Κυβερνο-ασφάλεια: Οι προτάσεις του ΣΕΒ για ασφαλείς επιχειρήσεις στην εποχή της 4ης Βιομηχανικής Επανάστασης

Η ταχεία υιοθέτηση ψηφιακών τεχνολογιών είναι σημαντικός παράγοντας προσαρμογής κάθε επιχείρησης στην 4η Βιομηχανική Επανάσταση. Όμως μαζί με την τεχνολογική προσαρμογή έρχεται και η ανάγκη διαχείρισης των αυξανόμενων κινδύνων του κυβερνοχώρου. Ένα σοβαρό περιστατικό μπορεί να **διαταράξει την εύρυθμη λειτουργία, ακόμα και να θέσει σε κίνδυνο την επιβίωση της επιχείρησης**. Είναι σημαντικό οι επιχειρήσεις να διαθέτουν αποτελεσματικές στρατηγικές κυβερνοασφάλειας με όλα τα οργανωτικά και τεχνολογικά μέτρα.

Οι κυβερνο-εγκληματίες εκμεταλλεύονται τα κενά ασφαλείας που παρουσιάζονται τόσο λόγω ελλιπούς κατανόησης των νέων τεχνολογιών από την επιχείρηση όσο και ελλιπούς πληροφόρησης στους εργαζόμενους-χρήστες από την επιχείρηση για τις νέες μορφές ψηφιακής παραπλάνησης. Οι κυβερνο-επιθέσεις μπορούν να πλήξουν την αξιοπιστία της επιχείρησης, να προκαλέσουν οικονομική ζημιά, να διακόψουν την παραγωγική λειτουργία, να υποκλέψουν πνευματική ιδιοκτησία, να διαρρεύσουν εμπιστευτικές πληροφορίες, να διακόψουν την πρόσβαση σε βάσεις δεδομένων, ή ακόμα και να εκβιάσουν για την «απελευθέρωση» των δεδομένων. Επίσης, μπορεί να επιφέρουν νομικούς κινδύνους λόγω ελλιπούς προστασίας προσωπικών δεδομένων (κανόνες GDPR).

Κάθε ηλεκτρονική συσκευή, εργαζόμενος, ή εξωτερικός συνεργάτης μπορεί να βρεθεί εκτεθειμένος σε «κυβερνο-κινδύνους». Όμως, λύση δεν είναι η καθυστέρηση της τεχνολογικής αναβάθμισης λόγω φόβου, αλλά μια **ξεκάθαρη πολιτική ασφάλειας με συνεχή προσαρμογή του επιπέδου κυβερνοασφάλειας στα τεχνολογικά δεδομένα**.

Αύξηση των κινδύνων κατά την πανδημία του κορωνοϊού

Εν μέσω πανδημίας, οι κίνδυνοι του κυβερνοχώρου έχουν αυξηθεί κατακόρυφα. Ενώ η πανδημία επιτάχυνε την ψηφιοποίηση δημόσιων οργανισμών και επιχειρήσεων, **δεν παρατηρείται ανάλογη αναβάθμιση και αναθεώρηση των συστημάτων και πολιτικών ασφαλείας**. Η αποτελεσματική κυβερνοασφάλεια όμως, προϋποθέτει την επαγρύπνηση των διοικήσεων, επαρκείς προϋπολογισμούς, υλοποίηση προτεραιοποιημένων δράσεων σε επίπεδο τεχνολογίας ασφαλείας, διαδικασιών, διακυβέρνησης και ανθρώπινου δυναμικού. Πρέπει να γίνει άμεσα αντιληπτό ότι **όσο γρήγορα εξελίσσονται οι τεχνικές ψηφιακών επιθέσεων, τόσο άμεσα πρέπει να επικαιροποιούνται και οι μέθοδοι προστασίας.**

Ποιοι είναι οι κίνδυνοι για τις επιχειρήσεις

Οι επιθέσεις εστιάζουν κυρίως σε τρεις κατηγορίες επιχειρήσεων: Στις βιομηχανικές επιχειρήσεις, στις μεσαίες και μεγάλες επιχειρήσεις ανεξαρτήτως κλάδου, και στις επιχειρήσεις με σημαντικό όγκο εμπιστευτικών πληροφοριών. Οι μικρότερες επιχειρήσεις αντιμετωπίζουν γενικά λιγότερες επιθέσεις, χωρίς αυτό να σημαίνει πως δεν πρέπει να λαμβάνουν μέτρα προστασίας. Ειδικότερα:

- Ο κλάδος της βιομηχανίας αντιμετωπίζει αυξανόμενες απειλές στην εποχή της 4ης Βιομηχανικής επανάστασης. Σε ευρωπαϊκό επίπεδο, το 2018 **4 στις 10 βιομηχανικές επιχειρήσεις** επηρεάστηκαν από **σοβαρό συμβάν ασφάλειας**, τα περιστατικά εκβιασμών αυξήθηκαν **3500%**, η ψηφιακή απάτη κατά **250%. Η μέση οικονομική ζημιά ανήλθε σε €330.000 ανά περιστατικό ενώ η αντίστοιχη μέση ζημιά από παραβίαση οικονομικών και εμπιστευτικών δεδομένων ήταν €7,5 εκ.** Σημειώνεται πως τα νούμερα παρουσιάζουν ισχυρά αυξητική τάση το 2019, ενώ η πανδημία αναμένεται να τα αυξήσει περισσότερο.
- Οι μεσαίες και μεγάλες επιχειρήσεις υιοθετούν εκτενώς νέες ψηφιακές τεχνολογίες (βλέπε πρόσφατη μελέτη σε 16 κλάδους) και βιώνουν ψηφιακές παραβιάσεις ιδιαίτερης σοβαρότητας. Την περίοδο 2014-2019, οι παραβιάσεις αυξήθηκαν κατά 67%, με αποτέλεσμα το 2019, το 40% των επιχειρήσεων **να βιώσει ψηφιακές παραβιάσεις, με αυξημένο κόστος και χρόνο αποκατάστασης.** Το μέσο κόστος αποκατάστασης μαζί με τη μέση επίπτωση στην καθημερινή λειτουργία υπολογίζεται σε **€13 εκ. ανά παραβίαση**. Η ζημιά αυτή παρουσιάζει σημαντική **αυξητική τάση κατά 72%** την τελευταία πενταετία. Το 2020 **πάνω από το 50%** των μεσαίων και μεγάλων επιχειρήσεων αναμένεται να απειληθεί από κάποιας μορφής κυβερνοεπίθεση.
- Για επιχειρήσεις με σημαντικό όγκο εμπιστευτικών πληροφοριών (όπως η πνευματική ιδιοκτησία), είναι ιδιαίτερα κρίσιμη η επαρκής προστασία. Σε πρόσφατη ανάλυση, το μέσο κόστος αποκατάστασης (τεχνική και λειτουργική) από κυβερνοεπίθεση ανέρχεται σε **€3,9 εκ. ανά παραβίαση, ενώ το μέσο χρονικό διάστημα για τον εντοπισμο και περιορισμό του περιστατικού** φτάνει τις **280 ημέρες**. Στην ίδια ανάλυση αναδεικνύονται και οι συνέπειες της πανδημίας, καθώς 3 στις 4 επιχειρήσεις αναμένουν σημαντική αύξηση του χρόνου εντοπισμού και αποκατάστασης τέτοιων περιστατικών, κυρίως λόγω της δυσκολίας ψηφιακής προστασίας σε περιπτώσεις απομακρυσμένης εργασίας.

Τομέας Βιομηχανίας, