Deloitte.

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

Κυβερνοασφάλεια

Παρατηρητήριο Ψηφιακού Μετασχηματισμού ΣΕΒ
Έκδοση: Ιούλιος 2020

ΨΗΦΙΑΚΟΣ
ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ
Κυβερνοασφάλεια

Πίνακας Περιεχομένων

Το Παρατηρητήριο Ψηφιακού Μετασχηματισμού του ΣΕΒ

Το Παρατηρητήριο Ψηφιακού Μετασχηματισμού αποτελεί μία πρωτοβουλία του Συνδέσμου Επιχειρήσεων & Βιομηχανιών (ΣΕΒ) το οποίο έχει ως στόχο τη συστημική και ουσιαστική παρακολούθηση της πορείας του ψηφιακού μετασχηματισμού της χώρας.

Το **Παρατηρητήριο Ψηφιακού Μετασχηματισμού** φιλοδοξεί να αποτελέσει ένα μόνιμο μηχανισμό του ΣΕΒ για την παρακολούθηση του ψηφιακού μετασχηματισμού στην Ελλάδα και τη διαμόρφωση κατάλληλων πολιτικών και προτάσεων με στόχο την ενίσχυση της ψηφιακής ωριμότητας των ελληνικών επιχειρήσεων, του δημόσιου τομέα και της ευρύτερης ελληνικής κοινωνίας. Αναλυτικότερα το Παρατηρητήριο αποσκοπεί:

01 Στην παρακολούθηση της πορείας του ψηφιακού μετασχηματισμού στην Ελλάδα, μέσω της **σύνθεσης και ανάλυσης δημοσιευμένων δεικτών από αξιόπιστες πηγές**, διαχρονικά και σε σύγκριση με τις υπόλοιπες χώρες της Ευρωπαϊκής Ένωσης. Για το σκοπό αυτό έχει δημιουργηθεί ένας νέος σύνθετος δείκτης, προσαρμοσμένος στις ανάγκες και τους στόχους του Παρατηρητηρίου, ο SEV Digital Maturity Index.

02 Στη μελέτη της ψηφιακής ωριμότητας των ελληνικών επιχειρήσεων μέσω **πρωτογενούς έρευνας** μεταξύ υψηλόβαθμων στελεχών, προκειμένου να διαπιστωθεί το επίπεδο των υφιστάμενων αλλά και προβλεπόμενων επενδύσεων των ελληνικών επιχειρήσεων σε νέες ψηφιακές τεχνολογίες.

03 Στην **επισκόπηση δράσεων ψηφιακού μετασχηματισμού**, με εστίαση στην παρακολούθηση πρωτοβουλιών ψηφιακής στρατηγικής και της πορείας υλοποίησης σημαντικών έργων ψηφιακού μετασχηματισμού του δημόσιου τομέα.

Απώτερος στόχος του Παρατηρητηρίου είναι η έναρξη ενός **εποικοδομητικού διαλόγου** ώστε να αναπτυχθούν **ρεαλιστικές και εφαρμόσιμες προτάσεις άμεσης προτεραιότητας** για τη βελτίωση της ψηφιακής ωριμότητας της χώρας.
Επιπλέον, καθώς η **έλλειψη τεχνογνωσίας και καλής κατανόησης** των ωφελειών που μπορούν να αποφέρουν οι νέες ψηφιακές τεχνολογίες έχει αναγνωριστεί ως σημαντικό εμπόδιο στην περαιτέρω ανάπτυξη της ψηφιακής ωριμότητας των ελληνικών επιχειρήσεων, το Παρατηρητήριο Ψηφιακού Μετασχηματισμού έχει αναλάβει την πρωτοβουλία δημοσίευσης μίας σειράς **επιμορφωτικού και ενημερωτικού χαρακτήρα συνοπτικών μελετών** επί θεμάτων που άπτονται της νέας ψηφιακής εποχής. Στόχος είναι να παρουσιαστούν νέες ψηφιακές τεχνολογίες, τα οφέλη που πηγάζουν από αυτές, πρακτικοί τρόποι προσέγγισης του ψηφιακού μετασχηματισμού καθώς επίσης και διεθνείς και ελληνικές βέλτιστες πρακτικές.
Η παρούσα μελέτη, με την ονομασία «**Η Κυβερνοασφάλεια στη Νέα Ψηφιακή Εποχή**» έχει εκπονηθεί σε συνεργασία με τη διεθνή εταιρία συμβουλευτικών υπηρεσιών Deloitte και εστιάζει στην ανάδειξη των κινδύνων στο χώρο της Κυβερνοασφάλειας για τις ελληνικές επιχειρήσεις από την ραγδαία ενσωμάτωση ψηφιακών τεχνολογιών καθώς και τρόπους αντιμετώπισής τους, με ιδιαίτερη έμφαση στις απειλές που αντιμετωπίζουν βιομηχανικές επιχειρήσεις και τα «έξυπνα εργοστάσια» την εποχή της 4ης βιομηχανικής επανάστασης.

ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ
Παρατηρητήριο ΣΕΒ

Το παρόν κείμενο, εστιάζει στην ανάδειξη των κινδύνων στο χώρο της Κυβερνοασφάλειας για τις ελληνικές επιχειρήσεις και αποτελεί μέρος μίας σειράς συνοπτικών μελετών που εκδίδει το Παρατηρητήριο Ψηφιακού Μετασχηματισμού του ΣΕΒ σε συνεργασία με τη διεθνή εταιρία συμβουλευτικών υπηρεσιών Deloitte, με στόχο την ενημέρωση / επιμόρφωση στελεχών των ελληνικών επιχειρήσεων σε θέματα που άπτονται του ψηφιακού μετασχηματισμού.

1 Κίνδυνοι & τάσεις Κυβερνοασφάλειας στη νέα ψηφιακή εποχή

Κίνδυνοι & τάσεις Κυβερνοασφάλειας στη νέα ψηφιακή εποχή

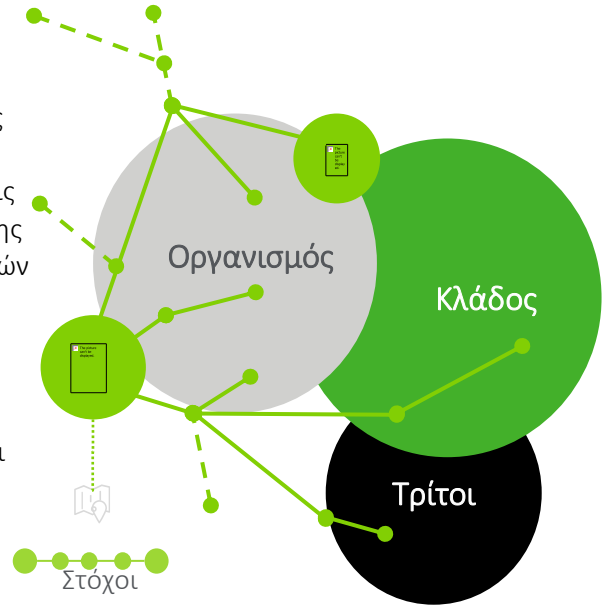
Το συνεχώς μεταβαλλόμενο περιβάλλον Κυβερνοασφάλειας

Η Κυβερνοασφάλεια δεν είναι τεχνολογικό αλλά επιχειρηματικό ζήτημα και στρατηγική επιλογή.

Η στρατηγική σημασία της κυβερονασφάλειας

Η ψηφιακή επανάσταση είναι μια πραγματικότητα και δεν μπορούμε – ούτε πρέπει – να τη αναχαιτίσουμε. Το επόμενο διάστημα, οι τεχνολογικές καινοτομίες θα είναι οι βασικοί πυλώνες ανάπτυξης, παρέχοντας άνευ προηγουμένου ευκαιρίες σε επιχειρήσεις και οργανισμούς, δημιουργώντας παράλληλα αξία και ανταγωνιστικό πλεονέκτημα. Όμως, για να ευδοκιμήσουν οι οργανισμοί σε ένα ψηφιακό μέλλον, **απαιτείται μια ισχυρή στρατηγική Κυβερνοασφάλειας** η οποία θα ωθήσει έναν οργανισμό στο να γίνει όσο το δυνατόν πιο ασφαλής, έτοιμος και ανθεκτικός σε Κυβερνοεπιθέσεις. Καθώς οι νέες τεχνολογίες οδηγούν στο φαινόμενο που είναι ευρέως γνωστό ως “digital disruption”, εισάγουν νέα είδη απειλών στον Κυβερνοχώρο και ενισχύουν τους υφιστάμενους, απαιτώντας εξελιγμένες ικανότητες επόμενης γενιάς που θα πρέπει να χτιστούν τώρα.

Οι οργανισμοί θα πρέπει να είναι σε θέση να κατανοούν διαρκώς τις ευκαιρίες και τους κινδύνους που σχετίζονται με την ψηφιακή καινοτομία, να εξισορροπήσουν την ανάγκη προστασίας τους από τις υφιστάμενες απειλές αλλά και την ανάγκη υιοθέτησης νέων επιχειρηματικών μοντέλων και νέων στρατηγικών που αξιοποιούν την ψηφιακή τεχνολογία και θέτουν τις βάσεις για ανάπτυξη. Στο πλαίσιο αυτό, οι οργανισμοί θα πρέπει να κατανοήσουν σε βάθος το προφίλ κινδύνου τους, να αξιολογήσουν το υφιστάμενο επίπεδο των μηχανισμών ασφάλειας και να καταρτήσουν ολιστικό πρόγραμμα Κυβερνοασφάλειας για την θωράκιση τους από τους κινδύνους του Κυβερνοχώρου.



Τάσεις που διαμορφώνουν την Κυβερνοασφάλεια στην εποχή μας

Έλλειψη περιμέτρου: Οι νέες τεχνολογίες όπως το υπολογιστικό νέφος θολώνουν το τοπίο όσον αφορά τα τεχνολογικά όρια αλλά και την περίμετρο που ένας οργανισμός καλείται να θωρακίσει.

Νέες τεχνολογίες: Η αυξανόμενη χρήση νέων τεχνολογιών (π.χ. ρομποτική, αυτοματοποίηση, τεχνητή νοημοσύνη, ευέλικτη ανάπτυξη - agile) αλλάζουν την ταχύτητα της επιχειρηματικής και τεχνολογικής καινοτομίας, ενισχύοντας τους κινδύνους στον Κυβερνοχώρο και περιπλέκοντας τα προγράμματα προστασίας των οργανισμών, τα οποία συχνά αναπτύσσονται γύρω από παραδοσιακές προσεγγίσεις και μεθόδους.

Internet of Things (IoT): Είτε περιλαμβάνει έξυπνους αισθητήρες σε ένα έξυπνο εργοστάσιο, είτε μια απομακρυσμένη σύνδεση με μια αντλία ινσουλίνης, το IoT αναμένεται να έχει θετικό αντίκτυπο στη ζωή μας. Ωστόσο, οι αυξημένοι κίνδυνοι του Κυβερνοχώρου και σημαντικές επιπτώσεις παραβίασης ενδέχεται να μετριάσουν την ανάπτυξη ή την αποδοχή αυτών των τεχνολογιών.

Δίκτυα φορητών συσκευών: Οι φορητές συσκευές δεν είναι μόνο εργαλείο αλλά ένας τρόπος ζωής. Δημιουργούνται νέες συμπεριφορές οι οποίες αυξάνουν σημαντικά το πεδίο και εύρος των Κυβερνοεπιθέσεων, καθώς τα δίκτυα φορητών συσκευών είναι εκ φύσεως γεωγραφικά διασκορπισμένα και ανομοιογενή.

Κατάργηση ορίων μεταξύ επαγγελματικής και προσωπικής ζωής: Η ευρεία χρήση των προσωπικών μας συσκευών για επαγγελματική χρήση αλλά και για χρήση κοινωνικών δικτύων έχουν ως αποτέλεσμα τη «μίξη» προσωπικών και εταιρικών δεδομένων καθιστώντας δύσκολη την προστασία τους.

Τεχνητή νοημοσύνη (AI): Η τεχνητή νοημοσύνη αρχίζει να συμπληρώνει ή να αντικαθιστά τους εξειδικευμένους επαγγελματίες, οδηγώντας σε βελτιωμένες δυνατότητες και μειωμένο κόστος. Ωστόσο, δημιουργεί νέους κινδύνους, όπως τα chatbots τα οποία με την κατάλληλη κακόβουλη παρέμβαση μπορεί να λειτουργήσουν ως εργαλεία του επιτιθέμενου.

Η μεταβαλλόμενη φύση της επιχείρησης: Οι καινοτόμοι οργανισμοί δημιουργούν νέα ψηφιακά μοντέλα παροχής υπηρεσιών τα οποία δημιουργούν προκλήσεις Κυβερνοασφάλειας σε όλα επίπεδα του οργανισμού.

Συνεργατικές πλατφόρμες: Λογισμικά που ενσωματώνουν τα κοινωνικά δίκτυα σε επιχειρηματικές διαδικασίες μπορούν να διευκολύνουν την προώθηση της καινοτομίας, αλλά αυξάνουν την έκθεση σε εξωτερικούς κινδύνους.

Κίνδυνοι & τάσεις Κυβερνοασφάλειας στη νέα ψηφιακή εποχή

Η Νέα Εποχή απαιτεί «Ασφάλεια Παντού»

Η διαχείριση κινδύνων στον Κυβερνοχώρο είναι μια δυναμικά μεταβαλλόμενη διαδικασία, βρίσκεται σε συνεχή εξέλιξη και μεταβάλλεται σύμφωνα με το εκάστοτε περιβάλλον απειλών. Η απεικόνιση της εξέλιξης του περιβάλλοντος Κυβερνοασφάλειας τα τελευταία δώδεκα χρόνια εμφανίζει ξεκάθαρα την ανάγκη για ολιστική προσέγγιση, εστιάζοντας στην πρόληψη ώστε να βρει σε θέση ισχύος τους οργανισμούς.

Η Κυβερνοασφάλεια αρχίζει να βρίσκεται στο επίκεντρο καθώς έχουμε την εδραίωση των πρώτων σημαντικών κανονιστικών προτύπων που στόχο έχουν να θέσουν τις ελάχιστες απαιτήσεις αλλά και να καθοδηγήσουν τους οργανισμούς στη σωστή κατεύθυνση όσον αφορά την προστασία τους.

Γίνονται γνωστά τα πρώτα μεγάλα διεθνή περιστατικά παραβίασης τα οποία αναβαθμίζουν την Κυβερνοασφάλειας στο να αποτελεί πλέον επιχειρησιακό πρόβλημα και όχι μόνο τεχνικό. Δίνεται έμφαση στη δημιουργία πλαισίων διαχείρισης κινδύνων και ανθεκτικότητας των οργανισμών.

Η εμφάνιση τεχνολογικών καινοτομιών (π.χ. ψηφιοποίηση, υπολογιστικό νέφος, IoT, τεχνητή νοημοσύνη) επιφέρει και αβεβαιότητα όσον αφορά τον τομέα της Κυβερνοασφάλειας. Έμφαση δίνεται πλέον στη διαχείριση κινδύνων εκτός της περιοχής ελέγχου των οργανισμών.

Κίνδυνοι & τάσεις Κυβερνοασφάλειας στη νέα ψηφιακή εποχή

Το «πεδίο μάχης» είναι μεγαλύτερο από ποτέ

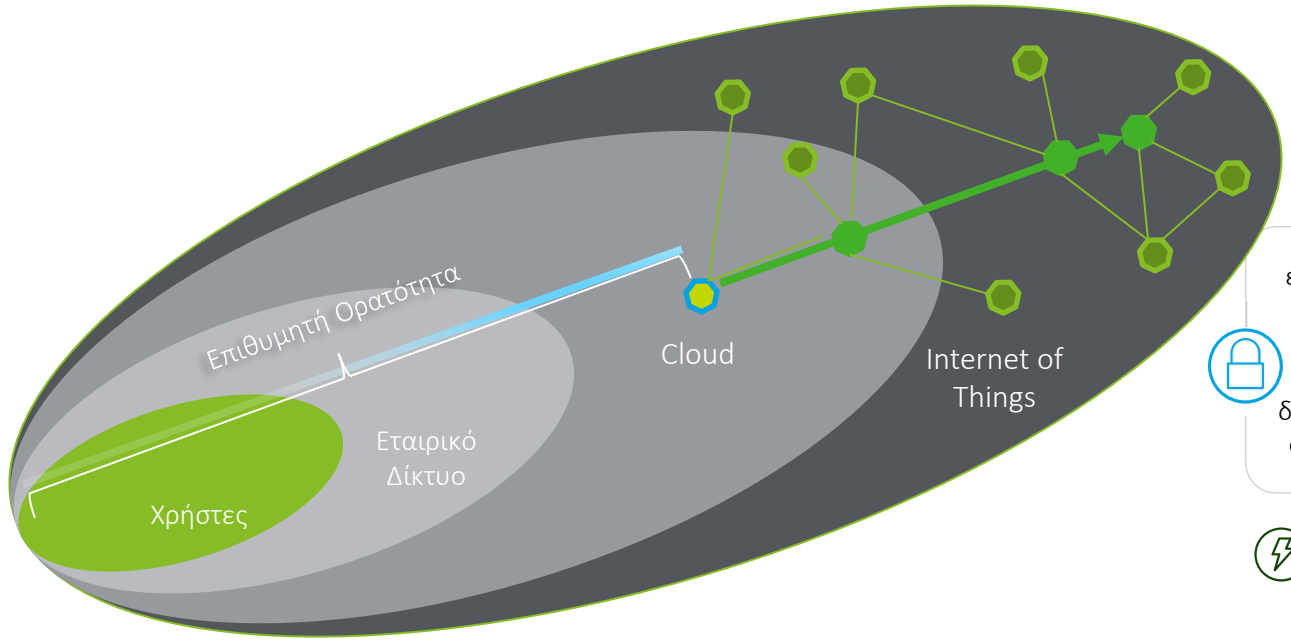
Επιτιθέμενοι

- ✓ Ανταγωνιστές
- ✓ Τρίτα μέρη
- ✓ Εσωτερικοί χρήστες
- ✓ Εγκληματίες
- ✓ Hack-τιβιστές
- ✓ Κρατικές υπηρεσίες

Αν χαρακτηρίσουμε το ευρύτερο τεχνολογικό περιβάλλον ως ένα «πεδίο μάχης» αυτό θα μπορούσαμε να θεωρήσουμε ότι είναι μεγαλύτερο από ποτέ. Οι εγκληματίες του κυβερνοχώρου, ανάλογα με τα κίνητρά τους, τα οποία συχνά δεν είναι μόνο οικονομικά, ποικίλουν και χρησιμοποιούν όλα τα μέσα και θα εργαστούν αργά, προσεκτικά και μεθοδικά για την επίτευξη των στόχων τους.

Πολύτιμα αγαθά

- ✓ Οικονομικά δεδομένα
- ✓ Δεδομένα πελατών
- ✓ Δεδομένα ταυτοποίησης
- ✓ Στρατηγικά σχέδια
- ✓ Πνευματική ιδιοκτησία
- ✓ Εγκαταστάσεις



Η αυξανόμενη εξάρτηση – κυρίως λόγω ευκολίας - σε διαμοιρασμένες τεχνολογίες και σε υπηρεσίες εξωπορισμού, καθιστά την ορατότητα του επιπέδου ασφάλειας των δεδομένων ενός οργανισμού εξαιρετικά δύσκολη, η οποία στην καλύτερη περίπτωση να φτάνει μέχρι τους ένα-δύο κύριους παρόχους κρίσιμων τεχνολογικών υπηρεσιών.

Μέθοδοι απειλής

- ✓ Επιθέσεις λυτρισμικού (ransomware)
- ✓ Κοινωνική μηχανική - Phishing
- ✓ Εκμετάλλευση ευπαθειών
- ✓ Τεχνητή νοημοσύνη
- ✓ Εφοδιαστική αλυσίδα

Οι κακόβουλοι οι οποίοι θα θέσουν ως στόχο έναν οργανισμό, τον παρακολουθούν σε συνεχή βάση, με υπομονή, με σκοπό να εντοπίσουν πιθανές αδυναμίες και να επιτεθούν τη κατάλληλη στιγμή. Τελικός στόχος είναι η απόκτηση μη εξουσιοδοτημένης πρόσβασης που θα τους δώσει τη δυνατότητα να ικανοποιήσουν τα κίνητρα τους, προκαλώντας πλήγμα στη φήμη του.

Επιπτώσεις

- ✓ Κλοπή
- ✓ Καταστροφική βλάβη
- ✓ Διαθεσιμότητα (π.χ. DDoS)
- ✓ Αλλοίωση δεδομένων
- ✓ Αρνητική δημοσιότητα
- ✓ Ανθρώπινη ασφάλεια και περιβάλλον (βιομηχανικό περιβάλλον)

Κίνδυνοι & τάσεις Κυβερνοασφάλειας στη νέα ψηφιακή εποχή

Από ποιους κινδυνεύουμε όμως και γιατί;

Απειλή εκ των έσω / εσωτερικοί χρήστες

Εσκεμμένη ή ακούσια
Κίνητρο: Εκδίκηση, οικονομικό όφελος
Επιχειρησιακές επιπτώσεις: Πλήγμα στη φήμη, οικονομική απώλεια, μη εναρμόνιση με κανονιστικές απαιτήσεις, διαρροή πληροφοριών

Οργανωμένο έγκλημα

Παγκόσμιο, δύσκολα ανιχνεύσιμο και διωκόμενο
Κίνητρο: Οικονομικό πλεονέκτημα, πιθανώς ευκαιριακό
Επιχειρησιακές επιπτώσεις: Οικονομική απώλεια, πλήγμα στη φήμη, κλοπή πληροφοριών.

Κρατικά χορηγούμενο κυβερνο-έγκλημα

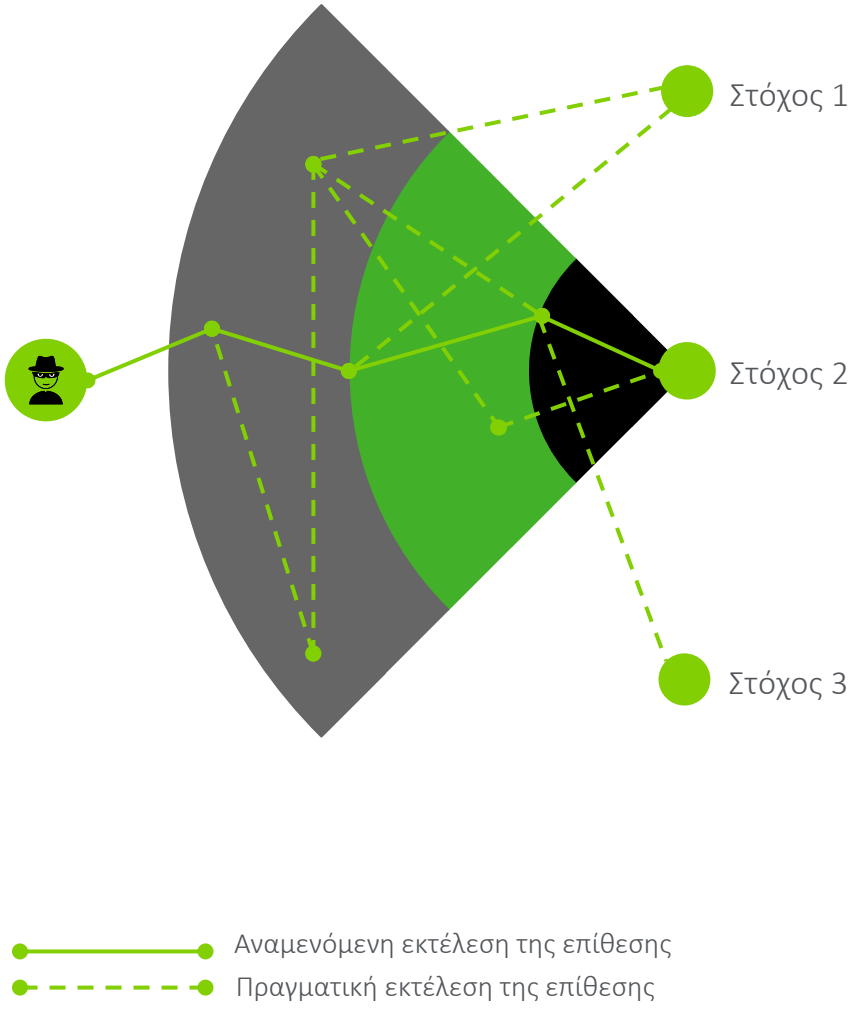
Κατασκοπεία και σαμποτάζ
Κίνητρο: Πολιτικό και οικονομικό όφελος
Επιχειρησιακές επιπτώσεις: Κλοπή πληροφοριών, διακοπή στη λειτουργία, οικονομική απώλεια

Ανταγωνιστές

Ανταγωνισμός
Κίνητρο: Ανταγωνιστικό πλεονέκτημα
Επιχειρησιακές επιπτώσεις: Ανταγωνιστικό μειονέκτημα, πλήγμα στη φήμη, απώλεια εμπιστευτικών πληροφοριών

Χάκερς ή Χακτιβιστές

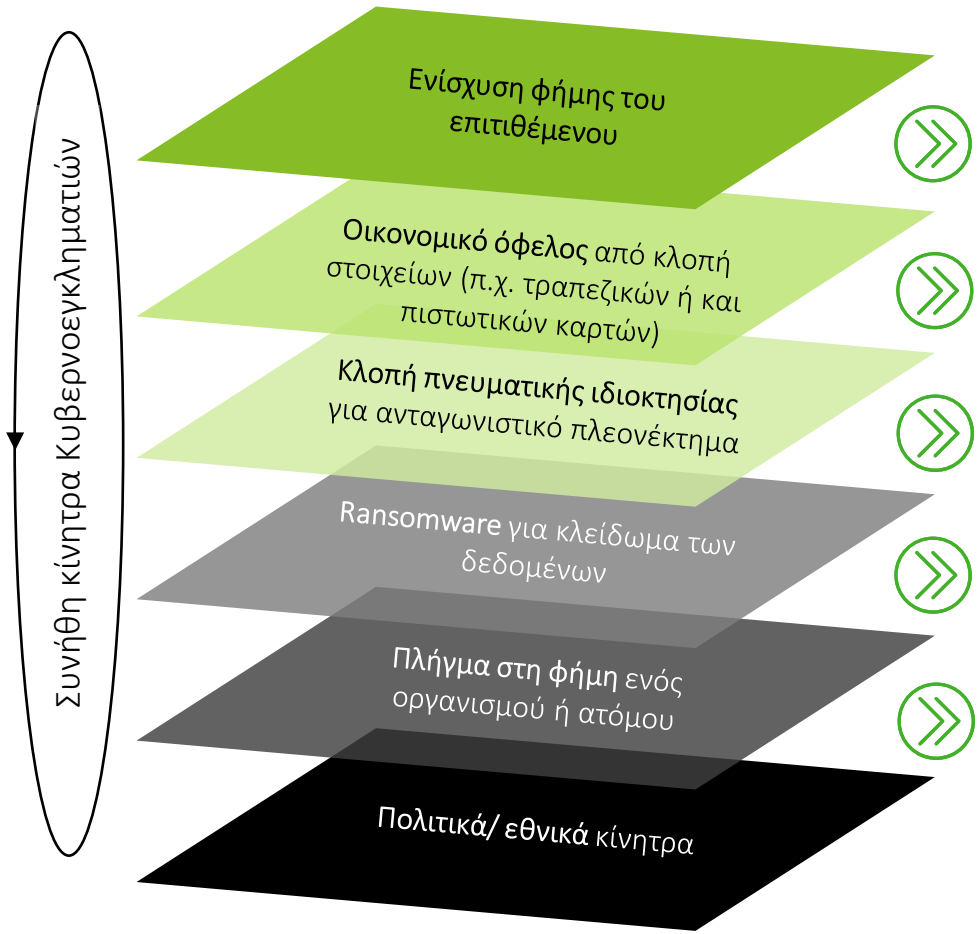
Για να τραβήξουν την προσοχή ή για αύξηση της δημοτικότητάς τους
Κίνητρο: Απρόβλεπτο, ποικίλει ανά περίπτωση
Επιχειρησιακές επιπτώσεις: Πλήγμα στη φήμη, διακοπή λειτουργιών οργανισμού, κλοπή πληροφοριών.



