κάνετε Κλικ ή Απαντήσετε
Γιατί έχει σημασία: Η Τεχνητή Νοημοσύνη μπορεί να **δημιουργήσει πειστικά ψεύτικα μηνύματα** που μιμούνται το στυλ γραφής, το λογότυπο ή τον τόνο σας.
Δράση: Ποτέ μην ανοίγετε συνημμένα ή συνδέσμους από μηνύματα που δεν περιμένετε. Επαληθεύστε ασυνήθιστα οικονομικά αιτήματα ή αιτήματα πρόσβασης χρησιμοποιώντας ένα εναλλακτικό αξιόπιστο κανάλι (τηλεφώνημα ή μήνυμα κειμένου). Δημιουργήστε έναν εσωτερικό κανόνα: «Όταν έχετε αμφιβολίες, προχωρήστε με προσοχή».
Πόροι: Μελέτη περίπτωσης 'ISC2 – Προσομοιώσεις ηλεκτρονικού 'ψαρέματος' με βάση την Τεχνητή Νοημοσύνη και ο αντίκτυπός τους'.

4. Ποτέ Μην Εμπιστεύεστε Άκριτα την Ταυτότητα ή τη Φωνή του Καλούντος
Γιατί έχει σημασία: Η κλωνοποίηση φωνής επιτρέπει στους απατεώνες να υποδύονται αξιόπιστα άτομα χρησιμοποιώντας "ηχητικά αποσπάσματα λίγων δευτερολέπτων".
Δράση: Καθιερώστε μια κωδική λέξη ή μια κοινή φράση για επαλήθευση κατά τη διάρκεια επειγουσών κλήσεων. Επαληθεύστε ασυνήθιστα φωνητικά αιτήματα μέσω ενός δεύτερου καναλιού (SMS ή επαληθευμένο email).
Παράδειγμα: '*Προειδοποίηση της Αμερικάνικης Προστασίας Καταναλωτή - Ομοσπονδιακή Επιτροπή Εμπορίου: Απατεώνες χρησιμοποιούν Τεχνητή Νοημοσύνη για να αλλοιώσουν πλάνα έκτακτης οικογενειακής ανάγκης*"'

Ιδιαίτερη Έμφαση: Οι ενισχυμένες από την Τεχνητή Νοημοσύνη απάτες θα απειλήσουν την Επιχείρησή σας:
10 Γρήγορες Μέθοδοι Προστασίας που κάθε Μικρή Επιχείρηση πρέπει να εφαρμόσει άμεσα

5. Επαληθεύστε Πάντα Ασυνήθιστα Αιτήματα Μέσω Ενός Δεύτερου Καναλιού
Γιατί έχει σημασία: Το Business Email Compromise (BEC)- Η παραβίαση επαγγελματικού email παραμένει μία από τις πιο δαπανηρές απάτες.
Δράση: Καλέστε γνωστές επαφές χρησιμοποιώντας αποθηκευμένους αριθμούς τηλεφώνου, όχι εκείνους που αναφέρονται σε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου. Απαίτηση «επαλήθευσης εκτός ζώνης» (OOB) για όλες τις χρηματοοικονομικές συναλλαγές.
Πόροι: Οδηγοί ηλεκτρονικού 'phising' από CISA-FBI-NSA.

6. Χρήση Αξιόπιστων Εργαλείων Ασφαλείας
Γιατί έχει σημασία: Οι τεχνικές προφυλάξεις συμπληρώνουν την ανθρώπινη επαγρύπνηση.
Δράση: Διατηρήστε ενημερωμένα τα προγράμματα προστασίας από ιούς, τα φίλτρα κατά του phishing και τις προστασίες του προγράμματος περιήγησης. Ενεργοποιήστε τις αυτόματες ενημερώσεις ασφαλείας.
Πόροι: Εργαλειοθήκη ENISA 'Κυβερνοασφάλεια για Μικρο-Μεσαίες Επιχειρήσεις'.

7. Προετοιμάστε Ένα Απλό Σχέδιο Συμβάντων
Γιατί έχει σημασία: Περιορισμός ζημιάς στα πρώτα *15 λεπτά* μετά την ανίχνευση.
Δράση: Διατηρήστε μια λίστα ελέγχου 1 σελίδας με άμεσα μέτρα, σημεία επαφής και συνδέσμους CSIRT. Αναφορά σοβαρών περιστατικών στο εθνικό CSIRT (βλ. τον διαδραστικό χάρτη της ENISA).

