ΠΙΝΑΚΑΣ ΕΛΕΓΧΟΥ ΚΙΝΔΥΝΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

ENCRYPT 4.0

Με συγχρηματοδότηση από το πρόγραμμα «Erasmus+» της Ευρωπαϊκής Ένωσης

Το έργο ENCRYPT4.0 (2020-1-RO01-KA202-079983) χρηματοδοτήθηκε με την υποστήριξη της Ευρωπαϊκής Επιτροπής.

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

Η παραγωγικότητα, η ποιότητα και το κόστος της μεταποίησης μπορούν να επωφεληθούν από μεγάλες βελτιώσεις λόγω της αυξανόμενης συνδεσιμότητας της Βιομηχανίας 4.0, τη χρήση ψηφιακών υπολογισμών και την αποθήκευση δεδομένων εκτός του χώρου εργασίας. Ωστόσο, υπάρχουν κίνδυνοι για τις ΜΜΕ μεταποίησης, όπως η δυνατότητα ανταγωνιστών και αντιπάλων να έχουν πρόσβαση στα δεδομένα τους. Οι κυβερνοεπιθέσεις γίνονται ολοένα και πιο συχνές και συνήθως γίνονται για την κλοπή εμπιστευτικών ή/και ιδιόκτητων δεδομένων, τη χειραγώγηση δεδομένων ώστε να προκαλέσουν ανεπιθύμητα αποτελέσματα και καταστροφή κεφαλαίων (Margot Hutchins & Stefanie Robinson, 2015). Οι κυβερνοεπιθέσεις μπορούν να οριστούν ως «μια επίθεση μέσω του κυβερνοχώρου, που στοχεύει στη χρήση του κυβερνοχώρου από μια επιχείρηση για να διαταράξει, απενεργοποιήσει, καταστρέψει ή κακόβουλα ελέγχει ένα υπολογιστικό περιβάλλον/υποδομή ή καταστροφή της ακεραιότητας των δεδομένων ή κλοπή ελεγχόμενων πληροφοριών »(Εθνικό Ινστιτούτο για Πρότυπα και Τεχνολογία, 2012, σελ. B3). Το Παγκόσμιο Οικονομικό Φόρουμ (2017) δίνει προτεραιότητα σε δύο λύσεις για την αντιμετώπιση των κινδύνων στον κυβερνοχώρο που βασίζονται στην καινοτομία: i) Μέτρηση κινδύνου στον κυβερνοχώρο και ii) Εκτίμηση της κυβερνοασφάλειας. Το 2019, η απάτη δεδομένων ή η κλοπή και οι κυβερνοεπιθέσεις προσδιορίστηκαν από το Παγκόσμιο Οικονομικό Φόρουμ ως ο τέταρτος και ο πέμπτος πιο πιθανός κίνδυνος (World Economic Forum, 2020), το 2020 εντόπισε θέματα που σχετίζονται με τον κυβερνοχώρο, όπως κυβερνοεπιθέσεις και απάτη δεδομένων ή κλοπή, στον κατάλογο των 10 κορυφαίων μακροπρόθεσμων κινδύνων.

Η Μεταποιητική Βιομηχανία χρειάζεται εργαλεία για να ενσωματώσει τους κινδύνους στον κυβερνοχώρο στις υπάρχουσες διαδικασίες διαχείρισης κινδύνων. Σε αυτό το πλαίσιο, το ENCRYPT 4.0 αντιμετωπίζει αυτήν την εντοπισμένη ανάγκη, εστιάζοντας στην αξιολόγηση της κυβερνοασφάλειας, αναπτύσσοντας τον Cyber Risk Audit Matrix (CRAM).. Ο CRAM είναι ένα ολοκληρωμένο εργαλείο που στοχεύει στη στήριξη των διευθυντών κατασκευαστικών ΜΜΕ να πραγματοποιήσουν μια ολοκληρωμένη ανάλυση των διαδικασιών τους λαμβάνοντας υπόψη τη χρήση καινοτόμων τεχνολογικών λύσεων που βασίζονται στη Βιομηχανία 4.0, εντοπίζοντας τους κινδύνους στον κυβερνοχώρο και υποστηρίζοντάς τους στο σχεδιασμό και τον καθορισμό αποτελεσματικών ελέγχων. Ο CRAM θα αναπτυχθεί λαμβάνοντας υπόψη την εμπειρογνωμοσύνη από εθνικά, ευρωπαϊκά και παγκόσμια πρότυπα (Παράρτημα Α) καθώς και την ανατροφοδότηση από ειδικούς στον τομέα της ασφάλειας στον κυβερνοχώρο από έξι ευρωπαϊκές χώρες - Αυστρία, Πορτογαλία, Ρουμανία, Βουλγαρία, Κύπρο και Ισπανία.

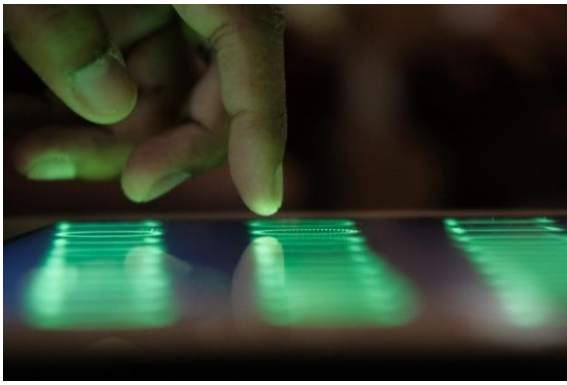
Το ENCRYPT 4.0 επικεντρώνεται στην αξιολόγηση της κυβερνοασφάλειας, αναπτύσσοντας τον Πίνακα Ελέγχου Κινδύνων στον Κυβερνοχώρο (Cyber Risk Audit Matrix-CRAM)

- Το παρόν έγγραφο περιλαμβάνει α) την πρόταση αξίας του CRAM, β) τη μεθοδολογία του CRAM, γ) την περιγραφή των κατηγοριών του CRAM, γ) τα βήματα για τη διενέργεια ελέγχων στον κυβερνοχώρο ασφάλειας δ) βιβλιογραφικές αναφορές.

2. ΠΡΟΤΑΣΗ ΑΞΙΑΣ CRAM

Ο **Πίνακας Ελέγχου Κινδύνων στον Κυβερνοχώρο(CRAM)** θα επιτρέψει στα έξυπνα εργοστάσια να προβούν σε συστηματική επισκόπηση του τοπίου τους στον κυβερνοχώρο και να δημιουργήσουν ένα ακριβές προφίλ του κινδύνου των κυβερνο-απειλών. Το Encrypt 4.0 CRAM, θα επιτρέψει στα έξυπνα εργοστάσια να πραγματοποιούν συνεπείς αναλύσεις δεδομένων σε πραγματικό χρόνο και να αξιολογούν τους κινδύνους στον κυβερνοχώρο, βάσει συγκεκριμένου και εκτεταμένου πίνακα.

Ο CRAM θα είναι ένα αναλυτικό εργαλείο που θα υποστηρίξει τις μεταποιητικές εταιρείες να εντοπίσουν, να αναλύσουν, να δώσουν προτεραιότητα στους κινδύνους και να θεσπίσουν άμεσα προστατευτικά μέτρα. Τα τελευταία χρόνια, ένα από τα πιο πιεστικά προβλήματα του ψηφιακού κόσμου είναι η ασφάλεια στον κυβερνοχώρο και η προστασία της ιδιωτικής ζωής των δεδομένων. Το 2019, το Παγκόσμιο Οικονομικό Φόρουμ (WEF) κατέταξε τις κυβερνοεπιθέσεις μεταξύ των πέντε κορυφαίων παγκόσμιων κινδύνων.



Το 2020, με την πανδημία του COVID-19, η μεγαλύτερη εξάρτηση από τη συνδεσιμότητα και την ψηφιακή υποδομή λόγω του παγκόσμιου αποκλεισμού αύξησε τις ευκαιρίες για κυβερνοεπιθέσεις. Ταυτόχρονα, για να μεγιστοποιήσουν τη ζημιά και το οικονομικό όφελος, οι εγκληματίες στον κυβερνοχώρο μετατοπίζουν τους στόχους τους από άτομα και μικρές επιχειρήσεις σε μεγάλες εταιρείες, κυβερνήσεις και κρίσιμες υποδομές, οι οποίες παίζουν καθοριστικό ρόλο στην αντιμετώπιση της επιδημίας (INTERPOL G. S., 2020). «Οι κυβερνοεπιθέσεις αποτελούν μεγαλύτερο κίνδυνο για τις δημοκρατίες και τις οικονομίες από ότι τα όπλα και τα άρματα μάχης» (Γιούνκερ, 2017).

Η Cybersecurity Ventures, ο κορυφαίος ερευνητής στον κόσμο στην παγκόσμια κυβερνοοικονομία, προέβλεψε ότι «οι παγκόσμιες ζημίες που σχετίζονται με το έγκλημα στον κυβερνοχώρο το 2021 θα φτάσουν τα έξι τρισεκατομμύρια δολάρια, που θα είναι περισσότερες από όλες τις φυσικές καταστροφές σε ένα χρόνο» (Cybersecurity Ventures, 2020). Η Επίσημη Ετήσια Έκθεση για το έγκλημα στον κυβερνοχώρο του 2019 αναφέρει ότι "στο τέλος του 2016, μια επιχείρηση έπεσε θύμα επίθεσης ransomware κάθε 40 δευτερόλεπτα" (Cybersecurity Ventures, 2019) και οι προβλέψεις είναι ότι ο αριθμός αυτός θα αυξηθεί σε κάθε 11 δευτερόλεπτα έως το 2021.