Κίνδυνοι & τάσεις Κυβερνοασφάλειας στη νέα ψηφιακή εποχή

Τα κίνητρα των επιτιθέμενων είναι πολλαπλά και οι επιπτώσεις δυσμενείς

Οι επενδυτές, οι κυβερνήσεις και οι ρυθμιστικές αρχές απαιτούν όλο και περισσότερο τις Διοικήσεις να επιδείξουν ενεργά την επιμέλεια στην πρόληψη, την αντιμετώπιση και την μείωση των πιθανών επιπτώσεων σε περίπτωση περιστατικών Κυβερνοασφάλειας είτε αυτά προκαλούνται ακούσια είτε από σκόπιμες Κυβερνοεπιθέσεις.



Επιπτώσεις

Οικονομικές κυρώσεις	Πρόστιμα από κρατικούς ή ρυθμιστικούς φορείς (π.χ. παραβιάσεις προσωπικών δεδομένων, αποζημίωση τρίτων για μη τήρηση συμβατικών υποχρεώσεων).
Αρνητική δημοσιότητα	Αρνητική δημοσιότητα που προκαλεί τη μείωση τη αξίας του οργανισμού και μείωση της εμπιστοσύνης από πελάτες και προμηθευτές και σχετιζόμενα τρίτα μέρη.
Πνευματική ιδιοκτησία	Κλοπή αγαθών που αποτελούν πνευματική ιδιοκτησία συμπεριλαμβανομένου υλικού με δίπλωμα ευρεσιτεχνίας και εμπορικού σήματος, καταστάσεις πελατών και εμπιστευτικά εμπορικά δεδομένα.
Υλικά αγαθά	Απώλεια ή αδυναμία πρόσβασης σε περιουσιακά στοιχεία ή πληροφορίες που οδηγούν σε καθυστερήσεις ή αποτυχία παράδοσης προϊόντων/ υπηρεσιών.
Χαμένος χρόνος	Η μη έγκαιρη διερεύνηση των περιστατικών, ενημέρωση της Διοίκησης ή και των μετόχων και η συνεργασία με τις Αρχές, οδηγεί έμμεσα σε οικονομικές απώλειες.
Διοικητικοί πόροι	Διοικητικοί πόροι που αφιερώθηκαν στην προσπάθεια επίλυσης του περιστατικού (π.χ. αποκατάσταση της εμπιστοσύνης των πελατών, η επικοινωνία με τις Αρχές, η αντικατάσταση υλικών αγαθών, η επαναφορά της συνέχειας των εργασιών), οδηγεί έμμεσα σε οικονομικές απώλειες.

2 Κυβερνοασφάλεια & το «έξυπνο» εργοστάσιο

Το «Έξυπνο» εργοστάσιο | ορισμός και βασικά χαρακτηριστικά

*Το «έξυπνο» εργοστάσιο είναι ένα ευέλικτο σύστημα που μπορεί να **αυτοβελτιστοποιεί την απόδοσή του** εντός του ευρύτερου δικτύου της ψηφιακής εφοδιαστικής αλυσίδας μιας μεταποιητικής επιχείρησης, να **προσαρμόζεται σε νέες συνθήκες** σε πραγματικό ή σχεδόν πραγματικό χρόνο και να **εκτελεί αυτόνομα** ολόκληρες διαδικασίες παραγωγής και να **λαμβάνει αποφάσεις**.*

Βασικά χαρακτηριστικά / Εργοστασίου»

Διασυνδεδεμένο (Connected)

- Πληροφοριακά συστήματα, μηχανήματα και εργαλεία, εργαζόμενοι, προϊόντα και υλικά, διασυνδέονται και επικοινωνούν αμφίδρομα συλλέγοντας και ανταλλάσσοντας δεδομένα σε πραγματικό χρόνο.
- Ανταλλαγή δεδομένων σε πραγματικό χρόνο με πελάτες και προμηθευτές, ενδυναμώνοντας τη συνεργασία με τρίτους στην αλυσίδα αξίας.
- Βελτιστοποιημένη συνεργασία, διευκολυνόμενη μέσω νέων τεχνολογιών, μεταξύ διαφορετικών τμημάτων και ομάδων.

Βελτιστοποιημένο (Optimized)

- Αξιόπιστη και προβλέψιμη παραγωγική δυναμικότητα.
- Αυξημένος χρόνος λειτουργικότητας μηχανών (uptime) και αποδοτικότητα παραγωγής.
- Αυτοματοποιημένη παραγωγική διαδικασία με ελαχιστοποιημένη την ανάγκη ανθρώπινης παρέμβασης και χειρωνακτικών εργασιών.
- Ελαχιστοποίηση κόστους παραγωγής και προβλημάτων ποιότητας.

Ευέλικτο (Agile)

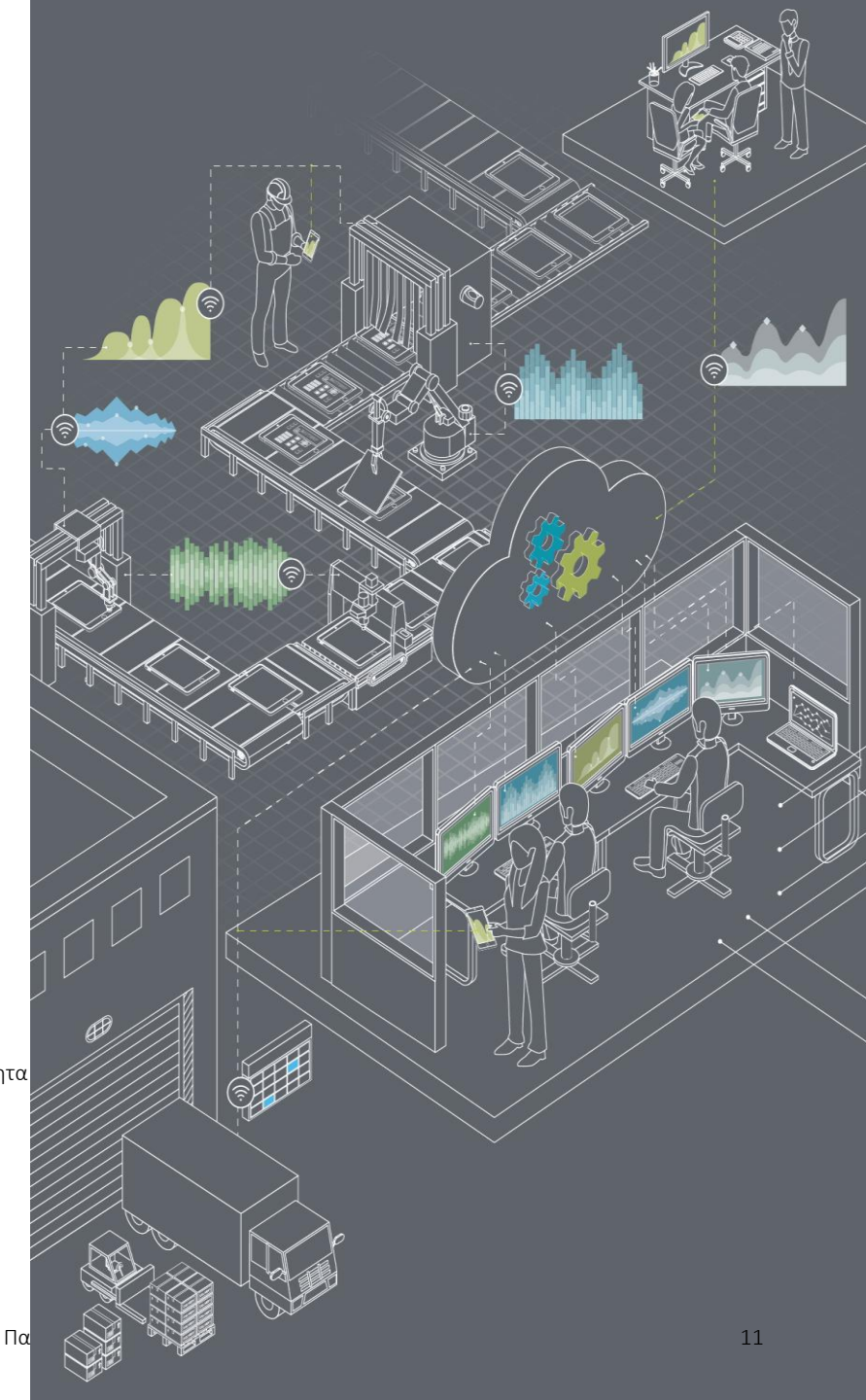
- Ευελιξία και προσαρμοστικότητα σε αλλαγές στον προγραμματισμό και σε περιπτώσεις αναπροσαρμογής των μηχανών.
- Δυνατότητα γρήγορης υλοποίησης αλλαγών στα χαρακτηριστικά του προϊόντος (π.χ. BoM) και καταγραφής επιπτώσεων στην παραγωγική διαδικασία σε πραγματικό χρόνο.
- Εύκολα διαμορφώσιμη διαρρύθμιση (layout) του εργοστασίου και (επανά)ρύθμιση εξοπλισμού κα εργαλείων.

Διάφανο (Transparent)

- Συλλογή δεδομένων από πληθώρα πηγών και εργαλεία που επιτρέπουν την ταχεία λήψη αποφάσεων, ακόμη και αυτοματοποιημένα.
- Δυνατότητα εντοπισμού και παρακολούθησης της θέσης φυσικών αντικειμένων και ανθρώπων.
- Διασύνδεση σε πραγματικό χρόνο με πελάτες (π.χ. δεδομένα προβλέψεων ζήτησης) και προμηθευτές (π.χ. δεδομένα προβλέψεων παραδόσεων) και δυνατότητα παρακολούθησης της πορείας υλοποίησης μίας παραγγελίας πελάτη από την αρχή μέχρι το τέλος.

Προδραστικό (Proactive)

- Δυνατότητα προληπτικής αναγνώρισης και επίλυσης ανωμαλιών στη λειτουργία (π.χ. βλάβες), κτλ.
- Αυτοματοποίηση στην αναπλήρωση υλικών, κτλ.
- Δυνατότητα γρήγορου ή ακόμη και προληπτικού εντοπισμού προβλημάτων σε παραλαβές από προμηθευτές.
- Παρακολούθηση παραμέτρων υγιεινής και ασφάλειας σε πραγματικό χρόνο.



Κυβερνοασφάλεια στο «έξυπνο εργοστάσιο»

Ο βιομηχανικός κλάδος αντιμετωπίζει αυξανόμενες απειλές στον Κυβερνοχώρο την εποχή της 4ης βιομηχανικής επανάστασης που διανύουμε. Η μετάβαση των ελληνικών επιχειρήσεων του κλάδου προς το έξυπνο, διασυνδεδεμένο εργοστάσιο οφείλει να λαμβάνει κατάλληλα μέτρα προστασίας από τις Κυβερνοαπειλές.

Το νεότερο κεφάλαιο στη βιομηχανική ανάπτυξη, ευρέως γνωστή και ως 4η Βιομηχανική Επανάσταση, επιφέρει μια εποχή τεράστιων δυνατοτήτων για καινοτομία και αυτοματοποιήσεις. Ταυτόχρονα αναδεικνύονται νέοι κίνδυνοι και προκλήσεις. Η αυξημένη χρήση ψηφιακών τεχνολογιών και της παγκόσμιας διασύνδεσης, σηματοδοτεί ένα νέο επίπεδο πολυπλοκότητας.

Η Κυβερνοασφάλεια δεν περιορίζεται πλέον μόνο σε ορισμένες λειτουργίες ή σε συγκεκριμένα άτομα, αλλά σχετίζεται με όλες τις πτυχές ενός οργανισμού και πιθανότατα με σημεία που οι ηγέτες της βιομηχανίας δεν έχουνε καν λάβει υπόψη. Κάθε υπάλληλος, κάθε συνεργάτης, κάθε ηλεκτρονική συσκευή, μηχάνημα ή τελικό προϊόν εμπεριέχει κινδύνους ως προς την ασφάλεια στον Κυβερνοχώρο και ενδεχομένως ορισμένοι κατασκευαστές δεν είναι κατάλληλα προετοιμασμένοι για τον πιθανό αντίκτυπο των κινδύνων που ενέχονται.

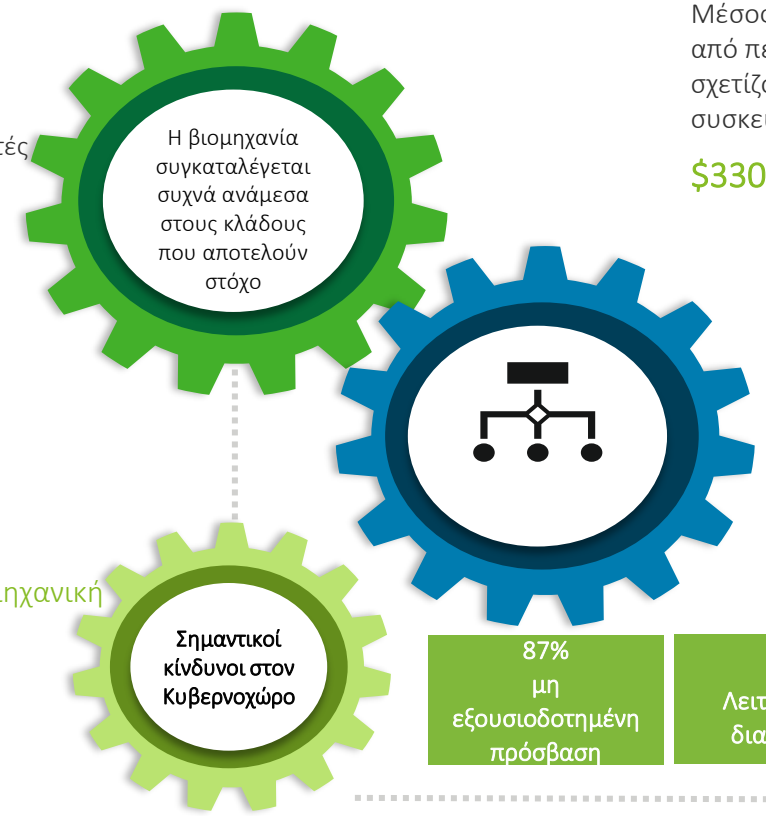
Στατιστικά Κυβερνοαπειλών

Η μελέτη της Deloitte και της Manufacturer's Alliance for Productivity and Innovation (MAPI) διαπίστωσε ότι περισσότεροι από 8 στους 10 κατασκευαστές που ρωτήθηκαν έχουν περιορισμένες δυνατότητες ανίχνευσης και ανταπόκρισης των απειλών του Κυβερνοχώρου.

4 στις 10 βιομηχανικές επιχειρήσεις που συμμετείχαν στην έρευνα κατέδειξαν ότι οι δραστηριότητές τους επηρεάστηκαν από περιστατικό ασφάλειας τους τελευταίους 12 μήνες

Τα περιστατικά ασφαλείας αυξήθηκαν κατά:

35x Εκβιασμοί
2.5x Εξαπάτηση
0.7x Κοινωνική μηχανική



Μέσος όρος οικονομικών επιπτώσεων από περιστατικά ασφάλειας που σχετίζονται με στις διασυνδεδεμένες συσκευές (Internet of Things – IoT)

$330,000

Μέσος όρος οικονομικών επιπτώσεων από παραβίαση δεδομένων το 2018

$7.5 εκ.

87% μη εξουσιοδοτημένη πρόσβαση

86% Λειτουργικές διαταραχές

85% κλοπή πνευματικής ιδιοκτησίας

Πηγή: Deloitte analysis of the 2019 Deloitte and MAPI Smart Factory Study data

Κυβερνοασφάλεια στο «έξυπνο εργοστάσιο»

Ψηφιοποιημένες επιχειρησιακές λειτουργίες

Οι έξυπνες εργοστασιακές λειτουργίες προσεγγίζονται συνήθως από τη σκοπιά της ψηφιοποίησης επιχειρησιακών λειτουργιών, όπου καινοτόμες τεχνολογίες συνδυάζονται με την αναβάθμιση των διαδικασιών για την υλοποίηση των επιχειρηματικών αναγκών. Ενδεικτικό παράδειγμα αποτελεί η ανίχνευση του επιπέδου ποιότητας και ο εντοπισμός σφαλμάτων μέσω της ενσωμάτωσής οπτικών συστημάτων ελέγχου, τεχνολογίες αιχμής (edge computing) και τεχνητής νοημοσύνη (AI) για τη μείωση του ποσοστού ελαττωματικών προϊόντων στη γραμμή παραγωγής.

Οι οργανισμοί θα μπορέσουν να κατανοήσουν τους κινδύνους στον Κυβερνοχώρο, τις απειλές και τις ευπάθειες του έξυπνου εργοστασίου μέσω της ανάλυσης των ψηφιοποιημένων επιχειρησιακών λειτουργιών σε βάθος, τον προσδιορισμό των τεχνολογικών απαιτήσεων, των διασυνδέσεων και των δεδομένων που απαιτούνται. Παρακάτω, παρατίθενται ενδεικτικές ψηφιακές δράσεις του έξυπνου εργοστασίου.

Πηγή: Deloitte analysis of the 2019 Deloitte and MAPI Smart Factory Study data

Κυβερνοασφάλεια και η 4η βιομηχανική επανάσταση

Κίνδυνοι Κυβερνοασφάλειας

Οι οργανισμοί προσπαθούν να ενοποιήσουν τον τομέα Πληροφορικής (IT) και της βιομηχανικής τεχνολογίας και τεχνολογίας παραγωγής (Operational Technology) στις λειτουργίες τους με σκοπό τον συγχρονισμό των δράσεων IT και OT, λαμβάνοντας υπόψη το υψηλό ποσοστό αλληλοεπικαλύψεων σε επίπεδο τεχνολογίας, διαδικασιών και ανθρώπινου δυναμικού. Για την πλειοψηφία των οργανισμών, οι δράσεις Κυβερνοασφάλειας εκτελούνται από τα στελέχη του εργοστασίου, με λιγότερη συμμετοχή από τα τμήματα Πληροφορικής και Κυβερνοασφάλειας. Αυτό μπορεί να οδηγήσει σε πληθώρα διαφορετικών τεχνολογιών, συχνά με διαφορετικές δυνατότητες ελέγχου ασφάλειας, οι οποίες πιθανότατα θα πρέπει να ενσωματωθούν και στη συνέχεια να υποστηριχθούν από τις υπάρχουσες υποδομές δικτύου πληροφορικής. Η ενοποίηση της ασφάλειας IT και OT περιλαμβάνει σημαντικές προκλήσεις καθώς οι διαδικασίες πληροφορικής και οι μηχανισμοί ασφάλειας μπορούν να οδηγήσουν σε σημαντικές διακοπές στην λειτουργία του εργοστασίου.

01

Η πολυπλοκότητα της σύγκλισης IT και OT

- Κρίσιμες υποδομές και λειτουργίες έχουν ανατεθεί σε εξωτερικούς συνεργάτες και τα στελέχη του εργοστασίου δεν έχουν πλήρη γνώση του περιβάλλοντος OT.
- Δεν έχουν θεσπιστεί ρόλοι και αρμοδιότητες για το σύνολο των συστημάτων OT και την Κυβερνοασφάλεια του εργοστασίου.
- Είναι απαραίτητη η εξειδικευμένη γνώση των βιομηχανικών διεργασιών, των τεχνολογικών αγαθών, των αρχιτεκτονικών δικτύων, των κινδύνων και των μηχανισμών Κυβερνοασφάλειας.

02

Σύγκλιση πλαισίων διαχείριση κινδύνων και μηχανισμών ασφάλειας

- Η διαχείριση κινδύνων πληροφοριακών συστημάτων βασίζεται στο τρίπτυχο της διασφάλισης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών ενώ η διαχείριση κινδύνων τεχνολογίας παραγωγής περιλαμβάνει επιπρόσθετα τη διασφάλιση της ασφάλειας των εργαζομένων και την περιβαλλοντολογική ασφάλεια.
- Τα μέτρα ασφάλειας πληροφοριακών συστημάτων συνήθως επικεντρώνονται στην εμπιστευτικότητα των δεδομένων ενώ η τεχνολογία παραγωγής στην διαθεσιμότητα και στην ομαλή λειτουργικότητα των συστημάτων.
- Η αξιολόγηση κινδύνων πληροφοριακών συστημάτων πραγματοποιείται σε επίπεδο απειλών ενώ η αξιολόγηση κινδύνων τεχνολογίας παραγωγής πραγματοποιείται σε επίπεδο συμβάντων.

02

Ενημέρωση λογισμικού

- Η υιοθέτηση μέτρων ασφαλείας, όπως ενημερώσεις λογισμικού ή έλεγχοι ευπαθειών (vulnerability scanning) προϋποθέτει τη λεπτομερή αξιολόγηση του περιβάλλοντος λόγω πιθανών επιπτώσεων στην παραγωγική λειτουργία του εργοστασίου.
- Η έλλειψη κοινής προσέγγισης για την ενημέρωση ασφάλειας των συστημάτων περιορίζει τη δυνατότητα του οργανισμού ως προς την αποτελεσματική ανταπόκριση σε αναγνωρισμένες ευπάθειες.
- Κρίνεται απαραίτητη η υιοθέτηση αρχιτεκτονικών defense-in-depth και η κατάτμηση των δικτύων για τον περιορισμό των Κυβερνοεπιθέσεων.

03

Απαρχαιωμένα συστήματα (legacy systems)

- Η πλειοψηφία των συστημάτων OT έχουν μεγάλο κύκλο ζωής (περισσότερο από 10 χρόνια) και δεν σχεδιάστηκαν με σκοπό την εξωτερική διασύνδεση και την εφαρμογή αυστηρών μηχανισμών ασφάλειας.
- Αλλαγές στις προκαθορισμένες από τους κατασκευαστές ρυθμίσεις των OT συστημάτων μπορεί να επιφέρει δυσλειτουργίες στη γραμμή παραγωγής.
- Δεν είναι εφικτή η απομόνωση των συστημάτων, λόγω της αύξησης των τεχνολογιών αιχμής (edge computing), της χρήσης υπολογιστικού νέφους και άλλων καινοτόμων τεχνολογιών.

04

Αποσταθεροποιημένη υποδομή

- Τα ιδιόκτητα πρωτόκολλα επικοινωνίας (proprietary protocols) του δικτυακού εξοπλισμού ενδέχεται να διαταραχθούν εάν αυξηθεί ο όγκος δεδομένων του δικτύου.
- Τα ήδη υπάρχοντα δίκτυα και οι αρχιτεκτονικές δεν σχεδιάστηκαν για την υποστήριξη των αυξημένων ροών δεδομένων που απαιτούνται για την υιοθέτηση νέων τεχνολογιών.
- Περιορισμένες διαδικασίες ελέγχου για την κατανόηση των κινδύνων ασφαλείας που απορρέουν από την χρήση των νέων τεχνολογιών, αυξάνοντας τον κίνδυνο των Κυβερνοεπιθέσεων.

05

Λειτουργικοί περιορισμοί

- Η επεξεργασία δεδομένων σε πραγματικό χρόνο είναι συνήθως απαραίτητη και η εισαγωγή πρόσθετων ελέγχων ασφαλείας θα μπορούσε να προκαλέσει καθυστέρηση στην γραμμή παραγωγής.
- Οι αλλαγές στα OT συστήματα ενδέχεται να προϋποθέτει την προσωρινή παύση ή διακοπή της παραγωγικής λειτουργίας. Ο χρόνος διακοπής λόγω συντήρησης πρέπει να περιορίζεται στα απόλυτα ελάχιστα διαστήματα, λόγω της κρισιμότητας των συστημάτων OT που πολλές φορές συνδέεται άμεσα και με την ανθρώπινη ασφάλεια.
- Ο καθορισμός σαφών ρόλων και αρμοδιοτήτων μεταξύ των τμημάτων IT και OT είναι ζωτικής σημασίας ώστε οι κίνδυνοι της Κυβερνοασφάλειας να προσεγγίζονται από δια-λειτουργικές ομάδες.

Κυβερνοασφάλεια και η 4η βιομηχανική επανάσταση

Απειλές και ευπάθειες σχετικά με ψηφιοποιημένες επιχειρησιακές λειτουργίες στο «έξυπνο εργοστάσιο»

Οι δράσεις ψηφιακού μετασχηματισμού και η σύνδεση των ΟΤ συστημάτων στο περιβάλλον πληροφορικής και στο Διαδίκτυο, αυξάνουν το βαθμό της ψηφιακής έκθεσης του περιβάλλοντος ΟΤ στο κυβερνοχώρο, αυξάνοντας ταυτόχρονα το πεδίο δράσης των επιτιθέμενων. Οι επιπτώσεις από ενδεχόμενα περιστατικά ασφάλειας στα περιβάλλοντα ΟΤ περιλαμβάνουν, επιπρόσθετα των επιπτώσεων στα περιβάλλοντα IT, απώλεια ανθρώπινων ζωών, καταστροφή βιομηχανικών υποδομών, περιβαλλοντολογικές καταστροφές και μη διαθεσιμότητα κρίσιμων Εθνικών υποδομών. Ως αποτέλεσμα, δημιουργείται μια υβριδική/συνδυαστική μορφή εκμετάλλευσης αδυναμιών ασφάλειας οι οποίες προέρχονται από διαφορετικά περιβάλλοντα και τεχνολογίες μέσα στον ίδιο οργανισμό.

Χρήση καινοτόμων τεχνολογικών δυνατοτήτων για βέλτιστη σχεδιαστική επάρκεια της παραγωγής

Εικονικά μοντέλα προϊόντων και συναρμολόγησης, πρόβλεψη απόδοσης προϊόντος και δημιουργία διαδοχικών σχεδιασμών.

Απειλές/ Ευπάθειες

- Μη εξουσιοδοτημένη πρόσβαση σε διασυνδεδεμένο λογισμικό.
- Κλοπή υλικού και διαρροή εμπιστευτικών πληροφοριών του οργανισμού και προσωπικών δεδομένων των εργαζομένων.
- Παραποίηση κρίσιμων δεδομένων και ρυθμίσεων των συστημάτων.
- Απενεργοποίηση συναγερμών και ειδοποιήσεων (alarms & alerts).

Συστήματα Προγραμματισμού Απαιτήσεων Υλικών (MRP)

Εκτίμηση απαιτούμενης ποσότητας υλικών, με χρήση δεδομένων παραγωγής και ζήτησης, με στοχαστικούς αλγόριθμους για τη βελτιστοποίηση της ροής υλικών στη διαδικασία κατασκευής, λαμβάνοντας υπόψη τις Κυβερνοαπειλές, ώστε να μπορούν να οριστούν σαφείς προτεραιότητες.

Απειλές/ Ευπάθειες

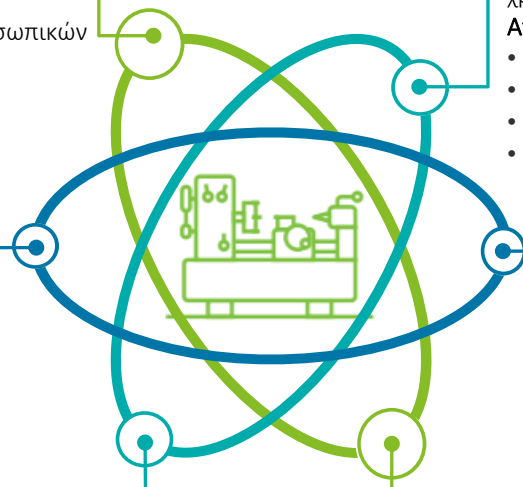
- Εκμετάλλευση των τεχνολογικών ευπαθειών.
- Επιθέσεις κοινωνικής μηχανικής και κρυπτογράφησης αρχείων.
- Απώλεια δεδομένων, μη δυνατότητα αναπλήρωση υλικού.
- Καθυστέρηση λειτουργιών παραγωγής.

Προηγμένες τεχνολογίες κατασκευής

Τεχνολογίες κατασκευής πρόσθετων υλών μέσω τρισδιάστατης εκτύπωσης (3D printing) με προηγμένα υλικά για ανταλλακτικά και κατασκευή πρωτοτύπων.

Απειλές/ Ευπάθειες

- Απώλεια σχεδιαστικών δεδομένων.
- Μείωση της παραγωγικότητας μέσω της πρόσβασης στους δικτυωμένους εκτυπωτές 3D.



Ρομποτική Αυτοματοποίηση Διαδικασιών (Robotic Process Automation – RPA) και Γνωστικός Αυτοματισμός (Cognitive Automation)

Προηγμένες τεχνολογίες όπως RPA, CA, Μηχανική Μάθηση (Machine Learning) και τεχνητή νοημοσύνη, μπορούν να αυτοματοποιήσουν επαναλαμβανόμενες και χρονοβόρες εργασίες στην παραγωγή.

Απειλές/ Ευπάθειες

- Μη εξουσιοδοτημένη πρόσβαση.
- Ύπαρξη ανεπιθύμητων προγραμμάτων «bots».
- Επιθέσεις τύπου άρνησης παροχής υπηρεσίας (Denial-of-Service).
- Διακοπή της γραμμής παραγωγής.

Ευφυή αγαθά εργοστασίου και διαχείριση απόδοσης

Προληπτική συντήρηση, χρήση Augmented Reality για υποστήριξη του προσωπικού συντήρησης και παρακολούθηση αγαθών μέσω αισθητήρων.

Απειλές/ Ευπάθειες

- Πρόσβαση σε περιβάλλον ΟΤ μέσω λογισμικού που μπορεί να έχει αναπτυχθεί χωρίς επαρκείς δικλείδες ασφαλείας.
- Διακοπή κρίσιμων λειτουργιών του εργοστασίου.

Κατανάλωση και διαχείριση ενέργειας βιομηχανικής μονάδας

Διαχείριση απορριμμάτων με αισθητήρες, αυτοματοποιημένη παρακολούθηση και διαχείριση κατανάλωσης ενέργειας, νερού και αποβλήτων.

Απειλές/ Ευπάθειες

- Μη εξουσιοδοτημένη πρόσβαση με αποτέλεσμα την διακοπή στην παροχή ενέργειας ή νερού στο εργοστάσιο, προκαλώντας ζημιές ή τραυματίζοντας το προσωπικό.

3 Παραδείγματα περιστατικών Κυβερνοεπίθεσης

Παραδείγματα περιστατικών κυβερνοεπίθεσης και σχετικών υπηρεσιών υποστήριξης

Κυβερνοεπίθεση σε εταιρία εφοδιασμού

Το υπόβαθρο

Στις 27 Ιουνίου του 2017 στις 04:00 τα ξημερώματα οι οθόνες των υπολογιστών σε εταιρία εφοδιασμού που δραστηριοποιείται σε παγκόσμιο επίπεδο άρχισαν να σβήνουν. Μία παγκόσμιας κλίμακας κυβερνοεπίθεση είχε προσβάλει το δίκτυο της εταιρίας σε λιμάνια και γραφεία σε 120 χώρες. Περισσότεροι από 4.000 διακομιστές και περίπου 45.000 υπολογιστές υπαλλήλων της εταιρίας τέθηκαν εκτός λειτουργίας. Χρειάστηκαν μόλις 2 δευτερόλεπτα ώστε να παραβιαστεί ο πρώτος υπολογιστής. Σε 13 δευτερόλεπτα οι υπολογιστές που είχαν χτυπηθεί από το κακόβουλο λογισμικό ανέρχονταν πλέον σε πάνω από 2.000. Περίπου σε 7 λεπτά από την έναρξη της επίθεσης, το κακόβουλο λογισμικό εξαπλώθηκε από το σημείο έναρξης (την Ουκρανία) στα κεντρικά γραφεία της εταιρίας. Το κακόβουλο λογισμικό χρειάστηκε 57 λεπτά ώστε να δημιουργήσει αρκετά αντίγραφα και να εξαπλωθεί σε όλο το δίκτυο της εταιρίας. Λίγα λεπτά αργότερα η επίθεση είχε προσβάλει την πλειοψηφία των διακομιστών και των υπολογιστών της εταιρίας παγκοσμίως. Σε λιγότερο από 90 λεπτά, η μεγαλύτερη εταιρία διανομής εμπορευματοκιβωτίων του κόσμου, είχε ακινητοποιηθεί. Η Κυβερνοεπίθεση που χτύπησε τον τομέα της μεταφοράς εμπορευματοκιβωτίων, ξεκίνησε από έναν έως τότε άγνωστο τύπο κακόβουλου λογισμικού (ιός), το οποίο έθεσε εκτός λειτουργίας όλα τα υπολογιστικά συστήματα της εταιρίας με αποτέλεσμα τη διακοπή της πλειοψηφίας των επιχειρησιακών λειτουργιών της εταιρίας σε όλον τον κόσμο.

Πως βοήθησε η Deloitte

Η Deloitte ανταποκρίθηκε μέσα σε λίγες μόνο ώρες και στις αμέσως επόμενες ημέρες και εβδομάδες η ομάδα απαρτιζόταν από 130 επαγγελματίες, οι οποίοι εργάζονταν σε βάρδιες 24 ώρες την ημέρα/ 7 ημέρες την εβδομάδα. Δημιουργήθηκε μία κοινή ομάδα που αποτελούνταν από στελέχη της εταιρίας και της Deloitte και είχε ως σκοπό την ανάκαμψη των πληροφοριακών συστημάτων και την επαναφορά της εταιρίας σε παραγωγική λειτουργία. Χρειάστηκαν 15 ημέρες για να αποκατασταθεί έστω και μερικώς η λειτουργία του δικτύου της εταιρίας και 30 ημέρες για να ξεκινήσουν να επανέρχονται τα πρώτα συστήματα σε κανονική λειτουργία. Καθώς η κοινή αυτή ομάδα εργαζόταν για την ανάκαμψη των πληροφοριακών συστημάτων της εταιρίας, ταυτόχρονα η ομάδα της Deloitte εργαζόταν στην ανάλυση του ιού, χρησιμοποιώντας πρακτικές αντίστροφης μηχανικής (reverse engineering). Μέσα σε λίγες ώρες από τη στιγμή που η ομάδα της Deloitte έφτασε στις εγκαταστάσεις της εταιρίας, παρείχε συγκεκριμένη καθοδήγηση σχετικά με το πώς θα αποφευχθεί η περαιτέρω διασπορά του ιού στο δίκτυο/ συστήματα της εταιρίας, πράγμα το οποίο θα δημιουργούσε πολλαπλάσια προβλήματα στις πολύ απαιτητικές προσπάθειες ανάκαμψης που είχαν ήδη ξεκινήσει.

Αποτέλεσμα και αντίκτυπος

Σε πέντε εβδομάδες η Deloitte βοήθησε τη εταιρία να επαναφέρει επιτυχώς το βασικό κορμό της Πληροφορικής, συμπεριλαμβανομένων πάνω από 60.000 φορητών υπολογιστών, επιβεβαιώνοντας την ασφαλή παραμετροποίηση περισσότερων από 1.200 διακομιστών σε όλο τον κόσμο, σε λιγότερο από 10 ημέρες. Επίσης, η Deloitte βοήθησε στη συνολική αναβάθμιση των συστημάτων σε νέο λειτουργικό σύστημα, στην αναδόμηση της υποδομής των διακομιστών της εταιρίας, στην παροχή πρόσβασης σε υπηρεσίες παρακολούθησης, καθώς και στην επαναλειτουργία του πιο εξελιγμένου και αυτοματοποιημένου τερματικού σταθμού του κόσμου. Το σημαντικότερο από όλα ήταν ότι τα πλοία της εταιρίας —και κατ' επέκταση μεγάλο μέρος του διεθνούς εμπορίου— λειτουργούσε ξανά.

Παραδείγματα περιστατικών κυβερνοεπίθεσης και σχετικών υπηρεσιών υποστήριξης

Κέντρο Κυβερνοασφάλειας της Πολιτείας της Καλιφόρνια

Το υπόβαθρο

Η οικονομία της Πολιτείας της Καλιφόρνια, λόγω του μεγέθους της (πέμπτη μεγαλύτερη οικονομία του κόσμου), γίνεται συχνά στόχος Κυβερνοεπιθέσεων. Το 2015, ο Κυβερνήτης της Καλιφόρνια εξέδωσε εκτελεστικό διάταγμα για τη δημιουργία του Κέντρου Ενοποίησης της Κυβερνοασφάλειας της Πολιτείας της Καλιφόρνια (California Cybersecurity Integration Center - Cal-CSIC). Ο στόχος δημιουργίας του Κέντρου ήταν η ενδυνάμωση της στρατηγικής Κυβερνοασφάλειας της Πολιτείας της Καλιφόρνια. Με τη δημιουργία αυτού του κέντρου η ηγεσία της Πολιτείας αποσκοπούσε στο να αποκτήσει μία ολοκληρωμένη εικόνα των Κυβερνοαπειλών καθώς επίσης να μειώσει την πιθανότητα και τον αντίκτυπο από πιθανά περιστατικά ασφάλειας.

Ενέργειες του Cal-CSIC

Το Cal-CSIC με τη διενέργεια αξιολόγησης αποκλίσεων (gap analysis) που πραγματοποίησε, προσπάθησε να εντοπίσει/ αξιολογήσει τις δυνατότητες Κυβερνοασφάλειας που είχε τη δεδομένη χρονική περίοδο. Μετά το πέρας της αξιολόγησης, το Κέντρο προέβη στο σχεδιασμό του πλαισίου και στον ορισμό της στρατηγικής για την ενδυνάμωση της Κυβερνοασφάλειας της Πολιτείας. Το Cal-CSIC προχώρησε σε συνεντεύξεις με υπεύθυνους Κυβερνοασφάλειας από όλη την Πολιτεία, με σκοπό να αναγνωρίσει τις κυριότερες επιχειρησιακές απαιτήσεις. Μετά από την ανάλυση των δεδομένων που συλλέχθηκαν από τις παραπάνω ενέργειες, υλοποιήθηκε ένα αυτοματοποιημένο σύστημα διαμοιρασμού πληροφοριών. Το σύστημα αυτό περιελάβανε την αναγνώριση και προμήθεια των κατάλληλων τεχνολογιών για μία πλατφόρμα μελέτης και ανάλυσης απειλών καθώς και μία πλατφόρμα για την αναφορά περιστατικών Κυβερνοασφάλειας για τη διαχείριση του συνόλου των περιστατικών όλων των Αρχών της Πολιτείας, οι οποίες θα συμμετείχαν στην πλατφόρμα. Με σκοπό την περαιτέρω ανάπτυξη των δυνατοτήτων της πλατφόρμας ανάλυσης απειλών, χρησιμοποιήθηκαν δεδομένα και από άλλες πηγές, όπως για παράδειγμα από τον ιδιωτικό τομέα καθώς και από άλλες κρατικές ή ομοσπονδιακές οντότητες. Τέλος, το Cal-CSIC προέβη στην ανάπτυξη ενός μοντέλου διακυβέρνησης, το οποίο θα υποστηρίζε τις μελλοντικές διαδικασίες λήψης αποφάσεων και επίλυσης περιστατικών ασφάλειας.

Αποτέλεσμα και αντίκτυπος

Το πρόγραμμα διαμοιρασμού πληροφοριών του Cal-CSIC συνεχίζει να αναπτύσσεται και οργανωτικές οντότητες της Πολιτείας επιλέγουν να εισαχθούν στο πρόγραμμα και ακόμη 10 επιχειρήσεις είναι στη διαδικασία εισαγωγής σε αυτό, συμπεριλαμβανομένων μίας ηγέτιδας εταιρίας παραγωγής ενέργειας και ενός τραπεζικού ιδρύματος. Ο απαιτούμενος χρόνος για την εισαγωγή νέων οντοτήτων στο πρόγραμμα έχει επίσης μειωθεί σημαντικά. Η συγκεκριμένη διαδικασία που αρχικά διαρκούσε τρεις με τέσσερις μήνες, σήμερα μπορεί να ολοκληρωθεί σε περίπου δύο μήνες. Η ηγεσία της Πολιτείας πλέον λαμβάνει τακτικές αναφορές σχετικά με τις απειλές Κυβερνοασφάλειας που αντιμετωπίζει η Πολιτεία της Καλιφόρνια. Σύντομα αναμένεται και η δυνατότητα του Κέντρου να εμβαθύνει στις μελέτες των απειλών και να τις διαχωρίζει ανά τομέα της οικονομίας. Το Cal-CSIC έχει επίσης κατορθώσει να αναγνωρίσει σημαντικό αριθμό επιθέσεων ηλεκτρονικού “ψαρέματος” (phishing) καθώς και άλλους τύπους κακόβουλων επιθέσεων (π.χ. ransomware) προς άλλες οργανωτικές οντότητες της Πολιτείας και σε κάποιες περιπτώσεις έχει αποτρέψει την περαιτέρω εξάπλωσή τους.

4 Βέλτιστες πρακτικές Κυβερνοασφάλειας

Βέλτιστες πρακτικές Κυβερνοασφάλειας

Η σύγχρονη εποχή απαιτεί το σχεδιασμό και την υιοθέτηση ολιστικής στρατηγικής Κυβερνοασφάλειας για την αποτελεσματική διαχείριση των συνεχώς αυξανόμενων κινδύνων του Κυβερνοχώρου μέσω της υλοποίησης κατάλληλων οργανωτικών και τεχνολογικών μέτρων προστασίας. Σε περίπτωση σοβαρού περιστατικού Κυβερνοεπίθεσης, διακυβεύεται η διατάραξη της εύρυθμης λειτουργίας και της βιωσιμότητας των οργανισμών. Γι' αυτό το λόγο, είναι ζωτικής σημασίας οι οργανισμοί να ανταποκριθούν στις τρέχουσες συνθήκες και να εξελιχθούν μέσω αυτών. Στο πλαίσιο αυτό, διεθνείς οργανισμοί έχουν αναπτύξει μεθοδολογίες/ πρακτικές με σκοπό να βοηθήσουν τις επιχειρήσεις σε αυτή την προσπάθεια. Ενδεικτικά παραδείγματα τέτοιων πρακτικών αποτελούν τα "Cybersecurity Best Practices" του Center for Internet Security (CIS), το "Special Publication SP 800-53" του NIST καθώς και μια σειρά από δημοσιεύσεις της Ευρωπαϊκής Αρχής για την Κυβερνοασφάλεια (ENISA) όπως η "Good practices under the National Cyber Security Strategies".

Οι οργανισμοί θα πρέπει να εφαρμόσουν μία ολιστική προσέγγιση με γνώμονα τις επιχειρησιακές τους ανάγκες και τις απειλές που διέπουν το περιβάλλον λειτουργίας τους, με σκοπό τη διαχείριση κινδύνων που σχετίζονται με θέματα Κυβερνοασφάλειας. Καθώς η ασφάλεια των αγαθών και των λειτουργιών ενός οργανισμού είναι ύψιστης σημασίας, οι έννοιες της προστασίας (secure) επίγνωσης (vigilant) και της ανθεκτικότητας (resilient) έναντι των Κυβερνοεπιθέσεων αποτελούν επιτακτική ανάγκη για έναν οργανισμό. Οι κίνδυνοι σχετικά με την Κυβερνοασφάλεια, οι οποίοι απασχολούν τους οργανισμούς από το παρελθόν, συνεχίζουν και παραμένουν ακόμη στο προσκήνιο. Το επίπεδο ετοιμότητας ενός οργανισμού έναντι πιθανών επιθέσεων ενδέχεται να ελαττωθεί, λόγω των μειωμένων δυνατοτήτων του τμήματος πληροφορικής, της μη ενημέρωσης του λογισμικού ή της έλλειψης εξιδεικευμένου προσωπικού Κυβερνοασφάλειας, με αποτέλεσμα να αυξάνεται η σοβαρότητα των επιθέσεων.

Κύριοι παράγοντες που ωθούν την ανάπτυξη κινδύνων στον κυβερνοχώρο

- Ανταλλαγή Πληροφοριών
- Καινοτομία
- Εμπιστοσύνη στους ανθρώπους

Κύριοι προβληματισμοί των οργανισμών

Έχουμε αξιολογήσει τη ψηφιακή μας ετοιμότητα για τη βέλτιστη διαχείριση των κινδύνων κατά τη χρήση νέων τεχνολογιών;

Ποιες τεχνολογικές επενδύσεις εξετάζουμε για να μειώσουμε το κόστος κανονιστικής συμμόρφωσης;

Πως μπορούμε να αξιοποιήσουμε την τεχνολογία για το μετασχηματισμό της διαχείρισης κινδύνων;

Υπεύθυνος Ασφάλειας

Το πλαίσιο ασφάλειας των επιχειρησιακών δραστηριοτήτων του οργανισμού που σχετίζονται με τη Κυβερνοασφάλεια, πρέπει να αναθεωρηθεί.

Διευθυντής Πληροφορικής

Θα πρέπει να πραγματοποιηθούν επιπλέον επενδύσεις για τη βελτιστοποίηση των δυνατοτήτων του οργανισμού σε θέματα Κυβερνοασφάλειας, έτσι ώστε ο οργανισμός να μπορεί να ανταποκριθεί επιτυχώς από περιστατικά ασφάλειας.

Διευθύνων Σύμβουλος

Η κατάρτιση μιας ισχυρής στρατηγικής Κυβερνοασφάλειας αποτελεί άμεση προτεραιότητα για τον οργανισμό.

Διοικητικό Συμβούλιο

Σχεδιασμός και υλοποίηση επαρκών διαδικασιών, με σκοπό την ενημέρωση αναφορικά με το επίπεδο ανθεκτικότητας του οργανισμού σε Κυβερνοεπιθέσεις.

Βέλτιστες πρακτικές Κυβερνοασφάλειας

Ο ρόλος του Υπεύθυνου Ασφάλειας Πληροφοριών (CISO) και της Εκτελεστικής Διοίκησης (C-Suite)

Παρά το βάρος που έχει δοθεί στην τεχνολογία και στην καινοτομία, η αποτελεσματική ασφάλεια πληροφοριών απαιτεί την υποστήριξη από την Διοίκηση και επαγγελματίες που διαθέτουν βαθιά εξειδίκευση και στρατηγικό όραμα. Τα τεχνολογικά εργαλεία ασφαλείας είναι σημαντικά, αλλά εξίσου ικανοί είναι και οι εγκληματίες του κυβερνοχώρου στην παράκαμψή τους. Για να είναι αποτελεσματική η ασφάλεια στον κυβερνοχώρο, απαιτείται **συνδυασμός ανθρώπινου δυναμικού, διαδικασιών και τεχνολογιών**.

Η αναβάθμιση του ρόλου του **Υπεύθυνου Ασφάλειας Πληροφοριών (ΥΑΠ)** ως μέλος της Διοίκησης ενός οργανισμού, αποτελεί θετική ένδειξη της οργανωτικής αποδοχής ότι η Κυβερνοασφάλεια απαιτεί πλήρη δέσμευση των ηγετικών στελεχών, καλύτερη διαχείριση κινδύνου στον Κυβερνοχώρο και αφομοίωση πρακτικών διαχείρισης κινδύνου σε ολόκληρο τον οργανισμό. Τα τελευταία 10 έτη, παρατηρήθηκε ότι ο ρόλος του ΥΑΠ επεκτάθηκε και πλέον από υπεύθυνο για τεχνολογικά θέματα, έχει μετεξελιχθεί σε σύμβουλο της Εκτελεστικής Διοίκησης. Οι οργανισμοί με ώριμο επίπεδο Κυβερνοασφάλειας, αναγνωρίζουν τον επιχειρησιακό κίνδυνο που ενέχει ο Κυβερνοχώρος και τον αντιμετωπίζουν σαν ένα ζήτημα που πρέπει να επιλυθεί συλλογικά. Οι ΥΑΠ σε τέτοιες περιπτώσεις αναλαμβάνουν ένα μετασχηματιστικό και στρατηγικό ρόλο, εστιάζοντας σε κινδύνους υψηλότερου επιπέδου, όπως εκείνοι που σχετίζονται με την χρήση νέων προϊόντων και εφαρμογών ή την ανταλλαγή πληροφοριών σε ολόκληρο τον οργανισμό.

Το **Διοικητικό Συμβούλιο και η Εκτελεστική Διοίκηση (C-Suite)**, κατευθύνουν και υποστηρίζουν τους οργανισμούς στον καθορισμό στρατηγικής για τη διαχείριση του περιβάλλοντος απειλών στον Κυβερνοχώρο. Καθώς τα Διοικητικά Συμβούλια και η Εκτελεστική Διοίκηση διαδραματίζουν όλο και πιο ενεργό ρόλο στην προστασία των οργανισμών τους, τα μέλη τους προσπαθούν να κατανοήσουν πώς μπορούν να κάνουν τον ρόλο τους πιο αποτελεσματικό (ποιες είναι οι ευθύνες τους, ποιες δεξιότητες πρέπει να αναπτύσσουν, ποιες είναι οι σωστές ερωτήσεις κ.λπ.).

Ενώ το επίπεδο Κυβερνοασφάλειας πρέπει να είναι ευέλικτο ανάλογα με το μέγεθος και το επίπεδο ωριμότητας ενός οργανισμού, το κλειδί είναι η διαμόρφωση ενός επιπέδου ασφάλειας που επιτρέπει τη πρόβλεψη, την άμυνα και την ανάκαμψη από τις συνήθεις αλλά και τις νέες απειλές του κλάδου που δραστηριοποιείται ο οργανισμός.

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

- Το Διοικητικό Συμβούλιο και η Εκτελεστική Διοίκηση, επιδεικνύουν τη δέουσα επιμέλεια, υπευθυνότητα και αποτελεσματικότητα στη διαχείριση της Κυβερνοασφάλειας.
- Ο οργανισμός έχει θεσπίσει την θέση του επικεφαλής ασφάλειας πληροφοριών ο οποίος συμμετέχει στις εκτελεστικές επιτροπές και έχει επαρκώς στελεχώσει το τμήμα Κυβερνοασφάλειας με τις κατάλληλες δεξιότητες.
- Η Διοίκηση προάγει την κουλτούρα Κυβερνοασφάλειας μέσω της εφαρμογής προγράμματος εκπαίδευσης του προσωπικού και την υιοθέτηση ρόλων και αρμοδιοτήτων για την ασφάλεια των πληροφοριακών πόρων του οργανισμού.
- Η Εκτελεστική Διοίκηση ενημερώνεται σε τακτά χρονικά διαστήματα για το προφίλ κινδύνου του οργανισμού και για το επίπεδο ωρίμανσης των μηχανισμών ασφάλειας.
- Ο οργανισμός έχει δημιουργήσει ένα κατάλληλο πλαίσιο κλιμάκωσης για τη διαχείριση των κινδύνων στον Κυβερνοχώρο και των περιστατικών ασφάλειας με την συμμετοχή της Εκτελεστική Διοίκησης, που λαμβάνει υπόψη την ανεκτικότητα του οργανισμού στους κινδύνους και τις υφιστάμενες ελλείψεις.
- Η Εκτελεστική Διοίκηση συμμετέχει ενεργά στην αξιολόγηση του προγράμματος ασφάλειας του οργανισμού, εστιάζει και επενδύει στους σωστούς τομείς με τις σωστές προτεραιότητες.

Βέλτιστες πρακτικές Κυβερνοασφάλειας

Οι ψηφιακές τεχνολογίες βοηθούν στη διαχείριση κινδύνων

Παρά το γεγονός ότι οι **ψηφιακές τεχνολογίες εισάγουν νέους κινδύνους**, **μπορούν επίσης να βελτιώσουν τη διαχείρισή τους**, παρέχοντας νέες δυνατότητες και αναδεικνύοντας ικανότητες που θεωρούνταν ανέφικτες στο παρελθόν. Οι επενδύσεις σε ψηφιακές τεχνολογίες για τη διαχείριση των κινδύνων ασφάλειας μπορούν να αυξήσουν την αποτελεσματικότητα και την αποδοτικότητα, ακόμη και να εισάγουν κανόνες που καθιστούν ορισμένους κινδύνους παρωχημένους. Οι οργανισμοί μπορούν να χρησιμοποιήσουν την ψηφιακή τεχνολογία ως εργαλείο για τη βελτιστοποίηση των πρακτικών διαχείρισης κινδύνου, για να μεγιστοποιήσουν την αποτελεσματικότητα των λειτουργιών τους και να επενδύσουν εκ νέου στον εκσυγχρονισμό διαχείρισης του κινδύνου.

ΕΝΔΕΙΚΤΙΚΑ ΠΑΡΑΔΕΙΓΜΑΤΑ

Αποτελεσματικότητα

Μείωση κόστους και επιτάχυνση εντοπισμού και αντιμετώπισης κινδύνων

Επιτάχυνση διαδικασιών
Αξιοποίηση εργαλείων ρομποτικής για την αυτοματοποίηση των διαδικασιών (Robotic Process Automation) βάσει συγκεκριμένων συνθηκών χωρίς την παρουσία του ανθρώπινου παράγοντα στο κομμάτι της λήψης αποφάσεων.

Ταχεία διαχείριση διαπιστευτηρίων πρόσβασης,
Αυτοματοποίηση διαδικασιών διαχείρισης αιτημάτων πρόσβασης και παροχής διαπιστευτηρίων μέσω Ρομποτικής Αυτοματοποίησης Διαδικασιών (Robotic Process Automation).

Παραγωγή αναφορών ελέγχου
Αυτοματοποίηση της δημιουργίας αναφορών ύποπτης δραστηριότητας με τη χρήση αυτοματοποιημένης αναγνώρισης γλώσσας (Natural Language Generation).

Διευκόλυνση στην πρόσβαση πληροφοριών συμμόρφωσης
Υλοποίηση τεχνολογιών chatbot για τον εντοπισμό κανονιστικών απαιτήσεων.

Ευφυΐα

Βελτίωση ποιότητας, ενίσχυση ακρίβειας και άντληση πληροφοριών για την αντιμετώπιση κινδύνων

Επαυξημένες δυνατότητες ανίχνευσης
Αυτοματοποιημένη επιθεώρηση επιχειρησιακών διαδικασιών μέσω εξειδικευμένων εφαρμογών παρακολούθησης των αρχείων καταγραφής.