8. Περιορίστε Ποιος Μπορεί Να Έχει Πρόσβαση Σε Τι
Γιατί είναι σημαντικό: Ο περιορισμός των δικαιωμάτων πρόσβασης μειώνει το εύρος των επιπτώσεων σε περίπτωση παραβίασης.
Δράση: Εφαρμόστε έλεγχο πρόσβασης *βάσει ρόλων*. Διαγράψτε αμέσως τους ανενεργούς λογαριασμούς.
Πόροι: 'Οδηγός ISC2 – Ένας Απλός Οδηγός για τον Έλεγχο Πρόσβασης'.

9. Ασφαλίστε την Παρουσία Σας Στο Διαδίκτυο
Γιατί είναι σημαντικό: Η υπερβολική κοινοποίηση πληροφοριών τροφοδοτεί την πλαστοπροσωπία με τη βοήθεια της Τεχνητής Νοημοσύνης.
Δράση: Αφαιρέστε περιττές προσωπικές πληροφορίες ή πληροφορίες εσωτερικών διαδικασιών από δημόσια αναρτημένες σελίδες. Ελέγξτε τις ρυθμίσεις απορρήτου των μέσων κοινωνικής δικτύωσης.
Πόροι: 'CISA – Περιορίστε το Ψηφιακό σας Αποτύπωμα'.

10. Προσέξτε τα Deepfakes και τα Συνθετικά Μέσα
Γιατί είναι σημαντικό: Η Τεχνητή Νοημοσύνη μπορεί να δημιουργήσει ρεαλιστικά βίντεο ή ζωντανές κλήσεις.
Δράση: Ζητήστε από τους συμμετέχοντες σε βιντεοκλήσεις να κάνουν χειρονομίες σε πραγματικό χρόνο ή να επιβεβαιώσουν έναν κοινό κωδικό. Χρησιμοποιήστε εργαλεία ανίχνευσης deepfake κατά την αξιολόγηση ύποπτων βίντεο.
Πόροι: 'ISC2 Insight – Χειραγώγηση από Deepfake Engineering: Νέα Ανησυχία για τις Διοικήσεις'.

Συνοπτικός Πίνακας: Προτεραιότητες Προστασίας

Επίπεδο Προτεραιότητας	Σημασία	Συνήθεις Ενέργειες
🔴 Κρίσιμο (10)	Απαραίτητο, άμεσο αποτέλεσμα	Εκπαίδευση προσωπικού, ενεργοποίηση ‘Ελέγχου Ταυτότητας Πολλών Παραγόντων’, επαλήθευση οικονομικών ενεργειών
🟠 Σημαντικό (7–9)	Υψηλή Απόδοση Επένδυσης (ROI) για προστασία	Σχέδιο αντιμετώπισης περιστατικών, έλεγχος πρόσβασης, επαλήθευση φωνής
🟡 Χρήσιμο (4–6)	Προσθέτει ανθεκτικότητα	Καθαρή - ασφαλής διαδικτυακή παρουσία, ευαισθητοποίηση σχετικά με τα deepfake

Συμπέρασμα

Οι απάτες που βασίζονται στην Τεχνητή Νοημοσύνη δεν είναι πλέον αναδυόμενες απειλές, αλλά η πραγματικότητα του σήμερα.
Οι πολύ μικρές επιχειρήσεις δεν μπορούν να συγκροτήσουν μεγάλες ομάδες κυβερνοασφάλειας, αλλά μπορούν να υιοθετήσουν έξυπνες συνήθειες:

- Εκπαιδεύστε και ενδυναμώστε κάθε υπάλληλο.
- Προστατέψτε τους λογαριασμούς με αυθεντικοποίηση πολλών επιπέδων.
- Επαληθεύστε πριν προβείτε σε ενέργειες.

Μικρά βήματα που εφαρμόζονται με συνέπεια θα μετατρέψουν την επιχείρησή σας σε έναν από τους πιο δύσκολους στόχους στην κατηγορία σας.