Οι κυβερνοεπιθέσεις σε κρίσιμες υποδομές, που χαρακτηρίστηκαν ως ο πέμπτος υψηλότερος κίνδυνος το 2020 από το δίκτυο

εμπειρογνωμόνων του WEF, έγιναν το νέο φυσιολογικό σε τομείς όπως η ενέργεια, η υγειονομική περίθαλψη και οι μεταφορές. Ωστόσο, η μεταποίηση υποφέρει από αυξανόμενες κυβερνοεπιθέσεις όπως έδειξε η Έκθεση Διερεύνησης Παραβίασης Δεδομένων για το 2020, αναφέροντας 922 περιστατικά, 381 με επιβεβαιωμένη αποκάλυψη δεδομένων, μόνο στις ΗΠΑ (Verizon, 2020). Οι οργανωμένες οργανώσεις του εγκλήματος στον κυβερνοχώρο ενώνουν τις δυνάμεις τους και η πιθανότητα εντοπισμού και δίωξης τους εκτιμάται ότι είναι μόλις 0,05% στις Ηνωμένες Πολιτείες, «το ηλεκτρονικό έγκλημα ως υπηρεσία είναι ένα αναπτυσσόμενο επιχειρηματικό μοντέλο, καθώς η αυξανόμενη πολυπλοκότητα των εργαλείων στο Darknet καθιστά τις κακόβουλες υπηρεσίες πιο προσιτές και εύκολα προσβάσιμες για οποιονδήποτε» (World Economic Forum, 2020).

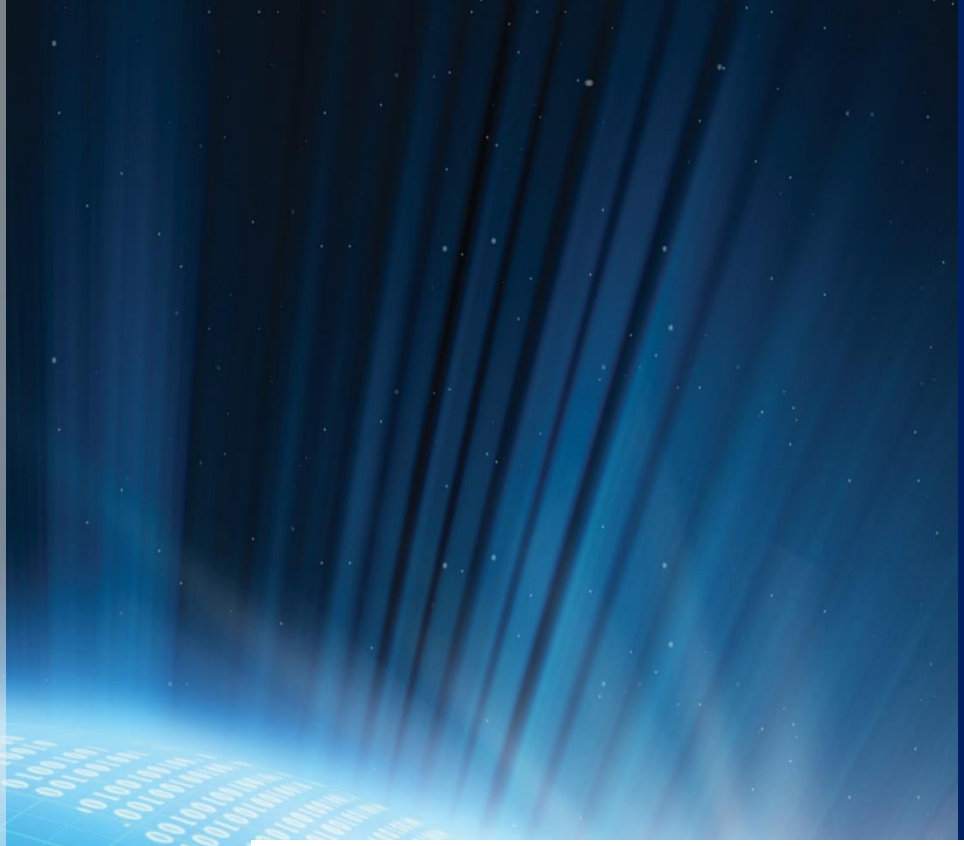
Η αμυντική ικανότητα των ΜΜΕ είναι συνήθως ασθενέστερη σε σύγκριση με τις μεγαλύτερες επιχειρήσεις και τα στοιχεία υποδηλώνουν ότι μόνο το 14% των επηρεαζόμενων ΜΜΕ μπορούν να ανακάμψουν μόνες τους. Επιπλέον, η Εθνική Συμμαχία Κυβερνοασφάλειας αναφέρει ότι το 60% των ΜΜΕ που υφίστανται κυβερνοεπίθεση χάνουν την επιχείρησή τους μέσα σε 6 μήνες και «οι μεταποιητικές επιχειρήσεις είναι πολύ πιο επιρρεπείς σε απειλές για την ασφάλειά τους λόγω της συνδεσιμότητας με ψηφιακά συστήματα και Λειτουργικές Τεχνολογίες μέσω της ψηφιοποίησης της βιομηχανίας 4.0» (Verizon, 2017).

Οι περισσότερες από τις μεταποιητικές εταιρείες, στην προσπάθειά τους να διατηρήσουν ένα ανταγωνιστικό πλεονέκτημα προσαρμόζοντας τις πρακτικές του Industry 4.0, καταβάλλουν σποραδικές προσπάθειες επενδύοντας σε συστήματα ελέγχου και εξωτερικούς συμβούλους, αλλά δεν διαθέτουν ολοκληρωμένη προσέγγιση στη διαχείριση του κυβερνοχώρου. Οι προσπάθειές τους αποτυγχάνουν να αντιμετωπίσουν αποτελεσματικά τις ραγδαία εξελισσόμενες απειλές στον κυβερνοχώρο, επειδή τα περισσότερα κατασκευαστικά συστήματα αναπτύχθηκαν παραδοσιακά για να εστιάζουν στην ασφάλεια και στις υψηλές επιδόσεις και όχι στην ασφάλεια. Επιπλέον, όσον αφορά την ασφάλεια, οι μεταποιητές ασχολήθηκαν ιστορικά κυρίως με τη διασφάλιση του περιβάλλοντος Λειτουργικών Τεχνολογιών, παραμελώντας συχνά την ασφάλεια πληροφορικής, «η εμφάνιση της Βιομηχανίας 4.0 εισάγει νέες τεχνολογίες σε παραδοσιακά περιβάλλοντα Λειτουργικών Τεχνολογιών και επομένως άτομα εξοικειωμένα με Λειτουργικές Τεχνολογίες που εργάζονται σε τέτοια περιβάλλοντα πρέπει να προσαρμόζονται» (EU Agency for Cybersecurity, 2019). Οι εργαζόμενοι συχνά χρησιμοποιούν δυνητικά αντικρουόμενες πληροφορίες για να περιγράψουν ή να αξιολογήσουν ορισμένες πτυχές του κινδύνου στον κυβερνοχώρο.

Ο CRAM θα περιγράψει δείκτες βασικών κινδύνων που θα μπορούν εύκολα να εφαρμοστούν σε δεδομένα σε πραγματικό χρόνο. Ο CRAM θα επιτρέψει στους υπαλλήλους όχι μόνο να καταρτίσουν μια μακροπρόθεσμη στρατηγική στον κυβερνοχώρο, αλλά και να εκτελέσουν γρήγορα καθημερινές αναφορές. Αυτό θα δείξει τα πραγματικά επίπεδα κινδύνου για τις διαδικασίες ανά πάσα στιγμή,

καίριας σημασίας στο περιβάλλον της μεταποίησης, καθώς η διατήρηση της παραγωγής σε εξέλιξη είναι κρίσιμη και η συντομότερη έλλειψη συγκεκριμένης διαδικασίας μπορεί να έχει ανεπανόρθωτο αντίκτυπο και να προκαλέσει τεράστιες οικονομικές απώλειες. Οι κίνδυνοι ασφάλειας στη μεταποίηση γίνονται όλο και πιο περίπλοκοι και εξελίσσονται, καθιστώντας τεράστια σημασία τον εξοπλισμό των μεταποιητικών ΜΜΕ με το κατάλληλο αναλυτικό εργαλείο για να σκιαγραφηθούν οι προφυλάξεις που πρέπει να λαμβάνονται υπόψη σε καθημερινή βάση στο περιβάλλον παραγωγής. Σε αντίθεση με τις αποτυχίες σε μηχανικές διεργασίες που μπορούν να κατηγοριοποιηθούν ως στατικές, οι αστοχίες στον κυβερνοχώρο είναι δυναμικές αφού σχετίζονται στενά με τις ανθρώπινες αλληλεπιδράσεις.

Ο κύριος στόχος του CRAM είναι να δώσει στους **ηγέτες της μεταποίησης** μια εικόνα για τους **πιθανούς κινδύνους κυβερνοασφάλειας στα συστήματά τους** και να τους υποστηρίξει να **υιοθετήσουν μια αποτελεσματική στρατηγική για τον μετριασμό των κινδύνων.** Δεδομένου ότι είναι διαθέσιμη περιορισμένη έρευνα στον τομέα της εκτίμησης κινδύνου στον κυβερνοχώρο σε συστήματα κατασκευής, το Encrypt 4.0 CRAM θα αντιπροσωπεύει ένα καινοτόμο εργαλείο που στοχεύει να ενσωματωθεί στην πολιτική διαχείρισης κινδύνων των μεταποιητικών εταιρειών.

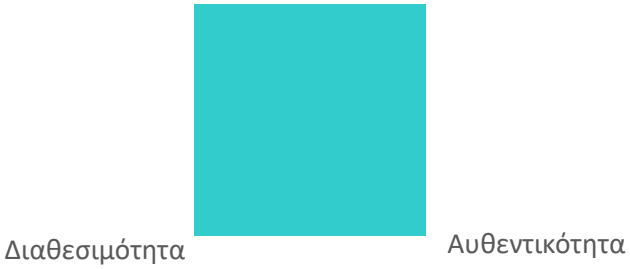


Ο κύριος στόχος του CRAM *είναι να δώσει στους ηγέτες της μεταποίησης μια εικόνα για τους πιθανούς κινδύνους κυβερνοασφάλειας στα συστήματά τους και να τους υποστηρίξει να υιοθετήσουν μια αποτελεσματική στρατηγική για τον μετριασμό των κινδύνων.*

Ο CRAM σχεδιάστηκε λαμβάνοντας υπόψη το κουαρτέτο της CIAA

3. ΜΕΘΟΔΟΛΟΓΙΑ ΤΟΥ CRAM

Ο CRAM σχεδιάστηκε λαμβάνοντας υπόψη το κουαρτέτο της **CIAA** για την **εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα** και την **αυθεντικότητα**. Θα μετρηθούν δύο κύριες πτυχές: **Πιθανότητα κινδύνου** και **Επίδραση κινδύνου**, προσαρμοσμένοι ώστε να **ανταποκρίνονται** στις ειδικές ανάγκες των μεταποιητικών ΜΜΕ με δυνατότητα να διαμορφώνονται εύκολα και να προσαρμόζονται στην ατομική οργανωτική κουλτούρα μιας δεδομένης εταιρείας.