Προσομοίωση διαχείρισης περιστατικών κρίσεων
Προσομοίωση πραγματικών γεγονότων κρίσης σε ρεαλιστικό περιβάλλον με σκοπό την βέλτιστη ανταπόκριση των εμπλεκομένων.

Μείωση του κινδύνου διαρροής εμπιστευτικών πληροφοριών
Αξιοποίηση προηγούμενων τεχνολογιών διαρροής εμπιστευτικών πληροφοριών για τη δημιουργία μοντέλου μηχανικής εκμάθησης που εντοπίζει ύποπτες συμπεριφορές.

Βελτιωμένη δέουσα επιμέλεια για εξωτερικούς συνεργάτες
Ενίσχυση της δέουσας επιμέλειας για εξωτερικούς συνεργάτες με αυτόματη αναζήτηση στο dark net, σε λίστες παρακολούθησης, λίστες κυρώσεων και ιστότοπους κανονιστικών αρχών.

Μετασχηματισμός

Υιοθέτηση νέας προσέγγισης για τον εντοπισμό και τη διαχείριση κινδύνων

Μείωση του κινδύνου εφοδιαστικής αλυσίδας
Παροχή αξιόπιστης και ταχείας διαδικασίας επαλήθευσης προέλευσης, ασφάλειας και γνησιότητας των προϊόντων σε όλη την εφοδιαστική αλυσίδα μέσω τεχνολογιών block-chain.

Ενίσχυση διαχείρισης του κινδύνου προμηθευτών
Αξιοποίηση πλατφόρμας στο υπολογιστικό νέφος που επιτρέπει την κοινή χρήση δεδομένων αξιολόγησης κινδύνου προμηθευτών.

Προληπτική διαχείριση του κινδύνου φήμης
Συνεχής παρακολούθηση των κινδύνων μέσω προγνωστικής ανάλυσης συμπεριφορών στο Διαδίκτυο και προληπτικής παρέμβασης.

Βελτιωμένη ασφάλεια και ποιότητα προϊόντων
Ανάλυση δεδομένων αισθητήρων σε μεγάλη κλίμακα και σε πραγματικό χρόνο για την πρόβλεψη σφαλμάτων και τον προγραμματισμό συντηρήσεων.

Βέλτιστες πρακτικές Κυβερνοασφάλειας

Σύνοψη μέτρων ασφάλειας

Οι οργανισμοί θα πρέπει να υιοθετήσουν ένα ολιστικό πρόγραμμα Κυβερνοασφάλειας για την αποτελεσματική διαχείριση των κινδύνων του Κυβερνοχώρου και την προστασίας τους από τις υπάρχουσες απειλές, ενώ, ταυτόχρονα, θα πρέπει να επενδύουν σε εξελισσόμενες τεχνικές προστασίας οι οποίες θα τους καταστήσουν έτοιμους για να αντιμετωπίσουν και τις επερχόμενες απειλές. Οι πρακτικές αυτές χωρίζονται σε τέσσερις βασικούς πυλώνες. Ο πρώτος πυλώνας, η **Διακυβέρνηση**, εστιάζει στο διαχειριστικό μέρος των τεχνικών προστασίας και πιο συγκεκριμένα σε θέματα που αφορούν τη στρατηγική του οργανισμού γύρω από τη Κυβερνοασφάλεια, τις αντίστοιχες πολιτικές που υποστηρίζουν τη στρατηγική καθώς και τη διαχείριση κινδύνων. Ο δεύτερος πυλώνας, η **Προστασία**, περιλαμβάνει μία ευρεία γκάμα από τεχνικές δικλείδες ασφαλείας που σκοπό έχουν να προστατεύσουν τον οργανισμό από Κυβερνοεπιθέσεις τόσο σε ψηφιακό όσο και σε φυσικό επίπεδο. Ο τρίτος πυλώνας αφορά την **Επίγνωση** όπου κάθε οργανισμός θα πρέπει να έχει έτσι, ώστε να έχει γνώση των δυνητικών απειλών που τον αφορούν και να είναι κατάλληλα προετοιμασμένος για τον περιορισμό και την αντιμετώπισή τους. Ο τελευταίος πυλώνας αφορά την **Ανθεκτικότητα** των οργανισμών και την ικανότητά τους να αντιδράσουν αποτελεσματικά και να διαχειριστούν με επιτυχία ένα περιστατικό ασφάλειας.

Διακυβέρνηση

1 **St** — Στρατηγική και μοντέλο λειτουργίας ασφάλειας

Προστασία

Προστασία πληροφοριών και πληροφοριακών συστημάτων με την εφαρμογή πλαισίου, προγράμματος, πολιτικών, διαδικασιών, προτύπων, οργανωτικών και τεχνολογικών μέτρων ασφάλειας για την αποτελεσματική διαχείριση των κινδύνων του Κυβερνοχώρου.

Επίγνωση

Έγκαιρη διαχείριση κινδύνων Κυβερνοχώρου για την ανίχνευση, εντοπισμό και περιορισμό αυτών.

Ανθεκτικότητα

3 2 **Ip** — Προετοιμασία για την αντιμετώπιση περιστατικών

Άμεση και αποτελεσματική διαχείριση περιστατικών ασφάλειας, ελαχιστοποίηση των επιπτώσεων τους και επαναφορά των επιχειρησιακών λειτουργιών το συντομότερο δυνατό.

2 **Pa** — Πολιτικές, πρότυπα και αρχιτεκτονική	5 **Cs** — Ασφάλεια υπολογιστικού νέφους	9 **S** — Ασφαλής ανάπτυξη εφαρμογών	13 **Es** — Προστασία συσκευών χρηστών	17 **Idm** — Διαχείριση ταυτοτήτων	21 **Dlp** — Περιορισμός διαρροής δεδομένων	25 **Cti** — Κυβερνοευφυία απειλών	29 **Sp** — Διαχείριση υποδομών ασφάλειας	33 **Ir** — Αντιμετώπιση περιστατικών ασφάλειας
3 **Aw** — Κουλτούρα διαχείρισης Κυβερνοκινδύνων	6 **Tp** — Διαχείριση κινδύνων εξωτερικών συνεργατών	10 **Ap** — Προστασία εφαρμογών	14 **Am** — Διαχείριση πληροφοριακών πόρων	18 **Pam** — Διαχείριση προσβάσεων διαχειριστών	22 **E** — Κρυπτογράφηση	26 **Bp** — Προστασία εταιρικής φήμης	30 **Pvm** — Διαχείριση τεχνολογικών ευπαθειών και κενών ασφάλειας	34 **Bc** — Διαχείριση επιχειρησιακής συνέχειας και ανθεκτικότητας
4 **Rm** — Διαχείριση, μέτρηση και αναφορά Κυβερνοκινδύνων	7 **Hs** — Ασφάλεια ανθρώπινου δυναμικού	11 **Mp** — Προστασία από κακόβουλα λογισμικά	15 **Ss** — Ασφάλεια συστημάτων	19 **Rbac** — Μηχανισμοί προσβάσεων ρόλων	23 **Dp** — Ιδιωτικότητα δεδομένων	27 **Td** — Εντοπισμός απειλών	31 **Pvi** — Δοκιμές παρείσδυσης	
	8 **Ps** — Φυσική ασφάλεια	12 **Nc** — Ασφάλεια δικτύων	16 **Ua** — Διαχείριση προσβάσεων χρηστών	20 **Ic** — Διαβάθμιση πληροφοριών	24 **Ilm** — Διαχείριση πληροφοριών	28 **Th** — Αντιμετώπιση απειλών		

- Διαχείριση Κυβερνοασφάλειας
- Εξωτερικό περιβάλλον
- Ανθρώπινο δυναμικό και χώροι εργασίας
- Ασφάλεια εφαρμογών
- Ασφάλεια υποδομών
- Διαχείριση ταυτότητας και προσβάσεων
- Ασφάλεια δεδομένων
- Αναγνώριση τεχνολογικών ευπαθειών
- Κυβερνοευφυΐα
- Λειτουργίες ασφάλειας
- Διαχείριση περιστατικών ασφάλειας
- Επιχειρησιακή ανθεκτικότητα

Βέλτιστες πρακτικές Κυβερνοασφάλειας

Διακυβέρνηση

Η αποτελεσματική αντιμετώπιση των υφιστάμενων αλλά και των μελλοντικών Κυβερνοαπειλών απαιτεί τη δημιουργία ενός ολιστικού πλαισίου διακυβέρνησης για την ασφάλεια των πληροφορίων. Η δόμηση του εν λόγω πλαισίου εξαρτάται από την κουλτούρα, το επιχειρηματικό και τεχνολογικό περιβάλλον, τον βαθμό ωριμότητας και την προσέγγιση για την επιχειρηματική βιωσιμότητα και ανθεκτικότητα σε επίπεδο οργανισμού.

Κατανόηση και αντιμετώπιση αναπτυσσόμενων απειλών

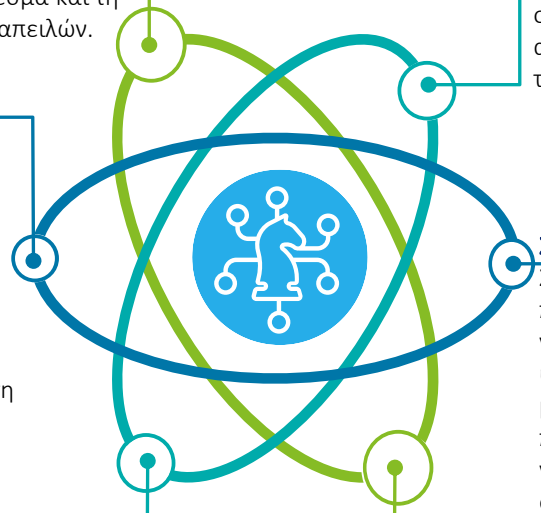
Οι οργανισμοί πρέπει να εξετάσουν τον αντίκτυπο και τον περιορισμό των απειλών στον Κυβερνοχώρο κατά τα αρχικά στάδια της κατάρτισης της επιχειρησιακής στρατηγικής. Η οικοδόμηση των απαραίτητων δυνατοτήτων Κυβερνοασφάλειας απαιτεί ενισχυμένη επαγρύπνηση και επίγνωση με στόχο τη λήψη τεκμηριωμένων αποφάσεων βραχυπρόθεσμα και τη δημιουργία ισχυρών θεμελίων για την αποτελεσματική αντιμετώπιση των μελλοντικών απειλών.

Σύνταξη πλαισίου διαχείρισης κινδύνων

Σύνταξη πλαισίου και μεθοδολογίας για την αναγνώριση, αξιολόγηση και παρακολούθηση κινδύνων Κυβερνοασφάλειας και των επιχειρηματικών επιπτώσεων. Κατάρτιση σχεδίου αντιμετώπισης και παρακολούθησης των κινδύνων με βάση το προφίλ κινδύνου του οργανισμού και το αποδεκτό επίπεδο αποδοχής κινδύνων. Οι οργανισμοί πρέπει να εξετάσουν τον αντίκτυπο και τον περιορισμό των απειλών στον κυβερνοχώρο από την αρχή, όταν αναπτύσσουν τη στρατηγική τους - όχι μήνες ή χρόνια αργότερα, όταν έχουν ήδη αρχίσει να υλοποιούν τα απαιτούμενα συστήματα και διαδικασίες και έχουν δεσμευθεί πόροι για την υλοποίηση μιας συγκεκριμένης στρατηγικής. Η διαχείριση κινδύνων θα πρέπει να εναρμονιστεί με τις διεργασίες για τη διαχείριση των επιχειρηματικών κινδύνων, ώστε να περιλαμβάνει τις παραμέτρους αντικτύπου για το σύνολο του οργανισμού. Η διοίκηση των οργανισμών λαμβάνει επαρκή πληροφόρηση για τη διαχείριση των κινδύνων σε τακτά χρονικά διαστήματα και προάγει την υλοποίηση μέτρων ασφάλειας για τη μετρίαση των σημαντικών κινδύνων με βάση το επίπεδο αποδοχής κινδύνων (risk appetite).

Υλοποίηση μοντέλου λειτουργίας

Σύνταξη επιχειρησιακού μοντέλου για τη λειτουργία του πλαισίου και του προγράμματος Κυβερνοασφάλειας το οποίο θα περιλαμβάνει τις οργανωτικές δομές, τους ρόλους και τις αρμοδιότητες των στελεχών των οργανισμών και των εξωτερικών συνεργατών, δίνοντας έμφαση στις υφιστάμενες αλλά και στις αναγκαίες δεξιότητες που απαιτούνται για την ορθή και πλήρη εφαρμογή του πλαισίου.



Ευθυγράμμιση της στρατηγικής Κυβερνοασφάλειας με την επιχειρησιακή στρατηγική

Κατάρτιση μεσοπρόθεσμης (1 έτους) και μακροπρόθεσμης (5 έτη) στρατηγικής Κυβερνοασφάλειας λαμβάνοντας υπόψη την υφιστάμενη και μελλοντική επιχειρησιακή στρατηγική και το μοντέλο λειτουργίας του οργανισμού. Η στρατηγική θα πρέπει να περιλαμβάνει τους απαιτούμενους πόρους, διαδικασίες και τεχνολογίες που απαιτούνται για τον αποτελεσματικό περιορισμό των απειλών του Κυβερνοχώρου.

Σύνταξη πλαισίου

Σύνταξη των δομών, ρόλων και αρμοδιοτήτων διακυβέρνησης, των πολιτικών, διαδικασιών και προτύπων Κυβερνοασφάλειας. Είναι σημαντικό να ενταχθεί η Κυβερνοασφάλεια στις καθημερινές λειτουργίες, στις ψηφιακές δράσεις ψηφιακού μετασχηματισμού, στη σύναψη συνεργασιών με εξωτερικούς συνεργάτες μέσω της χρήσης του μοντέλου DevSecOps. Το πλαίσιο, τα προγράμματα και οι δυνατότητες Κυβερνοασφάλειας θα πρέπει να ευθυγραμμίζονται με τα πρότυπα του κλάδου και άλλους αντίστοιχους οργανισμούς.

Υιοθέτηση κουλτούρας ασφάλειας

Υλοποίηση προγραμμάτων ευαισθητοποίησης με σκοπό τη διαρκή παρακολούθηση και βελτίωση του επιπέδου αφύπνισης και της κουλτούρας του οργανισμού για το αυξανόμενο περιβάλλον Κυβερνοαπειλών και τη σημαντικότητα της Κυβερνοασφάλειας για τη βιωσιμότητα του οργανισμού.

Βέλτιστες πρακτικές Κυβερνοασφάλειας

Προστασία

Η συνεχής θωράκιση των συστημάτων προλαμβάνει, σε μεγάλο βαθμό, τις Κυβερνοεπιθέσεις. Η αποτελεσματική διαχείριση των κινδύνων του Κυβερνοχώρου και η προστασία των πληροφοριών και των πληροφοριακών συστημάτων επιτυγχάνεται με την εφαρμογή πλαισίου, προγράμματος, πολιτικών, διαδικασιών, προτύπων, οργανωτικών και τεχνολογικών μέτρων ασφάλειας.

Υλοποίηση ισχυρού πλαισίου Κυβερνοασφάλειας

Αφού δημιουργηθεί μια συνολική στρατηγική προστασίας των κρίσιμών αγαθών, το επόμενο βήμα είναι η ανάπτυξη πλαισίου που ενσωματώνει τη στρατηγική Κυβερνοασφάλειας με την επιχειρησιακή στρατηγική. Το πλαίσιο περιλαμβάνει τα παρακάτω ενδεικτικά στοιχεία:

- Στρατηγική και επιχειρησιακό μοντέλο
- Πολιτικές, πρότυπα και αρχιτεκτονική
- Κουλτούρα Κυβερνοασφάλειας και αποδεκτές πρακτικές
- Διαχείριση κινδύνων, δείκτες απόδοσης και αναφορές
- Διαχείριση κύκλου ζωής πληροφοριών
- Διαχείριση μηχανισμών ασφάλειας

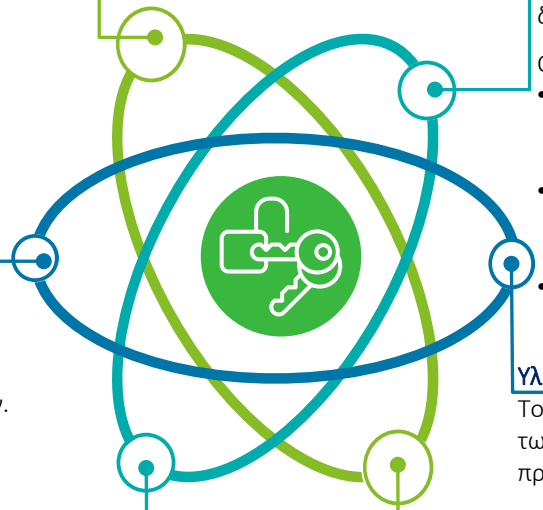
Προσδιορισμός και διασφάλιση των αγαθών στρατηγικής σημασίας

Αφού προσδιοριστούν τα αγαθά στρατηγικής σημασίας, επόμενο βήμα είναι η αξιολόγηση των απειλών στις οποίες είναι εκτεθειμένα και στη συνέχεια, ο εντοπισμός και η αποκατάσταση πιθανών αδυναμιών. Τα αγαθά στρατηγικής σημασίας περιλαμβάνουν:

- Ανθρώπινο δυναμικό: άτομα σε θέσεις ευθύνης που ενδέχεται να στοχοποιηθούν.
- Πληροφοριακά συστήματα και άλλα αγαθά κρίσιμα για την επίτευξη των επιχειρησιακών στόχων.
- Διαδικασίες: Κρίσιμες δραστηριότητες που ενδέχεται να διακοπούν ή να χρησιμοποιηθούν κακόβουλα.
- Πληροφορίες που ενδέχεται να χρησιμοποιηθούν για την εκτέλεση κακόβουλων ή/και μη ενδεδειγμένων ενεργειών.

Σχεδιασμός αρχιτεκτονικής ασφάλειας

Η αρχιτεκτονική ασφάλειας θα πρέπει να περιλαμβάνει το σύνολο των πληροφοριακών πόρων του οργανισμού και θα πρέπει να βασίζεται στις εις-βάθος ασφάλεια (in-depth security) και ζώνες ασφάλειας (security zones), δίνοντας έμφαση στις αρχιτεκτονικές μηδενικής εμπιστοσύνης (zero-trust).



Διαχείριση δεδομένων

Ο όγκος και η πολυπλοκότητα των δεδομένων αυξάνεται εκθετικά με τη χρήση νέων τεχνολογιών. Μια ολοκληρωμένη λύση είναι η εφαρμογή πρακτικών κεντρικοποιημένης διαχείρισης του κύκλου ζωής των πληροφοριών, η οποία αποτελεί μια συνολική προσέγγιση για τη διαχείριση και τη διασφάλιση όλων των σταδίων του κύκλου ζωής των δεδομένων, από τη δημιουργία έως τη διαγραφή.

Οι εν λόγω πρακτικές θα πρέπει να περιλαμβάνουν:

- Εντοπισμό των δεδομένων που επεξεργάζεται ο οργανισμός σε ηλεκτρονική και έντυπη μορφή με τη χρήση εξειδικευμένων εργαλείων e-Discovery και διακυβέρνησης δεδομένων (data governance).
- Διαβάθμιση πληροφοριών με βάση το επίπεδο εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας τους και υλοποίηση μηχανισμών σήμανσης (information labelling).
- Προσδιορισμός ελάχιστων μηχανισμών ασφάλειας με βάση το επίπεδο διαβάθμισης.

Υλοποίηση τεχνολογικών μέτρων ασφάλειας

Το είδος, το πλήθος και το εύρος των μέτρων για την ασφάλεια των υποδομών, των δικτύων, των εφαρμογών και των δεδομένων θα πρέπει να βασίζεται στο προφίλ κινδύνου το οργανισμού και στο αποδεκτό επίπεδο ανάληψης κινδύνου.

Ενσωμάτωση της Κυβερνοασφάλειας σε όλους τους τομείς από την αρχή

Ενσωμάτωση του πλαισίου Κυβερνοασφάλειας στις επιχειρηματικές διεργασίες, στις καθημερινές διαδικασίες και στο μοντέλο λειτουργίας του οργανισμού καθώς και στην καθιέρωση προτύπων ασφάλειας κατά τη διαδικασία ανάπτυξης υπηρεσιών και συστημάτων και τη διαχείριση τεχνολογίας από μονάδες διαφορετικές της πληροφορικής υιοθετώντας την αρχή της ασφάλειας εξ ορισμού και από τον σχεδιασμό (Security By Design and by Default).

Βέλτιστες πρακτικές Κυβερνοασφάλειας

Επίγνωση

Η ανάπτυξη ευαισθητοποίησης και η προληπτική ικανότητα αναγνώρισης απειλών απαιτεί ολιστική και σε βάθος κατανόηση του προφίλ κινδύνου του οργανισμού. Με την υλοποίηση των παρακάτω προηγμένων δυνατοτήτων ανίχνευσης απειλών σε κρίσιμες επιχειρησιακές διαδικασίες, εφαρμόζεται πρακτικά μια ολιστική προσέγγιση για τον περιορισμό εκ των γένεσει των απειλών Κυβερνοασφάλειας.

Προσδιορισμός προφίλ κινδύνου

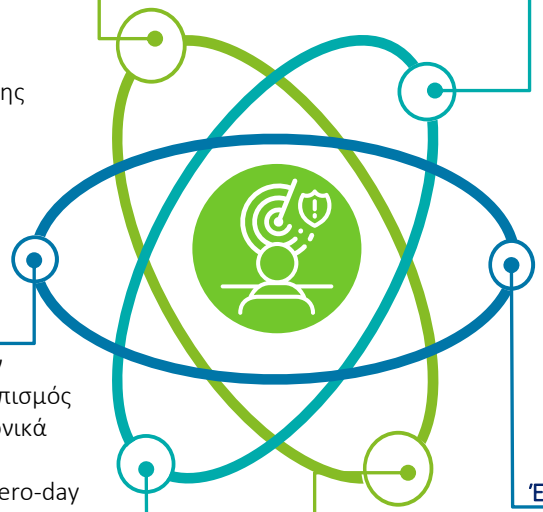
Αναγνώριση των Κυβερνοαπειλών, των κινήτρων, των μεθόδων και των τεχνικών που χρησιμοποιούν οι Κυβερνοεγκληματίες με σκοπό τον προσδιορισμό του προφίλ κινδύνου του οργανισμού και την προετοιμασία του για την προληπτική αντιμετώπιση των κινδύνων του Κυβερνοχώρου.
Επιπρόσθετα, οι οργανισμοί θα πρέπει να εντοπίζουν έγκαιρα αλλαγές οι οποίες θα μπορούσαν να τροποποιήσουν το τρέχον επίπεδο Κυβερνοασφάλειας. Παραδείγματα αλλαγών που πρέπει να αξιολογούνται αποτελούν οι συγχωνεύσεις και εξαγορές, τα εναλλακτικά μοντέλα λειτουργίας, οι νέοι προμηθευτές και οι αναθέσεις διεκπεραίωσης στρατηγικών λειτουργιών σε εξωτερικούς συνεργάτες. Επίσης, οι ενισχυμένες διαδικασίες παρακολούθησης και ελέγχου, καθιστούν δυνατή τη συνεχή και ολιστική αξιολόγηση του περιβάλλοντος ασφάλειας του οργανισμού.

Έγκαιρη διαχείριση τεχνολογικών ευπαθειών

Υλοποίηση τεχνολογιών για την πλήρη και αυτοματοποιημένη καταγραφή των πόρων πληροφορικής (Configuration Management Database - CMDB) και στη συνέχεια εντοπισμός και αξιολόγηση των τεχνολογικών ευπαθειών (vulnerability assessment) σε τακτά χρονικά διαστήματα και κατά την υλοποίηση νέων τεχνολογιών. Επιπρόσθετα, υλοποίηση μηχανισμών για την έγκαιρη αναγνώριση των νέων/μη δημοσιευμένων ευπαθειών (zero-day vulnerabilities) που κοινοποιούν οι κατασκευαστές και οι εταιρίες Κυβερνοασφάλειας. Στη συνέχεια, κατάρτιση πλάνου ενημέρωσης των ευπαθειών ή/και υλοποίηση αντισταθμιστικών μέτρων (compensative controls) για τον περιορισμό της πιθανότητας και της επίπτωσης εκμετάλλευσης αυτών.

Διαμοίραση πληροφοριών Κυβερνοευφυΐας

Υλοποίηση μηχανισμών (π.χ. η πλατφόρμα ανοικτού κώδικα MISSP – Malware Information Sharing Platform) για την αμφίδρομη διαμοίραση πληροφοριών Κυβερνοευφυΐας με πιστοποιημένα κέντρα (Computer Emergency Response Team, Computer Security Incident Response Team) αντιμετώπισης περιστατικών ασφάλειας, με παρόχους Κυβερνοασφάλειας και με οργανισμούς.



Προληπτικός εντοπισμός απειλών

Υλοποίηση προηγμένων τεχνολογιών τεχνητής νοημοσύνης (artificial intelligence), γνωστικής μάθησης (cognitive learning), ανάλυσης δεδομένων (deep data analytics), τεχνολογιών συσχέτισης (correlation technologies) και Κυβερνοευφυΐας (threat intelligence) για την ανάπτυξη προηγμένων επιπέδων επιχειρησιακής επίγνωσης. Οι τεχνολογίες ανάλυσης δεδομένων και συσχέτισης βοηθούν έναν οργανισμό να κατανοήσει πώς ξεκίνησε μια επίθεση, ποιο είναι το προφίλ των επιτιθέμενων και ποια σημεία εισόδου στοχεύουν οι Κυβερνοεγκληματίες. Επίσης, επιτρέπουν την προγνωστική ανίχνευση απειλών, βοηθώντας στην πρόβλεψη και τον περιορισμό των μελλοντικών απειλών. Η τεχνολογία ανάλυσης απειλών βοηθά στη παρακολούθηση πηγών πληροφοριών, συμπεριλαμβανομένου του δικτύου των Κυβερνοεγκληματιών (dark net), των αναφορών κακόβουλου λογισμικού και της Διαδικτυακής δραστηριότητας, για να εντοπίσουν κινδύνους που αφορούν συγκεκριμένα έναν οργανισμό. Είναι επίσης σημαντικό, να παρακολουθείται συνεχώς το εσωτερικό επιχειρησιακό περιβάλλον για ύποπτες, ασυνήθεις και μη προβλεπόμενες ενέργειες.

Έλεγχος ασφάλειας υποδομών

Διενέργεια ελεγχόμενων προσομοιώσεων παραβίασης της ασφάλειας των πληροφοριακών συστημάτων και των εφαρμογών (penetration tests), οι οποίες δύνανται να επιτρέψουν σε μια κακόβουλη οντότητα, χωρίς πρότερη γνώση, να παρεισδύσει στα συστήματα του οργανισμού με στόχο την αξιολόγηση της επάρκειας της ασφάλειας των πληροφοριακών συστημάτων και την τεκμηρίωση των σχετικών κινδύνων.

Προσδιορισμός μέτρων ασφάλειας

Προσδιορισμός, αναθεώρηση ή/και ενίσχυση των υφιστάμενων οργανωτικών και τεχνολογικών μέτρων ασφάλειας με βάση το προφίλ κινδύνου του οργανισμού.