Σχετικά Εργαλεία: Πρακτικές Πηγές για την Κυβερνο-Ανθεκτικότητα των ΜμΕ

Digital Skills & Jobs Platform

Σχετικά Εργαλεία: Πρακτικές Πηγές για την Κυβερνο-Ανθεκτικότητα των ΜμΕ

Τα ακόλουθα εργαλεία υποστηρίζουν τις **μικρές και πολύ μικρές επιχειρήσεις** στην ενίσχυση της ασφάλειας στον κυβερνοχώρο μέσω εντοπισμού κινδύνων, ετοιμότητας και ευαισθητοποίησης:

- Ο 'Κατάλογος Ελέγχου Απειλών για τις ΜμΕ' (βάσει κατευθύνσεων της ENISA) βοηθά στον προσδιορισμό κινδύνων και προτεραιοτήτων,
- Οι 'Ερωτήσεις Αυτοαξιολόγησης' (Ναι / Όχι / Σε εξέλιξη) διευκολύνουν την ταχεία εσωτερική επανεξέταση των υφιστάμενων μέτρων προστασίας,
- Το 'Πρότυπο Έκτακτου Σχεδίου Αντιμετώπισης Περιστατικών' περιγράφει σαφείς ενέργειες αντίδρασης,
- Οι Πλατφόρμες Δοκιμών Phishing και Ευαισθητοποίησης' συμβάλλουν στη διατήρηση της συνεχούς επαγρύπνησης του προσωπικού.

1. Κατάλογος ελέγχου απειλών για τις ΜμΕ (βάσει ENISA)

1.1. Κύριες Κατηγορίες Απειλών

Για καθεμία από αυτές, σημειώστε εάν η ΜμΕ σας είναι εκτεθειμένη / μερικώς προστατευμένη / έχει λάβει μέτρα μείωσης κινδύνων:

- Ransomware (Λυτρισμικό: κακόβουλο λογισμικό το οποίο απαιτεί λύτρα για να αποκαταστήσει δυσλειτουργίες που το ίδιο επέφερε),
- Malware (Κακόβουλο Λογισμικό: σχεδιασμένο να προκαλέσει ζημιά σε συστήματα),
- Κοινωνική χειραγώγηση ('ηλεκτρονικό ψάρεμα - phishing' ως τρόπος εξαπάτησης μέσω email ή στοχευμένο - εξατομικευμένο 'spear-phishing', 'smishing' μέσω SMS ή 'vishing' μέσω κλήσεων),
- Απειλές κατά των δεδομένων (παραβίαση, διαρροή, μη εξουσιοδοτημένη πρόσβαση),
- Απειλές κατά της λειτουργικότητας (*Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας*: DISTRIBUTED Denial of Service ATTACKS - DDoS, διακοπή υπηρεσιών),
- Χειραγώγηση πληροφοριών / διασπορά ψευδών ειδήσεων (fake news) / προπαγάνδα / παραπληροφόρηση,
- Επιθέσεις στην αλυσίδα εφοδιασμού / παραβίαση τρίτων.

