ΣΕΒΕ
ΣΥΝΔΕΣΜΟΣ ΕΞΑΓΩΓΕΩΝ

ΕΝΩΣΗ
ΑΣΦΑΛΙΣΤΙΚΩΝ
ΕΤΑΙΡΙΩΝ
ΕΛΛΑΔΟΣ

CYBER RISK INSURANCE

Σύγχρονες απειλές - Σύγχρονες λύσεις από την ασφαλιστική αγορά

Τετάρτη

12 ΟΚΤ 2022

17:00 - 19:00

Grand Hotel Palace
Μοναστηρίου 305
Θεσσαλονίκη, 546 28

ΣΑΜΑΡΑΣ & ΣΥΝΕΡΓΑΤΕΣ Ε.Π.Ε.
ΣΥΜΒΟΥΛΟΙ ΠΟΙΟΤΗΤΑΣ & ΑΣΦΑΛΕΙΑΣ ΕΡΓΑΣΙΑΣ

Μέλος του Ομίλου
30 YEARS of SUCCESS Samaras + Partners GROUP OF COMPANIES

CYBER RISK INSURANCE

Οργανωτικά μέτρα διαχείρισης κινδύνου-Συνήθη προβλήματα και βέλτιστες πρακτικές στη μέση ελληνική επιχείρηση

Βιβή Ασπρούλη
Διπλ. Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών
MSc, DPO Executive, ISO 27001 LA
Τηλ: 6970000192
email: vasprouli@exyppsamaras.gr
www.exyppsamaras.gr

Οργανωτικά μέτρα διαχείρισης κινδύνου-Συνήθη προβλήματα και βέλτιστες πρακτικές στη μέση ελληνική επιχείρηση

ΣΥΝΗΘΕΙΣ ΚΥΒΕΡΝΟΑΠΕΙΛΕΣ

Ώρα 4:00 μ.μ.
Καταφθάνει νέο email από άγνωστο παραλήπτη

Ώρα 04:10 μ.μ.
Ο χρήστης βλέπει το μήνυμα και ανοίγει το επισυναπτόμενο αρχείο

Ώρα 04:12 μ.μ.
Η επιχείρηση βρίσκεται ψηφιακά εκτός λειτουργίας

Παράδειγμα εντοπισμού email εξαπάτησης

Μια πολύ συχνή τακτική είναι η αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας
Όταν λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από κάποιο άτομο που δεν αναγνωρίζετε ή το Outlook το αναγνωρίζει ως νέο αποστολέα, αφιερώστε λίγο χρόνο για να το εξετάσετε προσεκτικά προτού συνεχίσετε.

Οργανωτικά μέτρα διαχείρισης κινδύνου-Συνήθη προβλήματα και βέλτιστες πρακτικές στη μέση ελληνική επιχείρηση

Επιπτώσεις στη μικρομεσαία επιχείρηση

- Διακοπή Λειτουργίας Επιχείρησης
- Καταστροφή φήμης
- Κλοπή περιουσιακών στοιχείων
- Διαρροή ευαίσθητων δεδομένων
- Δαπάνες σε hardware/software
- Πρόστιμα
- Απώλεια πελατολογίου
- Διαρροή τεχνογνωσίας

Οργανωτικά μέτρα διαχείρισης κινδύνου-Συνήθη προβλήματα και βέλτιστες πρακτικές στη μέση ελληνική επιχείρηση

Ενδεικτικά παραδείγματα κυβερνοεπιθέσεων στην Ελλάδα

10/2018- VIVARTIA
Στην Ελλάδα, το πρώτο καταγεγραμμένο περιστατικό κυβερνοεπίθεσης σε μεγάλη εταιρία με στόχο την απόσπαση λύτρων. Τότε hackers «αιχμαλώτισαν» για δύο ημέρες τα ηλεκτρονικά συστήματα, παγώνοντας κάθε διαδικασία, από τις ταμειακές μηχανές στα Everest και τα Goody's έως τα τιμολόγια για τα προϊόντα της ΔΕΛΤΑ.