Ο CRAM περιλαμβάνει επίσης: i) αριθμό κινδύνου, ii) κατηγορία κινδύνου, iii) πηγή κινδύνου, iv) περιγραφή κινδύνου, v) δυνητικό κόστος που σχετίζεται με τις συνέπειες του κινδύνου, vi) τμήμα οργάνωσης που μπορεί να επηρεαστεί, vii) μετριασμό/ ενέργειες που είχαν εφαρμοστεί προηγουμένως, viii) αντίκτυπος κινδύνου, ix) πιθανότητα κινδύνου, x) συνολικό επίπεδο κινδύνου, xi) ενεργοποιητές, xii) μετριασμός/ενέργειες που πρέπει να εφαρμοστούν, xiii) δυνητικό κόστος μετριασμού, xiv) προθεσμία, xv) υπεύθυνος για διαχείριση κινδύνου, xvi) επόπτης υπεύθυνος για την παρακολούθηση και xvii) αξιολόγηση της αποτελεσματικότητας.

Παρακάτω, η περιγραφή των βασικών εννοιών που περιλαμβάνουν τον πίνακα ελέγχου του κυβερνοχώρου:

Διαθεσιμότητα: Διασφάλιση έγκαιρης και αξιόπιστης πρόσβασης στις πληροφορίες.

Αυθεντικότητα: Διασφάλιση της ιδιοκτησίας των δεδομένων ως αυθεντικώνής, με δυνατότητα επαλήθευσης και εμπιστοσύνη στην εγκυρότητα μιας μετάδοσης, ενός μηνύματος ή ενός δημιουργού μηνύματος. (Encrypt project 4.0, 2020).

Αξιολόγηση κυβερνοασφάλειας: Ενισχυμένοι μηχανισμοί καθοδήγησης και αξιολόγησης της κυβερνοασφάλειας, συμπεριλαμβανομένων κοινών αρχών για αξιολογήσεις κυβερνοασφάλειας, μηχανισμού βαθμολόγησης βάσει σημείων και πρακτικών βημάτων βελτίωσης, που επιτρέπουν στις

εταιρείες να αξιολογούν και να βελτιώνουν την ετοιμότητά τους για κυβερνοασφάλεια (World Economic Forum , 2017).

Εμπιστευτικότητα: Διατήρηση (ελεγχόμενων) περιορισμών στην πρόσβαση και αποκάλυψη πληροφοριών, συμπεριλαμβανομένων μέσων για την προστασία της ιδιωτικής ζωής και των εμπιστευτικών πληροφοριών.

Επίπτωση: Ο εκτιμώμενος δυνητικός αντίκτυπος που προκύπτει από συμβιβασμό της εμπιστευτικότητας, της ακεραιότητας ή της διαθεσιμότητας ενός τύπου πληροφοριών, εκφρασμένος ως τιμή *χαμηλός, μέτριος ή υψηλός*.

Ακεραιότητα: Προστασία από ακατάλληλη τροποποίηση ή καταστροφή πληροφοριών και περιλαμβάνει τη διασφάλιση της μη απόρριψης και της γνησιότητας των πληροφοριών.

Πιθανότητα: Ένας σταθμισμένος παράγοντας που βασίζεται σε μια υποκειμενική ανάλυση της πιθανότητας ότι μια δεδομένη απειλή είναι ικανή να εκμεταλλευτεί μια δεδομένη ευπάθεια ή ένα σύνολο ευπαθειών.

Περιγραφές εμπνευσμένες από τον Οδηγό για τη διεξαγωγή αξιολογήσεων κινδύνου (National Institute of Standards and Technology, 2012).

4. ΠΙΝΑΚΑΣ ΕΛΕΓΧΟΥ ΚΙΝΔΥΝΩΝ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ - CYBER RISK AUDIT MATRIX (CRAM)

Το Encrypt 4.0 CRAM αντιπροσωπεύει ένα ολοκληρωμένο εργαλείο που στοχεύει στη στήριξη των διευθυντών μεταποιητικών ΜΜΕ για να πραγματοποιήσουν μια ολοκληρωμένη ανάλυση των διαδικασιών τους λαμβάνοντας υπόψη τη χρήση καινοτόμων τεχνολογικών λύσεων που βασίζονται στη Βιομηχανία 4.0 και να εντοπίσουν κινδύνους τους κυβερνοχώρους και να τους υποστηρίξουν στο σχεδιασμό και τον καθορισμό αποτελεσματικών ελέγχων.

4.1 ΚΑΤΗΓΟΡΙΕΣ CRAM

Αυτές οι κατηγορίες προήλθαν από διεξαχθείσα έρευνα και ανάλυση περισσότερων από 20 προτύπων (Παράρτημα Α) στον τομέα της ασφάλειας των πληροφοριών και της προστασίας δεδομένων, καθώς και από 12 εμπεριστατωμένες συνεντεύξεις που πραγματοποιήθηκαν με εμπειρογνώμονες στον τομέα της ασφάλειας στον κυβερνοχώρο από την Αυστρία, την Πορτογαλία, τη Ρουμανία, τη Βουλγαρία, την Κύπρο και την Ισπανία.

Πίνακας 1. Κατηγορίες Πίνακα Ελέγχου Κινδύνων στον Κυβερνοχώρο (CRAM)

Κατηγορία Κινδύνου	Περιγραφή Κατηγορίας Κινδύνου
Ανθρώπινο δυναμικό	Προσδιορισμός των κινδύνων που σχετίζονται με το ανθρώπινο δυναμικό της εταιρείας. Οι κίνδυνοι που σχετίζονται με τους ρόλους και τις ευθύνες του προσωπικού της εταιρείας, τη λήψη αποφάσεων, τη διαχείριση των ταυτοτήτων, τον έλεγχο των προσβάσεων, την ευαισθητοποίηση.
Πνευματική ιδιοκτησία	Προσδιορισμός των κινδύνων που σχετίζονται με την Πνευματική Ιδιοκτησία της εταιρείας. Η Πνευματική Ιδιοκτησία περιλαμβάνει τη Βιομηχανική Ιδιοκτησία, τα Πνευματικά δικαιώματα και τα Συγγενικά δικαιώματα και παρέχει το δικαίωμα αποκλειστικής χρήσης των αντίστοιχων τεχνικών, εμπορικών και βιομηχανικών πληροφοριών. Η Βιομηχανική Ιδιοκτησία στοχεύει στην προστασία εφευρέσεων, διπλωμάτων ευρεσιτεχνίας, brands και έργων που καλύπτονται από αποκλειστικά δικαιώματα χρήσης, παραγωγής και εμπορίας.
Ασφάλεια βιομηχανικών συστημάτων ελέγχου (ICS)	Η ασφάλεια ICS περιλαμβάνει τη φύλαξη και τη διασφάλιση βιομηχανικών συστημάτων ελέγχου καθώς και το απαραίτητο λογισμικό και υλικό που χρησιμοποιούνται από το σύστημα.
Προϊόντα	Προσδιορισμός των κινδύνων που σχετίζονται με τα προϊόντα. Η εμφάνιση αυτού του τύπου κινδύνου μπορεί να θέσει σε κίνδυνο τα προϊόντα που παράγει ο οργανισμός.
Νομικοί κίνδυνοι για την κυβερνοασφάλεια	Προσδιορισμός των κινδύνων που σχετίζονται με νομικές και κανονιστικές ευθύνες. Η εμφάνιση αυτού του τύπου κινδύνου μπορεί να θέσει σε κίνδυνο τις νομικές ή / και κανονιστικές ευθύνες του οργανισμού.
Επιθέσεις αλυσίδας εφοδιασμού	Εντοπισμός τρωτών σημείων στην αλυσίδα εφοδιασμού. Ο οργανισμός πρέπει να καθορίσει, να αξιολογήσει και να διαχειριστεί τις διαδικασίες διαχείρισης κινδύνου της αλυσίδας εφοδιασμού και εφοδιαστικής. Προσδιορισμός των συνδέσμων προς προμηθευτές με κακή στάση ασφαλείας.
Τεχνολογία, ICT και ασφάλεια λειτουργίας	Προσδιορισμός των κινδύνων που σχετίζονται με την τεχνολογία, τις ICT και τις δραστηριότητες της εταιρείας. Για την αντιμετώπιση των κινδύνων που προκύπτουν από λειτουργικές ανεπάρκειες της προβλεπόμενης λειτουργικότητας, λειτουργικές διαταραχές ή από εύλογα προβλέψιμη κακή χρήση/λάθη από τους συνεργάτες που σχετίζονται με την τεχνολογία, τις ICT και τις λειτουργίες.
Πελάτες	Η εμφάνιση ενός συγκεκριμένου κινδύνου μπορεί να θέσει σε κίνδυνο την υπηρεσία που παρέχεται στους πελάτες του οργανισμού ή να θέσει σε κίνδυνο τα δεδομένα των πελατών.
Φυσική κυβερνοασφάλεια	Η φυσική κυβερνοασφάλεια είναι η προστασία των φυσικών συστημάτων στον κυβερνοχώρο, οι συσκευές του Διαδικτύου των πραγμάτων, η προστασία των ανθρώπων, της περιουσίας και των φυσικών περιουσιακών στοιχείων από ενέργειες και γεγονότα που θα μπορούσαν να προκαλέσουν ζημιά ή απώλεια.

5. ΕΛΕΓΧΟΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

5.1 ΤΙ ΕΙΝΑΙ Ο ΕΛΕΓΧΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ;

Η τέταρτη βιομηχανική επανάσταση ή Industry 4.0 έφερε μια σειρά ή νέες τεχνολογίες που συνδέουν τον φυσικό και τον ψηφιακό κόσμο των επιχειρηματικών διαδικασιών σε ολοκληρωμένα έξυπνα συστήματα. Αυτό φέρνει πολλές ευκαιρίες για τη βελτίωση των διαδικασιών και τη συνολική απόδοση, αλλά και πολλές νέες ευθύνες και απειλές. Το υψηλότερο επίπεδο συνδεσιμότητας μεταξύ όλων των συστημάτων μέσω Διαδικτύου των Πραγμάτων, cloud computing και πολλών άλλων τεχνολογιών, εκτός από πολλά οφέλη, έχει νέες προκλήσεις για τις εταιρείες που σχετίζονται με την ασφάλεια των πληροφοριών, τα Μεγάλα δεδομένα κ.λπ., η οποία επεξεργάζεται από αυτά τα ολοκληρωμένα συστήματα, Μεγάλα Δεδομένα κτλ. Αυτός είναι ο λόγος για τον οποίο οι εταιρείες και ιδιαίτερα οι ΜΜΕ χρειάζονται εργαλεία για να τις υποστηρίξουν στη διαδικασία ελέγχου και ανάλυσης των αδυναμιών τους όσον αφορά την ασφάλεια των τεχνολογιών Industry 4.0 που έχουν θεσπίσει. Ένα αποτελεσματικό εργαλείο για την εφαρμογή αυτού του ελέγχου είναι η διενέργεια ελέγχου κυβερνοασφάλειας.

Ο έλεγχος στον κυβερνοχώρο αντιπροσωπεύει την αξιολόγηση της απόδοσης σύμφωνα με τις προδιαγραφές, τα πρότυπα, τους ελέγχους ή τις κατευθυντήριες γραμμές.

Ένας έλεγχος στον κυβερνοχώρο αντιπροσωπεύει μια αξιολόγηση της απόδοσης σύμφωνα με τις προδιαγραφές, τα πρότυπα, τους ελέγχους ή τις κατευθυντήριες γραμμές (CyLumena, 2020). Οι έλεγχοι στον κυβερνοχώρο γίνονται συνήθως με βάση μια λίστα ελέγχων (βιβλιοθήκη ελέγχων) που ορίζονται με βάση ορισμένα πρότυπα για την ασφάλεια στον κυβερνοχώρο (εθνικά, διεθνή, εσωτερικά για την εταιρεία) ή/και διαδικασίες και/ή πολιτικές της εταιρείας. Ο σκοπός ενός ελέγχου κυβερνοασφάλειας είναι να βοηθήσει τους οργανισμούς να εκτιμήσουν εάν διαθέτουν κατάλληλους μηχανισμούς ασφαλείας, εντοπίζοντας κενά ασφαλείας ή επικυρώνοντας τις εφαρμοζόμενες διαδικασίες και πολιτικές. Οι έλεγχοι στον κυβερνοχώρο βοηθούν τις επιχειρήσεις να επαληθεύσουν τι υπάρχει στο δίκτυό τους, τι πρέπει να προστατευθεί και ποια κενά υπάρχουν στις υπάρχουσες προστασίες τους, ώστε να μπορούν να κάνουν βελτιώσεις (Dosal, 2020).

ΕΛΕΓΧΟΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ VS. ΑΞΙΟΛΟΓΗΣΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Οι έλεγχοι στον κυβερνοχώρο διαφέρουν από τις εκτιμήσεις για την ασφάλεια στον κυβερνοχώρο. Ενώ ο έλεγχος της κυβερνοασφάλειας αφορά εάν υπάρχουν ορισμένοι έλεγχοι, η αξιολόγηση της κυβερνοασφάλειας στοχεύει στην αξιολόγηση της αποτελεσματικότητας αυτών των ελέγχων (Aldorisio, 2020). Οι αξιολογήσεις μπορεί να περιλαμβάνουν κάποιο βαθμό ελέγχου αλλά όχι πάντα. Οι έλεγχοι στον κυβερνοχώρο, ανάλογα με τον στόχο, θα μπορούσαν επίσης να εφαρμοστούν όταν ένας οργανισμός θέλει να αξιολογήσει τη συμμόρφωσή τους με ορισμένους νόμους ή πρότυπα, στην περίπτωση αυτή συνήθως ο έλεγχος διενεργείται από τρίτο εξωτερικό που έχει την απαραίτητη ικανότητα. Οι αξιολογήσεις κυβερνοασφάλειας, από την άλλη πλευρά, θα μπορούσαν να πραγματοποιηθούν εσωτερικά από άτομα εντός του οργανισμού που έχουν καλή γνώση της υποδομής κυβερνοασφάλειας.

ΕΞΩΤΕΡΙΚΟΙ VS. ΕΣΩΤΕΡΙΚΟΙ ΕΛΕΓΧΟΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

Οι εξωτερικοί έλεγχοι διενεργούνται από επαγγελματίες, ειδικά όταν ο σκοπός του ελέγχου είναι να παράσχει έδαφος για πιστοποίηση σύμφωνα με ορισμένα πρότυπα κυβερνοασφάλειας και αξιολόγηση συμμόρφωσης με επίσημα πρότυπα, νόμους κ.λπ. που γνωρίζει καλά τις διαδικασίες της εταιρείας και την αρχιτεκτονική κυβερνοασφάλειας. Σύμφωνα με τον GDPR (GDPR.EU Nd), κάθε εταιρεία υποχρεούται νομικά να έχει έναν διορισμένο Υπεύθυνο Προστασίας Δεδομένων ο οποίος να γνωρίζει τη διαχείριση δεδομένων - ποιες πληροφορίες εισέρχονται και εξέρχονται από την εταιρεία, σε ποιες διαδικασίες χρησιμοποιούνται και πώς χρησιμοποιούνται

διαχειρίστηκε. Επομένως, μια φυσική επιλογή για τη διενέργεια εσωτερικού ελέγχου κυβερνοασφάλειας θα μπορούσε να είναι ο διορισμένος Υπεύθυνος Προστασίας Δεδομένων ή μια ομάδα εταιρείας ανάλογα με το πεδίο του ελέγχου. Στις επόμενες ενότητες αυτού του εγγράφου θα παρουσιάσουμε μια συνδυασμένη προσέγγιση για τη διενέργεια εσωτερικού ελέγχου και αξιολόγησης της κυβερνοασφάλειας που βασίζεται σε αρκετές προαναφερθείσες κατηγορίες που πρέπει να ληφθούν υπόψη κατά τη διαδικασία ελέγχου.

5.2 ΠΩΣ ΓΙΝΕΤΑΙ Ο ΕΣΩΤΕΡΙΚΟΣ ΕΛΕΓΧΟΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ;

Σκοπός αυτής της ενότητας είναι να παρέχει εύκολες οδηγίες για τη διενέργεια ελέγχου αυτο-κυβερνοασφάλειας (εσωτερικός έλεγχος κυβερνοασφάλειας), ο οποίος θα μπορούσε να χρησιμεύσει ως αποτελεσματικό εργαλείο για την αξιολόγηση της ασφάλειας στον κυβερνοχώρο και των δεδομένων στον οργανισμό σας ή/και ως προετοιμασία για εξωτερικούς (third-party) ελέγχους κυβερνοασφάλειας.

ΒΗΜΑ 1: Καθορίστε τις προτεραιότητες ασφάλειας του οργανισμού σας και το εύρος του ελέγχου

Σε αυτό το στάδιο, το άτομο ή η ομάδα που έχει οριστεί για τη διενέργεια του ελέγχου πρέπει να προσδιορίσει ποιο θα είναι το πεδίο εφαρμογής της διαδικασίας ελέγχου. Ένα καλό σημείο εκκίνησης είναι να απαριθμήσετε όλα τα περιουσιακά στοιχεία του κυβερνοχώρου της εταιρείας, όπως θα μπορούσαν να είναι τα περιουσιακά στοιχεία στον κυβερνοχώρο που σχετίζονται με κρίσιμα περιουσιακά στοιχεία, όπως: συστήματα ελέγχου, συστήματα συλλογής δεδομένων, εξοπλισμός δικτύωσης, πλατφόρμες υλικού για εικονικές μηχανές ή χώρο αποθήκευσης. Δευτερεύοντα ή υποστηρικτικά συστήματα όπως σαρωτές ιών, συστήματα HVAC και αδιάλειπτα τροφοδοτικά (UPS) (η.δ., Versify Solutions);

Στη συνέχεια, πρέπει να αξιολογήσετε ποια είναι τα κρίσιμα στοιχεία στον κυβερνοχώρο (CCA). Σύμφωνα με το πρότυπο Critical Infrastructure Protection (CIP), έκδοση 4 από την North American Electric Reliability Corporation (NERC) ένα CCA είναι «κάθε συσκευή που χρησιμοποιεί δρομολογούμενο πρωτόκολλο για να επικοινωνεί έξω από την ηλεκτρονική περίμετρο ασφαλείας (ESP), χρησιμοποιεί δρομολογούμενο πρωτόκολλο εντός ένα κέντρο ελέγχου ή είναι προσβάσιμο μέσω τηλεφώνου. »(2011, Flick & Morehouse).

Με πιο απλά λόγια, τα περιουσιακά στοιχεία περιλαμβάνουν εξοπλισμό υπολογιστών, διάφορα συστήματα και ευαίσθητες πληροφορίες πελατών και εταιρειών, εσωτερικά έγγραφα και συστήματα επικοινωνίας.

Μόλις εντοπιστούν τα κρίσιμα περιουσιακά στοιχεία στον κυβερνοχώρο, θα πρέπει να προσδιορίσετε πού βρίσκονται οι κρίσιμες παράμετροι ασφάλειας και έτσι να τμηματοποιήσετε τι θα συμπεριληφθεί στο πεδίο ελέγχου (2019, LeCount). Οι παράμετροι ασφάλειας και τα περιουσιακά στοιχεία θα διαφέρουν πολύ από εταιρεία σε εταιρεία, επομένως αυτό το αρχικό βήμα και ο σωστός ορισμός του πεδίου ελέγχου είναι ζωτικής σημασίας για την αποτελεσματικότητα της διαδικασίας ελέγχου. Μόλις οριστεί το πεδίο ελέγχου, μπορείτε να προχωρήσετε στο επόμενο βήμα - προσδιορισμός πιθανών απειλών.