1.2. Για Κάθε Απειλή: Βασικοί Δείκτες Κινδύνου

Απειλή	Τυπικοί Φορείς Επίθεσης	Δείκτες Έκθεσης	Βασικά Μέτρα Προστασίας
Ransomware (Λυτρισμικό)	Κακόβουλα συνημμένα ηλεκτρονικού ταχυδρομείου, απομακρυσμένη πρόσβαση σε υπολογιστές	Ασυνήθιστη κρυπτογράφηση αρχείων, επιβράδυνση του συστήματος, σημείωμα εκβιασμού	Συχνά backups, επιδιορθώσεις, αρχή ελαχίστων δικαιωμάτων σε ρόλους, antivirus, offline backup
Κοινωνική χειραγώγηση	Ηλεκτρονικό Ταχυδρομείο (Email), SMS, Τηλέφωνο	Χρήστες που κάνουν κλικ σε συνδέσμους ηλεκτρονικού ψαρέματος, οι οποίοι ζητούν επαναφορά διαπιστευτηρίων	Ενημερωτικά Μαθήματα, φίλτρα email, δοκιμαστικές εκστρατείες ηλεκτρονικού ψαρέματος
Παραβίαση / Διαρροή Δεδομένων	Λανθασμένες ρυθμίσεις ή αδύναμοι έλεγχοι πρόσβασης	Απροσδόκητα αρχεία καταγραφής πρόσβασης σε δεδομένα, εργαλεία αφαίρεσης φίλτρων δεδομένων	Επανεξέταση πρόσβασης, κρυπτογράφηση, καταγραφή και ειδοποίηση, ελάχιστα προνόμια
Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσίας / Διαθεσιμότητας	Υπερφόρτωση δικτύων - συστημάτων, δίκτυα bot	Διακοπή λειτουργίας υπηρεσιών, υψηλή κίνηση δικτύου	Περιορισμός rate, εναλλακτική υποδομή, προστασία DDoS (cloud)
Εφοδιαστική Αλυσίδα	Third-party Λογισμικό, APIs προμηθευτών	Δημοσιοποίηση παραβιάσεων από προμηθευτές, μη ελεγμένες ενημερώσεις λογισμικού	Αναθεώρηση ασφάλειας προμηθευτών, συμβατικές ρήτρες ασφάλειας, επιδιόρθωση εξαρτημάτων προμηθευτών
Χειραγώγηση πληροφοριών	Ψεύτικο περιεχόμενο, deepfake	Επιθέσεις στο κύρος της επιχείρησης, ψευδείς αναφορές	Παρακολούθηση, ανασκόπηση μέσων ενημέρωσης, επαλήθευση

1.3 Αξιολόγηση και Ιεράρχηση Κινδύνων

- Κρίσιμο: Απειλές που έχουν χαρακτηριστεί ότι «εκθέτουν» βασικά επιχειρηματικά συστήματα (π.χ. ransomware, παραβίαση δεδομένων).
- Υψηλό: Απειλές που καλύπτονται εν μέρει, αλλά με υπολειπόμενα κενά.
- Μέτριο/Χαμηλό: Απειλές που έχουν ήδη μετριαστεί επαρκώς.

Κατατάξτε τις 2-3 κορυφαίες απειλές και διαθέστε πόρους (χρόνο, προϋπολογισμό) για την κάλυψη των κενών ασφαλείας.

2. Ερωτήσεις Αυτοαξιολόγησης (Ναι/ Όχι/ Σε εξέλιξη)

- Έχουν όλοι οι υπάλληλοι μοναδικούς λογαριασμούς (χωρίς κοινόχρηστες συνδέσεις);
- Είναι ενεργοποιημένη η επαλήθευση ταυτότητας πολλών παραγόντων (MFA) για όλα τα κρίσιμα συστήματα;
- Ενημερώνονται όλα τα λειτουργικά συστήματα και το λογισμικό εντός 30 ημερών από την κυκλοφορία τους;
- Διατηρείτε ένα offline ή offsite αντίγραφο ασφαλείας των κρίσιμων δεδομένων;
- Έχει λάβει το προσωπικό εκπαίδευση σχετικά με το phishing/την κοινωνική χειραγώγηση κατά τους τελευταίους 6 μήνες;
- Υπάρχει τεκμηριωμένο σχέδιο αντιμετώπισης περιστατικών (με επαφές και βήματα);
- Ελέγχετε τις πρακτικές ασφάλειας τρίτων/προμηθευτών πριν από τη συνεργασία;
- Παρακολουθείτε τα αρχεία καταγραφής/ειδοποιήσεις για ασυνήθιστη δραστηριότητα (αποτυχημένες προσπάθειες σύνδεσης, μεταφορές μεγάλων αρχείων);
- Είναι οι συσκευές δικτύου (routers, τείχη προστασίας) ενισχυμένες (αφαίρεση προεπιλεγμένων κωδικών πρόσβασης, περιορισμός θυρών);

3. Πρότυπο Σχέδιο Γρήγορης Αντίδρασης σε Περιστατικά

Phase	Action	Responsible	Notes
Ανίχνευση	Εντοπίστε ασυνήθιστα αρχεία ή μηνύματα	Υπάλληλος	Στιγμιότυπο οθόνης ως αποδεικτικό
Περιορισμός	Αποσυνδέστε τον επηρεαζόμενο υπολογιστή/δίκτυο	Προϊστάμενος	
Εξάλειψη	Καλέστε το IT ή χρησιμοποιήστε σάρωση με antivirus	Εσωτερικό Τμήμα/ Εξωτερικός Συνεργάτης	
Ανάκαμψη	Επαναφέρετε καθαρό αντίγραφο ασφαλείας	Προϊστάμενος	
Μετά το συμβάν	Τεκμηρίωση και αναφορά	Προϊστάμενος	Έκθεση GDPR, εάν απαιτείται

