ΣΕΒ

Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΟΔΗΓΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΔΙΑΔΙΚΑΣΙΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ ΓΙΑ ΑΣΦΑΛΕΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ ΣΤΗΝ ΨΗΦΙΑΚΗ ΕΠΟΧΗ

ΔΕΚΕΜΒΡΙΟΣ 2023

ΛΙΓΑ ΛΟΓΙΑ ΓΙΑ ΤΟΝ ΟΔΗΓΟ

Ο Οδηγός Κυβερνοασφάλειας του ΣΕΒ έχει σκοπό να βοηθήσει πρακτικά τις ελληνικές επιχειρήσεις να πλοηγηθούν με ασφάλεια στο σύνθετο περιβάλλον ευκαιριών και κινδύνων της ψηφιακής εποχής, ανεξαρτήτως μεγέθους, κλάδου, γεωγραφίας, ή τεχνολογιών που χρησιμοποιούν. Η ταχεία ανάπτυξη των τεχνολογιών Πληροφορικής και η ραγδαία εξέλιξη του Διαδικτύου κάνουν ακόμα πιο απαραίτητη την άμυνα απέναντι σε απειλές.

Ο Οδηγός προσφέρει συμβουλές για τη συστηματική διαχείριση ψηφιακών κινδύνων, με **οφέλη** όπως:

- **Μείωση οικονομικού κόστους** από απώλεια, κλοπή ή καταστροφή δεδομένων
- **Διασφάλιση επιχειρησιακής συνέχειας** σε περίπτωση κυβερνοεπίθεσης
- **Προστασία περιουσιακών στοιχείων**, φήμης και δικτύου συνεργατών
- **Κατάκτηση ανταγωνιστικών πλεονεκτημάτων**
- **Βελτίωση συμμόρφωσης** με ισχύοντα κανονιστικά πλαίσια
- **Καλλιέργεια κουλτούρας** κυβερνοασφάλειας

Ο Οδηγός Κυβερνοασφάλειας για Επιχειρήσεις αναπτύχθηκε από την Επιτροπή Ψηφιακής Οικονομίας του ΣΕΒ με την ειδικότερη συνδρομή των Designia Insurance Brokers, Eurobank, Eurolife, Grant Thornton, Netcompany-Intrasoft, και Uni Systems. Αξιοποιεί επίσης πληροφορίες προερχόμενες από την Ευρωπαϊκή Υπηρεσία Κυβερνοασφάλειας και την Εθνική Αρχή Κυβερνοασφάλειας.

ΜΕΓΑΣ ΧΟΡΗΓΟΣ

Digital Academy

EUROBANK

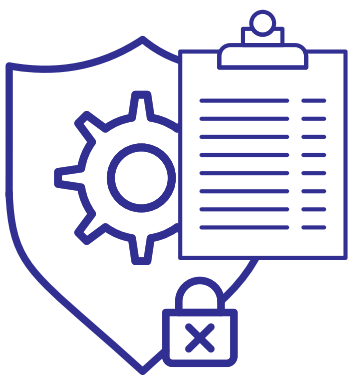
ΧΟΡΗΓΟΙ

CISCO COSMOTE Deloitte. Dynamic Integrated Solutions Google

ΟΜΑΔΑ ΕΡΓΑΣΙΑΣ

Designia EUROBANK EUROLIFE FFH A FAIRFAX Company Grant Thornton netcompany intrasoft uni systems

ΠΕΡΙΕΧΟΜΕΝΑ



Η ΣΗΜΑΣΙΑ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

ΤΙ ΕΙΝΑΙ κυβερνοασφάλεια:
Είναι άρρηκτο κομμάτι του ψηφιακού μετασχηματισμού και της επιχειρησιακής συνέχειας μιας επιχείρησης. Αναφέρεται σε ένα συνδυασμό τεχνολογιών, διαδικασιών και πρακτικών που είναι σχεδιασμένες για να προστατεύουν υπηρεσίες, δίκτυα, συσκευές, προγράμματα, δεδομένα, υλικά και άυλα περιουσιακά στοιχεία από μη εξουσιοδοτημένη πρόσβαση.

Κάθε **10 δευτερόλεπτα** συμβαίνει μια επίθεση ransomware.
Το **37%** των επιχειρήσεων που δέχτηκαν κυβερνοεκβιασμό το 2022 ήταν ΜμΕ.
Το **85%** των επιτυχημένων κυβερνοεπιθέσεων έχει προέλθει από ανθρώπινο λάθος.
$10,5τρισ. το εκτιμώμενο παγκόσμιο κόστος του κυβερνοεγκλήματος το 2025.

ΓΙΑΤΙ ΕΙΝΑΙ ΣΗΜΑΝΤΙΚΗ η θωράκιση από ψηφιακούς κινδύνους και απειλές:
Η διάρρηξη της ψηφιακής ασφάλειας μιας επιχείρησης επηρεάζει τους ανθρώπους της, τη συνέχεια των εργασιών της, τις υποχρεώσεις της απέναντι στις αρχές και το νόμο, τα περιουσιακά στοιχεία της, τη φήμη, τους πελάτες και τους προμηθευτές της, ακόμα και την επιβίωσή της.

ΚΟΣΤΗ ΕΝΟΣ ΠΕΡΙΣΤΑΤΙΚΟΥ ΚΥΒΕΡΝΟΕΠΙΘΕΣΗΣ

35,5%
δαπάνες ανίχνευσης της εισβολής

29,2%
κόστη διακοπής εργασιών

26,9%
δαπάνες αποκατάστασης και επαναφοράς

8%
δαπάνες ενημέρωσης τρίτων

ΟΙ ΚΙΝΔΥΝΟΙ ΠΟΥ ΣΥΝΔΕΟΝΤΑΙ ΜΕ ΤΗΝ ΨΗΦΙΑΚΗ ΑΣΦΑΛΕΙΑ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΧΕΙΑ

Δεν επαναλειτουργούν ποτέ **4** στις **10** ΜμΕ που υφίστανται απώλεια δεδομένων.

ΑΠΩΛΕΙΑ, ΚΛΟΠΗ Η ΑΛΛΟΙΩΣΗ ΔΕΔΟΜΕΝΩΝ

19% των επιθέσεων το 2022 αφορούσαν κλοπή δεδομένων και 11% τη διαρροή τους.

ΦΗΜΗ ΕΤΑΙΡΙΚΗ ΕΙΚΟΝΑ

40%-60% πιθανότητα να επηρεαστούν πελάτες, προμηθευτές και συνεργάτες μιας επιχείρησης από ένα περιστατικό κυβερνοασφάλειας

ΟΙΚΟΝΟΜΙΚΟΣ ΕΚΒΙΑΣΜΟΣ

Το ίδιο περιστατικό κλοπής δεδομένων μπορεί να καταλήξει σε διπλό ή τριπλό εκβιασμό (double/triple extortion):

Ο διπλός εκβιασμός αφορά την απαίτηση λύτρων για την «επιστροφή» δεδομένων που έχουν υποκλαπεί, αλλά και για την αποκρυπτογράφησή τους.

Σε περίπτωση τριπλού εκβιασμού, τίθεται και η απειλή επανάληψης της κυβερνοεπίθεσης.

ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ

57% των επιχειρήσεων που δέχτηκαν κυβερνοεπίθεση αύξησαν τις τιμές των αγαθών και υπηρεσιών τους για να ανταπεξέλθουν στο κόστος αποκατάστασης

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗΝ ΕΥΡΩΠΗ 2022

44%
ΤΩΝ ΕΠΙΘΕΣΕΩΝ RANSOMWARE ΠΑΓΚΟΣΜΙΩΣ

ΣΤΟΧΟΙ ΕΠΙΘΕΣΕΩΝ

25%
ΧΡΗΜΑΤΟΠΙΣΤΩΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

25%
ΕΠΑΓΓΕΛΜΑΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

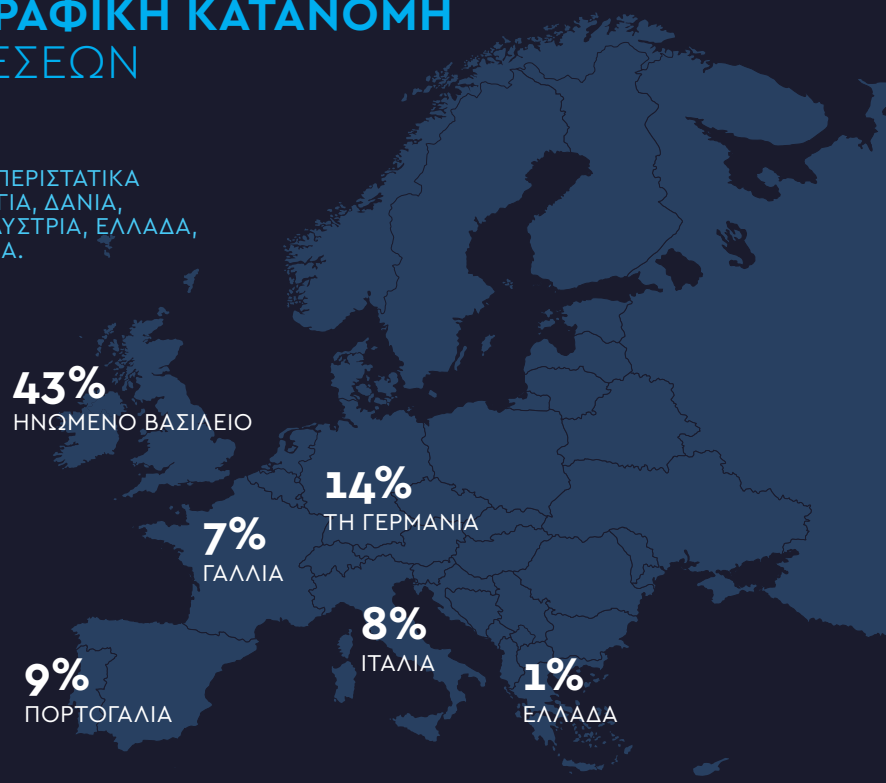
12%
ΒΙΟΜΗΧΑΝΙΑ

10%
ΕΝΕΡΓΕΙΑ

10%
ΥΓΕΙΑ

ΓΕΩΓΡΑΦΙΚΗ ΚΑΤΑΝΟΜΗ ΕΠΙΘΕΣΕΩΝ

ΛΙΓΟΤΕΡΑ ΠΕΡΙΣΤΑΤΙΚΑ ΣΕ ΝΟΡΒΗΓΙΑ, ΔΑΝΙΑ, ΕΛΒΕΤΙΑ, ΑΥΣΤΡΙΑ, ΕΛΛΑΔΑ, ΚΑΙ ΙΣΠΑΝΙΑ.