ΒΗΜΑ 2: Προσδιορίστε τους πιθανούς κινδύνους και απειλές

Με βάση 12 συνεντεύξεις με εμπειρογνώμονες στον τομέα της κυβερνοασφάλειας, η κοινοπραξία ENCRYPT 4.0 έχει εντοπίσει εννέα πιθανές κατηγορίες κινδύνων και έχει καταρτίσει μια λίστα με πιθανές απειλές που κάθε μία από αυτές τις κατηγορίες μπορεί να υπάρξει σε κρίσιμα περιουσιακά στοιχεία στον κυβερνοχώρο. Το μοντέλο ENCRYPT περιλαμβάνει τις ακόλουθες εννέα κατηγορίες κινδύνου που πρέπει να ληφθούν υπόψη: (1) Ανθρώπινοι πόροι. (2) Πνευματική ιδιοκτησία. (3) Ασφάλεια βιομηχανικών συστημάτων ελέγχου (ICS). (4) Προϊόντα. (5) Νομικοί κίνδυνοι για την ασφάλεια στον κυβερνοχώρο. (6) Επιθέσεις αλυσίδας εφοδιασμού. (7) Τεχνολογία, ICT και επιχειρησιακή ασφάλεια. (8) Πελάτες. (9) Φυσική ασφάλεια στον κυβερνοχώρο.

Έχετε υπόψη ότι, ανάλογα με τις επιχειρηματικές δραστηριότητες του οργανισμού σας, το επιχειρηματικό μοντέλο και τον τομέα δραστηριοτήτων, όλες οι κατηγορίες ενδέχεται να μην ισχύουν για εσάς ή μπορεί να αποφασίσετε ότι δεν έχετε κρίσιμα περιουσιακά στοιχεία στον κυβερνοχώρο που συνδέονται με αυτές τις κατηγορίες. Για κάνετε την αξιολόγηση αυτή δείτε το Παράρτημα 1 και επιλέξτε τις κατηγορίες που εφαρμόζονται στον οργανισμό σας και τις απειλές που θεωρείτε σχετικές, ανάλογα με τα αναγνωρισμένα κρίσιμα περιουσιακά στοιχεία στον κυβερνοχώρο εντός της εταιρείας σας.

ΒΗΜΑ 3: Δώστε προτεραιότητα στους κινδύνους

Σε αυτό το κρίσιμο βήμα πρέπει να ελέγξετε τη λίστα με τις πιθανές απειλές που θεωρείτε ότι ισχύουν για την εταιρεία σας και σύμφωνα με ένα σύνολο κριτηρίων να αποφασίσετε ποιοι κίνδυνοι είναι πολύ πιθανοί και με δυνητικά πιο σοβαρό αρνητικό αντίκτυπο. Για το λόγο αυτό, η κοινοπραξία ENCRYPT 4.0 έχει αναπτύξει μια μεθοδολογία εκτίμησης κινδύνου που λαμβάνει υπόψη τα ακόλουθα στοιχεία:

- Δυνητικό κόστος που σχετίζεται με τις συνέπειες του κινδύνου
- Τμήμα (-τα) του οργανισμού που μπορεί να επηρεαστεί (-ούν)
- Πιθανή επίπτωση
- Πιθανότητα - κατά την αξιολόγηση της πιθανότητας, λάβετε υπόψη τις τάσεις του κλάδου, προηγούμενες παραβιάσεις ασφαλείας
- Επίπεδο κινδύνου.

Μπορείτε να χρησιμοποιήσετε απευθείας το εργαλείο ENCRYPT 4.0 CRAM που αναπτύχθηκε για να ιεραρχεί εύκολα τους πιθανούς κινδύνους.

ΒΗΜΑ 4: Ελέγξτε τα ισχύοντα μέτρα ασφαλείας

Έχοντας εντοπίσει τις κατηγορίες κινδύνου και τις απειλές που εφαρμόζονται στον οργανισμό σας, το επόμενο βήμα είναι να αξιολογήσετε εάν τα κρίσιμα περιουσιακά στοιχεία και η υποδομή σας στον κυβερνοχώρο είναι ευάλωτα σε οποιαδήποτε από αυτές τις απειλές. Για το σκοπό αυτό, πρέπει να αξιολογήσετε τα πρωτόκολλα/διαδικασίες/μέτρα ασφαλείας που έχουν θεσπιστεί σχετικά με τον εντοπισμό πιθανών κενών ασφαλείας που πρέπει να αντιμετωπιστούν. Στον πίνακα 2 θα βρείτε μερικές καθοδηγητικές ερωτήσεις και συμβουλές για το πώς να αξιολογήσετε εάν τα μέτρα ασφαλείας είναι επαρκή, ωστόσο εξαρτάται επίσης από τις απειλές που θεωρείτε εφαρμοστέες σε κάθε κατηγορία.

Πίνακας 2. Συμβουλές για το πως να προσδιορίσετε τα μέτρα ασφαλείας που ισχύουν

Αρ.	Κατηγορία	Συμβουλές για τον τρόπο ελέγχου των μέτρων ασφαλείας που ισχύουν
1	**Ανθρώπινο δυναμικό**	Ελέγξτε την κατανομή των ρόλων και των ευθυνών που σχετίζονται με τη διαχείριση και την ασφάλεια των δεδομένων κυβερνοασφάλειας, τον έλεγχο συστήματος κ.λπ. Μιλήστε με τους υπεύθυνους υπαλλήλους σε αυτούς τους τομείς - ρωτήστε τους πώς θα αντιδρούσαν σε ορισμένες καταστάσεις, ποια πρωτόκολλα ασφαλείας θα εφάρμοζαν, έτσι θα μπορείτε να αξιολογήσετε εάν το προσωπικό είναι ενήμερο και προετοιμασμένο σε περίπτωση πραγματοποίησης ορισμένων κινδύνων κυβερνοασφάλειας. εάν χρειάζονται εκπαίδευση ή όχι. Αναλύστε ατυχήματα και παραβιάσεις ασφαλείας λόγω των λαθών των εργαζομένων και τον τρόπο χειρισμού τους. Σκεφτείτε αν υπάρχει κάτι περισσότερο που θα μπορούσε να γίνει για να ελαχιστοποιηθεί περαιτέρω η εμφάνιση αυτής της απειλής στο μέλλον.
2	**Πνευματική ιδιοκτησία**	Ελέγξτε την κατανομή των ρόλων και των ευθυνών που σχετίζονται με τη διαχείριση πνευματικής ιδιοκτησίας, καθώς και τα εμπορικά απόρρητα κ.λπ. Μιλήστε με τους υπεύθυνους υπαλλήλους, ανατρέξτε στη σχετική τεκμηρίωση σχετικά με την προστασία περιουσιακών στοιχείων, όπως διπλώματα ευρεσιτεχνίας, πνευματικά δικαιώματα εμπορικών σημάτων. Πώς διατηρείται και διαχειρίζεται αυτή η τεκμηρίωση, ποιος έχει πρόσβαση σε αυτήν; Υπήρξαν περιστατικά στο παρελθόν που σχετίζονται με παραβιάσεις πληροφοριών, ελλείψεις πληροφοριών σε αυτόν τον τομέα; Πώς χειρίστηκαν, ενημερώνεται το πρωτόκολλο ασφαλείας;
3	**Ασφάλεια βιομηχανικών συστημάτων ελέγχου (ICS)**	Ποιος έχει απομακρυσμένη ή/και φυσική πρόσβαση στο ICS; Πώς διαχειρίζεται η απομακρυσμένη πρόσβαση στο ICS; Υπάρχουν έλεγχοι ασφαλείας όπως ισχυρός έλεγχος ταυτότητας, έλεγχος πρόσβασης και κρυπτογράφηση για προστασία από μη εξουσιοδοτημένη πρόσβαση και εκμετάλλευση αυτών των συστημάτων; Τι είναι τα μέτρα φυσικού ελέγχου πρόσβασης; Χρησιμοποιείτε τείχη προστασίας που γνωρίζουν πρωτόκολλο ICS για να επιβάλλετε ελέγχους πρόσβασης στην κυκλοφορία δικτύου ICS; Έχετε εγκατεστημένο σύστημα πρόληψης εισβολής;

4	**Προϊόντα**	Ανάλογα με τη διαδικασία παραγωγής των προϊόντων, πρέπει να προσδιορίσετε σε ποιες διαδικασίες χειρίζονται ευαίσθητες πληροφορίες και με ποιον τρόπο διαχειρίζονται και διαχειρίζονται. Υπάρχουν εμπορικά μυστικά που σχετίζονται με την παραγωγή προϊόντων κ.λπ. Πώς διασφαλίζει η εταιρεία ότι αυτές οι πληροφορίες διαχειρίζονται με ασφάλεια; Τι είναι το πρωτόκολλο - ρόλοι και ευθύνες, διαδικασίες κλπ.; Υπάρχει έλεγχος φυσικής και απομακρυσμένης πρόσβασης σε υπολογιστές και δίκτυα; συστήματα παραγωγής κλπ.; Πώς διασφαλίζονται και ελέγχονται αυτά;
5	**Νομικοί κίνδυνοι για την κυβερνοασφάλεια**	Υπάρχει κάποιος έλεγχος της φυσικής και απομακρυσμένης πρόσβασης σε εταιρικούς υπολογιστές και δίκτυα; Πώς διασφαλίζονται και ελέγχονται αυτά; Πώς διαχειρίζονται και διαχειρίζονται νομικά δεδομένα; Είναι ασφαλής ο διακομιστής; Ποιος έχει πρόσβαση σε αυτές τις πληροφορίες; Υπήρξαν παραβιάσεις ασφαλείας στο παρελθόν; Πώς χειρίστηκαν; Υπάρχει τρόπος βελτίωσης των πρωτοκόλλων ασφαλείας με βάση τις πρόσφατες τάσεις/γεγονότα/τεχνολογικές εξελίξεις;
6	**Επιθέσεις αλυσίδας εφοδιασμού**	Ποιος έχει πρόσβαση σε συστήματα διαχείρισης εφοδιασμού; Υπάρχει Privileged Access Management; Ποιος έχει πρόσβαση σε ευαίσθητα δεδομένα; Πώς διασφαλίζεται αυτή η πρόσβαση; Έχετε εφαρμόσει Honeytokens; Ποιο είναι το επίπεδο ελέγχου της πρόσβασης από τους προμηθευτές υπηρεσιών; Πόσοι προμηθευτές έχουν πρόσβαση σε λογισμικό; Παρακολουθείται το δίκτυο προμηθευτών για ευπάθειες;
7	**Τεχνολογία, ICT και ασφάλεια λειτουργίας**	Έχετε αυστηρές πολιτικές ασφάλειας και προστασίας δεδομένων για κινητά; Είναι όλες οι εφαρμογές λογισμικού και τα λειτουργικά συστήματα ενημερωμένα; Υπάρχουν έλεγχοι πρόσβασης για κρίσιμα περιουσιακά στοιχεία κυβερνοασφάλειας; Παρακολουθείτε τη δραστηριότητα των λογαριασμών χρηστών, την καταγραφή και την πρόσβαση στο δίκτυό σας; Ελέγξτε εάν τα τείχη προστασίας έχουν διαμορφωθεί σωστά, βεβαιωθείτε ότι έχετε κρυπτογράφηση από άκρο σε άκρο για ευαίσθητα δεδομένα.