03/2022- ΕΛΤΑ
Hackers επιτέθηκαν στα πληροφοριακά τους συστήματα μέσω κακόβουλου λογισμικού με αποτέλεσμα να υπάρχει προσωρινή αναστολή λειτουργίας του εμπορικού πληροφοριακού συστήματος σε όλα τα ταχυδρομικά καταστήματα

08/2022- ΔΕΣΦΑ
Από τις διατυπώσεις και από φωτογραφικό υλικό από τα μηνύματα που εστάλησαν, προκύπτει ότι οι hackers κατάφεραν να υφαρπάξουν αρχεία, εισχώρησαν δηλαδή σε pc και εσωτερικούς διακομιστές. Η ειδοποίηση όμως είναι generic, ενώ το γεγονός απειλεί μόνο με δημοσίευση και δεν αποτρέπει την πρόσβαση στους υπολογιστές, καταδεικνύει ότι πρόκειται για low-key επίθεση.

Τον Νοέμβριο του 2021, η Ελλάδα βρέθηκε σε μια από τις υψηλότερες θέσεις της λίστας ως προς τον αριθμό των επιθέσεων σε βιομηχανικά συστήματα.
Πιο συγκεκριμένα, σύμφωνα με τα τελευταία στοιχεία της εταιρείας κυβερνοασφάλειας Kaspersky, η Ελλάδα κατατάσσεται στην 5η θέση, με το 32% των βιομηχανικών συστημάτων να έχουν υποστεί κάποιου είδους επίθεση.

Οργανωτικά μέτρα διαχείρισης κινδύνου-Συνήθη προβλήματα και βέλτιστες πρακτικές στη μέση ελληνική επιχείρηση

ΣΑΜΑΡΑΣ & ΣΥΝΕΡΓΑΤΕΣ Ε.Π.Ε.
ΣΥΜΒΟΥΛΟΙ ΠΟΙΟΤΗΤΑΣ & ΑΣΦΑΛΕΙΑΣ ΕΡΓΑΣΙΑΣ

Οργανωτικά μέτρα διαχείρισης κινδύνου-Οι πυλώνες

1. Ανάλυση Τρέχουσας Κατάστασης (Analyzing Current Scenario –GAP Analysis)
2. Διαχείριση και Εκτίμηση Κινδύνου (Cyber Risk Management/Assessment)
3. Διαχείριση Συμβάντων/Σχέδιο Αντιμετώπισης Συμβάντων (Incident Management/Response Plan)
4. Διαχείριση Επιχειρισιακής Συνέχειας (Cybersecurity Contingency Plan)
5. Ανάλυση Αντικτύπου (Impact Analysis)
6. Πολιτικές Ασφαλείας (Security Policies)

Οργανωτικά μέτρα διαχείρισης κινδύνου-Συνήθη προβλήματα και βέλτιστες πρακτικές στη μέση ελληνική επιχείρηση

ΣΑΜΑΡΑΣ & ΣΥΝΕΡΓΑΤΕΣ Ε.Π.Ε.
ΣΥΜΒΟΥΛΟΙ ΠΟΙΟΤΗΤΑΣ & ΑΣΦΑΛΕΙΑΣ ΕΡΓΑΣΙΑΣ

Οργανωτικά μέτρα διαχείρισης κινδύνου-Οι πυλώνες

7 Διαχείριση Διαδικασιών και Εγγράφων (Document Management)

8 Εκτίμηση Φυσικής Ασφάλειας (Security Assessment)

9 Κοινωνική Μηχανική-Ευαισθητοποίηση Εμπλεκόμενου Προσωπικού (Social Engineering)

10 Ρόλοι και αρμοδιότητες -Ορισμός CISO (Roles and Responsibilities)

11 Διαχείριση Budget (Budget for Effective Cybersecurity Management)

12 Εκτίμηση Ευπαθειών (Vulnerability Assessment)

13 Δοκιμές Διείσδυσης (Penetration Test)

Οργανωτικά μέτρα διαχείρισης κινδύνου-Συνήθη προβλήματα και βέλτιστες πρακτικές στη μέση ελληνική επιχείρηση

ΣΑΜΑΡΑΣ & ΣΥΝΕΡΓΑΤΕΣ Ε.Π.Ε.
ΣΥΜΒΟΥΛΟΙ ΠΟΙΟΤΗΤΑΣ & ΑΣΦΑΛΕΙΑΣ ΕΡΓΑΣΙΑΣ

Μέτρα φυσικής ασφάλειας

1. Πολιτική φυσικής και περιβαλλοντικής ασφάλειας, που θα περιγράφει σκοπό, πεδίο εφαρμογής, ρόλους και ευθύνες
2. Προστασία από μη εξουσιοδοτημένη φυσική πρόσβαση στους servers του Οργανισμού (computer room)
3. Συστήματα προστασίας computer room
4. Έκθεση εγγράφων
5. Προστασία φορητών μέσων αποθήκευσης
6. Μεταφορά φακέλων
7. Εναλλακτικές εγκαταστάσεις

Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας

1. Πολιτική εκπαίδευσης χρηστών
   - Σύνδεσης με τις συσκευές και το δίκτυο με ασφαλή τρόπο
   - Δημιουργία ισχυρών κωδικών πρόσβασης και την πολυπαραγοντική αυθεντικοποίηση
   - την ανίχνευση διαφόρων μορφών επιθέσεων κοινωνικής μηχανικής όπως π.χ. phishing emails, τηλεφωνικές κλήσεις πλαστοπροσωπίας
   - την αναγνώριση ενδείξεων παραβίασης συστημάτων και περιστατικών εκ των έσω απειλών (insider threats).
2. Διενέργεια εκπαιδευτικών προγραμμάτων ευαισθητοποίησης βασισμένα σε διακριτούς ρόλους και στοχευμένα σε διαφορετικές κατηγορίες εργαζομένων με βάση το επίπεδο τεχνικής εξειδίκευσης.
3. Διενέργεια ανάλυσης γνωσιακών κενών του προσωπικού (knowledge gap analysis), με σκοπό τη σύνταξη ενός πλάνου δημιουργίας διαδοχικών εκπαιδεύσεων
4. Πρακτικές ασκήσεις προσομοίωσης περιστατικών κυβερνοασφάλειας και των επιπτώσεών τους, όπως π.χ. την επίσκεψη σε κακόβουλη ιστοσελίδα

Οργανωτικά μέτρα διαχείρισης κινδύνου-Συνήθη προβλήματα και βέλτιστες πρακτικές στη μέση ελληνική επιχείρηση

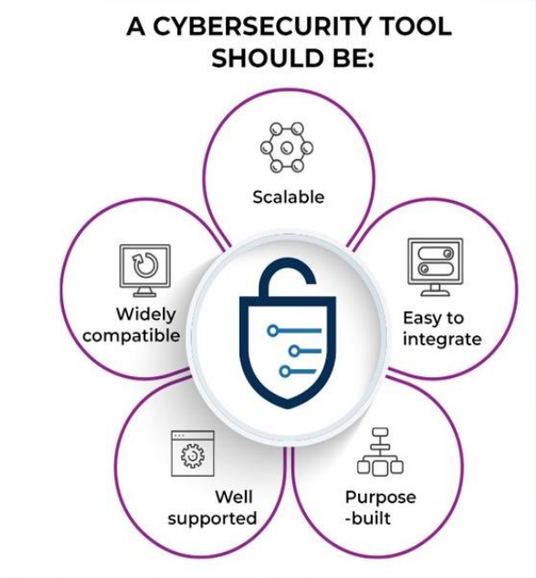
ΣΑΜΑΡΑΣ & ΣΥΝΕΡΓΑΤΕΣ Ε.Π.Ε.
ΣΥΜΒΟΥΛΟΙ ΠΟΙΟΤΗΤΑΣ & ΑΣΦΑΛΕΙΑΣ ΕΡΓΑΣΙΑΣ

Βέλτιστες πρακτικές για την υιοθέτηση και εφαρμογή ολιστικής και αποτελεσματικής στρατηγικής Κυβερνοασφάλειας

- Δέουσα επιμέλεια, υπευθυνότητα και αποτελεσματικότητα στη διαχείριση της Κυβερνοασφάλειας
- Ορισμός επικεφαλούς ασφάλειας πληροφοριών (CISO)
- Προαγωγή κουλτούρας Κυβερνοασφάλειας μέσω της εφαρμογής προγράμματος εκπαίδευσης και την υιοθέτηση ρόλων και αρμοδιοτήτων
- Τακτική ενημέρωση διοίκησης για το προφίλ κινδύνου του οργανισμού και για το επίπεδο ωρίμανσης των μηχανισμών ασφάλειας.
- Δημιουργία πλαισίου κλιμάκωσης για τη διαχείριση των κινδύνων στον Κυβερνοχώρο και των περιστατικών ασφάλειας με την συμμετοχή της Διοίκησης, που λαμβάνει υπόψη την ανεκτικότητα του οργανισμού στους κινδύνους και τις υφιστάμενες ελλείψεις.
- Ενεργή συμμετοχή της διοίκησης στην αξιολόγηση του προγράμματος ασφάλειας του οργανισμού, εστιάζει και επενδύει στους σωστούς τομείς με τις σωστές προτεραιότητες.