ΠΩΣ ΑΝΑΠΤΥΣΣΕΤΑΙ η κυβερνοάμυνα:

Η ετοιμότητα διαχείρισης των κυβερνοαπειλών αποτελεί επιχειρηματική απόφαση, και δεν απαιτεί μόνο τεχνική γνώση. Προϋποθέτει δέσμευση της Διοίκησης, στρατηγικό σχεδιασμό, προσαρμοστικότητα στις αλλαγές του περιβάλλοντος, και ικανότητα πρόβλεψης εξελίξεων.

ΟΛΑ ΑΥΤΑ ΜΕΣΑ ΑΠΟ **10 ΒΑΣΙΚΑ ΒΗΜΑΤΑ**

Με πληροφορίες από FBI, Deloitte, IBM, Uni Systems, WEF

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΟΔΗΓΟΣ
ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΒΗΜΑ 1°
Η ΑΞΙΟΛΟΓΗΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΩΣ ΣΗΜΕΙΟ ΕΚΚΙΝΗΣΗΣ

Τι είναι;

Πρόκειται για μια διαδικασία που χαρτογραφεί τα τρωτά σημεία της επιχείρησης και εξετάζει την επάρκεια και ωριμότητα των εφαρμοζόμενων διαδικασιών και τεχνολογιών να αντιμετωπίσουν κυβερνοαπειλές. Συμπληρωματικές αξιολογήσεις μπορούν να διεξαχθούν για τα επίπεδα ανθεκτικότητας σε επιθέσεις (πχ με ελέγχους ασφαλείας, όπως penetration tests, vulnerability assessments ή phishing tests), την κανονιστική συμμόρφωση του οργανισμού, την ευαισθητοποίηση προσωπικού, κ.α.

Γιατί είναι σημαντικό;

Τα ευρήματα της αξιολόγησης αποτελούν θεμέλιο για τη διαμόρφωση του στρατηγικού σχεδίου δράσης της επιχείρησης για την κυβερνοασφάλεια.

ΤΟ 26% ΤΩΝ ΤΡΩΤΩΝ ΣΗΜΕΙΩΝ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΗΘΗΚΑΝ ΣΕ ΜΙΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΗ ΤΟ 2022 ΗΤΑΝ ΗΔΗ ΓΝΩΣΤΑ ΣΤΗΝ ΕΠΙΧΕΙΡΗΣΗ.

Πώς γίνεται;

Κάθε επιχείρηση μπορεί να προβεί σε **αυτοαξιολόγηση** με την καθοδήγηση αξιόπιστων εργαλείων, όπως ο Οδηγός Αυτοαξιολόγησης της Εθνικής Αρχής Κυβερνοασφάλειας. Υπάρχουν, επίσης, ειδικά σχεδιασμένα εργαλεία αυτοαξιολόγησης για μεσαίες και μικρές επιχειρήσεις, όπως το ερωτηματολόγιο για την κυβερνο-ωριμότητα των ΜμΕ της Ευρωπαϊκής Υπηρεσίας για την Κυβερνοασφάλεια (ENISA).

Οδηγός Αυτοαξιολόγησης

Ερωτηματολόγιο ENISA

Μέσα από **προσομοιώσεις** περιστατικών κυβερνοεπιθέσεων, οι επαγγελματίες της κυβερνοασφάλειας (penetration testers / red teams) δοκιμάζουν τις κυβερνοάμυνες μιας επιχείρησης, και προτείνουν κατάλληλα βήματα για την ενίσχυσή τους.

Αξιολόγηση εστιασμένη σε εξειδικευμένες υπηρεσίες ή συστήματα πραγματοποιείται από ομάδες ειδικών, με εργαλεία που αποτυπώνουν την τρέχουσα κατάσταση και προτείνουν συγκεκριμένες δέσμες διορθωτικών ενεργειών, κατάλληλα προσαρμοσμένων στο περιβάλλον και τις ανάγκες της επιχείρησης.

Η ΑΞΙΟΛΟΓΗΣΗ ΜΠΟΡΕΙ ΝΑ ΠΡΑΓΜΑΤΟΠΟΙΗΘΕΙ ΕΙΤΕ ΕΣΩΤΕΡΙΚΑ, ΕΙΤΕ ΜΕ ΤΗ ΣΥΝΔΡΟΜΗ ΕΞΕΙΔΙΚΕΥΜΕΝΩΝ ΕΞΩΤΕΡΙΚΩΝ ΣΥΝΕΡΓΑΤΩΝ.

Με πληροφορίες από: IBM, Εθνική Αρχή Κυβερνοασφάλειας, ENISA, Netcompany-Intrasoft

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΟΔΗΓΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΒΗΜΑ 2°
ΚΑΤΑΡΤΙΣΗ ΟΔΙΚΟΥ ΧΑΡΤΗ ΔΡΑΣΗΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Τι είναι;

Πρόκειται για τις στρατηγικές και αρχιτεκτονικές ψηφιακής άμυνας, όπως και τις ενέργειες για τη διασφάλιση της συνέχειας των εργασιών μιας επιχείρησης σε περίπτωση κυβερνοεπίθεσης. Πυλώνας του είναι το σχέδιο αντιμετώπισης περιστατικών (Incident Response Plan).

6,9% ΤΩΝ ΕΛΛΗΝΙΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ VS. 25,5% ΣΤΗΝ ΕΕ ΠΡΟΧΩΡΗΣΑΝ ΣΕ ΕΠΙΚΑΙΡΟΠΟΙΗΣΗ ΤΟΥΣ ΣΤΡΑΤΗΓΙΚΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΟΥΣ ΤΟΥΣ ΤΕΛΕΥΤΑΙΟΥΣ 12 ΜΗΝΕΣ.

Γιατί είναι σημαντικό;

Γιατί επιτρέπει την αποτελεσματική διαχείριση κινδύνων, αλλά και το σχεδιασμό, την παρακολούθηση και την προσαρμογή κάθε δικλείδας ασφαλείας σε ενδογενείς και εξωγενείς απειλές, σύμφωνα με τις εκάστοτε ανάγκες της επιχείρησης.

Ως δυναμικό εργαλείο ψηφιακής άμυνας, μπορεί να επικαιροποιηθεί και να προσαρμοστεί στις ανάγκες της επιχείρησης, όπως έπειτα από επέκταση, αναδιοργάνωση, αλλαγές συστημάτων IT/OT, κ.α. Διευκολύνει την ενσωμάτωση νέων τεχνολογιών, εργαλείων και λύσεων ψηφιακής άμυνας, καθώς κακόβουλοι παράγοντες ανακαλύπτουν συνεχώς νέες τεχνικές επιθέσεων.

30% ΠΕΡΙΣΣΟΤΕΡΟ ΑΝΘΕΚΤΙΚΕΣ ΚΑΙ ΒΙΩΣΙΜΕΣ ΕΠΕΙΤΑ ΑΠΟ ΚΥΒΕΡΝΟΕΠΙΘΕΣΗ ΟΙ ΕΠΙΧΕΙΡΗΣΕΙΣ ΠΟΥ ΕΠΕΝΔΥΟΥΝ ΣΕ 3ΜΗΝΙΑΙΑ ΑΝΑΒΑΘΜΙΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ IT ΣΕ ΣΧΕΣΗ ΜΕ 2ΕΤΗ Η 3ΕΤΗ ΚΥΚΛΟ ΑΝΑΒΑΘΜΙΣΗΣ ΤΟΥΣ.

Τι περιλαμβάνει;

Ένας οδικός χάρτης δράσης διαμορφώνεται ανάλογα με τις ειδικές ανάγκες κάθε επιχείρησης, μέσα από κατάλληλες δράσεις σε διαστάσεις, όπως:

1. Προληπτική αναβάθμιση των τεχνολογιών ασφαλείας της επιχείρησης και επενδύσεις σε δυνατότητες εντοπισμού απειλών με υψηλή ακρίβεια
2. Προληπτική ενσωμάτωση τεχνολογιών κυβερνοασφάλειας σε ολοκληρωμένα συστήματα IT/OT
3. Πρωτόκολλα έγκαιρης αντίδρασης σε περιστατικά κυβερνοεπιθέσεων, και διαδικασίες για τη διακυβέρνηση θεμάτων κυβερνοασφάλειας
4. Ετοιμότητα για την ταχεία αποκατάσταση της καταστροφής, απώλειας ή βλάβης, με γνώμονα την επιχειρησιακή ανθεκτικότητα και συνέχεια
5. Κουλτούρα κυβερνοασφάλειας
6. Συνεχής ενσωμάτωση συμπερασμάτων από ασκήσεις ετοιμότητας, αλλά και από τυχόν περιστατικά κυβερνοασφάλειας
7. Συνεργασία με κατάλληλους ειδικούς για την υιοθέτηση σύγχρονων και κατάλληλων λύσεων για τις ανάγκες της επιχείρησης
8. Άλλες προληπτικές πρωτοβουλίες, όπως η επιδίωξη πιστοποιήσεων και ασφάλισης έναντι κυβερνοκινδύνων

ΤΟ ΕΓΧΕΙΡΙΔΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΤΗΣ ΕΘΝΙΚΗΣ ΑΡΧΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΑΠΟΤΕΛΕΙ ΕΝΑ ΧΡΗΣΙΜΟ ΕΡΓΑΛΕΙΟ ΓΙΑ ΤΗΝ ΚΑΤΑΡΤΙΣΗ ΕΝΟΣ ΟΔΙΚΟΥ ΧΑΡΤΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ.