		Έχετε θεσπίσει μηχανισμούς για την αναγνώριση και την αποφυγή επιθέσεων όπως το phishing και το pharming;
8	**Πελάτες**	Ποιος έχει πρόσβαση σε σημαντικά δεδομένα πελατών; Έχετε αντίγραφο ασφαλείας σημαντικών επιχειρηματικών δεδομένων και πληροφοριών;
9	**Φυσική κυβερνοασφάλεια**	Πώς διαχειρίζεται η συντήρηση του εξοπλισμού και των κρίσιμων στοιχείων του κυβερνοασφάλειας; Ποιος έχει φυσική πρόσβαση σε εξοπλισμό και κρίσιμα περιουσιακά στοιχεία κυβερνοασφάλειας; Πώς διασφαλίζεται η πρόσβαση;

ΒΗΜΑ 5: Ορίστε/ ενημερώστε τα πρωτόκολλα ασφαλείας βάσει του ελέγχου

Μόλις ολοκληρώσετε το ΒΗΜΑ 4, πρέπει να έχετε τον κατάλογό σας με τις πιθανές απειλές που ισχύουν για τον οργανισμό σας, να γνωρίζετε τι κάνετε ήδη και τι ίσως λείπει και να προσδιορίσετε επαρκείς ελέγχους ασφάλειας πληροφοριών για να εξουδετερώσετε ή να εξαλείψετε τον κίνδυνο απειλής (2020 , LeCount).

Οι έλεγχοι ασφάλειας πληροφοριών είναι μέτρα που λαμβάνονται για τη μείωση των κινδύνων ασφάλειας πληροφοριών, όπως παραβιάσεις συστημάτων πληροφοριών, κλοπή δεδομένων και μη εξουσιοδοτημένες αλλαγές σε ψηφιακές πληροφορίες ή συστήματα (Garcia, 2019). Ο κύριος στόχος των ελέγχων ασφαλείας είναι η προστασία της διαθεσιμότητας, του απορρήτου και της ακεραιότητας των δεδομένων και των δικτύων εντός μιας εταιρείας. Όπως αναφέρθηκε, οι έλεγχοι ασφαλείας εφαρμόζονται συνήθως μετά από εκτίμηση κινδύνου πληροφοριών ή κυβερνοασφάλειας και αντιπροσωπεύουν το επιθυμητό αποτέλεσμα των εκτιμήσεων και των ελέγχων στον κυβερνοχώρο σχετικά με την αντιμετώπιση των εντοπισμένων πραγματικών ή πιθανών κενών ασφάλειας.

Στον πίνακα 3, σε συνδυασμό με το ENCRYPT 4.0 CRAM βάσει συνεντεύξεων με εμπειρογνώμονες στον τομέα της ασφάλειας στον κυβερνοχώρο από 6 χώρες της ΕΕ, εντοπίσαμε δύο τύπους ελέγχων - προληπτικούς και διορθωτικούς σε καθεμία από τις εννέα κατηγορίες κινδύνου. Με βάση τον έλεγχο που διεξήχθη στο ΒΗΜΑ 4, γνωρίζετε ήδη τις διαδικασίες κυβερνοασφάλειας που ισχύουν στον οργανισμό σας. Στον πίνακα 3, μπορείτε να βρείτε μερικές προτάσεις προληπτικών και διορθωτικών ελέγχων για καθεμία από τις κατηγορίες που ενδέχεται να χάσετε στον οργανισμό σας.

Πίνακας 3. Προληπτικοί και διορθωτικοί έλεγχοι για την κυβερνοασφάλεια

Κατηγορία Κινδύνου	Προληπτικά μέτρα	Διορθωτικά μέτρα
Ανθρώπινο δυναμικό	Καθιέρωση προγράμματος κατάρτισης και ευαισθητοποίησης Προσδιορίστε με σαφήνεια τη διαχείριση των ταυτοτήτων, τον έλεγχο ταυτότητας και τον έλεγχο των προσβάσεων Η εταιρεία έχει πολιτική που περιλαμβάνει: ● Κατάλογο εγκεκριμένου λογισμικού. ● Εξουσιοδοτημένο αποθετήριο λογισμικού και μητρώο αδειών. ● Πειθαρχικές κυρώσεις που σχετίζονται με τη μη συμμόρφωση με αυτούς τους κανονισμούς. Περιστροφή των κωδικών πρόσβασης σε τριμηνιαία βάση ("ισχυρή πολιτική κωδικού πρόσβασης") Αναπτύξτε λύσεις αποκατάστασης καταστροφών και σχέδια συνέχειας των επιχειρήσεων	Ελέγξτε τις άδειες χρήσης. Εφαρμόστε το Σύστημα Ανίχνευσης Εισβολής (IDS) για να εντοπίσετε μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή ή δίκτυο Αλλάξτε όλους τους κωδικούς πρόσβασης μετά από πιθανή παραβίαση δεδομένων Κλείδωμα λογαριασμών υπόπτων για μη εξουσιοδοτημένη πρόσβαση Ορίστε τον έλεγχο ταυτότητας δύο παραγόντων, όταν είναι δυνατόν, ο οποίος θα παρέχει έλεγχο ταυτότητας δύο παραγόντων
Πνευματική ιδιοκτησία	Σωστές πολιτικές και ευθύνες για τη διαχείριση της πνευματικής ιδιοκτησίας Όλα τα ισχύοντα περιουσιακά στοιχεία πρέπει να προστατεύονται από κατοχυρωμένα διπλώματα ευρεσιτεχνίας, πνευματικά δικαιώματα και εμπορικά σήματα. Τα σχετικά περιουσιακά στοιχεία πρέπει να παρακολουθούνται και να προστατεύονται από ασφαλίσεις. Ανάπτυξη μέτρων, πολιτικών και ευθυνών για τη διαχείριση της φήμης	Τακτική αξιολόγηση και ενημέρωση πολιτικών και αρμοδιοτήτων Εάν λείπει το καταχωρημένο δίπλωμα ευρεσιτεχνίας, πρέπει να αποκτηθεί προσωρινό δίπλωμα ευρεσιτεχνίας, εμπορικό σήμα και πνευματικά δικαιώματα Τακτική αξιολόγηση και ενημέρωση πολιτικών και αρμοδιοτήτων
Ασφάλεια βιομηχανικών συστημάτων ελέγχου (ICS)	Ανάπτυξη μέτρων, πολιτικών, ευθυνών και ταχεία αντίδραση σε περίπτωση εμφάνισης	Τακτική αξιολόγηση και ενημέρωση πολιτικών και αρμοδιοτήτων.
Προϊόντα	Αξιολόγηση διαδικασιών ροής εργασίας Τυποποίηση και εξέλιξη Ελέγξτε τη φυσική πρόσβαση σε υπολογιστές και στοιχεία δικτύου	Εφαρμόστε μια πολυεπίπεδη προσέγγιση για κάθε κίνδυνο ή τουλάχιστον για εκείνους που έχουν μεγάλες δυνατότητες στη συγκεκριμένη περίπτωση, προκειμένου να έχετε τουλάχιστον μερικά επίπεδα προστασίας, ανεξάρτητα από την τεχνολογία,