Βέλτιστες πρακτικές Κυβερνοασφάλειας

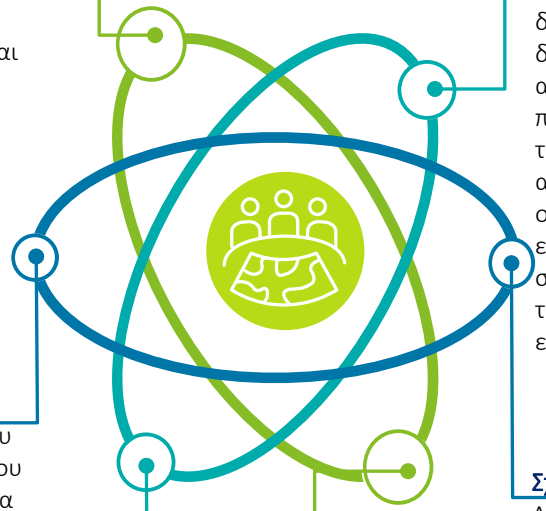
Ανθεκτικότητα

Οι οργανισμοί θα πρέπει να υιοθετήσουν την αντίληψη ότι σε μεσοπρόθεσμο χρονικό ορίζοντα η ασφάλειά τους θα παραβιαστεί. Για το λόγο αυτό απαιτείται η εκ των προτέρων προετοιμασία των οργανισμών για την άμεση και αποτελεσματική διαχείριση περιστατικών ασφάλειας, ελαχιστοποίηση των επιπτώσεων τους και επαναφορά των επιχειρησιακών λειτουργιών το συντομότερο δυνατό.

Υλοποίηση σχεδίου ανθεκτικότητας

Ένα αποτελεσματικό σχέδιο ανθεκτικότητας πρέπει να αναπτυχθεί νωρίς, και πρέπει να είναι σαφές, συνοπτικό και να περιλαμβάνει τουλάχιστον τα εξής στοιχεία:

- **Διακυβέρνηση**: Καθιέρωση διαλειτουργικού συντονισμού, διαχείρισης τεκμηρίωσης και επικοινωνίας με τα εμπλεκόμενα μέρη.
- **Στρατηγική**: Δημιουργία ισχυρής και ευθυγραμμισμένης στρατηγικής για την αντιμετώπιση περιστατικών Κυβερνοασφάλειας.
- **Τεχνολογία**: Κατανόηση των τεχνικών παραμέτρων της διαχείρισης περιστατικών και της τεκμηρίωσης παραβιάσεων.
- **Επιχειρησιακές λειτουργίες**: Υλοποίηση διασυνδεδεμένων διαδικασιών επιχειρησιακής συνέχειας και ανάκαμψης από καταστροφή με έμφαση στην αποτελεσματική επικοινωνία.
- **Διαχείριση κινδύνου και συμμόρφωση**: Διαμόρφωση σχεδίου ανθεκτικότητας το οποίο ενσωματώνει τις λειτουργίες της διαχείρισης κινδύνου και κανονιστικής συμμόρφωσης.



Σχεδιασμός σεναρίων

Καταγραφή συγκεκριμένων σεναρίων επιθέσεων και ενεργειών αντιμετώπισης για του κινδύνους υψηλής επικινδυνότητας που απειλούν τα αγαθά στρατηγικής σημασίας του οργανισμού. Τα σενάρια αυτά περιγράφουν τη σειρά των γεγονότων που ενδέχεται να συμβούν καθώς εξελίσσεται ένας συγκεκριμένος τύπος επίθεσης και αναλύουν τις ενέργειες που πρέπει να εκτελεστούν για να ελαχιστοποιηθεί ο αντίκτυπος. Η προετοιμασία αυτή παρέχει στον οργανισμό μια ευρεία εικόνα των πιθανών απειλών, ώστε να μπορούν να οριστούν σαφείς προτεραιότητες.

Ενημέρωση σχεδίων

Το σχέδιο αντιμετώπισης περιστατικών Κυβερνοασφάλειας θα πρέπει να αξιολογείται και να εξελίσσεται ανάλογα με τις αλλαγές στο περιβάλλον του οργανισμού τουλάχιστον μία φορά το χρόνο.

Δοκιμή σχεδίων αντιμετώπισης περιστατικών

Μετά την εφαρμογή των σχεδίων, οι οργανισμοί θα πρέπει να διεξάγουν συστηματικές δοκιμές σε ελεγχόμενο περιβάλλον ώστε να αξιολογείται συνεχώς η λειτουργικότητά τους. Οι δοκιμές μπορούν να περιλαμβάνουν την προσομοίωση επί χάρτου (war gaming) περιστατικών ασφάλειας με εκτεταμένη διάρκεια και με τη συμμετοχή όλων των εμπλεκόμενων μελών των ομάδων διαχείρισης κρίσεων. Επίσης, βέλτιστη πρακτική αποτελεί η εκτέλεση επίμονων δοκιμών παρείσδυσης μέσω της προσομοίωσης ρεαλιστικών Κυβερνοεπιθέσεων από ανεξάρτητη εταιρία και χωρίς τη γνώση των ομάδων αντιμετώπισης περιστατικών του οργανισμού (red teaming). Μόλις παραβιαστεί η ασφάλεια του οργανισμού από την επιτιθέμενη ομάδα (red team), τότε μπορεί να αξιολογηθεί πόσο γρήγορα και αποτελεσματικά η ομάδα άμυνας του οργανισμού αναγνώρισε και ανταποκρίθηκε στην επίθεση. Οι εν λόγω δοκιμές επιτρέπουν σε έναν οργανισμό να αξιολογήσει συνολικά το επίπεδο ασφάλειας σε οργανωτικό, διαδικαστικό και τεχνολογικό επίπεδο, την αποτελεσματικότητα των σχεδίων απόκρισης του και να εντοπίσει τρωτά σημεία που πρέπει να ενισχυθούν.

Σχεδιασμός ενιαίας προσέγγισης

Ανάπτυξη ενιαίας και συγκροτημένης προσέγγισης για το σχέδιο απόκρισης κατά τη διαχείριση περιστατικών ασφάλειας για τη βέλτιστη ανταπόκριση συνδυάζοντας όλες τις απαραίτητες επιχειρησιακές λειτουργίες με συγκροτημένο τρόπο, βελτιώνοντας έτσι την ανθεκτικότητα και τη συμμόρφωση του οργανισμού με τις κανονιστικές απαιτήσεις.

Προληπτικός έλεγχος παραβιάσεων

Προληπτική ανάλυση ενδείξεων παραβίασης (indications of compromise) με σκοπό την εξακρίβωση εάν υφίσταται κακόβουλη παρουσία στα συστήματα του οργανισμού.

5 Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Ο οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας προϋποθέτει την πλήρη κατανόηση του υφιστάμενου και μελλοντικού επιχειρησιακού περιβάλλοντος του οργανισμού, του επιπέδου ωριμότητας των υφιστάμενων μηχανισμών ασφάλειας για την υλοποίηση ολιστικών δράσεων με σκοπό την αποτελεσματική διαχείριση των κινδύνων του Κυβερνοχώρου. Στις επόμενες σελίδες παρατίθενται τα 5 επίπεδα ασφάλειας και ενδεικτικά μέτρα για κάθε ένα από αυτά.

Συνοπτικά, ο οδικός χάρτης θα πρέπει να περιλαμβάνει τις παρακάτω δράσεις για την επίγνωση, την προστασία και την ανθεκτικότητα της Κυβερνοασφάλειας:

13. Υλοποίηση αρχιτεκτονικής ασφάλειας και χρήση προηγμένων τεχνολογιών για την προληπτική αναγνώριση και αντιμετώπιση των απειλών.
14. Κατανόηση και αντιμετώπιση απειλών που ενέχουν κίνδυνο να εξαπλωθούν εκθετικά αν δεν αντιμετωπιστούν εγκαίρως και ανάπτυξη κοινής προσέγγισης.

Ανθεκτικότητα

Ανθεκτικότητα

15. Ανάπτυξη και εφαρμογή σχεδίου ανθεκτικότητας με σκοπό τη συνεχή βελτίωση του επιπέδου Κυβερνοασφάλειας.
16. Περιοδικός έλεγχος του επιπέδου ανθεκτικότητας.

5. Ενσωμάτωση στρατηγικής Κυβερνοασφάλειας στην επιχειρησιακή στρατηγική.
6. Υλοποίηση πολιτικής για την αναγνώριση και καταγραφή των σημαντικότερων αγαθών του οργανισμού και σχεδιασμός δικλείδων ασφάλειας για την προστασία τους.
7. Ανάπτυξη ενός ισχυρού πλαισίου διαχείρισης της Κυβερνοασφάλειας και υλοποίηση μοντέλου λειτουργίας.

Προστασία

Προστασία

8. Διασφάλιση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας των αγαθών στρατηγικής σημασίας
9. Υλοποίηση και εφαρμογή πολιτικών και δικλείδων ασφάλειας.
10. Ενσωμάτωση δικλείδων ασφάλειας σε όλους τους τομείς του οργανισμού.
11. Ανάπτυξη βέλτιστων μεθόδων διαχείρισης της Κυβερνοασφάλειας
12. Εφαρμογή βέλτιστων πρακτικών στις καθημερινές λειτουργίες του οργανισμού.

Επίγνωση

Επίγνωση

2. Κατανόηση του ισχύοντος επιπέδου ωριμότητας των δυνατοτήτων σχετικά με την Κυβερνοασφάλεια.
3. Αξιολόγηση κινδύνων και απειλών.
4. Υιοθέτηση κουλτούρας Κυβερνοασφάλειας.

1. Κατανόηση του επιχειρηματικού πλαισίου, των στόχων και του προφίλ κινδύνου του οργανισμού.

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Ανάπτυξη στρατηγικής Κυβερνοασφάλειας

Η στρατηγική θα πρέπει να υποστηρίζεται από ένα αποτελεσματικό και αποδοτικό πλαίσιο διαχείρισης Κυβερνοασφάλειας, το οποίο θα έχει ως γνώμονα τις επιχειρησιακές ανάγκες, απειλές και δυνατότητες του οργανισμού. Το πλαίσιο αυτό θα πρέπει να εφαρμόζει αποτελεσματική μεθοδολογία με σκοπό την αξιολόγηση της ανθεκτικότητας του οργανισμού σε θέματα Κυβερνοασφάλειας και διαχείρισης των σχετικών κινδύνων. Στο πλαίσιο αυτό υπάρχουν παγκοσμίως αναγνωρισμένα πρότυπα τα οποία ορίζουν πολύ συγκεκριμένες μεθοδολογίες για την αναγνώριση και τη διαχείριση των κινδύνων από Κυβερνοεπιθέσεις. Οι μεθοδολογίες αυτές περιλαμβάνουν σαφώς ορισμένα βήματα και πρακτικές για την διαχείριση των σχετικών επιχειρησιακών κινδύνων. Ενδεικτικές διαδεδομένες και παγκοσμίως αναγνωρισμένες και αποδεκτές μεθοδολογίες είναι το **ISO 2700x**, το πλαίσιο Κυβερνοασφάλειας του NIST (**NIST cybersecurity framework**), και η μεθοδολογία του **Information Security Forum** για τη διαχείριση κινδύνων (**IRAM2**).

Ένα αποτελεσματικό πρόγραμμα διαχείρισης κινδύνων που άπτεται σε θέματα Κυβερνοασφάλειας, μπορεί να προάγει την ανάπτυξη, να προστατεύσει την αξία του οργανισμού καθώς επίσης και να βοηθήσει να αποκτηθεί επίγνωση για τις Κυβερνοαπειλές.

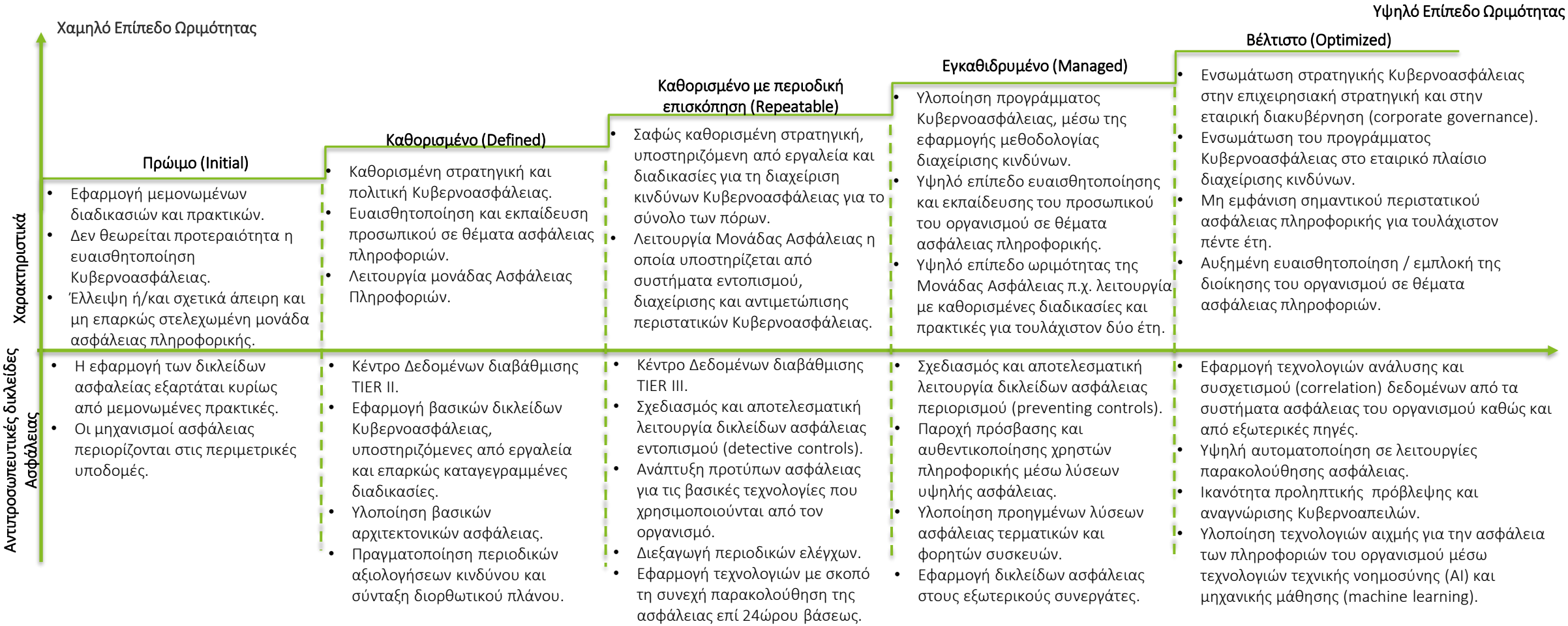
Ο οδικός χάρτης για την ανάπτυξη της στρατηγικής Κυβερνοασφάλειας θα πρέπει να περιλαμβάνει τις παρακάτω δράσεις:

- Κατανόηση του επιχειρηματικού πλαισίου και των στόχων του οργανισμού
- Κατανόηση του περιβάλλοντος απειλών
- Κατανόηση του ισχύοντος επιπέδου ωριμότητας των δυνατοτήτων σχετικά με την Κυβερνοασφάλεια
- Εστίαση στις σωστές προτεραιότητες
- Καθορισμός του επιθυμητού επιπέδου ωριμότητας των δυνατοτήτων Κυβερνοασφάλειας
- Ανάπτυξη στρατηγικής, πλαισίου, προγράμματος και σχεδίου δράσης Κυβερνοασφάλειας
- Μεγιστοποίηση της απόδοσης από τις επενδύσεις στην Κυβερνοασφάλεια
- Επικοινωνία με ενδιαφερόμενους φορείς εντός και εκτός του οργανισμού

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Χαρακτηριστικά επίπεδων ωριμότητας ασφάλειας – αντιπροσωπευτικές δικλείδες ασφάλειας ανά επίπεδο ωριμότητας

Η υλοποίηση της στρατηγικής Κυβερνοασφάλειας και ο ορισμός ενός μοντέλου ασφάλειας το οποίο θα αποτελείται από βραχυπρόθεσμες και μακροπρόθεσμες δράσεις, προϋποθέτει, αρχικά την κατανόηση του ισχύοντος επιπέδου ωριμότητας και στη συνέχεια τον καθορισμό του επιθυμητού επιπέδου ωριμότητας των δυνατοτήτων Κυβερνοασφάλειας. Για το παραπάνω, σημαντική παράμετρος αποτελεί ο καθορισμός των κατάλληλων στόχων για το επιθυμητό επίπεδο ωριμότητας που ο εκάστοτε οργανισμός είναι σκόπιμο να επιτύχει. Ο καθορισμός του επιθυμητού επιπέδου ωριμότητας του οργανισμού είναι άμεσα συνδεδεμένο με την αποδοχή κινδύνων (risk appetite), η οποία με τη σειρά της συσχετίζεται με μία σειρά από παράγοντες. Οι παράγοντες αυτοί αποτελούνται από το υφιστάμενο επίπεδο ωριμότητας, το επιχειρησιακό πλαίσιο, όπως ο τομέας δραστηριοποίησης του οργανισμού, καθώς και το πεδίο των απειλών που αφορούν τον οργανισμό. Ακολουθούν τα πέντε (5) επίπεδα ωριμότητας ανάλογα με τα χαρακτηριστικά και τα εφαρμοζόμενα μέτρα ασφάλειας.



Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Εκπαίδευση

Οι χρήστες των πληροφοριακών συστημάτων αποτελούν τον πιο αδύναμο ή τον πιο ισχυρό κρίκο της ασφάλειας. Τα προγράμματα Κυβερνοασφάλειας εφαρμόζονται και οι διαδικασίες τηρούνται από τους χρήστες. Για αυτό το λόγο είναι απαραίτητη η περαιτέρω εκπαίδευση των χρηστών για τους κινδύνους και τις απειλές που Κυβερνοχώρου και τις πρακτικές ασφάλειας που εφαρμόζει ο οργανισμός.

Πρώιμο (Initial)	Καθορισμένο (Defined)	Καθορισμένο με περιοδική επισκόπηση (Repeatable)	Εγκαθιδρυμένο (Managed)	Βέλτιστο (Optimized)
▪ Επικοινωνία των πολιτικών Κυβερνοασφάλειας και των βέλτιστων πρακτικών προστασίας κατά τη διαδικασία πρόσληψης. ▪ Ευαισθητοποίηση σχετικά με την αποφυγή προσπέλασης ή «κατεβάσματος» (downloading) συνημμένων αρχείων και εγκατάσταση μη εξουσιοδοτημένων προγραμμάτων. ▪ Ευαισθητοποίηση σχετικά με την ασφαλή χρήση του Διαδικτύου, την αποφυγή παροχής των διαπιστευτηρίων τους σε τρίτους, να μην ανταποκρίνονται σε ύποπτα μηνύματα ή κλήσεις που ζητούν προσωπικά στοιχεία και κωδικούς πρόσβασης και να μην χρησιμοποιούν εταιρικούς κωδικούς πρόσβασης σε μη εταιρικούς ιστότοπους. ▪ Παροχή οδηγιών για την άμεση ενημέρωση των στελεχών Κυβερνοασφάλειας και πληροφορικής σε περίπτωση πιθανής παραβίασης.	▪ Θεωρείται προτεραιότητα η ευαισθητοποίηση Κυβερνοασφάλειας και έχει θεσπισθεί πολιτική και διαδικασία εκπαίδευσης που περιλαμβάνει και πρακτικές φυσικής ασφάλειας, μέσων κοινωνικής δικτύωσης και απομακρυσμένης τηλεργασίας. ▪ Επικοινωνία των πολιτικών Κυβερνοασφάλειας και των βέλτιστων πρακτικών προστασίας σε τακτά χρονικά διαστήματα. ▪ Εκπαίδευση των χρηστών σχετικά με τους τρόπους με τους οποίους μπορεί να εμφανιστεί μια απειλή, εστιασμένη σε επιθέσεις κοινωνικής μηχανικής (social engineering). ▪ Υψηλό επίπεδο αναγνώρισης κακόβουλων μηνυμάτων με βάση τον αποστολέα, το θέμα, το ύφος και τη σύνταξη του μηνύματος. ▪ Υλοποίηση αυτοματοποιημένων μηχανισμών ενημέρωσης των στελεχών Κυβερνοασφάλειας και πληροφορικής σε περίπτωση πιθανής παραβίασης.	▪ Θέσπιση ετήσιου προγράμματος εκπαίδευσης το οποίο αναθεωρείται σε τακτά χρονικά διαστήματα με βάση το προφίλ κινδύνου του οργανισμού και το επίπεδο ευαισθητοποίησης των υπαλλήλων. ▪ Εκπαίδευση των χρηστών με τις βασικές απαιτούμενες ενέργειες για την πρόληψη περιστατικών ασφάλειας (π.χ. ασφάλεια κωδικών / διαπιστευτηρίων, ορθή και ενδεδειγμένη χρήση πληροφοριακών συστημάτων, βέλτιστες πρακτικές στη χρήση ηλεκτρονικής αλληλογραφίας για την αποφυγή ανεπιθύμητης αλληλογραφίας, μηνυμάτων απάτης κτλ.). ▪ Εξειδικευμένη εκπαίδευση των στελεχών Κυβερνοασφάλειας και Πληροφορικής. ▪ Εκτέλεση επίμονων δοκιμών παρείσδυσης (red teaming) μέσω της προσομοίωσης ρεαλιστικών Κυβερνοεπιθέσεων από ανεξάρτητη εταιρία και χωρίς την γνώση των ομάδων αντιμετώπισης περιστατικών του οργανισμού.	▪ Η Διοίκηση προάγει την κουλτούρα Κυβερνοασφάλειας μέσω της εφαρμογής προγράμματος εκπαίδευσης του προσωπικού και την υιοθέτηση ρόλων και αρμοδιοτήτων για την ασφάλεια των πληροφοριακών πόρων του οργανισμού. ▪ Προσομοίωση πραγματικών Κυβερνοεπιθέσεων σε ρεαλιστικό περιβάλλον με σκοπό την βέλτιστη ανταπόκριση των εμπλεκομένων. ▪ Υλοποίηση προγραμμάτων ευαισθητοποίησης με την χρήση εξειδικευμένης πλατφόρμας εκπαίδευσης (user awareness training platform) με σκοπό την διαρκή εκτέλεση, παρακολούθηση και βελτίωση του επιπέδου αφύπνισης και της κουλτούρας του οργανισμού. ▪ Πιστοποίηση των στελεχών Κυβερνοασφάλειας και Πληροφορικής σε θέματα ασφάλειας και τεχνολογιών.	▪ Επικαιροποίηση του προγράμματος εκπαίδευσης σε τακτά χρονικά διαστήματα λαμβάνοντας υπόψη το περιβάλλον Κυβερνοαπειλών. ▪ Θέσπιση προγράμματος επιβράβευσης για την τήρηση των πρακτικών Κυβερνοασφάλειας και την άμεση αναγνώριση και με ενδεδειγμένο τρόπο αντιμετώπιση περιστατικών ασφάλειας. ▪ Εκτέλεση προσομοιώσεων επί-χάρτου (war gaming) με εκτεταμένη διάρκεια με την συμμετοχή όλων των εμπλεκόμενων μελών των ομάδων διαχείρισης κρίσεων.

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Θωράκιση

Οι Κυβερνοεγκληματίες χρησιμοποιούν αυτοματοποιημένους μηχανισμούς για την ανίχνευση τεχνολογικών ευπαθειών και διαμοίρασης σχετικών πληροφοριών μεταξύ τους. Η συνεχής θωράκιση των συστημάτων προλαμβάνει τις Κυβερνοεπιθέσεις και περιορίζει σημαντικά τον βαθμό παρείσδυσης και τις επιπτώσεις των περιστατικών ασφάλειας.

Πρώιμο (Initial)	Καθορισμένο (Defined)	Καθορισμένο με περιοδική επισκόπηση (Repeatable)	Εγκαθιδρυμένο (Managed)	Βέλτιστο (Optimized)
▪ Μη θεσμοθετημένη εγκατάσταση των τελευταίων ενημερώσεων και οδηγιών ασφάλειας για τα πληροφοριακά συστήματα και των υποδομών. ▪ Θωράκιση συστημάτων με βάση τις οδηγίες των κατασκευαστών. ▪ Υλοποίηση βασικών μηχανισμών πιστοποίησης και αυθεντικοποίησης και συστημικών ρόλων (Role-based Access Control) στα κύρια πληροφοριακά συστήματα. ▪ Υλοποίηση συστημάτων αντιικού λογισμικού (antivirus). ▪ Υλοποίηση περιμετρικών τοίχων προστασίας (Firewall). ▪ Υλοποίηση εσωτερικών εικονικών δικτύων (Virtual LANs). ▪ Υλοποίηση συστημάτων περιορισμού δικτυακών επιθέσεων (Network Intrusion Prevention Systems).	▪ Εγκατάσταση των τελευταίων ενημερώσεων σε τακτά χρονικά διαστήματα π.χ. σε μηνιαία βάση και οδηγιών ασφάλειας για τα πληροφοριακά συστήματα και των υποδομών που είναι εκτεθειμένα στο Διαδίκτυο. ▪ Υλοποίηση ισχυρών μηχανισμών πιστοποίησης και αυθεντικοποίησης στο σύνολο των πληροφοριακών συστημάτων και υποδομών. ▪ Υιοθέτηση αρχιτεκτονικής περιμετρικής ασφάλειας. ▪ Υλοποίηση τοίχων προστασίας για τις Διαδικτυακές εφαρμογές (Web Application Firewall) και τις υποδομές του εσωτερικού δικτύου (Internal Firewall και Database Firewall) με την χρήση αυστηρών κανόνων πρόσβασης (Access control lists). ▪ Υλοποίηση συστημάτων περιορισμού δικτυακών επιθέσεων (Host Intrusion Prevention systems). ▪ Υλοποίηση συστημάτων για περιορισμό των προηγμένων απειλών (Advanced Persistent Threats). ▪ Υλοποίηση συστημάτων περιορισμού επιθέσεων άρνησης υπηρεσιών (Denial of Service attacks).	▪ Θεσμοθετημένη εγκατάσταση των τελευταίων ενημερώσεων σε τακτά χρονικά διαστήματα π.χ. σε μηνιαία βάση και οδηγιών ασφάλειας για το σύνολο των πληροφοριακών συστημάτων και υποδομών. ▪ Υλοποίηση μηχανισμών πολλαπλών παραγόντων πιστοποίησης και αυθεντικοποίησης (MFA). ▪ Υλοποίησης συστημάτων πιστοποίησης και αυθεντικοποίησης (Privileged Access Management) για τις προσβάσεις προνομιακής διαχείρισης. ▪ Υιοθέτηση ζωνών (zones) αρχιτεκτονικής ασφάλειας για το εσωτερικό δίκτυο. ▪ Υλοποίηση συστημάτων για τον περιορισμό της δικτυακής πρόσβασης (Network Access Control). ▪ Υλοποίηση συστημάτων για την ασφάλεια των εταιρικών και προσωπικών φορητών υπολογιστών (Mobile Device Management/ Enterprise Mobility Management). ▪ Υλοποίηση εξειδικευμένων συστημάτων διαχείρισης περιστατικών ασφάλειας. ▪ Υλοποίηση συστημάτων περιορισμού κατανεμημένων επιθέσεων άρνησης υπηρεσιών (Distributed Denial of Service attacks).	▪ Εγκατάσταση των τελευταίων ενημερώσεων και οδηγιών ασφάλειας σε τακτά χρονικά διαστήματα π.χ. σε εβδομαδιαία βάση για το σύνολο των πληροφοριακών συστημάτων και υποδομών. ▪ Υλοποίηση αυστηρών προδιαγραφών ασφάλειας και ελάχιστων μηχανισμών ασφάλειας (Security Baselines) κατά τη βάση υλοποίησης. ▪ Υλοποίηση ισχυρών μηχανισμών πιστοποίησης και αυθεντικοποίησης με βάση τις αρχές need-to-know και need-to-have για το σύνολο των πληροφοριακών συστημάτων και υποδομών και υλοποίηση μηχανισμών μοναδικής πιστοποίησης (Single Sign-On). ▪ Υιοθέτηση αρχιτεκτονικής πολλαπλών επιπέδων (in-depth) ασφάλειας. ▪ Προσδιορισμός απαιτήσεων ασφάλειας για τους εξωτερικούς συνεργάτες. ▪ Ενσωμάτωση κατάλληλης τεχνολογικής λύσης για την ασφαλή πρόσβαση σε εφαρμογές υπολογιστικού νέφους (Cloud Access Security Broker). ▪ Υλοποίηση μηχανισμών κρυπτογράφησης της δικτυακής επικοινωνίας.	▪ Ημί-αυτοματοποιημένη εγκατάσταση των τελευταίων ενημερώσεων και οδηγιών ασφάλειας σε διάστημα μιας ημέρας και μιας εβδομάδας για τις κρίσιμες και υψηλού κινδύνου ευπάθειες, αντίστοιχα. ▪ Ενσωμάτωση των μηχανισμών θωράκισης κατά τη διαδικασία ανάπτυξης συστημάτων, υιοθετώντας την αρχή Security By Design. ▪ Περιοδική παρακολούθηση των μηχανισμών ασφάλειας και αξιολόγηση του υπολειπόμενου κινδύνου. ▪ Υλοποίηση συστημάτων (Identity Access Management) για την διαχείριση των προσβάσεων και ενσωμάτωση αυτών στις διαδικασίες του Ανθρώπινου Δυναμικού. ▪ Υιοθέτηση αρχιτεκτονικής ασφάλειας μηδενικής εμπιστοσύνης. ▪ Υλοποίηση μηχανισμών για την χρήση μόνο εξουσιοδοτημένων προγραμμάτων (application whitelisting). ▪ Υλοποίηση μηχανισμών κρυπτογράφησης για τις εμπιστευτικές πληροφορίες.