Εγχειρίδιο Κυβερνοασφάλειας

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΙ **ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ**

Η ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ (ΤΝ) ΑΠΟΤΕΛΕΙ ΕΝΑ ΑΠΟ ΤΑ ΠΟΛΛΑ ΕΠΙΠΕΔΑ ΜΙΑΣ ΣΥΝΟΛΙΚΗΣ ΠΡΟΣΕΓΓΙΣΗΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΜΙΑΣ ΕΠΙΧΕΙΡΗΣΗΣ.

Πώς συνδέεται με την κυβερνοασφάλεια;

Η Τεχνητή Νοημοσύνη (ΤΝ) μπορεί να χρησιμοποιηθεί τόσο για την ενίσχυση της κυβερνοασφάλειας, όσο και για την απειλή της. Για το λόγο αυτό, χρειάζεται συνδυασμός εφαρμογών ΤΝ που βελτιώνουν τις ψηφιακές άμυνες της επιχείρησης, και παράλληλα προσφέρουν θωράκιση έναντι κυβερνοαπειλών που δημιουργούνται μέσω κακόβουλης χρήσης της **ΤΝ**.

108 ΛΙΓΟΤΕΡΕΣ ΗΜΕΡΕΣ, ΚΑΤΑ Μ.Ο., ΓΙΑ ΝΑ ΕΝΤΟΠΙΣΟΥΝ ΚΑΙ ΝΑ ΔΙΑΧΕΙΡΙΣΤΟΥΝ ΚΥΒΕΡΝΟΑΠΕΙΛΕΣ ΧΡΕΙΑΖΟΝΤΑΙ ΟΙ ΕΠΙΧΕΙΡΗΣΕΙΣ ΠΟΥ ΧΡΗΣΙΜΟΠΟΙΟΥΝ ΤΝ ΚΑΙ ΑΥΤΟΜΑΤΙΣΜΟΥΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΤΟΥΣ, ΣΕ ΣΧΕΣΗ ΜΕ ΕΚΕΙΝΕΣ ΠΟΥ ΔΕΝ ΥΙΟΘΕΤΟΥΝ ΤΕΤΟΙΕΣ ΛΥΣΕΙΣ.

ΤΥΠΙΚΟΙ ΚΙΝΔΥΝΟΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΑΠΟ ΚΑΚΟΒΟΥΛΗ ΧΡΗΣΗ **ΤΝ**

Επιθέσεις με Χρήση ΤΝ	Αξιοποιώντας πολύπλοκες τεχνικές μηχανικής μάθησης και αυτοματοποίησης για επιθέσεις μεγάλης κλίμακας ή διακοπής υποδομών.
Κοινωνική Μηχανική	Επιτυγχάνουν την αποκάλυψη προσωπικών ή ευαίσθητων επιχειρηματικών πληροφοριών, ή ακόμα και την εκτέλεση ανεπιθύμητων ενεργειών (πχ μεταφορές μεγάλων χρηματικών ποσών).
Αυξημένος Κίνδυνος Phishing	Με πιο πειστικές και προηγμένες επιθέσεις, που παράγουν αληθοφανή αλλά πλαστά μηνύματα ή ιστοσελίδες που παραπλανούν τους χρήστες.
Διακίνηση Ευαίσθητων Πληροφοριών	Αφού η ΤΝ κάνει ευκολότερο τον εντοπισμό και την εξαγωγή πληροφοριών, που στη συνέχεια μπορούν να χρησιμοποιηθούν κακόβουλα.

Χρειάζονται επιπλέον βήματα ψηφιακής άμυνας;

Οι κυβερνοκίνδυνοι που πηγάζουν από τη χρήση της ΤΝ εξελίσσονται ραγδαία, πράγμα που απαιτεί ευαισθητοποίηση και συνεχή ενημέρωση των εργαζομένων για τη σχέση της κυβερνοασφάλειας με την ΤΝ. Είναι επίσης σημαντική η μέριμνα ενός σχεδίου αντιμετώπισης περιστατικών για σύνθετες επιθέσεις με βάση την ΤΝ, και η στενότερη συνεργασία με ειδικούς για κάθε αναγκαία επικαιροποίηση και προσαρμογή του οδικού χάρτη για την κυβερνοασφάλεια της επιχείρησης.

21% ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΠΑΓΚΟΣΜΙΩΣ ΠΟΥ ΕΧΟΥΝ ΕΝΣΩΜΑΤΩΣΕΙ ΛΥΣΕΙΣ GENAI ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΤΟΥΣ ΤΟΥΣ ΤΕΛΕΥΤΑΙΟΥΣ ΜΗΝΕΣ, ΔΙΑΠΙΣΤΩΝΟΥΝ ΗΔΗ ΩΦΕΛΕΙΕΣ.

Με πληροφορίες από: CISCO, Deloitte Insights, Eurostat, Grant Thornton, IBM, Netcompany-Intrasoft, PwC

ΒΗΜΑ 3ο
ΜΗΧΑΝΙΣΜΟΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Τι αφορά;

Πρόκειται για τις εσωτερικές πολιτικές και διαδικασίες λήψης αποφάσεων, την ανάθεση αρμοδιοτήτων και ευθυνών, και την καθιέρωση πρωτοκόλλων δράσης κάθε ρόλου για την αντιμετώπιση περιστατικών και την ειδοποίηση παραβίασης δεδομένων.

Γιατί είναι σημαντικό;

Επειδή η ομαδικότητα και η ενεργοποίηση διαφορετικών στελεχών εντός της επιχείρησης – από την ανώτερη διοίκηση και το νομικό τμήμα, μέχρι τα τμήματα IT, παραγωγής, ανθρώπινου δυναμικού, επικοινωνίας, κα. – είναι η βάση για την αποτελεσματική διαχείριση κυβερνοκινδύνων.

Η ΕΝΔΟΕΠΙΧΕΙΡΗΣΙΑΚΗ ΣΥΝΕΡΓΑΣΙΑ ΓΙΑ ΤΗΝ ΕΦΑΡΜΟΓΗ ΕΝΟΣ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΤΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΒΕΛΤΙΩΝΕΙ ΤΗΝ ΚΥΒΕΡΝΟΑΝΘΕΚΤΙΚΟΤΗΤΑ ΜΙΑΣ ΕΠΙΧΕΙΡΗΣΗΣ

92% ΤΩΝ ΟΡΓΑΝΙΣΜΩΝ ΠΟΥ ΕΠΕΝΔΥΟΥΝ ΣΤΟΥΣ ΑΝΘΡΩΠΟΥΣ, ΣΤΙΣ ΔΙΑΔΙΚΑΣΙΕΣ ΚΑΙ ΤΗΝ ΤΕΧΝΟΛΟΓΙΑ ΔΙΑΘΕΤΟΥΝ ΥΨΗΛΕΣ ΔΥΝΑΤΟΤΗΤΕΣ ΕΝΤΟΠΙΣΜΟΥ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΚΥΒΕΡΝΟΑΠΕΙΛΩΝ

Πώς γίνεται;

Ένας μηχανισμός διακυβέρνησης της κυβερνοσφάλειας θέτει ρυθμίσεις αντιμέτρων ασφαλείας, ρόλους και αρμόδιες ομάδες ή άτομα για την παρακολούθηση απειλών, και διαδικασίες τακτικών αναφορών και ενημερώσεων με την αυτόματη αποστολή emails στα κατάλληλα πρόσωπα. Προβλέπει, επίσης, τη συμμετοχή της Διοίκησης και την ενημέρωσή της για τους κινδύνους και τα κόστη των απειλών, τις υποχρεώσεις συμμόρφωσης με κανονισμούς, την αποτίμηση του κόστους λύσεων OPEX ανά εργαζόμενο, και τις δυνατότητες συνεργασίας με εξειδικευμένους συμβούλους ασφαλείας.

x3 ΠΙΟ ΣΥΣΤΗΜΑΤΙΚΗ Η ΣΥΜΜΕΤΟΧΗ ΤΗΣ ΔΙΟΙΚΗΣΗΣ ΣΤΟ ΣΧΕΔΙΑΣΜΟ ΔΙΑΔΙΚΑΣΙΩΝ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΚΑΙ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ ΣΕ ΕΠΙΧΕΙΡΗΣΕΙΣ ΜΕ ΥΨΗΛΗ ΩΡΙΜΟΤΗΤΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ, ΣΕ ΣΧΕΣΗ ΜΕ ΤΙΣ ΛΙΓΟΤΕΡΟ ΩΡΙΜΕΣ.

ΕΝΔΕΙΚΤΙΚΕΣ ΔΙΑΔΙΚΑΣΙΕΣ, ΕΥΘΥΝΕΣ ΚΑΙ ΡΟΛΟΙ
ΣΕ ΕΝΑ ΣΥΣΤΗΜΑ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Υπεύθυνος κυβερνοσφάλειας ή ασφαλείας ΤΠΕ (CISO)

Καταρτίζει το σχέδιο δράσης για την κυβερνοασφάλεια, χωρίς να θέτει προσκόμματα στη λειτουργία της επιχείρησης. Διευθύνει τη διαδικασία αξιολόγησης και παρακολουθεί το σχέδιο δράσης κυβερνοασφάλειας. Ενημερώνει όλο τον οργανισμό για τις εξελίξεις στη στρατηγική κυβερνοασφάλειας, σε συνεργασία με τα αρμόδια πρόσωπα

Υπεύθυνος συστημάτων ΤΠΕ (CIO)

Συνεργάζεται με τη Διοίκηση και καθοδηγεί την ανάπτυξη του προγράμματος κυβερνοασφάλειας και των απαραίτητων ψηφιακών δυνατοτήτων της επιχείρησης. Διασφαλίζει την εναρμόνιση της στρατηγικής κυβερνοασφάλειας με την επιχειρηματική στρατηγική και τις προτεραιότητες της Διοίκησης. Επικοινωνεί την αποστολή, τη στρατηγική και τους στόχους σε ολόκληρο τον οργανισμό.