4. Πλατφόρμες δοκιμών και ενημέρωσης για το ‘ηλεκτρονικό ψάρεμα’ - phishing

Οι τακτικές προσομοιώσεις phishing βοηθούν τους οργανισμούς να αξιολογήσουν πόσο καλά αναγνωρίζουν και ανταποκρίνονται οι υπάλληλοι σε ύποπτα μηνύματα. Όταν πραγματοποιούνται με ηθικό τρόπο και με τη συγκατάθεση των ενδιαφερομένων, αυτές οι εκστρατείες ευαισθητοποιούν και μειώνουν τις επικίνδυνες συμπεριφορές σε όλες τις ομάδες. Συνιστώμενες πλατφόρμες και πόροι:

- **Phish-Test** — Διεξάγετε ελεγχόμενες δοκιμές phishing στο 10-15% των χρηστών κάθε 1-2 μήνες για να μετρήσετε τις τάσεις ευαισθητοποίησης και να επαπροσδιορίσετε τις ανάγκες εκπαίδευσης.
- **GoPhish** — Ένα πλαίσιο ανοιχτού κώδικα για τη δημιουργία και την παρακολούθηση προσαρμοσμένων προσομοιώσεων phishing, κατάλληλο για μικρούς οργανισμούς και περιβάλλοντα εκπαίδευσης.
- **PhishingBox** — Παρέχει πρότυπα, πίνακες ελέγχου αναφορών και αυτοματοποιημένες εκστρατείες για επαναλαμβανόμενες δοκιμές ευαισθητοποίησης.
- **SANS OUCH! Newsletter** — Ένα δωρεάν μηνιαίο ενημερωτικό δελτίο που προσφέρει σαφείς, μη τεχνικές ενημερώσεις σχετικά με θέματα κυβερνοασφάλειας και βέλτιστες πρακτικές, ιδανικό για ενημερώσεις ομάδων και συνεχή ευαισθητοποίηση.

Συμβουλή εφαρμογής:
Ενσωματώστε σύντομα τεστ phishing ή επαναληπτικά μαθήματα ευαισθητοποίησης στους τακτικούς κύκλους εκπαίδευσης — ιδανικά κάθε λίγους μήνες — για επαγρύπνηση και ενίσχυση των θετικών συνηθειών στον τομέα της κυβερνοασφάλειας.

Σημείωση συμμόρφωσης:
Όλες οι προσομοιώσεις εκστρατειών phishing πρέπει να συμμορφώνονται με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR) και τους σχετικούς εργασιακούς κανονισμούς. Οι εργαζόμενοι πρέπει να ενημερώνονται ότι οι δοκιμές αποτελούν μέρος ενός εγκεκριμένου προγράμματος ευαισθητοποίησης σε θέματα ασφάλειας, ότι δεν θα χρησιμοποιηθούν προσωπικά τους δεδομένα για τιμωρητικούς σκοπούς και ότι τα αποτελέσματα θα αναλυθούν μόνο συνολικά με σκοπό τη βελτίωση της ανθεκτικότητας του οργανισμού.

Δείτε επίσης το **Βήμα 2 – Μείωση των ανθρώπινων σφαλμάτων (ευαισθητοποίηση και αλλαγή κουλτούρας)** και το **Βήμα 7 – Τακτική επικύρωση και αναθεώρηση**, όπου η ανατροφοδότηση από την εκπαίδευση και η περιοδική αξιολόγηση ενσωματώνονται στην ευρύτερη διακυβέρνηση της κυβερνοασφάλειας.