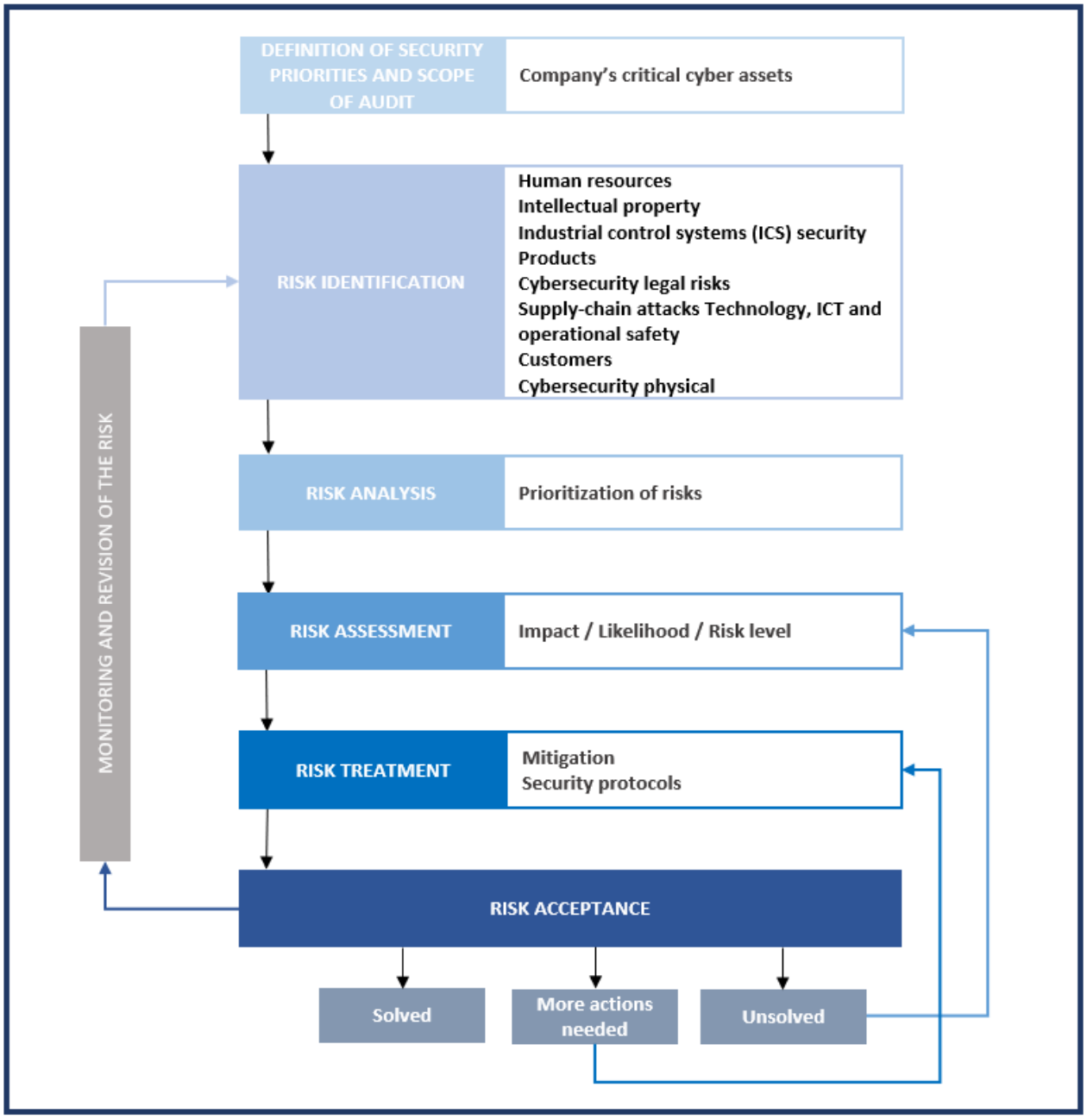
Κατηγορία Κινδύνου	Προληπτικά μέτρα	Διορθωτικά μέτρα
		τους υπαλλήλους, τις διαδικασίες, τους πελάτες κ.λπ.
Νομικοί κίνδυνοι για την κυβερνοασφάλεια	Κρατήστε μόνο ό, τι χρειάζεστε. Απογραφή του τύπου και της ποσότητας των πληροφοριών στα αρχεία σας και στους υπολογιστές σας Δεδομένα διασφάλισης Καταστροφή πριν από τη διάθεση Διαδικασίες ενημέρωσης Εκπαίδευση Υπαλλήλων Έλεγχος χρήσης υπολογιστή. Ασφαλίστε όλους τους υπολογιστές.	Προσδιορίστε τα επηρεαζόμενα μέρη Ειδοποιήστε τα επηρεαζόμενα άτομα Αναζητήστε νομικό σύμβουλο
Επιθέσεις αλυσίδας εφοδιασμού	Εφαρμόστε Honeytokens Ασφαλής Διαχείριση Προνομιακής Πρόσβασης Προσδιορίστε όλα τα πιθανά εσωτερικά νήματα Εντοπισμός και προστασία ευάλωτων πόρων Ελαχιστοποιήστε την πρόσβαση σε ευαίσθητα δεδομένα Στείλτε τακτικές εκτιμήσεις κινδύνου τρίτων Παρακολουθήστε το δίκτυο προμηθευτών για ευπάθειες Προσδιορίστε όλες τις διαρροές δεδομένων προμηθευτή	Ελέγξτε τις άδειες σε όλη την αλυσίδα εφοδιασμού των MME Αναζητήστε τα δεδομένα επαφής της προληπτικής και διορθωτικής συντήρησης μηχανημάτων MME σε όλη την αλυσίδα εφοδιασμού σε περιφερειακό/τοπικό επίπεδο
Τεχνολογία, ICT και ασφάλεια λειτουργίας	Κατεβάστε και εγκαταστήστε ενημερώσεις λογισμικού για τα λειτουργικά συστήματα και τις εφαρμογές σας, καθώς αυτές είναι διαθέσιμες Ενημερωμένα λειτουργικά συστήματα και υλικολογισμικό Εγκαταστήστε τείχος προστασίας μεταξύ του Διαδικτύου και του LAN Προσδιορίστε κρίσιμα περιουσιακά στοιχεία Ευαισθητοποίηση για την ασφάλεια, Δημιουργία αντιγράφων ασφαλείας και ανάκτηση, Ευπάθεια και διαχείριση επιδιορθώσεων, Εφαρμόστε στοιχεία ελέγχου πρόσβασης, Χρήση περιεχομένου και φιλτραρίσματος λευκής λίστας,	Ελέγξτε όλες τις προθεσμίες λειτουργικού συστήματος και υλικολογισμικού που έχετε στις MME σας και εποπτεύετε όλες τις ενημερώσεις Για να εγκαταστήσετε τείχος προστασίας μεταξύ Internet και LAN. Κατάργηση λογισμικού που είναι παράνομο ή δεν επιτρέπεται στο χώρο αποθήκευσης λογισμικού Τυπικές εγκαταστάσεις για όλο τον εξοπλισμό υπολογιστών

Κατηγορία Κινδύνου	Προληπτικά μέτρα	Διορθωτικά μέτρα
	Σωστή διαμόρφωση τελικών σημείων, Δημιουργία διαδικασιών απόκρισης περιστατικών, Χρησιμοποιήστε λύσεις και συστήματα ευφυΐας απειλών. Τα σωστά διαμορφωμένα τείχη προστασίας, οι αυστηρές πολιτικές ασφαλείας για κινητά, η κρυπτογράφηση από άκρο σε άκρο, η καταγραφή ελέγχου και η εξουσιοδότηση συσκευών για πρόσβαση στο δίκτυο είναι μερικές από τις πρακτικές που μειώνουν τις απειλές από τη χρήση κινητών συσκευών σε εταιρικό δίκτυο. Αξιολογήστε το λογισμικό σε σχέση με τις αρχές ασφάλειας στον κυβερνοχώρο. Βεβαιωθείτε ότι τα λειτουργικά συστήματα και όλες οι εφαρμογές λογισμικού είναι ενημερωμένες, Βεβαιωθείτε ότι τα ευαίσθητα δεδομένα είναι κρυπτογραφημένα, Χρησιμοποιήστε λογισμικό προστασίας δεδομένων, Παρακολουθεί τακτικά τη δραστηριότητα των λογαριασμών χρηστών, Διαχειριστείτε τις ρυθμίσεις απορρήτου για εφαρμογές για κινητά, Επιβολή αυστηρών ελέγχων συσκευής για αφαιρούμενα μέσα, Δημιουργήστε μηχανισμούς για την αναγνώριση και την αποφυγή επιθέσεων όπως το phishing και το pharming. Λειτουργία βασισμένη σε πολιτικές και κανόνες ασφαλείας.	Για να διαμορφώσετε το VPN εάν είναι απαραίτητο να συνδεθείτε από έξω. Προσδιορισμός και διόρθωση του ζητήματος. Έλεγχος και ενημέρωση των πολιτικών και των κανόνων ασφαλείας.
Πελάτες	Δημιουργήστε αντίγραφα ασφαλείας σημαντικών επιχειρηματικών δεδομένων και πληροφοριών	Ορίστε τον έλεγχο ταυτότητας δύο παραγόντων, όταν είναι δυνατόν, ο οποίος θα παρέχει έλεγχο ταυτότητας δύο παραγόντων Κλείδωμα λογαριασμών υπόπτων για μη εξουσιοδοτημένη πρόσβαση Αποκλεισμός διευθύνσεων IP ύποπτων φορέων απειλής με βάση δραστηριότητες που εντοπίστηκαν

Κατηγορία Κινδύνου	Προληπτικά μέτρα	Διορθωτικά μέτρα
Φυσική κυβερνοασφάλεια	Για την εφαρμογή ενός σχεδίου ασφαλείας σε περίπτωση πυρκαγιών, πλημμυρών, κλοπών, απωλειών... Απενεργοποιήστε τυχόν εργαλεία ή εξοπλισμό που δεν χρησιμοποιούνται Για να έχετε εφεδρική αδιάλειπτη τροφοδοσία ή να λάβετε δεύτερη πηγή ενέργειας έκτακτης ανάγκης Ελέγχετε τακτικά όλες τις συσκευές Κάντε αντίγραφα ασφαλείας Κατά προτίμηση όλα τα δεδομένα φιλοξενούνται στο cloud	Στις εγκαταστάσεις, ενημερωθείτε σχετικά με την ασφάλεια των κτιρίων και εφαρμόστε αντιπυρικά μέτρα. Για να έχετε εφεδρική μπαταρία για τον υπολογιστή σας ή να λάβετε μια δεύτερη πηγή ενέργειας έκτακτης ανάγκης. Για να κάνετε ένα "αντίγραφο ασφαλείας" Κάντε έναν διακόπτη ασφαλείας Αντικαταστήστε ή επιδιορθώστε συσκευές που έχουν υποστεί βλάβη ή έχουν αποτύχει

ΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ ΜΕ ΤΟ CRAM

Εδώ παρουσιάζεται η γραφική επισκόπηση της διαδικασίας ελέγχου χρησιμοποιώντας το Encrypt 4.0 CRAM ως εργαλείο που περιγράφει τα αντίστοιχα μέτρα που πρέπει να ληφθούν από το υπεύθυνο πρόσωπο στην κατασκευή ΜΜΕ για την εκτενή ανάλυση των διαδικασιών τους εντοπίζοντας τους κινδύνους στον κυβερνοχώρο και υποστηρίζοντάς τους ο σχεδιασμός και ο καθορισμός αποτελεσματικών ελέγχων στον τόπο σύμφωνα με την προοδευτική φύση της κυβερνοεπίθεσης.