Εξωτερικοί συνεργάτες, Ομάδες επαγγελματιών ασφαλείας (Cybersecurity professionals)

Αξιολογούν το περιβάλλον απειλών, την επιχειρησιακή λειτουργία και την τεχνολογική ωριμότητα της επιχείρησης, για να σχεδιάσουν πολιτικές ασφαλείας ΤΠΕ, και να ενεργοποιήσουν την εφαρμογή και τις μεθόδους διακυβέρνησής τους στην πράξη. Μπορεί να εμπλακούν και στην ανάπτυξη σχετικών δεξιοτήτων, στο βαθμό που είναι απαραίτητο.

Ομάδες ή πρόσωπα με αρμοδιότητες για τις εφαρμογές και το λογισμικό

... που εστιάζουν στην εφαρμογή και λειτουργία του προγράμματος ασφαλείας και των δραστηριοτήτων της επιχείρησης.

Ομάδες ή πρόσωπα με αρμοδιότητες για συστήματα και τεχνολογίες ΤΠΕ στα επί μέρους τμήματα της επιχείρησης

... που εργάζονται για την έγκαιρη κατανόηση των απαιτήσεων κυβερνοασφάλειας σε ολόκληρη την επιχείρηση

Ομάδες ή πρόσωπα με αρμοδιότητες για τις υποδομές και τα επιχειρησιακά συστήματα

... με έμφαση τους κεντρικούς άξονες του εκάστοτε προγράμματος ασφαλείας.

Ομάδες ή πρόσωπα με αρμοδιότητες διαχείρισης ασφάλειας και κινδύνων

... και ειδικότερα την ενσωμάτωση της κυβερνοασφάλειας στο συνολικό πρόγραμμα και τις διαδικασίες για τη διακυβέρνηση κυβερνοασφάλειας, κινδύνων και συμμόρφωσης.

Ομάδες ή πρόσωπα με αρμοδιότητες διαχείρισης έργων (PMO)

... με στόχο τη διευκόλυνση των απαραίτητων συνεργασιών και προσαρμογών στην εφαρμογή και το συντονισμό του προγράμματος ασφάλειας. Διαχειρίζονται τους διαθέσιμους πόρους, μειώνουν τους κινδύνους και διευκολύνουν τις επιχειρησιακές λειτουργίες, ώστε να τηρούνται οι διαδικασίες του συστήματος διακυβέρνησης της κυβερνοασφάλειας

Ρόλοι και αρμοδιότητες ανά διαδικασία μπορούν να αποτυπωθούν και να παρακολουθούνται σε πίνακες RACI (Responsible, Accountable, Consulted, Informed).

ΠΑΡΑΔΕΙΓΜΑ ΠΙΝΑΚΑ RACI
ΓΙΑ ΤΗ ΔΙΑΔΙΚΑΣΙΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ

Βήμα	Help Desk	Συντονιστής Περιστατικών Κυβερνοασφάλειας	Τμήμα IT	Άμεσα επηρεαζόμενο Τμήμα	Νομικό Τμήμα
Καταγραφή περιστατικού	AR	CI	I	I	
Διεξαγωγή αρχικής διαλογής		AR	C	I	I
Καθορισμός σοβαρότητας		AR		CI	CI
Καθορισμός επόμενων δράσεων		AR	C	I	
Επίλυση περιστατικού βάση τακτικής διαδικασίας	I	I	AR	CI	CI

Με πληροφορίες από: CISCO, Deloitte, Gartner

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΟΔΗΓΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΒΗΜΑ 4° ΘΩΡΑΚΙΣΗ ΕΞΟΠΛΙΣΜΟΥ, ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ

Τι αφορά;

Όλα τα συνδεδεμένα πληροφοριακά και επιχειρησιακά συστήματα (IT/OT) και συσκευές, μιας και αποτελούν εν δυνάμει τρωτά σημεία, καθώς ο ψηφιακός μετασχηματισμός άρει τα στεγανά μεταξύ λειτουργιών, εξοπλισμού, διαδικασιών, συστημάτων και ροών δεδομένων.

Γιατί είναι σημαντικό;

Κάθε συνδεδεμένη συσκευή αποτελεί δυνητική δίοδο πρόσβασης στο δίκτυο μιας επιχείρησης, τις λειτουργίες και τα δεδομένα της. Η ψηφιακή θωράκιση του εξοπλισμού και των συστημάτων μιας επιχείρησης είναι ανάλογη με την προστασία κάθε σημείου εισόδου σε ένα χώρο.

41% ΒΕΛΤΙΩΜΕΝΕΣ ΔΥΝΑΤΟΤΗΤΕΣ ΕΝΤΟΠΙΣΜΟΥ ΑΠΕΙΛΩΝ ΜΕ ΤΗ ΧΡΗΣΗ ΟΛΟΚΛΗΡΩΜΕΝΩΝ ΣΥΣΤΗΜΑΤΩΝ ΓΙΑ ΤΟΝ ΠΡΟΣΔΙΟΡΙΣΜΟ ΚΡΙΣΙΜΩΝ ΠΕΡΙΟΥΣΙΑΚΩΝ ΣΤΟΙΧΕΙΩΝ ΚΑΙ ΚΙΝΔΥΝΩΝ (CRITICAL ASSETS AND RISKS)

PHISHING

16%
των επιτυχημένων επιθέσεων του 2023 παγκοσμίως εκδηλώθηκαν μέσω phishing

94%
των κακόβουλων προγραμμάτων παραδίδονται με email

62%
των επιθέσεων μέσω phishing χρησιμοποιούν επισυναπτόμενα αρχεία

3εκ.
αποστολές emails μέσα από 12.000 παραβιασμένους λογαριασμούς ηλεκτρονικής αλληλογραφίας το 2021

> 80%
των περιπτώσεων hacking χρησιμοποιούν το phishing μέσω email ως κύριο φορέα μόλυνσης

$183
το κόστος ανάκτησης δεδομένων ανά πελάτη έπειτα από περιστατικό

15%
των περιστατικών του 2023 προέκυψε με υποκλοπή κωδικών πρόσβασης (credentials harvesting)

Πώς γίνεται;

ΒΗΜΑΤΑ ΠΡΟΣΤΑΣΙΑΣ ΑΠΟ ΣΥΝΗΘΙΣΜΕΝΕΣ, ΚΑΘΗΜΕΡΙΝΕΣ ΑΠΕΙΛΕΣ

	Γιατί	Ενέργεια	Μέθοδος
Ασφάλεια passwords	Τα αδύναμα passwords είναι εύκολη «λεία». Αν κλαπούν, μπορούν να χρησιμοποιηθούν σε πολλούς λογαριασμούς	• Δυνατά και διαφορετικά passwords για κάθε λογαριασμό • Διαφορετικά προσωπικά και επαγγελματικά passwords • Πιστοποίηση πολλαπλού παράγοντα (multi-factor authentication / MFA) όπου παρέχεται	• Passwords με συνδυασμό γραμμάτων, αριθμών και συμβόλων • Αποφυγή κοινών λέξεων, γενεθλίων, ονομάτων παιδιών, κλπ • Χρήση password manager για τη διαχείριση και υπενθύμιση κωδικών, εφόσον είναι μοναδικοί και ισχυροί
Ασφάλεια email	Είναι ο συνηθέστερος τρόπο εκδήλωσης απειλών	• Ιδιαίτερη προσοχή με emails από αγνώστους: μην πατάτε links και μην κατεβάζετε επισυναπτόμενα. • Roll-over στο email του αποστολέα, ώστε να εμφανιστεί η πλήρης ηλεκτρονική διεύθυνση	• Προσπάθεια επιβεβαίωσης εγκυρότητας του email, και επικοινωνία με το τμήμα IT, ή τον αποστολέα, ειδικά όταν καλεί σε αλλαγή διαδικασιών (πχ νέος λογαριασμός κατάθεσης)
Ενημερώσεις ασφαλείας	Οι ευπάθειες παλαιών λειτουργικών συστημάτων και προγραμμάτων αποτελούν κερκόπορτες	• Τακτικές ενημερώσεις ασφαλείας λειτουργικών συστημάτων, browsers και όλων των εφαρμογών	• Ενεργοποίηση αυτόματων ενημερώσεων
Χρήση δημόσιων Wi-Fi	Οι πληροφορίες που κυκλοφορούν στα δημόσια Wi-Fi μπορούν να ανιχνευθούν εύκολα, ειδικά όταν ζητείται κωδικός πρόσβασης	• Αποφυγή σύνδεσης σε δημόσια WiFi χωρίς λόγο • Αφαίρεση δυνατότητας αυτόματης επανασύνδεσης σε δημόσια WiFi	• Χρήση σύνδεσης VPN για επιπλέον ασφάλεια, εφόσον είναι δυνατόν • Περιορισμός online ενεργειών κατά τη διάρκεια μιας Wi-Fi σύνδεσης, και ειδικά των σημαντικών ενεργειών

	Γιατί	Ενέργεια	Μέθοδος
Προστασία συσκευών και δεδομένων	Η κλοπή συσκευών μπορεί να οδηγήσει σε υποκλοπή κωδικών, εγγράφων και άλλων πληροφοριών, κάνοντας απαραίτητη την φυσική προστασία τους	• Πλήρης απενεργοποίηση συσκευών όταν δεν χρησιμοποιούνται, και αποθήκευσή τους σε ασφαλές μέρος για την αποφυγή εύκολης πρόσβασης • Χρήση κρυπτογράφησης όπου εφικτό • Αποφυγή χρήσης δωρεάν λύσεων λογισμικού, καθώς δεν προορίζονται για εταιρική χρήση, και συνήθως δεν παρέχουν υποστήριξη ή εγγύηση καλής λειτουργίας σε περίπτωση ανάγκης	• Αξιοποίηση δυνατοτήτων λειτουργικού συστήματος για κρυπτογράφηση (πχ BitLocker, FireVault) • Κρυπτογράφηση εξωτερικών συσκευών (πχ δίσκοι USB) • Λειτουργία δικλείδων ασφαλείας σε κάθε επίπεδο αποθήκευσης, επεξεργασίας και ροής δεδομένων • Διενέργεια ολοκληρωμένης μελέτης ασφαλείας, ή ενός penetration test
Αντίγραφα ασφαλείας	Η καταστροφή ή απώλεια δεδομένων μπορεί να επέλθει από κάποιο Ransomware, σφάλμα λογισμικού ή υλικού, αλλά και ακούσια ή εκούσια διαγραφή από κάποιον εργαζόμενο	Αξιολόγηση συστημάτων και θέσπιση προγράμματος λήψεως και δοκιμής αντιγράφων ασφαλείας	Χρήση λογισμικών backup και διατήρηση αντιγράφων σε ασφαλή χώρο και διαφορετικές τοποθεσίες – π.χ. σε κάποιον εξωτερικό πάροχο ή το cloud • Τακτική δοκιμή δυνατότητας επαναφοράς πληροφοριών από τα αντίγραφα • Αξιολόγηση δυνατότητας διενέργειας μελέτης για την επιχειρησιακή συνέχεια στις περισσότερες περιπτώσεις απώλειας δεδομένων