Παρακολούθηση προόδου και μέτρηση της μείωσης κινδύνου

Digital Skills & Jobs Platform

Για τη διαχρονική αποτελεσματικότητα των προληπτικών ενεργειών ασφαλείας, οι μικρές και πολύ μικρές επιχειρήσεις θα πρέπει να παρακολουθούν ορισμένους **βασικούς δείκτες απόδοσης (KPIs)**. Αυτοί οι δείκτες επαληθεύουν, απλά και μετρήσιμα, τη συνεπή εφαρμογή βασικών πρακτικών κυβερνοασφάλειας: εγκατάσταση ενημερώσεων, δημιουργία αντιγράφων ασφαλείας, ενημέρωση προσωπικού. **Κάθε KPI είναι 1 προληπτικός έλεγχος.** Κρίσιμα σημεία: τακτική παρακολούθηση, ποσοτικοποίηση προόδου, συμμόρφωση με ENISA και Οδηγία NIS2, εστίαση σε τρωτά σημεία.
Ο παρακάτω πίνακας συνοψίζει τους πιο σχετικούς KPIs για τη συνεχή παρακολούθηση της κυβερνοασφάλειας σε μικρές και πολύ μικρές επιχειρήσεις:

KPI	Τι Μετράει	Παρακολούθηση	Στόχος
Ποσοστό ενημερωμένου λογισμικού	% των συσκευών που έχουν ενημερωθεί	Μηνιαίος έλεγχος	>95%
Ποσοστό επιτυχών αντιγράφων ασφαλείας	% ημερών με έγκυρο αντίγραφο ασφαλείας	Αυτοματοποιημένη αναφορά	100%
Ενημέρωση για το ‘Phishing’	% προσωπικού που έχει περάσει δοκιμαστικές εξετάσεις	Τριμηνιαία δοκιμή	>80%
Έκταση Ελέγχου Ταυτότητας Πολλαπλών Παραγόντων (MFA)	% των κρίσιμων λογαριασμών με 2FA	Χειροκίνητος έλεγχος	100%
Χρόνος απόκρισης σε περιστατικά	Χρόνος απομόνωσης συμβάντος	Αρχείο ασκήσεων/ δοκιμών	<15 min

Κενά/ Ευκαιρίες βελτίωσης για τους KPIs

Καταγραφή Στοιχείων & Εκτίμηση Κινδύνων (Βήμα 1) — προσωρινά έμμεση μέτρηση.

- Πιθανός KPI: “Πληρότητα Αποθέματων Στοιχείων” (% συσκευών/λογαριασμών καταχωρισμένων στο απόθεμα).
- Αιτιολόγηση: Ποσοτικοποίηση καταγραφής — μείωση «τυφλών σημείων» επίθεσης.

Απειλή από προμηθευτές/τρίτους (Βήμα 7, αξιολόγηση προμηθευτών) — επίσης δεν παρακολουθείται.

- Πιθανός KPI: “Κάλυψη Αξιολόγησης Ασφάλειας Προμηθευτών” (% ενεργών προμηθευτών που αξιολογήθηκαν για ρήτρες ασφάλειας στον κυβερνοχώρο).
- Αιτιολόγηση: Το NIS2 τονίζει ρητά τη δέουσα επιμέλεια αναφορικά με την αλυσίδα εφοδιασμού.

Κάλυψη ανίχνευσης (Βήμα 6) — Ο “Χρόνος Απόκρισης σε Περιστατικά” είναι δείκτης καθυστερημένης ένδειξης.

- Πιθανός δείκτης KPI: “Κάλυψη παρακολούθησης” (% συστημάτων που δημιουργούν αρχεία καταγραφής ή ειδοποιήσεις).
- Αιτιολόγηση: Αντικατοπτρίζει την προληπτική ικανότητα ανίχνευσης πριν από την εμφάνιση ενός συμβάντος.

Η προσθήκη 1-2 προαιρετικών δεικτών θα καθιστούσε το επίπεδο παρακολούθησης πιο ολοκληρωμένο και ανιχνεύσιμο, αν και δεν απαιτείται αυστηρά για τις περισσότερες ΜμΕ.

Ακόμα Κι Ένα Βήμα Θα Κάνει Τη Διαφορά

Digital Skills & Jobs Platform

Ποιος μπορεί να επωφεληθεί από αυτό το εγχειρίδιο;

Η κυβερνοασφάλεια δεν είναι ένα αφηρημένο τεχνικό ζήτημα — είναι το θεμέλιο της εμπιστοσύνης που επιτρέπει σε κάθε μικρή επιχείρηση να αναπτυχθεί, να εμπορεύεται και να καινοτομεί με ασφάλεια.