Ο Encrypt 4.0 CRAM είναι μια συστηματική, συνεχής διαδικασία. Είναι μια κυκλική διαδικασία που μόλις εντοπίσει, αναλύσει, αξιολογήσει, αντιμετωπίσει και αποδεχτεί τους κινδύνους, πρέπει να πραγματοποιήσει μια διαδικασία παρακολούθησης και επανεξέτασης των κινδύνων. Σε περίπτωση που το πρόβλημα επιμένει, θα χρειαστεί να εφαρμόσετε περαιτέρω συμπληρωματικές ενέργειες για την επίλυση του προβλήματος και για αυτό, θα πρέπει να επιστρέψετε στο προηγούμενο βήμα της θεραπείας κινδύνου. Και αν το πρόβλημα παραμένει άλυτο, θα χρειαστεί να επανεκτιμήσετε τον κίνδυνο.

6. ΕΡΓΟ ΚΑΙ ΕΤΑΙΡΟΙ

ENCRYPT 4.0

Κοινή πρωτοβουλία για την ανάπτυξη εργατικού δυναμικού στον κυβερνοχώρο για να μπορέσει η ευρωπαϊκή βιομηχανία να ξεπεράσει την έλλειψη επαγγελματιών στον τομέα της ασφάλειας στο διαδίκτυο.

Το έργο ENCRYPT4.0 (2020-1-RO01-KA202-079983) έχει ως στόχο να επιτρέψει στη διοίκηση των ΜΜΕ της μεταποίησης να υιοθετήσουν μια προληπτική προσέγγιση για την ασφάλεια στον κυβερνοχώρο, υποστηρίζοντάς τους στη διαδικασία ανάλυσης, εντοπισμού και αντιμετώπισης των κυβερνοκινδύνων και απειλών που εφαρμόζονται στον οργανισμό τους. Προωθώντας τη διαδραστική μάθηση που βασίζεται σε έργα όσον αφορά την ενίσχυση των δεξιοτήτων και των ικανοτήτων κυβερνοασφάλειας των εργαζομένων των ΜΜΕ ή/και των επαγγελματιών στον τομέα της ασφάλειας στον κυβερνοχώρο.

"George Emil Palade" University of Medicine, Pharmacy, Sciences and Technology of Târgu Mureș - Romania

European Center for Quality Ltd., Consulting company - Bulgary

Instituto de Soldadura e Qualidade, Technological institution - Portugal

Avantalia, technology-based SME - Spain

FH Joanneum, University of Applied Sciencies - Austria

PCX Management, Computers & Information Systems Ltd. - Cyprus

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

Aldorisio, J., 2020. Best Practices for Cybersecurity Auditing [a Step-by-Step Checklist]. Security Scorecard. Retrieved from https://securityscorecard.com/blog/best-practices-for-a-cybersecurity-audit

Cybersecurity Ventures. (2019). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/annual-cybercrime-report-2019/

Cybersecurity Ventures. (2020). *Cybersecurity Ventures Official Annual Cybercrime Report.* Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

EU Agency for Cybersecurity. (2019). *Industry 4.0 Cybersecurity: Challenges & recommendations.*

European Union Agency for Cybersecurity. (2015). *Information security and privacy standards for SMEs - Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises.* ENISA. doi: 10.2824/829076

Juncker, C. P.-C. (2017). Retrieved from https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

Margot Hutchins, R. B., & Stefanie Robinson, J. S. (2015). Framework for Identifying Cybersecurity Risks in. *U.S. Department of Energy*, 17.

National Institute for Standards and Technology. (2012). *Guide for Conducting Risk Assessments.* Gaithersburg: Special Publication 800-30.

Verizon. (2017). *Verizon Data Breach Investigations Report.* Retrieved from https://www.verizondigitalmedia.com/blog/2017-verizon-data-breach-investigations-report/

Verizon. (2020). *Manufacturing*. Retrieved from Verizon: https://enterprise.verizon.com/resources/reports/dbir/2020/data-breach-statistics-by-industry/manufacturing-data-breaches/

World Economic Forum . (2017). *Innovation-Driven Ciber-risk to Costumer Data in Financial Services.* Cologny/Geneva.

World Economic Forum. (2020). *The Global Risks Report.*

World Economic Forum. (2020). *Wild Wide Web - Consequences of Digital Fragmentation*. Retrieved from World Economic Forum: https://reports.weforum.org/global-risks-report-2020/wild-wide-web/

ΠΑΡΑΡΤΗΜΑ Α - ΣΥΛΛΟΓΗ ΥΠΑΡΧΟΝΤΩΝ ΠΡΟΤΥΠΩΝ ΓΙΑ ΚΙΝΔΥΝΟΥΣ ΣΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

	ΠΡΟΤΥΠΑ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
Ασφάλεια πληροφοριών (Cross-Industry)	ISO/IEC 27001:2018 Information security management systems – Requirements
	ISO/IEC 27002:2018 Code of practice for information security controls
	ISO/IEC 27003:2017 Information security management systems guidance
	ISO/IEC 27004:2016 Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation
	International Organisation for Standardisation and International Electrotechnical Commission
	ISO/IEC 27014:2013 Governance of information security
	ISO/IEC TR 27016:2014 Information security management - Organisational economics
	ISO/IEC 27032:2012 Guidelines for information security
	ISO/IEC 27033-1:2015 Network security - Part 1: Overview and concepts
	ISO/IEC 27033-2:2012 Network security - Part 2: Guidelines for the design and implementation of network security
	ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues
	ISO/IEC 27033-4:2014 Network security - Part 4: Securing communications between networks using security gateways
	ISO/IEC 27033-5:2013 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)
	ISO/IEC 27033-6:2016 Network security - Part 6: Securing wireless IP network access
	ISO/IEC 27034-1:2011 Application security - Part 1: Overview and concepts
	ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS)
	ISO/IEC 27040:2015 Storage security
	CSA Cloud Controls Matrix
	BSI PAS 555:2013 Cybersecurity risk. Governance and management. Specification
	PCI Data Security Standard
	ISF The Standard of Good Practice for Information Security
	UK Gov. Security policy framework
	UK Gov. Cyber essentials scheme
	ETSI GS ISI 001 Part 1: A full set of operational indicators for organisations to use to benchmark their security posture
	ETSI TR 103 305 Critical Security Controls for Effective Cyber Defence
	BSI 100-1 Information Security Management Systems (ISMS)
	BSI 100-2: IT- Grundschutz Methodology
	BSI 200-1 Information Security Management Systems (ISMS)

	BSI 200-2: IT- Grundschutz Methodology
	ISO/IEC 15408-1:2009 Evaluation criteria for IT security - Part 1: Introduction and general model
	ISO/IEC 15408-2:2008 Evaluation criteria for IT security - Part 2: Security functional components
	ISO/IEC 15408-3:2008 Evaluation criteria for IT security - Part 3: Security assurance components
	ISO/IEC 19790:2012 Security requirements for cryptographic modules
	ISO/IEC 27006:2015 Requirements for bodies providing audit and certification of information security management systems
	ISO/IEC 27007:2017 Guidelines for information security management systems auditing
	ISO/IEC 27014:2020 Governance of information security
	ISO/IEC 27017:2015: Code of practice for information security controls based on ISO/IEC 27002 for cloud services
	ISO/IEC 29147:2018: Vulnerability disclosure
	ISO/IEC 30111:2019: Vulnerability handling processes
	OENORM A 7700-3:201910 Web Applications - Part 3: Security requirements
	ISO/IEC 27701:2019 Security techniques- Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines
	ISO/IEC TS 27100:2020 Information technology -Cybersecurity- Overview and concepts

	ΠΡΟΤΥΠΑ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
Διαχείριση κινδύνου	ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000
	ISO/IEC 27005:2016 Information security risk management
	ISO/IEC 31000 Risk management - Risk assessment techniques
	IEC 31010:2009 Risk management - Risk assessment techniques
	BSI BIP 0076 Information security risk management. Handbook for ISO/IEC 27001
	BSI 100-3: Risk Analysis based on IT-Grundschutz
	BSI 200-3: Risk Analysis based on IT-Grundschutz
	ISO/IEC 27005:2018 Information security risk management
	ISO/IEC 27102:2019 Information security management — Guidelines for cyber-insurance

	ΠΡΟΤΥΠΑ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
Διαχείριση Συνέχειας Επιχειρήσεων	ISO 22301:2012 Business continuity management systems – Requirements
	ISO 22313:2012 Business continuity management systems – Guidance
	ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
	100-4: Business Continuity Management
	OENORM A 7700-4:201910 Web Applications - Part 4: Requirements for secure operations

	ΠΡΟΤΥΠΑ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
Προστασία δεδομένων και απόρρητο	ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ISO/IEC 29100:2011 Privacy framework
	ISO/IEC 29101:2013 Privacy architecture framework
	BSI BS 10012:2009 Data protection. Specification for a personal information management system
	CEN CWA 16113:2010 Personal Data Protection Good Practices
	OEVE/OENORM 17529:2020: Data protection and privacy by design and by default
	OENORM A 7700-2:201912 Web Applications - Part 2: Data protection requirements
	ISO/IEC 27018:2019: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
	ISO/IEC 29134:2017: Guidelines for privacy impact assessment
	ÖNORM EN 419231:2019 11 01: Protection profile for trustworthy systems supporting time stamping
	ÖNORM EN 419241-1:2019 03 15: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements
	ÖNORM EN 419241-2:2019 06 01: Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing

	ΠΡΟΤΥΠΑ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
Διαχείριση περιστατικών	ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management
	ISO/IEC 27036-2:2014 Information security for supplier relationships - Part 2: Requirements
	ISO/IEC 27036-3:2013 Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
	ISO/IEC 27035-1:2016 Information security incident management — Part 1: Principles of incident management
	ISO/IEC 27035-1:2016 Information security incident management — Part 2: Guidelines to plan and prepare for incident response

	ΠΡΟΤΥΠΑ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
Διαχείριση τρίτων	ISO/IEC 27036-1:2014 Information security for supplier relationships - Part 1: Overview and concepts
	ISO/IEC 27035:2011 Information security incident management
	ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence

	ΠΡΟΤΥΠΑ ΓΙΑ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
Βιομηχανική ασφάλεια	OVE EN IEC 62443-4-1:2018 11 01: Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements
	OVE EN IEC 62443-4-2:2020 01 01: Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components
	OVE IEC TS 62351-100-1:2020 06 01