Με πληροφορίες από: Barracuda, CISCO, Designia Insurance Brokers, IBM, Uni Systems

ΒΗΜΑ 5° ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΠΡΟΣΩΠΙΚΟΥ

85% ΤΩΝ ΕΠΙΤΥΧΗΜΕΝΩΝ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ ΕΧΕΙ ΠΡΟΕΛΘΕΙ ΑΠΟ ΑΝΘΡΩΠΙΝΟ ΛΑΘΟΣ. Η ΕΠΕΝΔΥΣΗ ΣΤΗΝ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΤΟΥ ΠΡΟΣΩΠΙΚΟΥ ΣΕ ΘΕΜΑΤΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΕΙΝΑΙ ΕΞΙΣΟΥ ΣΗΜΑΝΤΙΚΗ ΜΕ ΤΙΣ ΕΠΕΝΔΥΣΕΙΣ ΣΤΑ ΤΕΧΝΟΛΟΓΙΚΑ ΜΕΣΑ

Τι αφορά;

Καθώς το ανθρώπινο λάθος αποτελεί το συνηθέστερο παράγοντα επιτυχίας μιας κυβερνοεπίθεσης, η ενημέρωση και ευαισθητοποίηση των στελεχών για τις ψηφιακές απειλές είναι απαραίτητο βήμα για την ενίσχυση της ανθεκτικότητάς της απέναντι σε κυβερνοαπειλές.

Γιατί είναι σημαντικό;

Η κουλτούρα κυβερνοασφάλειας και η συνολική εγρήγορση για τους κυβερνοκινδύνους είναι οριζόντια ανάγκη για τις επιχειρήσεις. Οι ψηφιακές λύσεις ενσωματώνονται στην καθημερινότητα όλων των εργαζομένων, και δεν αφορούν μόνο τα τμήματα IT.

75% ΤΩΝ ΕΡΓΑΖΟΜΕΝΩΝ ΘΑ ΧΕΙΡΙΖΟΝΤΑΙ Ή ΘΑ ΔΗΜΙΟΥΡΓΟΥΝ ΤΕΧΝΟΛΟΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΕΚΤΟΣ ΤΗΣ ΕΠΙΒΛΕΨΗΣ ΤΟΥ ΤΜΗΜΑΤΟΣ IT ΜΕΧΡΙ ΤΟ 2027, ΑΠΟ 41% ΤΟ 2022

350% ΠΙΟ ΣΥΧΝΕΣ ΟΙ ΕΠΙΘΕΣΕΙΣ ΚΟΙΝΩΝΙΚΗΣ ΜΗΧΑΝΙΚΗΣ (SOCIAL ENGINEERING) ΣΕ ΒΑΡΟΣ ΕΡΓΑΖΟΜΕΝΩΝ ΜΙΚΡΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΣΕ ΣΧΕΣΗ ΜΕ ΕΠΙΧΕΙΡΗΣΕΙΣ ΜΕ >100 ΕΡΓΑΖΟΜΕΝΟΥΣ (ΗΠΑ, 2021)

Τι περιλαμβάνει;

Η κουλτούρα κυβερνοασφάλειας ως αναπόσπαστο μέρος της ευρύτερης ψηφιακής κουλτούρας μιας επιχείρησης, συμπεριλαμβάνει και τις σχέσεις με τους συνεργάτες της.

ΧΤΙΖΟΝΤΑΣ ΚΟΥΛΤΟΥΡΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

01 **Πρωτοβουλία Διοίκησης για το σύνολο του οργανισμού.**

02 **Εκπαίδευση επιλεγμένων στελεχών με κρίσιμους ρόλους, όπως στη Διοίκηση και το Λογιστήριο.**

03 **Τακτικές ασκήσεις, σεμινάρια και γενικές ενημερώσεις σε όλα τα τμήματα της επιχείρησης, σε συνεργασία με ειδικούς, ή μέσα από δωρεάν πλατφόρμες εκπαίδευσης.**

04 **Μόνιμες υπενθυμίσεις επαγρύπνησης, π.χ. αφίσες στους κοινόχρηστους χώρους.**

05 **Συνεργασία με πελάτες και προμηθευτές για την υιοθέτηση εναρμονισμένων πρακτικών.**

Με πληροφορίες από: Barracuda, CISCO, Designia Insurance Brokers, ENISA, IBM, ISACA

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΟΔΗΓΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΒΗΜΑ 6°
ΕΝΤΑΞΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΣΤΟ ΣΧΕΔΙΟ ΔΙΑΣΦΑΛΙΣΗΣ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ

Τι αφορά;

Ένα πλάνο επιχειρησιακής συνέχειας (Business Continuity Plan – BCP) εστιάζει σε προληπτικές δράσεις για τη διασφάλιση ή διευκόλυνση της λειτουργίας μιας επιχείρησης σε περίπτωση έκτακτων συνθηκών που θέτουν σε κίνδυνο τη συνέχειά της.

ΑΠΑΙΤΟΥΝΤΑΙ ΤΟΥΛΑΧΙΣΤΟΝ 23 ΗΜΕΡΕΣ ΓΙΑ ΤΗΝ ΑΝΑΚΑΜΨΗ ΕΡΓΑΣΙΩΝ ΕΠΕΙΤΑ ΑΠΟ ΕΠΙΘΕΣΗ RANSOMWARE

Γιατί είναι σημαντικό;

Ο κίνδυνος κυβερνοεπίθεσης αποτρέπεται, μετριάζεται ή γίνεται διαχειρίσιμος αν συμπεριληφθεί στο σχέδιο επιχειρησιακής συνέχειας. Αυτό διευκολύνει:

- τη διαρκή **συμμόρφωση** της επιχείρησης με τις υποχρεώσεις της προς τις αρχές και τρίτους σε θέματα κυβερνοασφάλειας και προστασίας δεδομένων
- τη συνολική διαχείριση του περιστατικού σύμφωνα με **ασφαλή και έγκυρα πρωτόκολλα,** χάρη στην εξοικείωση της επιχείρησης με σχετικά διεθνή πρότυπα και πιστοποιήσεις
- την ενίσχυση της ευρύτερης ψηφιακής **κουλτούρας**
- τη **μείωση του κόστους ανάκαμψης** από ένα περιστατικό κυβερνοασφάλειας, πχ με την αξιοποίηση προϊόντων κυβερνοασφάλισης ή την ενεργοποίηση δικλείδων που επιτρέπουν την πρόσβαση σε δεδομένα και πληροφορίες σε σύντομο χρόνο
- την **προστασία του εταιρικού brand,** μέσα από κατάλληλη επικοινωνιακή διαχείριση ενός πλήγματος

ΠΕΡΙΠΟΥ 50% ΤΩΝ ΜΜΕ ΠΟΥ ΥΦΙΣΤΑΝΤΑΙ ΑΠΩΛΕΙΑ ΔΕΔΟΜΕΝΩΝ, ΠΑΥΟΥΝ ΤΗ ΛΕΙΤΟΥΡΓΙΑ ΤΟΥΣ ΕΝΤΟΣ 2 ΕΤΩΝ.

Τι περιλαμβάνει;

Την προετοιμασία της αντίδρασης σε περίπτωση πλήγματος, και προδραστικές ενέργειες που θα επιτρέψουν στην επιχείρηση να ανακάμψει γρήγορα, με το χαμηλότερο δυνατό κόστος. Μπορεί να αναπτυχθεί στο εσωτερικό της επιχείρησης, ή και σε συνεργασία με κατάλληλους εξωτερικούς συνεργάτες και εμπειρογνώμονες.

ΚΑΘΕ ΠΛΑΝΟ ΕΠΙΧΕΙΡΗΣΙΑΚΗΣ ΣΥΝΕΧΕΙΑΣ ΠΡΟΒΛΕΠΕΙ ΕΝΕΡΓΕΙΕΣ ΣΕ ΤΕΣΣΕΡΕΙΣ ΔΙΑΣΤΑΣΕΙΣ:

PLAN

Σχεδιασμός σεναρίων γύρω από ανθρώπους, διαδικασίες, εγκαταστάσεις και προμηθευτές.

DO

Ανάπτυξη κατάλληλων μέτρων δράσης για κάθε σενάριο.

CHECK

Δοκιμή, έλεγχος, προσομοίωση και επαλήθευση της αποτελεσματικότητας των μέτρων.

ACT

Δράση για τη διόρθωση και προσαρμογή των μέτρων.

Με πληροφορίες από: CISCO, Gartner, IBM, Verizon

ΒΗΜΑ 7°
ΕΝΕΡΓΟΠΟΙΗΣΗ ΣΧΕΔΙΟΥ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ (Incident Response Plan)

Η ΕΠΕΝΔΥΣΗ ΣΤΗΝ ΠΡΟΕΤΟΙΜΑΣΙΑ ΓΙΑ ΜΙΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΗ ΑΠΟΔΙΔΕΙ ΠΟΛΛΑΠΛΑ ΟΦΕΛΗ ΣΤΗΝ ΠΡΑΞΗ.