Αυτό το εγχειρίδιο έχει δείξει ότι η προστασία δεν εξαρτάται από το μέγεθος ή τον προϋπολογισμό, αλλά **από τη νοοτροπία και τη συνέπεια**. Κάθε ενισχυμένος κωδικός πρόσβασης, κάθε ύποπτο email που αμφισβητείται και κάθε ενημέρωση που εφαρμόζεται δημιουργεί μια ασφαλέστερη ψηφιακή κοινότητα γύρω από την επιχείρησή σας.

- Για **τους ιδιοκτήτες και τους διευθυντές**, αυτή είναι η στιγμή να περάσουν από την ευαισθητοποίηση σε μετρήσιμες ενέργειες. Αντιμετωπίστε την κυβερνοασφάλεια ως μια μορφή επιχειρηματικής συνέχειας — όχι ως κόστος, αλλά ως επένδυση στην αξιοπιστία.
- Για **το διοικητικό προσωπικό και το IT**, κάντε ορατή κάθε μικρή βελτίωση: μοιραστείτε την πρόοδο, ορίστε τριμηνιαίους στόχους και αξιολογείστε θετικά την μείωση των δεικτών κινδύνου.
- Για **τις οικονομικές και ελεγκτικές υπηρεσίες**, ενσωματώστε την ασφάλεια στις καθημερινές διαδικασίες: επαλήθευση, τεκμηρίωση και υπευθυνότητα.
- Για **τους συμβούλους και τους συνεργάτες**, διαδώστε το μήνυμα σε όλη την τοπική οικονομία — βοηθώντας περισσότερες πολύ μικρές επιχειρήσεις να υιοθετήσουν την ίδια προληπτική κουλτούρα.

Αν δράσετε τώρα, όχι μόνο προστατεύετε την επιχείρησή σας, αλλά συμβάλλετε και στη δημιουργία ενός ασφαλέστερου ευρωπαϊκού ψηφιακού οικοσυστήματος, στο οποίο οι μικρές επιχειρήσεις είναι αξιόπιστοι εταίροι και όχι εύκολοι στόχοι. Η κυβερνοασφάλεια είναι συλλογική υπόθεση: όταν μια επιχείρηση γίνεται ισχυρότερη, ολόκληρη η κοινότητα αποκτά ανθεκτικότητα.

Η ανθεκτικότητα ξεκινά με τη δράση, και η δράση ξεκινά με ένα απλό βήμα σήμερα: Φτιάξτε μια λίστα, επιλέξτε ένα μέτρο και ξεκινήστε!

Για αυτό το λόγο, οικειοποιηθείτε το παρόν εγχειρίδιο. Προσαρμόστε το, μοιραστείτε το, διδάξτε το και μετατρέψτε απλές, καλές συμβουλές σε καθημερινές συνήθειες για την εξασφάλιση του μέλλοντος της επιχείρησής σας και όσων εξαρτώνται από αυτήν.

Κανονιστικό Πλαίσιο & Όρια Παρόντος Εγχειριδίου

Το παρόν εγχειρίδιο έχει σχεδιαστεί για μια εφικτή και πρακτική κυβερνοασφάλεια για πολύ μικρές και μικρές επιχειρήσεις. Εστιάζει σε ενημέρωση, πρόληψη και απλή τεχνική υγιεινή και όχι σε επίσημες διαδικασίες συμμόρφωσης. Αν και είναι **σύμφωνο με το πνεύμα της ισχύουσας νομοθεσίας της ΕΕ για την κυβερνοασφάλεια**, **δεν εγγυάται πλήρη νομική συμμόρφωση**. Οι ακόλουθες σημειώσεις διευκρινίζουν τους περιορισμούς του και παραθέτουν πρόσθετες ενέργειες για την επίτευξη της συμμόρφωσης, όπου ισχύει.