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Εντοπισμός

Ο αποτελεσματικός εντοπισμός των Κυβερνοαπειλών προϋποθέτει την εξέλιξη της υποκειμενικής αξιολόγησης κινδύνων σε υιοθέτηση αντικειμενικών προτεραιοτήτων ευφυΐας μέσω της συλλογής, επεξεργασίας και παρουσίασης πληροφοριών όχι μόνο από τα συστήματα ασφάλειας του οργανισμού αλλά και από εξωτερικούς φορείς, ο μετασχηματισμός αυτών στα επιχειρηματικά και τεχνολογικά δεδομένα του οργανισμού και της υλοποίησης εφαρμόσιμων διορθωτικών ενεργειών.

Πρώιμο (Initial)	Καθορισμένο (Defined)	Καθορισμένο με περιοδική επισκόπηση (Repeatable)	Εγκαθιδρυμένο (Managed)	Βέλτιστο (Optimized)
▪ Έλεγχος των αρχείων καταγραφής μόνο κατά την ανάλυση περιστατικών ασφάλειας. ▪ Τα αρχεία καταγραφής περιλαμβάνουν μόνο τα προκαθορισμένα από τους κατασκευαστές. ▪ Υλοποίηση συστημάτων εντοπισμού δικτυακών επιθέσεων (Network Intrusion Detection systems). ▪ Συλλογή πληροφοριών Κυβερνοευφυΐας από τους προμηθευτές συστημάτων ασφάλειας.	▪ Ενεργοποίηση των αρχείων καταγραφής για τα κύρια πληροφοριακά συστήματα και τις υποδομές. ▪ Υλοποίηση συστημάτων για την κεντροκοποιημένη διαχείριση των αρχείων καταγραφής (Security Information Event Management). ▪ Υλοποίηση συστημάτων εντοπισμού επιθέσεων στα πληροφορικά συστήματα και τις υποδομές (Host Intrusion Detection systems). ▪ Ενσωμάτωση των πληροφοριών Κυβερνοευφυΐας στα συστήματα ασφάλειας. ▪ Υλοποίηση συστημάτων εντοπισμού και περιορισμού διαρροής πληροφοριών (Data Loss Prevention). ▪ Υλοποίηση συστημάτων για την παρακολούθηση κρίσιμων λειτουργιών και αναφοράς ζητημάτων που έχουν σχέση με την ασφάλεια και την ενδεδειγμένη χρήση και λειτουργία των συστημάτων. ▪ Βελτιστοποίηση παραγωγής αναφορών και ελαχιστοποίηση των λανθασμένων προειδοποιήσεων (false positives/ false negatives).	▪ Ενεργοποίηση των αρχείων καταγραφής για το σύνολο των πληροφοριακών συστημάτων και υποδομών. ▪ Υλοποίηση αναφορών για τον εντοπισμό μη ενδεδειγμένων ενεργειών όπως η ανίχνευση νέων συστημάτων τα οποία δεν συμπεριλαμβάνονται στο μητρώο της πληροφορικής, η ανίχνευση συνδέσεων στα συστήματα του οργανισμού σε μη εργάσιμες ώρες και μέρες από χώρες που δεν δραστηριοποιείται ο οργανισμός, η αυξημένη χρήση λογαριασμών διαχειριστών, κτλ. ▪ Υλοποίηση συστημάτων εντοπισμού και περιορισμού επιθέσεων στους σταθμούς εργασίας και στις φορητές συσκευές (Endpoint Detection & Response). ▪ Υλοποίηση μηχανισμών για την έγκαιρη αναγνώριση των νέων/μη δημοσιευμένων ευπαθειών (zero-day vulnerabilities). ▪ Δυνατότητα ανάλυσης του προφίλ του επιτιθέμενου, των κινήτρων, των τεχνικών και των ενεργειών του.	▪ Ενσωμάτωση των διαδικασιών διαχείρισης περιστατικών ασφάλειας στα πλάνα επιχειρησιακής συνέχειας και ανάκαμψης. ▪ 24/7 κεντρικοποιημένη παρακολούθηση των αρχείων καταγραφής για το σύνολο των εφαρμογών, πληροφοριακών συστημάτων και υποδομών. ▪ 24/7 παρακολούθηση των Κυβερνοαπειλών που ενδέχεται να στοχεύσουν τον οργανισμό όπως, καμπάνιες κοινωνικής μηχανικής, δημιουργία παραποιημένων εταιρικών ονομάτων δικτύου (Domain Names), εφαρμογών έξυπνων κινητών και ιστότοπων. ▪ Διαμοίραση πληροφοριών Κυβερνοευφυΐας με συστήματα έγκαιρης προειδοποίησης και ενημέρωσης (CERT). ▪ Υλοποίηση εξειδικευμένων κανόνων στα συστήματα Data Loss Prevention με βάση το σχήμα διαβάθμισης και σήμανσης πληροφοριών. ▪ Υλοποίηση τεχνολογικών λύσεων για την ανάλυση συμπεριφοράς (User Behavior Analytics) και της εκμάθησης σε βάθος (deep learning).	▪ Υλοποίηση προηγμένων τεχνολογιών τεχνητής νοημοσύνης, γνωστικής μάθησης, ανάλυσης δεδομένων (Data Analytics), των τεχνολογιών συσχέτισης (Correlation Technologies) και της Κυβερνοευφυΐας (Threat Intelligence) για την ανάπτυξη προηγμένων επιπέδων επιχειρησιακής επίγνωσης. ▪ Υλοποίηση εξειδικευμένων αναφορών προειδοποίησης με βάση το προφίλ κινδύνου του οργανισμού (Risk-Based Use Cases). ▪ 24/7 παρακολούθηση διαρροής εταιρικών πληροφοριών στον Διαδίκτυο συμπεριλαμβανομένου του deep και dark net. ▪ Αξιοποίηση των πληροφοριών Κυβερνοευφυΐας σε πραγματικό χρόνο και ενημέρωση των συστημάτων ασφάλειας όπως ο περιορισμός των κακόβουλων προσβάσεων μέσω κανόνων δικτυακής πρόσβασης. ▪ Υλοποίηση τεχνολογικών λύσεων για την ανάλυση τάσεων (Trend Analytics). ▪ Υλοποίηση ενοποιημένων μηχανισμών ανίχνευσης απειλών (Unified Threat Management).

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Ανταπόκριση

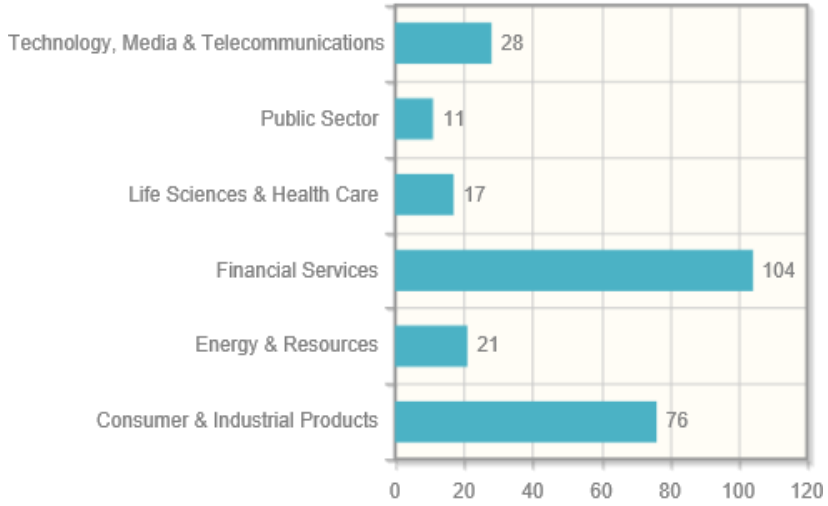
Οι μηχανισμοί ανταπόκρισης και αντιμετώπισης είναι εξίσου σημαντικοί με τους μηχανισμούς περιορισμού και πρόληψης και για την μείωση των επιπτώσεων από τα περιστατικά ασφάλειας. Οι εν λόγω μηχανισμοί δεν θα πρέπει να περιορίζονται στις Κυβερνοεπιθέσεις αλλά θα πρέπει να περιλαμβάνουν την ανταπόκριση στις οργανωτικές και τεχνολογικές αλλαγές του οργανισμού καθώς και του ευρύτερο πεδίου του Κυβερνοχώρου.

Πρώιμο (Initial)	Καθορισμένο (Defined)	Καθορισμένο με περιοδική επισκόπηση (repeatable)	Εγκαθιδρυμένο (Managed)	Βέλτιστο (Optimized)
▪ Εφαρμογή πολιτικής διαχείρισης περιστατικών ασφάλειας πληροφοριακών συστημάτων. ▪ Αναγνώριση και ιεράρχηση της ανάκαμψης των σημαντικότερων επιχειρησιακών λειτουργιών που είναι απαραίτητες για την παροχή υπηρεσιών και την συνολική λειτουργία της επιχείρησης στο ελάχιστο επίπεδο. ▪ Εφαρμογή μη τυποποιημένων πρακτικών για τη διαχείριση των περιστατικών ασφάλειας. ▪ Υλοποίηση βελτιώσεων και διορθωτικών ενεργειών ώστε να καλυφθούν οι αδυναμίες που εντοπίστηκαν και κατ' επέκταση αξιοποιήθηκαν από τους Κυβερνοεγκληματίες.	▪ Εφαρμογή πολιτικής και διαδικασιών διαχείρισης περιστατικών ασφάλειας για το σύνολο των πληροφοριακών πόρων και πληροφοριών συμπεριλαμβανομένου και των εξωτερικών συνεργατών. ▪ Στελέχωση ομάδας διαχείρισης περιστατικών ασφάλειας. ▪ Υλοποίηση ενός ιεραρχημένου σχεδίου ανάκαμψης με σαφείς ενέργειες με σκοπό την λειτουργία του οργανισμού σε αρχικό και μεσοπρόθεσμο διάστημα. ▪ Αναγνώριση του περιστατικού ασφάλειας και περιορισμός του με χρήση βέλτιστων πρακτικών (π.χ. περιορισμός της πρόσβασης των μολυσμένων εφαρμογών ή συσκευών στο Διαδίκτυο, απενεργοποίηση πρόσβασης στα συστήματα του οργανισμού, επαναφορά κωδικών πρόσβασης, κτλ.). ▪ Χρήση απομονωμένων από το εσωτερικό δίκτυο και πλήρως ελεγχόμενων καναλιών επικοινωνίας και διαχείρισης των περιστατικών.	▪ Αναθεώρηση του πλαισίου Κυβερνοασφάλειας, των διαδικασιών διαχείρισης περιστατικών ασφάλειας και των μηχανισμών ασφάλειας με βάση τα εγγενή αίτια (root causes) και των συμπερασμάτων (lessons learned) των παραβιάσεων. ▪ Εφαρμογή αναλυτικών διαδικασιών (playbooks) διαχείρισης περιστατικών ασφάλειας. ▪ Τα στελέχη της Κυβερνοασφάλειας συμμετέχουν ενεργά στον καθορισμό και στην εκτέλεση των διαδικασιών διαχείρισης κρίσεων. ▪ Η ομάδα διαχείρισης περιστατικών ασφάλειας είναι επαρκώς στελεχωμένη και εξειδικευμένη. ▪ Εφαρμογή κατάλληλων δικλείδων ασφάλειας για τη βελτίωση του συνολικού επιπέδου ασφάλειας και των περιορισμό αντίστοιχων περιστατικών ασφάλειας. ▪ Προστασία των σημαντικότερων συστημάτων μέσω απομόνωσης τους από το δίκτυο, ή από συγκεκριμένες εφαρμογές που έχουν παραβιαστεί.	▪ Ανάπτυξη ενιαίας και συγκροτημένης προσέγγισης για το σχέδιο απόκρισης κατά τη διαχείριση περιστατικών ασφάλειας για την βέλτιστη ανταπόκριση συνδυάζοντας όλες τις απαραίτητες επιχειρησιακές λειτουργίες με συγκροτημένο τρόπο, βελτιώνοντας έτσι την ανθεκτικότητα και τη συμμόρφωση του οργανισμού με τις κανονιστικές απαιτήσεις. ▪ Υλοποίηση αυτοματοποιημένων ροών και προγραμμάτων για την συλλογή πειστηρίων και την απομόνωση των προσβεβλημένων υπολογιστών. ▪ Ανάλυση σε βάθος των περιστατικών ασφάλειας, μέσω της εξέτασης των αρχείων καταγραφής των παραβιασμένων συστημάτων και των διαδικασιών που εκτελέστηκαν (post incident review) ▪ Υλοποίησης συστημάτων honeynets για την εκμάθηση των συστημάτων ασφάλειας και την βελτίωση των οδηγιών (playbooks). ▪ Θεσμοθέτηση επιπέδων και ορίων ανταπόκρισης με βάση την κρισιμότητα του περιστατικού.	▪ Περιοδική μέτρηση της αποτελεσματικότητας των διαδικασιών διαχείρισης περιστατικών ασφάλειας και ενσωμάτωση των αποτελεσμάτων στο πλαίσιο διαχείρισης κινδύνων του οργανισμού. ▪ Πιστοποίηση του πλαισίου διαχείρισης περιστατικών ασφάλειας ως CERT/ CSIRT. ▪ Υλοποίηση αυτοματοποιημένων μηχανισμών για τον περιορισμό των περιστατικών ασφάλειας μέσω του περιορισμού των προσβεβλημένων πληροφοριακών συστημάτων. ▪ Προληπτική ανάλυση ενδείξεων παραβίασης (Indications of Compromise) με σκοπό τον εντοπισμό κακόβουλων ή/και μη εξουσιοδοτημένων ενεργειών (Threat Hunting / Compromise Assessment). ▪ Ανάλυση σε βάθος των περιστατικών ασφάλειας, μέσω της εξέτασης των αρχείων καταγραφής για το σύνολο των πληροφοριακών συστημάτων του οργανισμού και προσομοίωση του περιστατικού σε εικονικό περιβάλλον μετά την υλοποίηση των διορθωτικών ενεργειών.

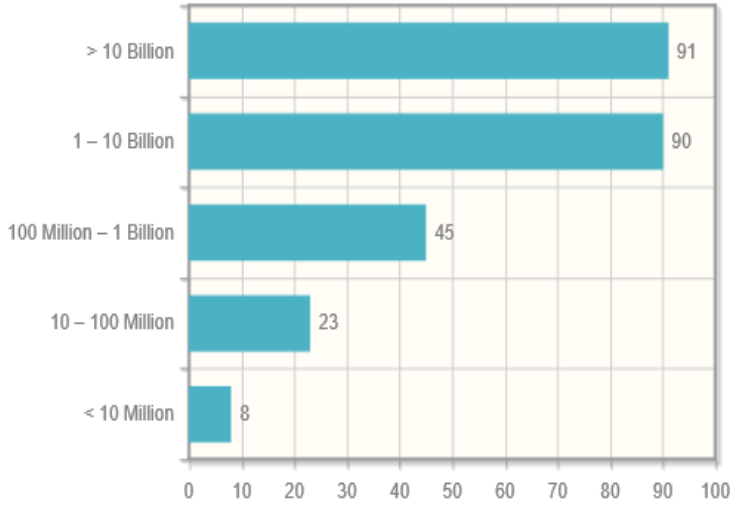
Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Συγκριτικά στοιχεία - Εισαγωγή

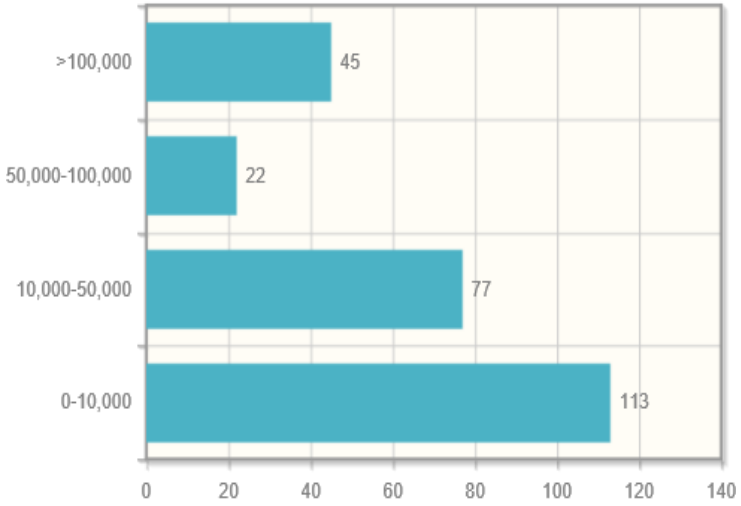
Ένας βασικός μηχανισμός που χρησιμοποιούν οι οργανισμοί αποτελεί η χρήση συγκριτικών στοιχείων (benchmark data). Τα συγκριτικά στοιχεία προσφέρουν τη δυνατότητα στους οργανισμούς να αναγνωρίσουν με αποδοτικό και αξιόπιστο τρόπο την υφιστάμενη κατάσταση καθώς και να καθορίσουν τις διαδικασίες λήψης αποφάσεων και στοχοθεσίας που θα οδηγήσουν τον οργανισμό στην επιθυμητή κατάσταση από άποψη επιπέδου ωριμότητας. Στον τομέα της Κυβερνοασφάλειας, η Deloitte μέσω των εξειδικευμένων υπηρεσιών και εργαλείων που προσφέρει, έχει αποκτήσει σημαντική γνώση σχετικά με την ωριμότητα των οργανισμών σε παγκόσμιο επίπεδο. Ειδικότερα, η μεθοδολογία/ εργαλείο Deloitte Strategy Framework (DSF) έχει σχεδιαστεί με βάση παγκοσμίως αναγνωρισμένα πρότυπα (όπως ISO 27001:2013, NIST Cybersecurity Framework, FFIEC κ.λπ.) και βέλτιστες πρακτικές (όπως CIS Security Controls κ.λπ.). Παρακάτω απεικονίζονται πληροφορίες αναφορικά με τα στοιχεία των οργανισμών (κλάδος, μέγεθος εσόδων και προσωπικού) σε παγκόσμιο επίπεδο που συμμετέχουν στη μελέτη. Στις επόμενες διαφάνειες, παρατίθενται πληροφορίες αναφορικά με το υφιστάμενο και το επιθυμητό επίπεδο ωριμότητας των οργανισμών ανά κλάδο, σε επίπεδο Κυβερνοασφάλειας.



Αριθμός οργανισμών που συμμετέχουν στη μελέτη, ανά επιχειρηματικό τομέα



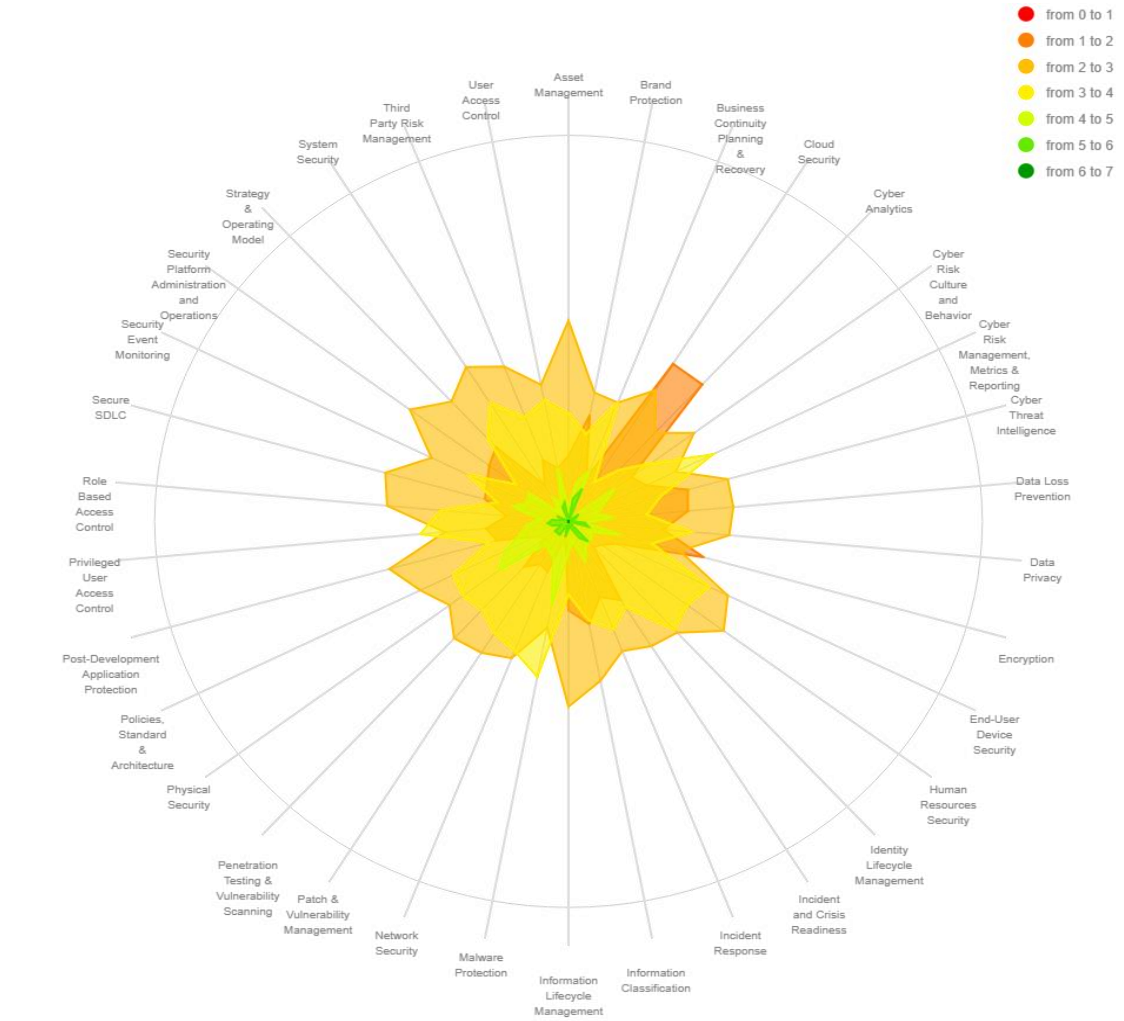
Αριθμός οργανισμών που συμμετέχουν στη μελέτη, με βάση τα ετήσια έσοδά τους



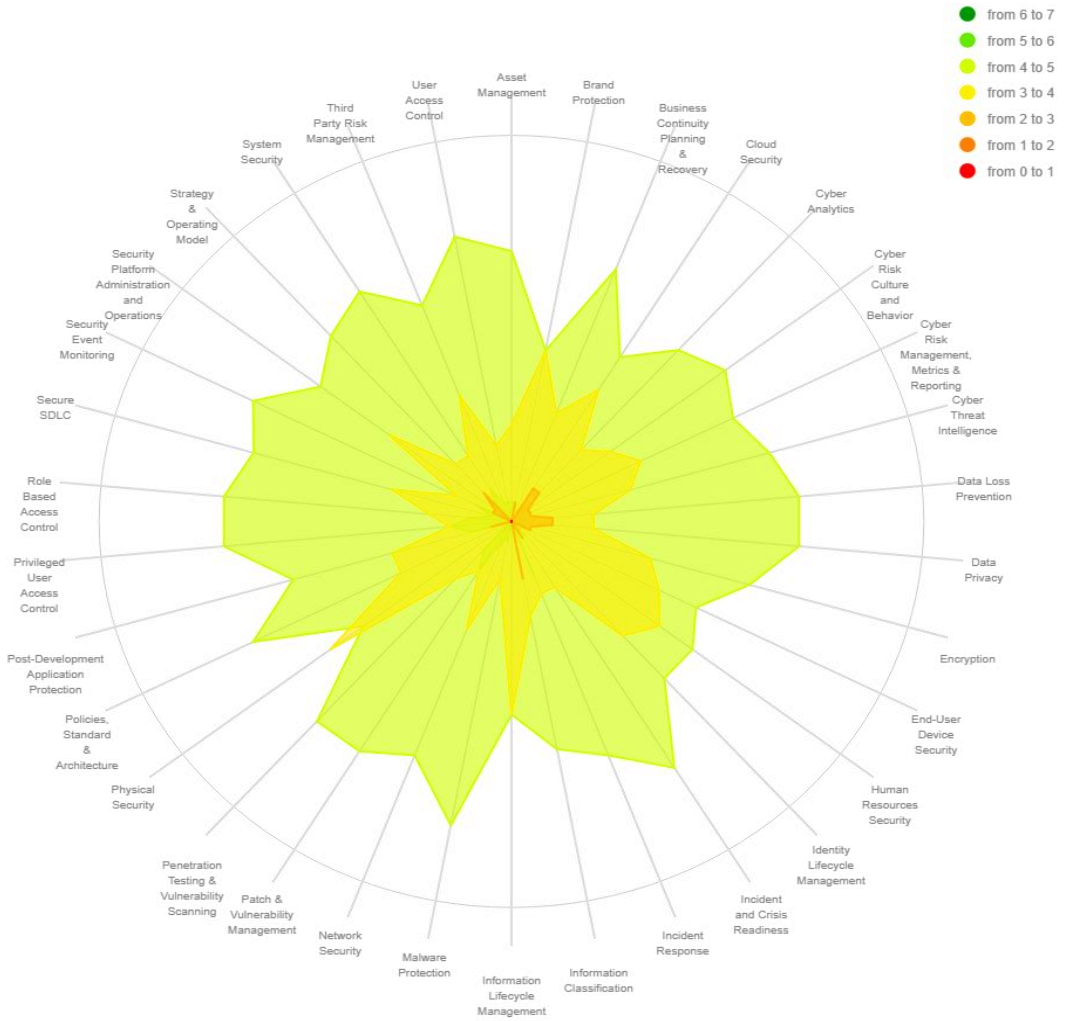
Αριθμός οργανισμών που συμμετέχουν στη μελέτη, σε σχέση με το μέγεθός του προσωπικού