Τι αφορά;

Καθορίζει τις ενέργειες προετοιμασίας, διαχείρισης και ανάκαμψης από μια κυβερνοεπίθεση. Εάν καμφθούν οι ψηφιακές άμυνες, και οι ενέργειες προετοιμασίας δεν αποδώσουν, η επιχείρηση καλείται να προχωρήσει σε ενέργειες διαχείρισης του περιστατικού και των επιπτώσεών του.

Γιατί είναι σημαντικό;

Όταν η επιχείρηση βρίσκεται σε κίνδυνο, και δεν λειτουργεί υπό κανονικές συνθήκες, η ενεργοποίηση της αντιμετώπισης περιστατικών:

- επιδιώκει ανάσχεση της περαιτέρω κακόβουλης διείσδυσης (containment)
- περιορίζει τις οικονομικές και άλλες επιπτώσεις του περιστατικού
- διασφαλίζει την τήρηση των νομικών υποχρεώσεων έναντι τρίτων
- Επίσης, έτσι, η επιχείρηση πληροί μια απαραίτητη δέσμευση ενός συμβολαίου κυβερνοασφάλισης

Πώς γίνεται;

Με το σχεδιασμό ενεργειών προετοιμασίας για την αντιμετώπιση κυβερνοεπίθεσης, ενεργειών διαχείρισης του περιστατικού, και ενεργειών ανάκαμψης από αυτό. Εφόσον η επιχείρηση δεχτεί επίθεση, τίθενται σε δράση οι ενέργειες διαχείρισης και ανάκαμψης.

ΕΝΕΡΓΕΙΕΣ ΠΟΥ ΕΝΤΑΣΣΟΝΤΑΙ ΣΕ ΕΝΑ ΣΧΕΔΙΟ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΠΕΡΙΣΤΑΤΙΚΩΝ

Ενέργειες προετοιμασίας

- ορισμός υπεύθυνου κυβερνοασφάλειας,
- κατάρτιση και εφαρμογή πολιτικών για τους ανθρώπους, τις διαδικασίες, τις εγκαταστάσεις και τους προμηθευτές,
- δημιουργία αντιγράφων ασφαλείας δεδομένων και πληροφοριών
- εκπαίδευση και ευαισθητοποίηση του προσωπικού
- επιλογή εξειδικευμένου συνεργάτη για τη διαχείριση σύνθετων περιστατικών

Ενέργειες διαχείρισης

- απομόνωση συστημάτων που έχουν πληγεί
- αναγνώριση του μέσου της επίθεσης
- προσδιορισμός έκτασης περιστατικού
- απόφαση για εσωτερική διαχείριση ή την αναζήτηση συνεργασίας εξειδικευμένων συμβούλων
- παρακολούθηση για τυχόν επανεμφάνιση του προβλήματος

Ενέργειες ανάκαμψης

- ενημέρωση όλων των εμπλεκόμενων, εντός και εκτός της επιχείρησης
- αλλαγή κωδικών πρόσβασης σε όλες τις συσκευές που έχουν επηρεαστεί
- αποκατάσταση προβλήματος
- επανεγκατάσταση λογισμικού και δεδομένων από αξιόπιστα αντίγραφα

Με πληροφορίες από: Gartner, IBM, Verizon

ΒΗΜΑ 8°
ΥΙΟΘΕΤΗΣΗ ΠΡΟΤΥΠΩΝ ΚΑΙ ΠΙΣΤΟΠΟΙΗΣΕΩΝ

Τι είναι;

Πρόκειται για κανόνες και κατευθύνσεις που πηγάζουν από Ευρωπαϊκά πρότυπα και Οδηγίες, όπως το GDPR και το NIS 2, με έμφαση στην ασφάλεια πληροφοριών, τη διαχείριση κινδύνων και την προστασία της ιδιωτικότητας. Το υφιστάμενο πλαίσιο κανόνων εστιάζει στην ανάπτυξη και εφαρμογή στρατηγικών, πρακτικών και τεχνολογιών που μετριάζουν τους κινδύνους και προστατεύουν έναντι των κυβερνοεπιθέσεων.

Γιατί είναι σημαντικό;

Η προσαρμογή σε πλαίσια, όπως το ISO 27001, ISO 27002, ISO 27701 ή το NIST, προσφέρει βελτιωμένα επίπεδα κυβερνοασφάλειας, κανονιστική συμμόρφωση, βελτιωμένα επίπεδα προστασίας δεδομένων, αλλά και επιχειρησιακή ανθεκτικότητα.

ΩΦΕΛΕΙΕΣ ΠΙΣΤΟΠΟΙΗΣΕΩΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΙΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

- Η επίτευξή τους σημαίνει πως η επιχείρηση τηρεί επαρκή μέτρα για την ψηφιακή της ασφάλεια, πράγμα που διαπιστώνεται από ανεξάρτητο αξιολογητή
- Η διατήρησή τους συνεπάγεται την αδιάλειπτη τήρηση των υποχρεώσεων μιας επιχείρησης ως προς τη συμμόρφωση με νόμους, κανονισμούς και καλές πρακτικές
- Ενισχύουν τη φήμη και την εμπιστοσύνη μεταξύ της επιχείρησης και των συνεργατών της (πελάτες, προμηθευτές, επενδυτές, κ.α.)
- Αντανακλούν τη δέσμευση της επιχείρησης να διατηρεί συνεχώς υψηλά επίπεδα ασφάλειας των συστημάτων και όλων των υλικών και άυλων περιουσιακών της στοιχείων, βελτιώνοντας την ανθεκτικότητά της έναντι επιθέσεων και παραβιάσεων

ΟΙ ΠΙΣΤΟΠΟΙΗΣΕΙΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΕΠΙΔΡΟΥΝ ΘΕΤΙΚΑ ΣΤΗ ΦΗΜΗ ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ, ΑΝΑΒΑΘΜΙΖΟΥΝ ΤΗΝ ΠΟΙΟΤΗΤΑ ΕΤΑΙΡΙΚΗΣ ΔΙΑΚΥΒΕΡΝΗΣΗΣ ΚΑΙ ΤΙΣ ΕΠΙΔΟΣΕΙΣ ESG, ΕΝΩ ΣΥΝΔΕΟΝΤΑΙ ΑΜΕΣΑ ΜΕ ΤΗ ΔΥΝΑΤΟΤΗΤΑ ΑΣΦΑΛΙΣΗΣ ΕΝΑΝΤΙ ΚΥΒΕΡΝΟΚΙΝΔΥΝΩΝ (CYBER INSURANCE).

ΜΕΧΡΙ ΤΟ 2025, 60% ΤΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ ΘΑ ΛΑΜΒΑΝΟΥΝ ΥΠΟΨΗ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΚΑΤΑ ΤΗ ΔΙΕΞΑΓΩΓΗ ΤΩΝ ΣΥΝΑΛΛΑΓΩΝ ΤΟΥΣ ΩΣ ΣΗΜΑΝΤΙΚΟ ΠΑΡΑΓΟΝΤΑ ΠΡΟΣΤΑΣΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ, ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΥΠΟΔΟΜΩΝ.

Πώς γίνεται;

Οι πιστοποιήσεις συμμόρφωσης επιτυγχάνονται υιοθετώντας – και εφαρμόζοντας – πρακτικές που διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών των επιχειρήσεων. Πρόκειται για βήματα και ενέργειες ως προς τη διαχείριση κυβερνοκινδύνων, ελέγχους ασφαλείας, εκπαίδευση και ευαισθητοποίηση του προσωπικού, αντίδραση σε περιστατικά κυβερνοασφάλειας, αλλά και συμμόρφωση με κλαδικά πρότυπα, ειδικούς κανόνες και ηθικές νόρμες. Οι πιστοποιήσεις μπορούν να συνδυαστούν ανάλογα με τις ειδικές ανάγκες κάθε επιχείρησης, τα κλαδικά πρότυπα που υποχρεούται να πληροί, και το εγχώριο ρυθμιστικό πλαίσιο στο οποίο οφείλει να συμμορφώνεται.

ΣΗΜΑΝΤΙΚΟΤΕΡΑ ΠΡΟΤΥΠΑ ΠΙΣΤΟΠΟΙΗΣΕΩΝ

ISO 27001

Καθορίζει τις απαιτήσεις για τη δημιουργία, εφαρμογή, συντήρηση και συνεχή βελτίωση ενός Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS). Συμβάλει στον εντοπισμό πιθανών απειλών και τρωτών σημείων, και αξιολογεί την επίδρασή τους στην ποιότητα των αποφάσεων προστασίας ευαίσθητων πληροφοριών

ISO 27002

Συμπληρωματικό στο ISO 27001, που παρέχει λεπτομερή καθοδήγηση για πρακτικές εφαρμογής ελέγχων ασφαλείας και μέτρων για την προστασία πληροφοριών, με στόχο την αναβάθμιση των πρακτικών ασφαλείας πληροφοριών