Οργανωτικά μέτρα διαχείρισης κινδύνου-Συνήθη προβλήματα και βέλτιστες πρακτικές στη μέση ελληνική επιχείρηση

Εργαλεία για την αποτελεσματική ασφάλεια πληροφοριών



Οργανωτικά μέτρα διαχείρισης κινδύνου-Συνήθη προβλήματα και βέλτιστες πρακτικές στη μέση ελληνική επιχείρηση

Πλεονεκτήματα Συμμόρφωσης με το διεθνές πρότυπο ISO 27001:2013

- Ενίσχυση των τεχνολογικών μεθόδων και μέτρων ασφαλείας για τη διαχείριση των πληροφοριών.
- Αίσθημα εμπιστοσύνης στο συνολικό περιβάλλον της επιχείρησης, μέσω της δέσμευσης του οργανισμού για τη διαχείριση της ασφάλειας των πληροφοριών.
- Διεθνής αναγνωσιμότητα και ισχύς του πιστοποιητικού.
- Δημιουργία προστιθέμενης αξίας κατά την παροχή υπηρεσιών ενός οργανισμού μέσω της δημιουργίας στρατηγικής διαχείρισης ασφάλειας πληροφορίας.
- Αντικειμενική απόδειξη της δέσμευσης του οργανισμού για τη διαχείριση της ασφάλειας των πληροφοριών
- Υιοθέτηση πολιτικής για την αντιμετώπιση διαρροής πληροφοριών.
- Δημιουργία δικλείδων ασφαλείας για τον κίνδυνο διαρροής/απώλειας/κλοπής των δεδομένων.
- Προσδίδει εικόνα αξιοπιστία και εμπιστοσύνη για την επιχείρηση.
- Τεκμηριώνεται δέσμευση ως προς την ασφάλεια πληροφοριών από όλους και σε όλα τα επίπεδα του οργανισμού.
- Διασφάλιση της επαλήθευσης τήρησης σχετικών νόμων και κανονισμών.
- Μείωση κόστους που ενδέχεται να προκύψει από απώλεια πληροφορίας.
- Απτή απόδειξη της γνώση του οργανισμού σχετικά με την επάρκεια και συμμόρφωση του συστήματος ως προς την ασφαλή διαχείριση πληροφοριών.
- Ετήσιος έλεγχος συμμόρφωσης και βελτίωσης του συστήματος από ανεξάρτητο διαπιστευμένο φορέα πιστοποίησης

Βιβή Ασπρούλη
Διπλ. Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών
MSc, DPO Executive, ISO 27001 LA
Τηλ: 6970000192
email: vasprouli@exyppsamaras.gr
www.exyppsamaras.gr

ΣΑΜΑΡΑΣ & ΣΥΝΕΡΓΑΤΕΣ Ε.Π.Ε.
ΣΥΜΒΟΥΛΟΙ ΠΟΙΟΤΗΤΑΣ & ΑΣΦΑΛΕΙΑΣ ΕΡΓΑΣΙΑΣ

ΘΕΣΣΑΛΟΝΙΚΗ
26ης ΟΚΤΩΒΡΙΟΥ 43 - ΕΜΠΟΡΙΚΟ ΚΕΝΤΡΟ "LIMANI CENTER"
ΤΗΛ. 2310 540.280 & 2310 552.562, ΦΑΞ: 2310 540.280

ΑΘΗΝΑ
ΠΑΝΕΠΙΣΤΗΜΙΟΥ 10, ΣΥΝΤΑΓΜΑ
ΤΗΛ. 210 958.00.00 & 210 959.00.30, ΦΑΞ: 210 959.00.31

Url: www.exyppsamaras.gr / Mail: info@exyppsamaras.gr

Σας ευχαριστώ

ΣΕΒΕ
ΣΥΝΔΕΣΜΟΣ ΕΞΑΓΩΓΕΩΝ

ΕΝΩΣΗ
ΑΣΦΑΛΙΣΤΙΚΩΝ
ΕΤΑΙΡΙΩΝ
ΕΛΛΑΔΟΣ

CYBER RISK INSURANCE

Σύγχρονες απειλές - Σύγχρονες λύσεις από την ασφαλιστική αγορά

Τετάρτη

12 ΟΚΤ 2022

17:00 - 19:00

Grand Hotel Palace
Μοναστηρίου 305
Θεσσαλονίκη, 546 28