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Συγκριτικά στοιχεία - Δεδομένα οργανισμών του Χρηματοπιστωτικού Κλάδου



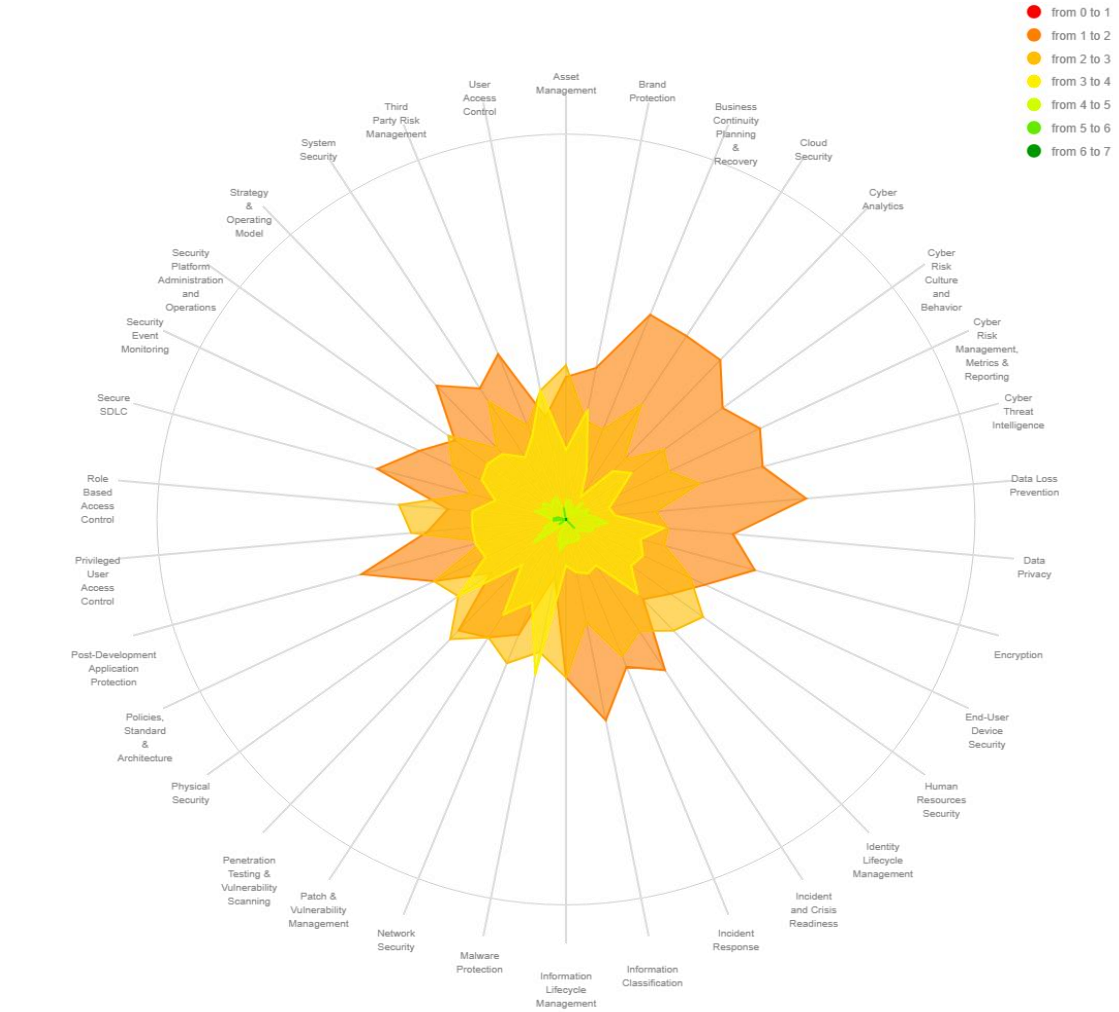
Υφιστάμενο επίπεδο ωριμότητας



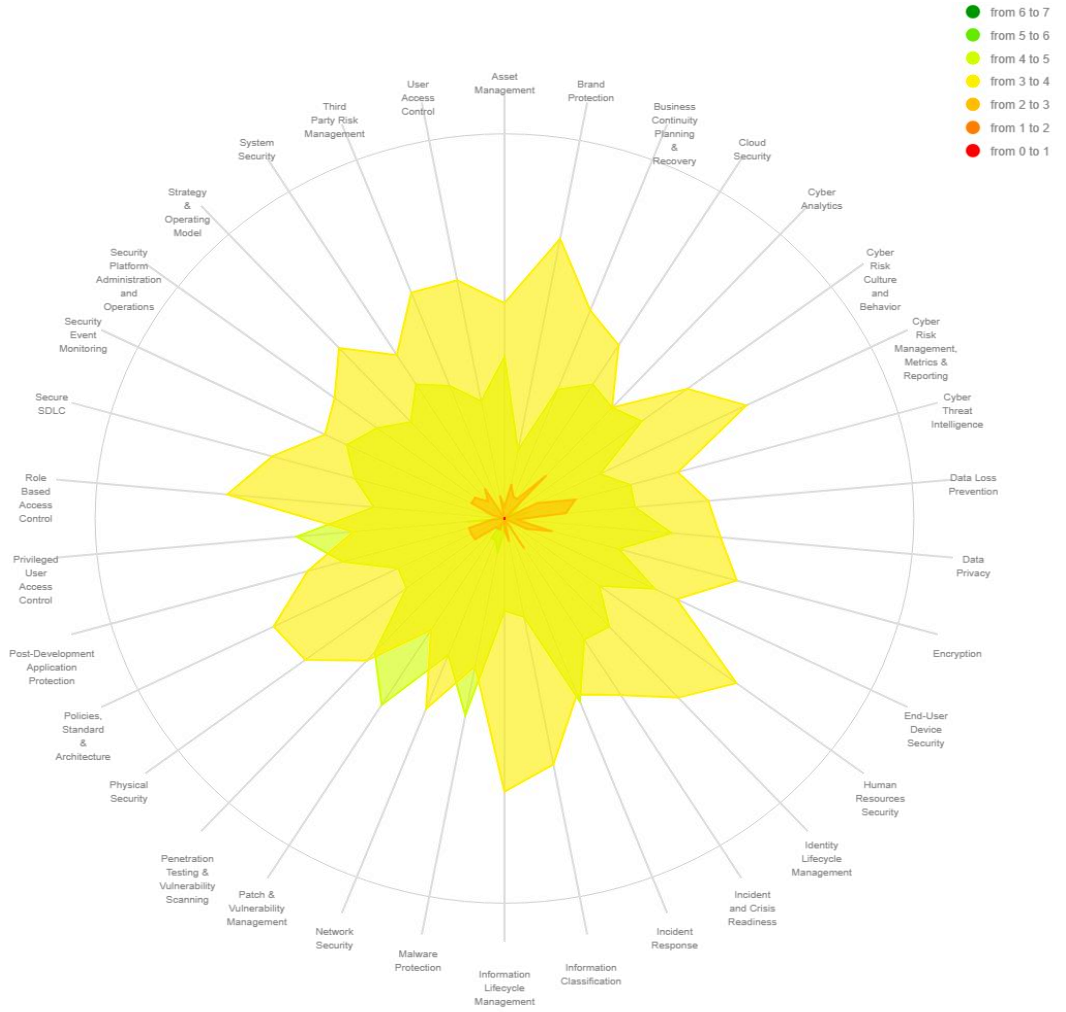
Επιθυμητό επίπεδο ωριμότητας

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Συγκριτικά στοιχεία - Δεδομένα οργανισμών του Καταναλωτικού και Βιομηχανικού Κλάδου



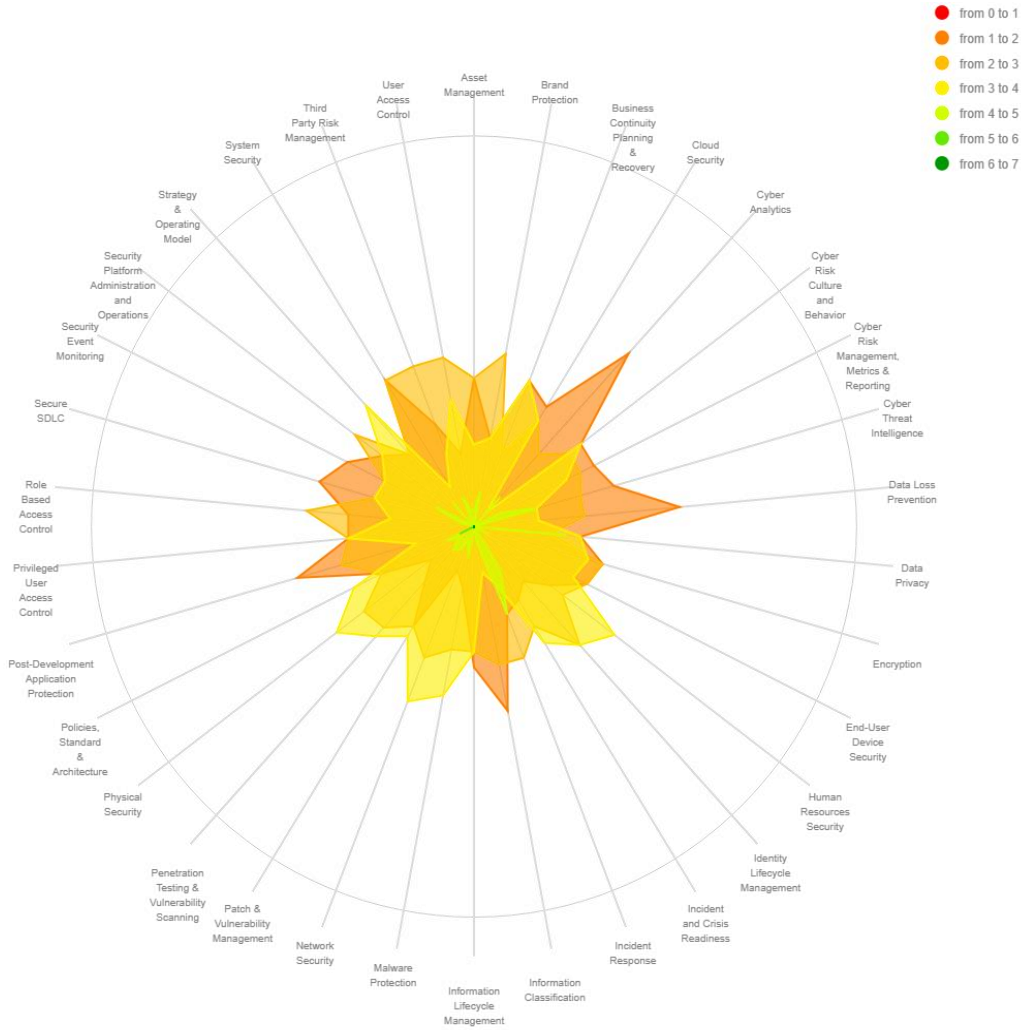
Υφιστάμενο επίπεδο ωριμότητας



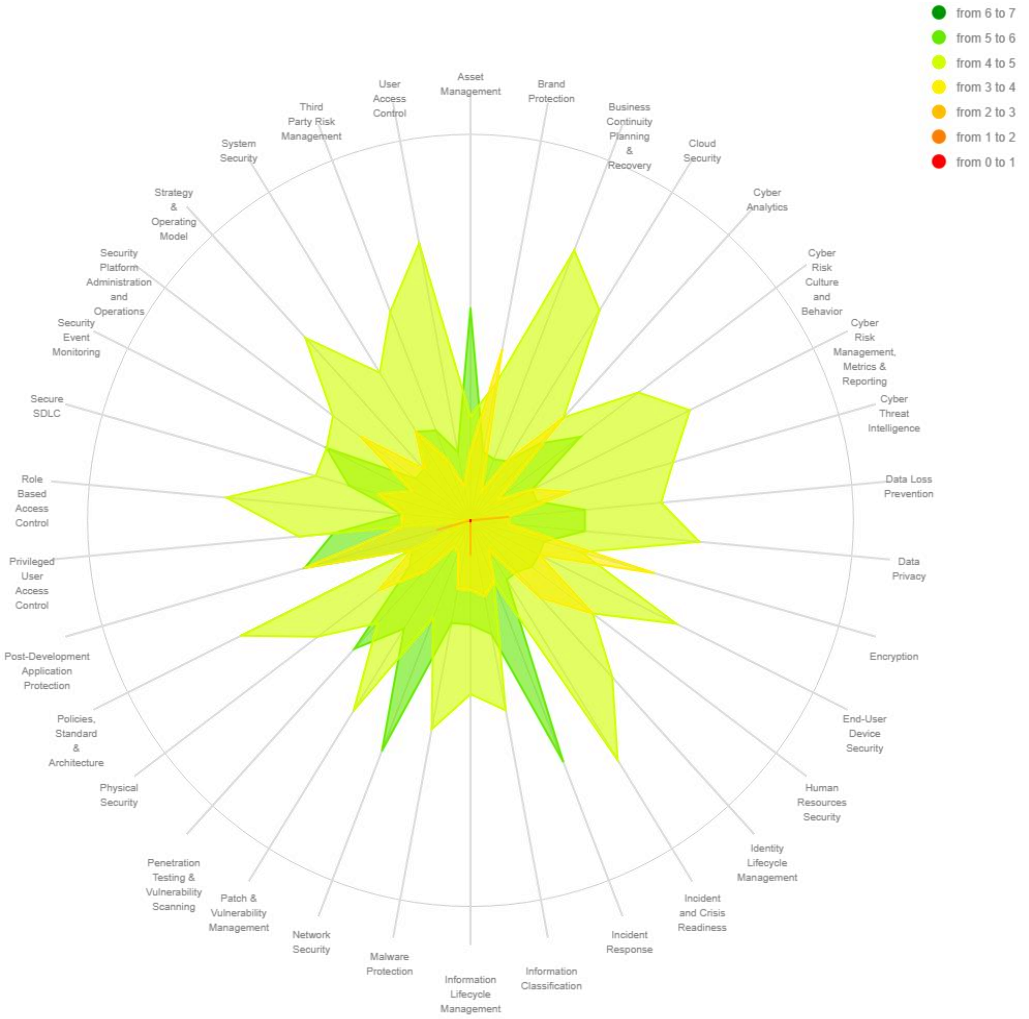
Επιθυμητό επίπεδο ωριμότητας

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Συγκριτικά στοιχεία - Δεδομένα οργανισμών Τεχνολογίας και Τηλεπικοινωνιών



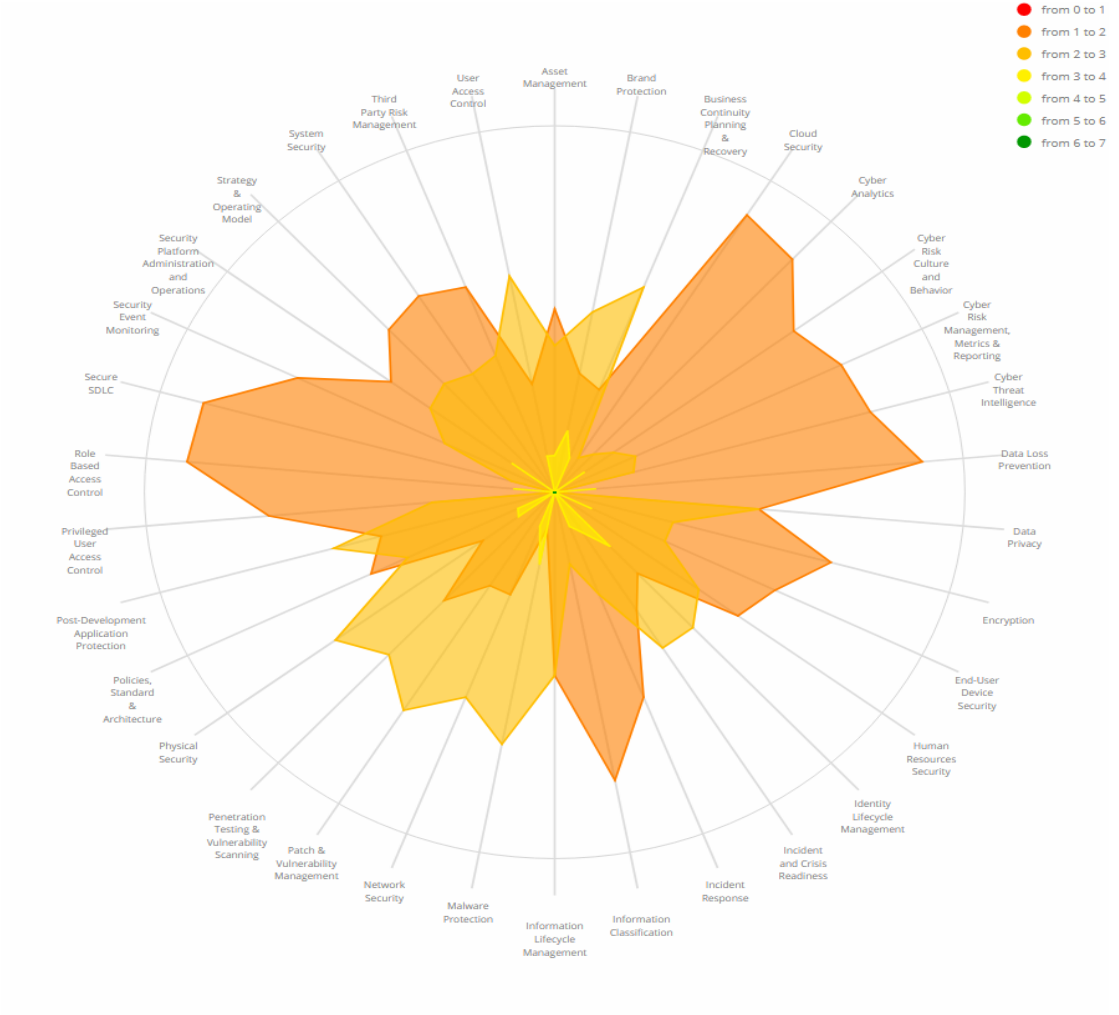
Υφιστάμενο επίπεδο ωριμότητας



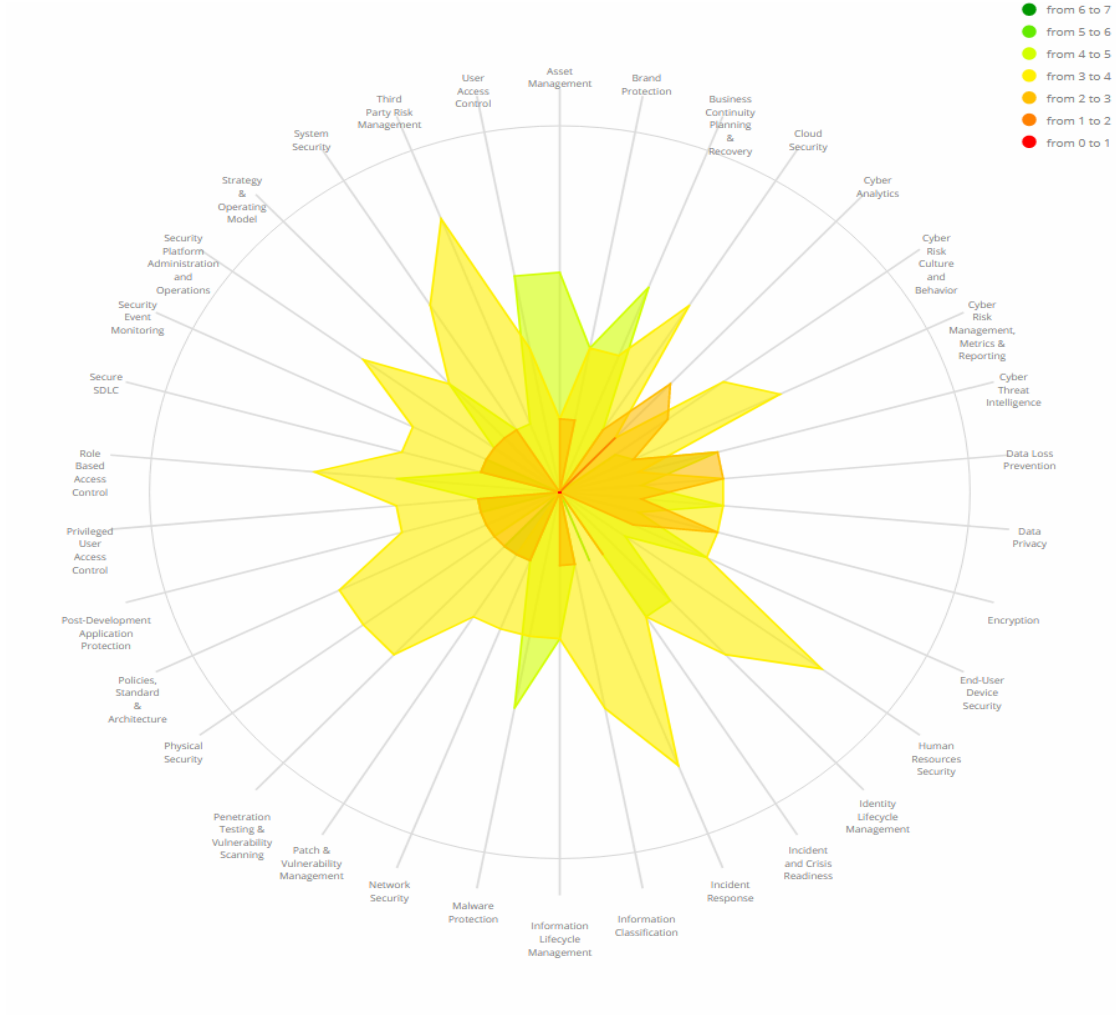
Επιθυμητό επίπεδο ωριμότητας

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Συγκριτικά στοιχεία - Δεδομένα οργανισμών του Δημόσιου Τομέα



Υφιστάμενο επίπεδο ωριμότητας



Επιθυμητό επίπεδο ωριμότητας

Οδικός χάρτης για την ωρίμανση του επιπέδου ασφάλειας

Συγκριτικά στοιχεία – Δεδομένα ωριμότητας οργανισμών σε παγκόσμιο επίπεδο

Το επίπεδο ωριμότητας των οργανισμών σχετικά με την Κυβερνοασφάλεια σχετίζεται άμεσα με τον τομέα δραστηριοποίησής τους. Παρακάτω παρατίθενται δεδομένα τα οποία παρουσιάζουν το υφιστάμενο επίπεδο ωριμότητας οργανισμών γύρω από τις κυριότερες δυνατότητες (capabilities) Κυβερνοασφάλειας ανά τομέα δραστηριοποίησης σε παγκόσμιο επίπεδο. Η βαθμολογική κλίμακα κυμαίνεται από το 0 (χαμηλότερο επίπεδο ωριμότητας) έως το 5 (υψηλότερο επίπεδο ωριμότητας).

Δυνατότητες στην Κυβερνοασφάλεια / Οργανισμοί διαφόρων κλάδων	Οργανισμοί Χρηματοοικονομικού Κλάδου	Οργανισμοί Καταναλωτικού και Βιομηχανικού Κλάδου	Οργανισμοί Τεχνολογικού και Τηλεπικοινωνιακού Κλάδου	Δημόσιος Τομέας
Διαχείριση πληροφοριακών αγαθών (Asset management)	2,5	2,5	2,5	1,5
Επιχειρησιακή συνέχεια (Business continuity)	3,5	2	3,5	2,5
Ασφάλεια στο υπολογιστικό νέφος (Cloud security)	2	1,5	3	1
Διαχείριση, παρακολούθηση και αναφορά κινδύνων κυβενοασφάλειας (Cyber risk management, metrics & reporting)	3,5	2,5	3	1,5
Αναγνώριση και ανάλυση κυβερνοαπειλών (Cyber threat intelligence)	2,5	2	2	1,5
Προστασία δεδομένων (Data privacy & protection)	3,5	2	3,5	2,5
Διαχείριση τρίτων μερών/ συνεργατών (Third party risk management)	3	2	2,5	1,5
Διαχείριση προσβάσεων (Identity lifecycle management)	4	3	3,5	2
Διαχείριση συμβάντων (Incident management)	2,5	2,5	2,5	1,5
Ασφάλεια δικτύων (Network security)	3,5	2,5	3,5	2,5
Προστασία από κακόβουλο λογισμικό (Malware protection)	4	3,5	4	2,5
Φυσική ασφάλεια (Physical security)	3	3,5	3,5	3

6 Η Κυβερνοασφάλεια σε εθνικό επίπεδο

Η Κυβερνοασφάλεια σε εθνικό επίπεδο

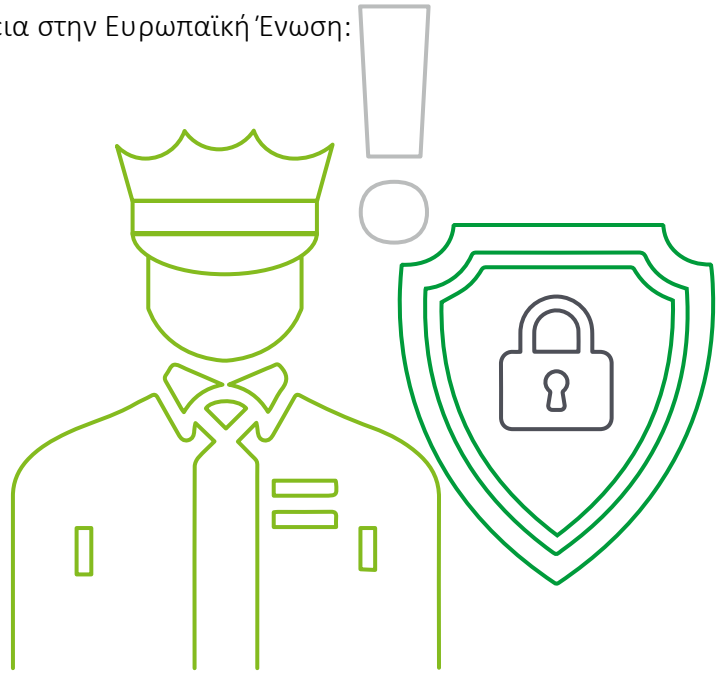
Το υφιστάμενο περιβάλλον της Κυβερνοασφάλειας

Οι βασικοί παράγοντες που επηρεάζουν την Κυβερνοασφάλεια είναι η τεχνολογική πρόοδος, οι απαιτήσεις των κανονισμών σχετικά με την Κυβερνοασφάλεια και οι συνεχείς αλλαγές στο τύπο και το είδος των απειλών. Οι ταχύτατες εξελίξεις δημιουργούν σοβαρές προκλήσεις στη διασφάλιση της δημόσιας ασφάλειας και στο συντονισμό μίας διεθνούς συνεργασίας σε επίπεδο κρατών. Επομένως, όλες αυτές οι προκλήσεις πρέπει να λαμβάνονται υπόψη κατά τα στάδια της ανάπτυξης, της εφαρμογής και της αξιολόγησης των εθνικών στρατηγικών της Κυβερνοασφάλειας.