- **Οδηγία NIS2 (EU 2022/2555)** – Το εγχειρίδιο καλύπτει υποχρεώσεις πρόληψης και ευαισθητοποίησης, αλλά όχι υποχρεωτικές διαδικασίες αναφοράς περιστατικών ή την επίσημη κυβερνητική λογοδοσία βάσει των άρθρων 21-23.
- ➜ *Προσθέστε έναν ρόλο υπευθύνου ασφάλειας και εφαρμόστε ροή εργασίας αναφοράς περιστατικών 24/72/30 ωρών για μια λειτουργική συμμόρφωση.*
- **Κανονισμός Ευρωπ. Επιτροπής (2024/2690)** – Το παρόν έγγραφο συνάδει εννοιολογικά με τα σύνολα ελέγχων που βασίζονται σε ISO, αλλά δεν περιλαμβάνει επίσημη δήλωση εφαρμογής και κριτήρια για την βαρύτητα των συμβάντων.
- ➜ *Υιοθετήστε ένα απλό πρότυπο SoA (service-oriented architecture) για να τεκμηριώσετε την εφαρμοσιμότητα του ελέγχου.*
- **Νόμος για την Ψηφιακή Επιχειρησιακή Ανθεκτικότητα (DORA - Digital Operational Resilience Act - 2022/2554)** – Απευθύνεται σε χρηματοπιστωτικούς οργανισμούς και απαιτεί δοκιμές από ΤΠΕ, αξιολόγηση κρίσιμων παραγόντων από τρίτους και λεπτομερή αναφορά, στοιχεία τα οποία δεν καλύπτονται εδώ.
- ➜ *Εάν ανήκετε στον χρηματοπιστωτικό τομέα, ενσωματώστε ένα ειδικό πλαίσιο DORA που περιλαμβάνει δοκιμές ανθεκτικότητας.*
- **Πράξη για την Κυβερνο-ανθεκτικότητα - Cyber Resilience Act (CRA)** – Ως οδηγός για τους χρήστες, το παρόν εγχειρίδιο δεν αναφέρεται σε υποχρεώσεις των κατασκευαστών προϊόντων ή στις σχεδιαστικές απαιτήσεις ασφάλειας.
- ➜ *Εφαρμόστε τις οδηγίες προμηθειών που λαμβάνουν υπόψη την Πράξη CRA κατά την επιλογή προμηθευτών υλικού και λογισμικού.*
- **Σχέδιο Δράσης της ΕΕ για την Ασφάλεια στον Κυβερνοχώρο για Νοσοκομεία και Υγειονομική περίθαλψη (2025)** – Η εστίαση του εγχειριδίου στην ευαισθητοποίηση συνάδει με τον προληπτικό πυλώνα αυτού του του Σχεδίου Δράσης, αλλά παραλείπει μηχανισμούς συντονισμού, ειδικά για την υγειονομική περίθαλψη.
- ➜ *Οι οργανισμοί υγειονομικής περίθαλψης θα πρέπει να ανατρέξουν στο μελλοντικό Κέντρο Υποστήριξης της ENISA και στις εθνικές επαφές CSIRT για την υγεία.*

Όλα τα παραδείγματα, τα εργαλεία και οι αναφορές σε αυτό το εγχειρίδιο προέρχονται από δημόσια διαθέσιμες πηγές της ΕΕ και διεθνείς πηγές για την κυβερνοασφάλεια (ENISA, CISA, ISC, FTC, ISO). Το περιεχόμενο έχει αναδιατυπωθεί για εκπαιδευτικούς σκοπούς και δεν αναπαράγει κανένα αποκλειστικό ή περιορισμένης πρόσβασης υλικό.

Πρωτότυπη έκδοση

Small Businesses- Strong Defences: a playbook for micro SMEs - Δεκέμβριος 2025

Μετάφραση στα Ελληνικά

Εθνική Συμμαχία για τις Ψηφιακές Δεξιότητες και την Απασχόληση (Ελλάδα)

Τμήμα Ψηφιακής Οικονομίας, Επενδύσεων και Ψηφιακών Δεξιοτήτων
Διεύθυνση Ψηφιακής Στρατηγικής
Γενική Διεύθυνση Ψηφιακής Διακυβέρνησης
Γενική Γραμματεία Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης
Υπουργείο Ψηφιακής Διακυβέρνησης

Επιμέλεια

Έμμη Ανδρουλάκη

Φεβρουάριος 2026