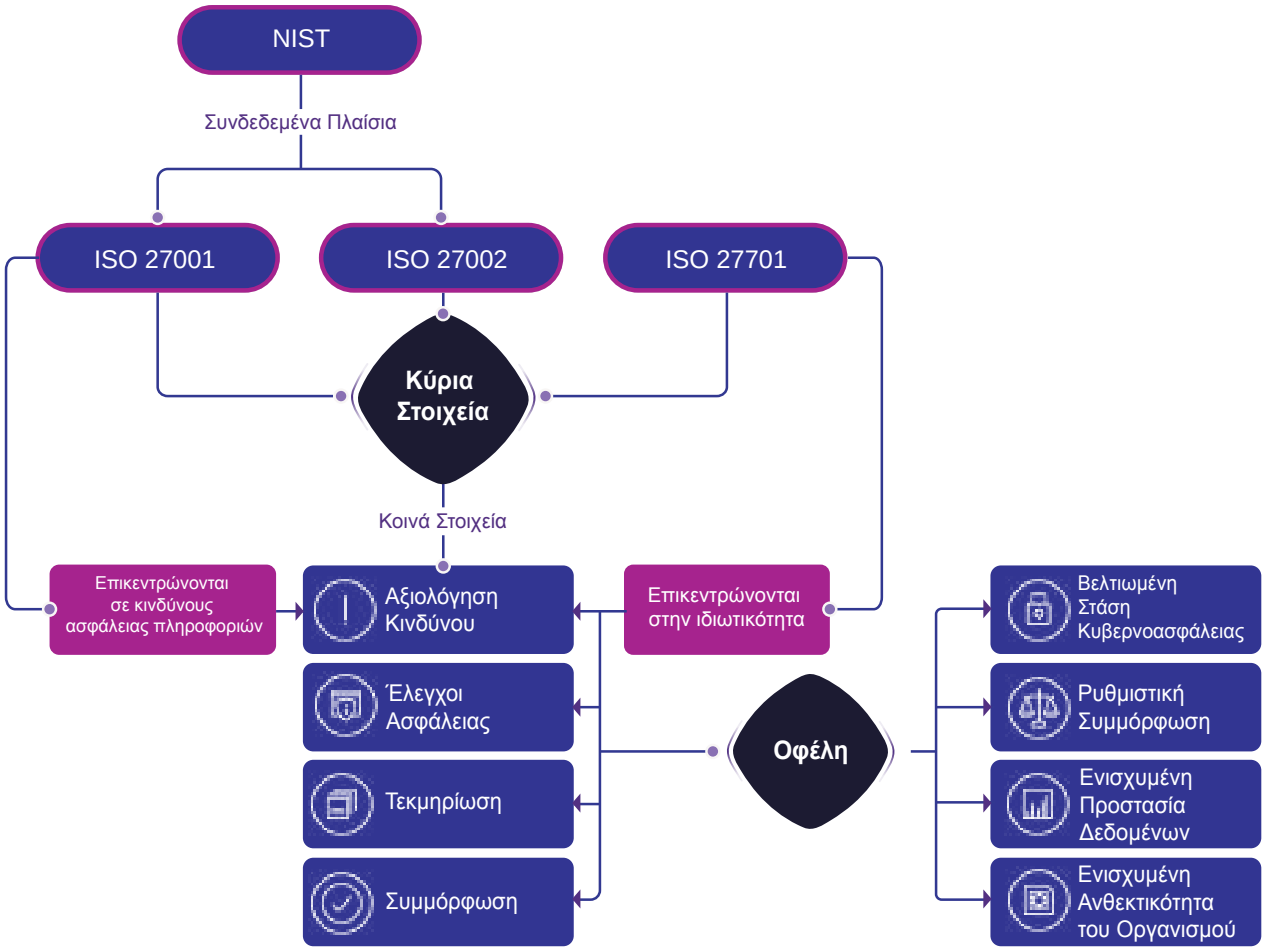
ISO 27701

Πρότυπο που επικεντρώνεται στη δημιουργία, εφαρμογή, συντήρηση και συνεχή βελτίωση ενός συστήματος διαχείρισης της ιδιωτικότητας (PIMS), με κύριο πυλώνα τη διαχείριση κινδύνων γύρω από την ιδιωτικότητα των πληροφοριών εντός ενός οργανισμού και των προσωπικών δεδομένων που χειρίζεται.

NIST SP 800-53

Αποτελεί έναν ολοκληρωμένο κατάλογο ελέγχων ασφαλείας που μπορεί να προσαρμοστεί στις ειδικές ανάγκες κυβερνοασφάλειας ενός οργανισμού, επιτρέποντας τη δομημένη διαχείριση κινδύνων κυβερνοασφάλειας, και την αναβάθμιση πρακτικών ασφαλείας.

ΚΟΙΝΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΑΙ ΩΦΕΛΕΙΕΣ
ΑΠΟ ΤΗΝ ΥΙΟΘΕΤΗΣΗ ΠΡΟΤΥΠΩΝ



Με πληροφορίες από: ENISA, Gartner, Grant Thornton, Uni Systems

ΒΗΜΑ 9°
ΑΣΦΑΛΙΣΗ ΕΝΑΝΤΙ ΚΥΒΕΡΝΟΚΙΝΔΥΝΩΝ (CYBER INSURANCE)

Η ΑΣΦΑΛΙΣΗ CYBER INSURANCE ΕΙΝΑΙ ΜΙΑ ΟΛΟΚΛΗΡΩΜΕΝΗ ΥΠΗΡΕΣΙΑ ΓΙΑ ΤΗ ΔΙΑΧΕΙΡΙΣΗ ΚΑΙ ΤΗ ΧΡΗΜΑΤΟΔΟΤΗΣΗ ΠΕΡΙΣΤΑΤΙΚΩΝ ΚΥΒΕΡΝΟΚΙΝΔΥΝΟΥ. ΤΑ ΠΡΟΪΟΝΤΑ CYBER INSURANCE ΔΕΝ ΥΠΟΚΑΘΙΣΤΟΥΝ ΣΕ ΚΑΜΙΑ ΠΕΡΙΠΤΩΣΗ ΤΑ ΑΠΑΡΑΙΤΗΤΑ ΜΕΤΡΑ ΠΟΥ ΠΡΕΠΕΙ ΝΑ ΛΑΜΒΑΝΕΙ ΚΑΘΕ ΕΠΙΧΕΙΡΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ ΤΗΣ, ΑΛΛΑ ΛΕΙΤΟΥΡΓΟΥΝ ΣΥΜΠΛΗΡΩΜΑΤΙΚΑ ΜΕ ΑΛΛΕΣ ΕΝΕΡΓΕΙΕΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΝΘΕΚΤΙΚΟΤΗΤΑ ΤΗΣ.

Τι είναι;

Τα ασφαλιστικά προϊόντα cyber insurance συνδυάζουν ασφαλιστική προστασία με εργαλεία διαχείρισης κινδύνου. Η ασφάλιση cyber insurance καλύπτει τους οικονομικούς κινδύνους που προκύπτουν από αλλοίωση ή καταστροφή δεδομένων, απώλεια ή κλοπή δεδομένων, κυβερνο-εκβιασμούς, απαιτήσεις τρίτων, ή και αρνητική δημοσιότητα λόγω περιστατικού κυβερνοασφάλειας.

Πώς γίνεται;

- Πριν, μετά ή και κατά τη διάρκεια ενός περιστατικού, αναζητώντας τη συνδρομή ειδικών συμβούλων ασφάλισης cyber insurance.
- Με τη βοήθεια εξειδικευμένων συμβούλων Brokers για την αξιολόγηση του κινδύνου, το σχεδιασμό της κάλυψης και την έρευνα αγοράς προκειμένου να γίνει η ασφάλιση.
- Σε περίπτωση περιστατικού, γίνεται συντονισμός όλων των εμπλεκομένων (επιχείρηση, ειδικοί σύμβουλοι, ασφαλιστικός πάροχος, broker) για την αποτελεσματική διαχείριση του συμβάντος.

ΠΑΡΟΧΕΣ ΑΣΦΑΛΙΣΤΙΚΩΝ ΠΡΟΪΟΝΤΩΝ
CYBER INSURANCE

- ☑ Εξειδικευμένη ομάδα διαχείρισης περιστατικού κυβερνοασφάλειας
- ☑ IT Forensics: έλεγχος δεδομένων που έχουν επηρεαστεί από την παραβίαση, διερεύνηση αιτιών παραβίασης και τρόπου αντιμετώπισης περιστατικού
- ☑ Ειδικοί διαπραγματευτές λύτρων
- ☑ Νομικοί Σύμβουλοι: βοήθεια κατά τη γνωστοποίηση περιστατικού στην αρμόδια Αρχή και σε όσους έχουν υποστεί παραβίαση δεδομένων
- ☑ Σύμβουλοι Επικοινωνίας: διαχείριση κρίσης και αντιμετώπιση δυσφήμισης
- ☑ Υπηρεσίες εκπαίδευσης και ευαισθητοποίησης προσωπικού για την αναγνώριση και τον εντοπισμό κακόβουλων ενεργειών, μέσα από πλατφόρμες εκπαίδευσης, καμπάνιες προσομοίωσης phishing, κ.α.
- ☑ Αξιολόγηση ψηφιακής ασφάλειας και προτάσεις για παρεμβάσεις βελτίωσης
- ☑ Οικονομική αποκατάσταση της ζημίας μέσω της αποζημίωσης

Γιατί είναι σημαντικό;

Τα ασφαλιστικά προϊόντα cyber insurance προσφέρουν δίχτυ προστασίας για την αντιμετώπιση οικονομικών επιπτώσεων και δαπανών. Βοηθούν να μετριαστεί ο κίνδυνος πλήγματος στην εταιρική φήμη, και εξοικειώνουν τις επιχειρήσεις με τη διαχείριση της αυξανόμενης ευθύνης που συνεπάγεται η διαχείριση μεγάλου όγκου δεδομένων πελατών.

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΟΔΗΓΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

ΒΗΜΑ 10°
ΨΗΦΙΑΚΗ ΑΣΦΑΛΕΙΑ ΠΕΛΑΤΩΝ ΚΑΙ ΠΡΟΜΗΘΕΥΤΩΝ

Τι είναι;
Η μέριμνα για την προστασία του δικτύου πελατών, προμηθευτών και συνεργατών μιας επιχείρησης από τη δική της έκθεση σε κυβερνοκινδύνους, μια σχέση που πρέπει να είναι αμφίδρομη.

Γιατί είναι σημαντικό;
Η χρήση διαφορετικών συστημάτων IT/OT και πρωτοκόλλων ψηφιακής ασφάλειας κατά μήκος της αλυσίδας εφοδιασμού μιας επιχείρησης αυξάνει τις πιθανότητες να βρεθεί εκτεθειμένη σε απειλές τόσο η ίδια, όσο και οι συνεργάτες της.

ΔΕΥΤΕΡΟΣ ΣΥΝΗΘΕΣΤΕΡΟΣ ΣΤΟΧΟΣ ΚΥΒΕΡΝΟ-ΠΑΡΑΒΙΑΣΕΩΝ Η ΕΦΟΔΙΑΣΤΙΚΗ ΑΛΥΣΙΔΑ: 17% ΤΩΝ ΚΑΚΟΒΟΥΛΩΝ ΕΙΣΒΟΛΩΝ ΤΟ 2021 ΠΡΟΗΛΘΑΝ ΑΠΟ ΤΗΝ ΑΛΥΣΙΔΑ ΕΦΟΔΙΑΣΜΟΥ, ΣΕ ΣΧΕΣΗ ΜΕ 1% ΤΟ 2020.