Οι κυβερνοαπειλές αποτελούν μία από τις σημαντικότερες απειλές σε εθνικό επίπεδο, ενώ θεωρούνται εφάμιλλες με την τρομοκρατία και το οργανωμένο έγκλημα. Σε ένα μεγάλο ποσοστό, τα κράτη έχουν αναγνωρίσει την απειλή που προκύπτει από την ανάπτυξη του κυβερνοχώρου και γι' αυτό το λόγο έχουν εφαρμόσει ή αναπτύσσουν μία εθνική στρατηγική σχετικά με την Κυβερνοασφάλεια. Η Ελλάδα διαθέτει από το 2018 Εθνική Στρατηγική Κυβερνοασφάλειας, ενώ πρόσφατα υπέγραψε μνημόνιο συνεργασίας με το Ισραήλ για την ανταλλαγή καλών πρακτικών και τεχνογνωσίας.

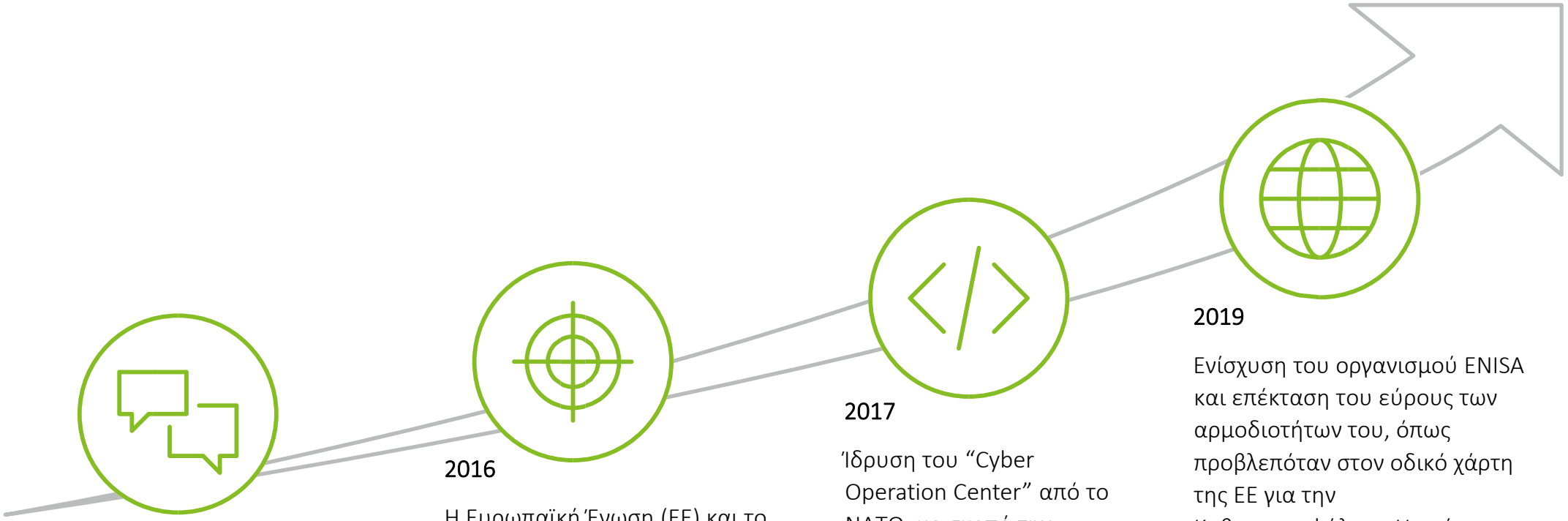
Παρακάτω αναφέρονται τα κυριότερα σημεία της κατάστασης που επικρατεί στις μέρες μας αναφορικά με την Κυβερνοασφάλεια στην Ευρωπαϊκή Ένωση:

- Τα περισσότερα κράτη της Ευρωπαϊκής Ένωσης (ΕΕ) έχουν σχεδιάσει και αναπτύξει μια εθνική στρατηγική Κυβερνοασφάλειας. Πολλές από αυτές τις στρατηγικές έχουν σχεδιαστεί πριν από τέσσερα χρόνια ή και περισσότερα, χωρίς να έχουν ενημερωθεί προσφάτως. Παράλληλα, έχει διαπιστωθεί ότι πολλά από τα συμβάντα Κυβερνοασφάλειας που έλαβαν χώρα σε παγκόσμιο επίπεδο δεν οδήγησαν σε αναδιαμόρφωση των στρατηγικών.
- Ορισμένα ευρωπαϊκά κράτη έχουν θέσει ένα συγκεκριμένο χρονικό όριο επανεξέτασης των στρατηγικών τους, με σκοπό την ενημέρωση και την επικαιροποίηση τους ώστε να ανταποκρίνονται στις νέες εξελίξεις στον κυβερνοχώρο. Παρότι, βέβαια, υπάρχει ο σχετικός σχεδιασμός ελάχιστα κράτη τον εφαρμόζουν στη πράξη.
- Ο διαχωρισμός των καθηκόντων, που συμπεριλαμβάνεται στις περισσότερες εθνικές στρατηγικές, δεν είναι ξεκάθαρος, ενώ ελάχιστες στρατηγικές αναφέρουν και εφαρμόζουν μία ολιστική προσέγγιση συνεργασίας (networked approach). Η συγκεκριμένη προσέγγιση περιλαμβάνει τη συνεργασία κρατικών φορέων και ιδιωτικών οργανισμών με σκοπό την αποτελεσματική διαχείριση και αντιμετώπιση σοβαρών περιστατικών Κυβερνοασφάλειας, όπως είναι οι υβριδικές απειλές.
- Παρόλο που η Ευρωπαϊκή Ένωση και το ΝΑΤΟ έχουν κάνει σημαντικά βήματα στη θέσπιση μίας γενικά αποδεκτής ορολογίας στον τομέα της Κυβερνοασφάλειας, πολλές ευρωπαϊκές χώρες χρησιμοποιούν διαφορετικές ορολογίες και ορισμούς στις στρατηγικές τους. Σε πολλές περιπτώσεις επικρατεί σύγχυση σχετικά με τους ορισμούς και τους θεσμοθετημένους κανόνες στο χώρο της Κυβερνοασφάλειας, καθώς τα διάφορα κράτη ερμηνεύουν με διαφορετικό τρόπο την υφιστάμενη ορολογία.



Η Κυβερνοασφάλεια σε εθνικό επίπεδο

Διεθνείς πρωτοβουλίες ανάπτυξης σχεδίου Κυβερνοασφάλειας



2013

Πρωτοβουλία του Οργανισμού Ηνωμένων Εθνών (ΟΗΕ) για οριοθέτηση και ανάπτυξη ενός διεθνούς δικαίου σχετικά με την Κυβερνοασφάλεια.

2016

Η Ευρωπαϊκή Ένωση (ΕΕ) και το ΝΑΤΟ σε κοινή τους διακήρυξη δήλωσαν τη πρόθεσή τους για συνεργασία στο χώρο της Κυβερνοασφάλειας, υποδηλώνοντας έτσι τη σπουδαιότητα της Κυβερνοασφάλειας σε παγκόσμιο επίπεδο.

2017

Ίδρυση του “Cyber Operation Center” από το ΝΑΤΟ, με σκοπό την άμεση δυνατότητα διαχείρισης κυβερνοαπειλών.

2019

Ενίσχυση του οργανισμού ENISA και επέκταση του εύρους των αρμοδιοτήτων του, όπως προβλεπόταν στον οδικό χάρτη της ΕΕ για την Κυβερνοασφάλεια. Η επέκταση έγινε μέσα από τον Κανονισμό για την Κυβερνοασφάλεια (Cybersecurity Act) της ΕΕ (Regulation (EU) 2019/881).

Η Κυβερνοασφάλεια σε εθνικό επίπεδο

Έννοιες και οι απαιτήσεις που εισάγονται με κανονιστικές αποφάσεις σε ευρωπαϊκό και εθνικό επίπεδο

Τα τελευταία χρόνια έχουν εισαχθεί στο ευρωπαϊκό αλλά και στο εθνικό δίκαιο μία σειρά από νομοθετήματα που ορίζουν τις έννοιες αλλά και τις απαιτήσεις σχετικά με την Κυβερνοασφάλεια για τα κράτη μέλη αλλά και για τις επιχειρήσεις που δραστηριοποιούνται εντός της Ε.Ε.

ΕΕ 2008 / 114 – Οδηγία για την προστασία των κρίσιμων υποδομών

- Καθορισμός κρίσιμων υποδομών από τα Κράτη Μέλη της Ε.Ε. και αναγνώριση αλληλεξαρτήσεων με τις κρίσιμες υποδομές άλλων κρατών.
- Δημιουργία σχεδίων ασφάλειας οργανισμών (OSPs) τα οποία θα χρησιμοποιηθούν για τον καθορισμό των κρίσιμων υποδομών.
- Καθορισμός υπευθύνων ασφάλειας (SLOs) για κάθε κρίσιμη υποδομή.

ΠΔ 82 / 2017 - Σύσταση Εθνικής Αρχής Κυβερνοασφάλειας

Η Εθνική Αρχή Κυβερνοασφάλειας εγκαθιδρύεται και συγκροτείται από τα ακόλουθα Τμήματα:

- Το Τμήμα Ασφάλειας Πληροφοριών και Δικτύων.
- Το Τμήμα Ελέγχου Ασφάλειας.
- Το Τμήμα Συντονισμού και Ονομάτων Χώρου Δημοσίου.

Απ. 3218 / 2018 - Εθνική στρατηγική Κυβερνοασφάλειας

- Με τη θέσπιση της Εθνικής Στρατηγικής Κυβερνοασφάλειας ορίζονται οι βασικές αρχές για τη δημιουργία ενός ασφαλούς διαδικτυακού περιβάλλοντος στην Ελλάδα, τίθενται οι στρατηγικοί στόχοι και το πλαίσιο δράσεων μέσω του οποίου αυτοί θα εκπληρωθούν.
- Την εφαρμογή της Εθνικής Στρατηγικής Κυβερνοασφάλειας αναλαμβάνει η Εθνική Αρχή Κυβερνοασφάλειας, τόσο στο δημόσιο όσο και στον ιδιωτικό τομέα.
- Η Εθνική Αρχή Κυβερνοασφάλειας θα αποτιμά, θα αναθεωρεί και θα επικαιροποιεί την Εθνική Στρατηγική Κυβερνοασφάλειας εφόσον είναι αναγκαίο και το αργότερο κάθε τριετία.

Απ. 1027 / 2019 - Θέματα εφαρμογής του Ν. 4577

- Καθορισμός των βασικών απαιτήσεων ασφαλείας συστημάτων δικτύου και πληροφοριών.
- Καθορισμός της διαδικασίας παροχής πληροφοριών και κοινοποίησης συμβάντων ασφάλειας στις αρμόδιες Αρχές.

ΕΕ 2016 / 1148 – Ευρωπαϊκή οδηγία για την ασφάλεια πληροφοριακών συστημάτων και δικτύων (NIS-D) και ενσωμάτωση αυτής στο εθνικό δίκαιο (Ν. 4577 / 2018)

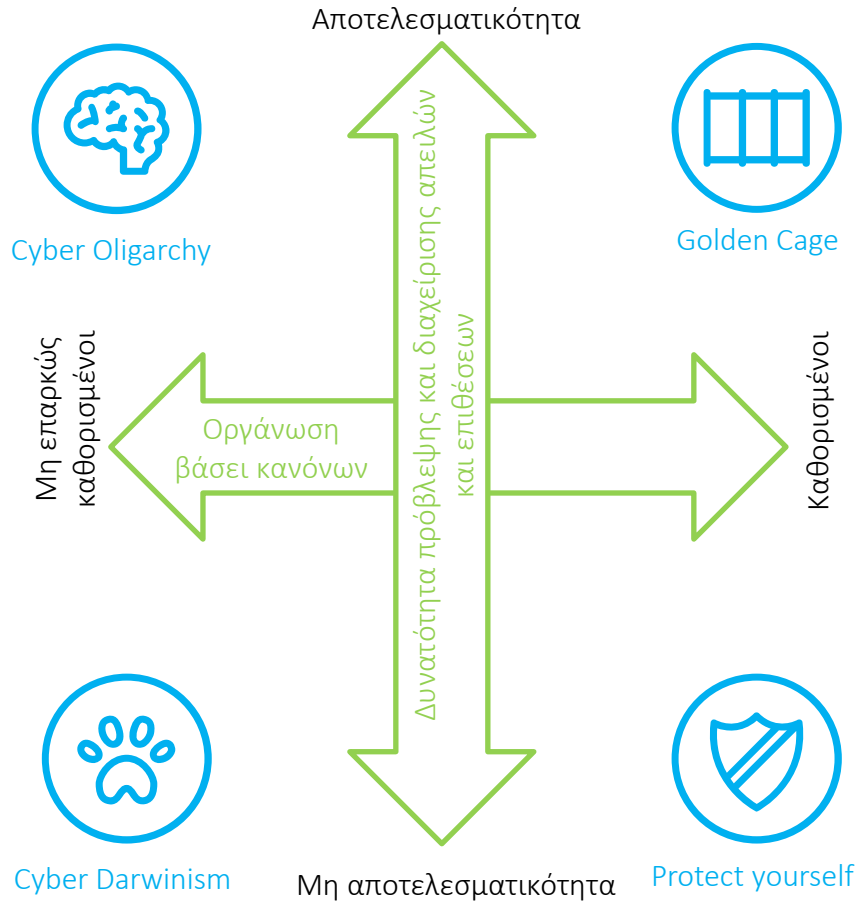
- Εγκαθίδρυση εθνικών ομάδων αντιμετώπισης συμβάντων ασφαλείας πληροφοριών (CSIRT) καθώς και εθνικής αρχής Κυβερνοασφάλειας από όλα τα Κράτη Μέλη.
- Προτροπή συνεργασίας ανάμεσα στα Κράτη Μέλη μέσα από τη δημιουργία μίας ομάδας συνεργασίας (cooperation group) και ενός δικτύου εθνικών CSIRT που θα βοηθήσει στην καλύτερη ανταλλαγή πληροφοριών ανάμεσα στα Κράτη Μέλη.
- Δημιουργία κουλτούρας Κυβερνοασφάλειας σε όλους τους τομείς που είναι κρίσιμοι για την οικονομία και την κοινωνία. Οι οργανισμοί που δραστηριοποιούνται σε αυτούς τους τομείς θα πρέπει να εφαρμόζουν συγκεκριμένες δικλείδες ασφάλειας και να ενημερώνουν τις εθνικές αρχές σε περίπτωση συμβάντος ασφάλειας.
- Κρίσιμοι πάροχοι ψηφιακών υπηρεσιών (μηχανές αναζήτησης, υπολογιστικά συστήματα στο νέφος (cloud), ηλεκτρονικά καταστήματα) θα πρέπει να συμμορφώνονται με τις απαιτήσεις και τις οδηγίες και του αντίστοιχου εθνικού νόμου.

Η Κυβερνοασφάλεια σε εθνικό επίπεδο

Το περιβάλλον της Κυβερνοασφάλειας το 2030

Η ανάλυση μελλοντικών σεναρίων αναφορικά με το επίπεδο Κυβερνοασφάλειας των κρατών της ΕΕ, μπορεί να αποτελέσει ένα χρήσιμο εργαλείο κατά το σχεδιασμό και την υλοποίηση στρατηγικών Κυβερνοασφάλειας. Παρότι το μέλλον δεν μπορεί να προβλεφθεί με ακρίβεια, σενάρια όπως αυτά που αναφέρονται παρακάτω δίνουν την ευκαιρία για κατάλληλη προετοιμασία, προβάλλοντας ταυτόχρονα δυνατότητες και κινδύνους, που μπορεί να προκύψουν στο μέλλον:

- **Golden cage**: Σε αυτό το σενάριο το επίπεδο Κυβερνοασφάλειας στα κράτη είναι αρκετά υψηλό σε σχέση με τις ήδη γνωστές απειλές. Παρά το υψηλό κόστος, οι επιχειρήσεις διατηρούν ένα ώριμο επίπεδο Κυβερνοασφάλειας. Ωστόσο, υπάρχει ελάχιστη καινοτομία και υψηλή ευπάθεια σε απρόβλεπτες απειλές.
- **Protect yourself:** Σε αυτό το σενάριο τα κράτη της ΕΕ λειτουργούν αυτόνομα, χωρίς συγκροτημένη στρατηγική ως προς την Κυβερνοασφάλεια και την τεχνολογία. Η ιδιωτική πρωτοβουλία έχει αναλάβει σημαντικό κομμάτι της Κυβερνοασφάλειας και συμπράττει με τους δημόσιους φορείς της εκάστοτε χώρας για την αντιμετώπιση σημαντικών απειλών. Προκειμένου να θεσμοθετηθεί ένα κοινό πλαίσιο Κυβερνοασφάλειας, οι διπλωματικές διαπραγματεύσεις μεταξύ των κρατών αυξάνονται σημαντικά, ωστόσο, επικρατεί δυσπιστία και τα κράτη αδυνατούν να επιβάλουν τους θεσμοθετημένους κανόνες.
- **Cyber Darwinism:** Σε αυτό το σενάριο η ΕΕ έχει αποδυναμωθεί στο χώρο της Κυβερνοασφάλειας και οι ιδιωτικοί οργανισμοί έχουν κυριαρχήσει. Αυτό δημιουργεί κράτη/ περιοχές με υψηλή ασφάλεια στον Κυβερνοχώρο, ενώ το σύνολο της ΕΕ παραμένει εκτεθειμένο σε πιθανούς κινδύνους. Ο εθνικός σχεδιασμός υπερτερεί της συνεργατικής προσέγγισης και οι ιδιωτικοί οργανισμοί έχουν μεταφερθεί σε κράτη/ περιοχές με αυστηρά καθορισμένους κανονισμούς Κυβερνοασφάλειας.
- **Cyber Oligarchy:** Σε αυτό το σενάριο η ελεύθερη αγορά επωφελείται από τη μειωμένη κρατική εποπτεία και ορισμένοι ισχυροί οργανισμοί ελέγχουν τον τομέα της Κυβερνοασφάλειας. Παρότι, ο ιδιωτικός τομέας αναπτύσσεται μέσα από την καινοτομία, η αυτοματοποίηση της αγοράς οδηγεί σε υψηλή ανεργία και κοινωνική ανισότητα. Παράλληλα, οι Κυβερνοεπιθέσεις αυξάνονται, και δεδομένης της έλλειψης κρατικής πρωτοβουλίας, οι ιδιωτικοί οργανισμοί αναλαμβάνουν ενεργό ρόλο στο σχεδιασμό και τη διαχείριση του περιβάλλοντος της Κυβερνοασφάλειας.



Τα κράτη θα πρέπει να σχεδιάσουν ευέλικτες στρατηγικές για να αντιμετωπίσουν και να διαχειριστούν μελλοντικές κυβερνοαπειλές. Θεωρούμε ότι η πιο πιθανή εκδοχή για το μέλλον της Κυβερνοασφάλειας βρίσκεται ανάμεσα στα τέσσερα ακραία σενάρια που αναφέρθηκαν πιο πάνω. Κοινός παρονομαστής και στα τέσσερα αυτά σενάρια είναι η συνεργασία τόσο σε εθνικό όσο και σε παγκόσμιο επίπεδο. Δημόσιοι φορείς, ιδιωτικοί και παγκόσμιοι οργανισμοί θα πρέπει να συνεργαστούν με σκοπό τον σχεδιασμό ενός δυναμικού στρατηγικού χάρτη για την Κυβερνοασφάλεια.

Η Κυβερνοασφάλεια στην ελληνική Δημόσια Διοίκηση

Κρίσιμοι παράγοντες επιτυχίας της εθνικής στρατηγικής Κυβερνοασφάλειας

1. **Ενημέρωση και επικαιροποίηση στρατηγικών**
   Η χώρα πρέπει εγκαίρως να προετοιμαστεί για την εφαρμογή της στρατηγικής, με σκοπό να μπορεί να ανταπεξέλθει στις νέες συνθήκες και να ανταποκριθεί στις αυξανόμενες ανάγκες που δημιουργεί και ένα ευρωπαϊκό στρατηγικό πλαίσιο διαχείρισης.

2. **Διαμόρφωση και ενημέρωση των στρατηγικών σύμφωνα με τις πιο πρόσφατες μελέτες**
   Η αντίληψη των απειλών και η ικανότητα της στρατηγικής να ανταποκρίνεται στις συνθήκες, θα πρέπει να επανεξετάζεται σε τακτά χρονικά διαστήματα και με αυτόν τον τρόπο δυναμικά θα γίνεται η επικαιροποίηση των στρατηγικών ασφαλείας.

3. **Υιοθέτηση κοινών ελάχιστων προτύπων ασφάλειας στους φορείς της Δημόσιας Διοίκησης**
   Υιοθέτηση κοινών προτύπων ασφάλειας χρηστών / εφαρμογών / διαχείρισης δεδομένων και η σταδιακή μετάβαση προς το κυβερνητικό νέφος ευνοεί τον ενιαίο σχεδιασμό.

4. **Σαφής ορισμός καθηκόντων στους φορείς του Δημοσίου**
   Θα πρέπει να υπάρχει σαφής ορισμός διαχείρισης και ευθύνης για θέματα Κυβερνοασφάλειας στους φορείς του Δημοσίου και να λειτουργούν βάσει των κεντρικών οδηγιών της Γενικής Διεύθυνσης Κυβερνοασφάλειας του Υπ. Ψηφιακής Διακυβέρνησης.

5. **Υλοποίηση «επιθετικής» άμυνας με στόχο την ενίσχυση της Κυβερνοασφάλειας**
   Η εφαρμογή μέτρων «επιθετικής» άμυνας για την πρόληψη και την αντιμετώπιση κινδύνων θα πρέπει να βρίσκεται στο σχεδιασμό των επιμέρους πολιτικών Κυβερνοασφάλειας των δημοσίων φορέων.

6. **Δημιουργία μίας εθνικής πλατφόρμας ανταλλαγής πληροφοριών και κοινών ασκήσεων προσομοίωσης**
   Η ύπαρξη μίας εθνικής πλατφόρμας ανταλλαγής πληροφοριών και κοινών ασκήσεων προσομοίωσης Κυβερνοεπιθέσεων θα αποτελέσει ευκαιρία για την ανάπτυξη διαλόγου μεταξύ των φορέων, με στόχο τη λήψη κοινών αποφάσεων για την καλύτερη προστασία τους.

Επίλογος

Επίλογος

Η Κυβερνοασφάλεια θεωρείται πλέον ως ένα σημαντικό συστατικό της βιωσιμότητας των οργανισμών. Η αποτελεσματική διαχείριση των υφιστάμενων κινδύνων του Κυβερνοχώρου δημιουργεί προκλήσεις στου οργανισμούς αναφορικά με το υφιστάμενο επίπεδο ασφάλειας, τον απαιτούμενο προϋπολογισμό και το προφίλ κινδύνου του οργανισμού. Η διαχείριση των μελλοντικών κινδύνων δημιουργεί νέες, πιο σύνθετες και πολύπλοκες προκλήσεις. Οι σημαντικότερες προκλήσεις για τους Ελληνικούς οργανισμούς είναι η μειωμένη διορατικότητα, η έλλειψη ολιστικής στρατηγικής και υλοποίηση μεμονωμένων δράσεων, οι περιορισμένοι προϋπολογισμοί, η έλλειψη επαρκούς στελέχωσης και τεχνικής κατάρτισης των στελεχών Κυβερνοασφάλειας, το μειωμένο επίπεδο ευαισθητοποίησης και η έλλειψη κουλτούρας, καθώς και η συμμόρφωση με τις αυξημένες κανονιστικές απαιτήσεις.

Επιπρόσθετα, η πανδημία συντέλεσε στην επιτάχυνση των εξελίξεων, σε ότι αφορά την ψηφιακή μετάβαση των οργανισμών, σε ένα νέο καθεστώς που γεφυρώνει ένα «ψηφιακό χάσμα» δεκαετιών, μέσα σε πολύ μικρό χρονικό διάστημα. Οι δράσεις ψηφιακού μετασχηματισμού, η ραγδαία τεχνολογική εξέλιξη και οι τεχνολογίες όπως Internet of Things, Artificial Intelligence, Big Data, Cloud εισάγουν πολυπλοκότητα, υπερσυνδεσιμότητα και αυξάνουν τους κινδύνους Κυβερνοασφάλειας, όμως μπορούν να αξιοποιηθούν για την αντιμετώπιση των προκλήσεων της πανδημίας και για την αύξηση των επενδύσεων που σχετίζονται με τη θωράκιση της ασφάλειας των οργανισμών.

Αποτελεί παρελθόν η πεποίθηση των οργανισμών ότι η πιθανότητα στοχοποίησής τους από τους Κυβερνοεγκληματίες είναι περιορισμένη, λόγου του επιπέδου προσέλκυσης ή του χρόνου που θα πρέπει να απαιτηθεί. Η συχνότητα και η πολυπλοκότητα των Κυβερνοεπιθέσεων αυξάνεται, οι επιτιθέμενοι εφαρμόζουν έξυπνες τεχνικές για την διαμοίραση πληροφοριών Κυβερνοευφυΐας, τη μείωση των απαιτήσεων που σχετίζονται με τους τεχνολογικούς πόρους, την ανθρωπροσπάθεια και την τεχνογνωσία για την παραβίαση των οργανισμών.

Η Κυβερνοασφάλεια είναι αμιγώς στρατηγικό θέμα, οι οργανισμοί μπορούν να αποκτήσουν ανταγωνιστικό πλεονέκτημα εάν διασφαλίσουν την εμπιστοσύνη των μετόχων και πελατών τους για την ασφάλεια, την ανθεκτικότητα, τη διαφάνεια και την αξιοπιστία των πληροφοριών τους. Οι διοικήσεις των οργανισμών καλούνται να προσδιορίσουν τις τρέχουσες και μελλοντικές ανάγκες για την Κυβερνοασφάλεια υλοποιώντας μια ολιστική και αποτελεσματική στρατηγική η οποία θα αποτελεί αναπόσπαστο συστατικό για την επίτευξη της επιχειρηματικής βιωσιμότητας, ανθεκτικότητας, την προστασία των πληροφοριακών αγαθών και την προστασία της αξιοπιστίας του ψηφιακού λειτουργικού περιβάλλοντος.

- Η αποτελεσματική Κυβερνοασφάλεια προϋποθέτει την επαγρύπνηση των διοικήσεων των οργανισμών, επαρκούς προϋπολογισμούς, υλοποίηση προτεραιοποιημένων δράσεων σε επίπεδο τεχνολογίας, διαδικασιών, διακυβέρνησης και ανθρώπινου δυναμικού.
- Κρίνεται αναγκαία η θέσπιση ηγετικού ρόλου με τις κατάλληλες εξουσιοδοτήσεις για την εφαρμογή της στρατηγικής και του πλαισίου Κυβερνοασφάλειας.
- Απαιτείται ευκινησία, ευελιξία, συνεργασία και ένταξη της Κυβερνοασφάλειας στις επιχειρησιακές διεργασίες για τη διασφάλιση της επιχειρηματικής βιωσιμότητας και ανθεκτικότητας των οργανισμών.
- Η αυτοματοποίηση, η ταχύτητα και η διορατικότητα θα καθορίσει το μέλλον της αποτελεσματικής Κυβερνοασφάλειας.

Deloitte.

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ
Κυβερνοασφάλεια