Πώς γίνεται;
Τα βήματα κυβερνο-προστασίας της εφοδιαστικής αλυσίδας ενός οργανισμού περιλαμβάνουν
- συνεχή ανταλλαγή πληροφοριών και ενημέρωσης μεταξύ συνεργατών
- διαμόρφωση στρατηγικής προσέγγισης για τη διαχείριση κινδύνων που πηγάζουν από τρίτους (third party risk assessment – TRM),
- επενδύσεις σε αξιόπιστες τεχνολογίες IT/OT και συστηματικές επικαιροποιήσεις κώδικα ασφαλείας για τα εν λόγω ευάλωτα σημεία (patching)
- προσδιορισμό αρμόδιων ρόλων και ευθυνών εντός της επιχείρησης,
- συνεργασία με πιστοποιημένους προμηθευτές και πελάτες,
- ενιαίος τρόπος επικοινωνίας σχετικά με τις εφαρμοζόμενες πρακτικές κυβερνοασφάλειας στην εφοδιαστική αλυσίδα τόσο στο εσωτερικό της επιχείρησης, όσο και προς τρίτους

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΤΗΣ ΕΦΟΔΙΑΣΤΙΚΗΣ ΑΛΥΣΙΔΑΣ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΕΠΙΧΕΙΡΗΣΕΩΝ (ENISA, 2023)

76%
δεν διαθέτουν αρμόδιους ρόλους για την ψηφιακή ασφάλεια της εφοδιαστικής αλυσίδας

37%
δεσμεύονται από δράσεις δέουσας επιμέλειας ή αξιολόγησης κινδύνου

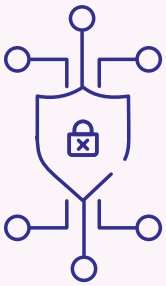
Μόνο **9%** δεν αξιολογούν καθόλου τους κινδύνους της εφοδιαστικής τους αλυσίδας

52%
εφαρμόζει αυστηρές πολιτικές επικαιροποίησης του κώδικα ασφάλειάς τους (security patches) για τουλάχιστον 80% των περιουσιακών στοιχείων τους

46%
πραγματοποιούν επικαιροποιήσεις του κώδικα ασφαλείας κάθε μήνα, και 46% εντός 6μήνου.

61% ΑΠΑΙΤΟΥΝ ΠΙΣΤΟΠΟΙΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΑΠΟ ΤΟΥΣ ΠΡΟΜΗΘΕΥΤΕΣ ΤΟΥΣ

Με πληροφορίες από: ENISA



ΠΑΡΑΡΤΗΜΑ
ΜΙΚΡΟ ΛΕΞΙΚΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Κυβερνο-απειλές (cyber threats)
Κυβερνοαπειλή αποτελεί οποιαδήποτε συνθήκη ή συμβάν που μπορεί, μέσω ενός ψηφιακού συστήματος, να επιδράσει αρνητικά στις λειτουργίες ενός οργανισμού, στα περιουσιακά του στοιχεία, σε πρόσωπα, άλλους οργανισμούς ή τη χώρα, εξαιτίας:
- μη εξουσιοδοτημένης πρόσβασης σε πληροφορίες,
- καταστροφής, δημοσιοποίησης ή αλλοίωσης και φθοράς πληροφοριών
- άρνησης παροχής υπηρεσιών στους χρήστες του συστήματος.

Κακόβουλοι παράγοντες στον κυβερνοχώρο (cyber threat actors – CTAs)
Κακόβουλοι παράγοντες στον κυβερνοχώρο είναι άτομα ή ομάδες που εμπλέκονται σε δράσεις με στόχο την πρόκληση βλάβης σε ψηφιακές υπηρεσίες και συστήματα, χρησιμοποιώντας Η/Υ, ηλεκτρονικές συσκευές, ψηφιακά συστήματα ή δίκτυα – δηλαδή κυβερνοεπιθέσεις.

Κυβερνοασφάλεια (cyber security)
Ο όρος «κυβερνοασφάλεια» αναφέρεται σε ένα συνδυασμό τεχνολογιών, διαδικασιών και πρακτικών που είναι σχεδιασμένες για να προστατεύουν δίκτυα, συσκευές, προγράμματα, δεδομένα και υλικά και άυλα περιουσιακά στοιχεία από εξωτερικές απειλές, επιθέσεις, φθορές ή μη εξουσιοδοτημένη πρόσβαση. Δεδομένης της αυξανόμενης διασύνδεσης των συστημάτων IT και OT, ο όρος πλέον δεν αφορά μόνο την ασφάλεια των πληροφοριακών συστημάτων, αλλά τη συνολική ψηφιακή ασφάλεια ενός οργανισμού

Κυβερνοανθεκτικοτητα (cyber resilience)
Η κυβερνοανθεκτικότητα αναφέρεται στην ικανότητα ενός οργανισμού
- να προστατέψει τα ηλεκτρονικά δεδομένα και συστήματά του από κυβερνοεπιθέσεις
- να εντοπίσει και να αντιμετωπίσει περιστατικά κυβερνοασφάλειας με τρόπο έγκαιρο και αποτελεσματικό
- να επανέλθει σε κανονική λειτουργία σύντομα έπειτα από μια επιτυχημένη κυβερνοεπίθεση

Malware
Κακόβουλο λογισμικό που μπορεί να καταστρέψει, φθείρει ή να καταχραστεί συστήματα IT. Εντοπίζεται με διαφορετικές μορφές (viruses, worms, ransomware, spyware, trojans, κ.α.)

email phishing
Τα emails ηλεκτρονικού ψαρέματος (email phishing) επιδιώκουν να ξεγελάσουν τον παραλήπτη για να αποσπάσουν πολύτιμες πληροφορίες, χρήματα ή να μεταδώσουν ιούς και κακόβουλο λογισμικό.

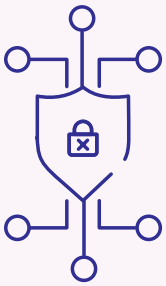
Κυβερνο-εκβιασμός (digital extortion)
Οι κυβερνο-εκβιασμοί στοχεύουν στην κλοπή δεδομένων με «σπάσιμο» του κώδικα κρυπτογράφησης που τα προστατεύει, επιδιώκοντας την είσπραξη κυβερνολύτρων (ransom) για την αποδέσμευσή τους.

Επίθεση DDoS (Distributed denial of service attacks)
Μια επίθεση DDoS σημαίνει ότι hackers «βομβαρδίζουν» ένα σύστημα ή μια ιστοσελίδα με αιτήματα σύνδεσης ή παροχής υπηρεσιών, βραχυκυκλώνοντας τη δυνατότητά του να ανταποκριθεί στα αιτήματα των χρηστών. Οι επιθέσεις πραγματοποιούνται μέσω botnets, δηλ. δικτύων Η/Υ που έχουν μολυνθεί με malware. Αποσκοπούν σε οικονομικό εκβιασμό, δολιοφθορά, επίδειξη τεχνικών δεξιοτήτων, κ.α.

Λειτουργική Τεχνολογία (OT)
Αναφέρεται στο υλικό και το λογισμικό που χρησιμοποιούνται για την αλλαγή, την παρακολούθηση ή τον έλεγχο φυσικών συσκευών, διαδικασιών και συμβάντων σε μια εταιρεία ή οργανισμό.

Τεχνητή Νοημοσύνη (ΤΝ)
Αναφέρεται στην ικανότητα μιας μηχανής να αναπαράγει τις γνωστικές λειτουργίες ενός ανθρώπου, όπως είναι η μάθηση, ο σχεδιασμός και η δημιουργικότητα.

Πηγές: Cisco, Gartner, IBM, Netcompany-Intrasoft, NIST



ΚΥΡΙΕΣ ΠΗΓΕΣ

- Εθνική Αρχή Κυβερνοασφάλειας, Εγχειρίδιο Κυβερνοασφάλειας
- Εθνική Αρχή Κυβερνοασφάλειας, Οδηγός Αυτοαξιολόγησης
- Barracuda, Spear-phishing report: Social engineering and growing complexity of attacks, 2022
- Cisco, Security Outcomes Study, 2022
- Deloitte, 2023 Global Future of Cyber Survey, 2023
- Deloitte Insights, Tech Trends 2022
- ENISA, Artificial Intelligence and Cybersecurity Research, 2023
- ENISA, Cybersecurity Maturity Assessment Tool for SMEs, 2023
- ENISA, Good Practices for Supply Chain Cybersecurity, 2023
- ENISA, Identifying Emerging Cyber Security Threats and Challenges for 2030, 2023
- ENISA, Threat Landscape 2023
- FBI Cyber Crime Report 2021
- Gartner, 3 Must-haves In Your Cybersecurity Incident Response, 2022
- Gartner, 4 Ways to Achieve Secure Employee Behaviors, 2023
- Gartner, Protect Business Assets With a Roadmap for Maturing Information Security, 2021
- Grant Thornton, Cyber Resilience and Business, 2022
- Grant Thornton, ChatGPT: The Role of AI in Cybersecurity, 2023
- IBM, Definitive Guide to Ransomware, 2022
- IBM, Security Data Breach Report, 2023
- IBM, Cost of a Data Breach Report, 2023
- IBM, X Force Threat Intelligence Index, 2023
- ISACA, Better Cybersecurity Awareness Through Research, 2022
- OMDIA, Enterprise Evolution and the Role of Cyber Security, 2022
- PriceWaterhouseCoopers, Global Digital Trust Insights 2024 Report, 2023
- Verizon, Data Breach Investigation Report 2023
- World Economic Forum, Global Security Outlook Report, 2023

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών

Τομέας Βιομηχανίας, Ανάπτυξης, Τεχνολογίας και Καινοτομίας

www.sev.org.gr

E. industrial@sev.org.gr
T. 211 5006 165

SEV Hellenic Federation of Enterprises
ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών
SEV_Fed
SEVFed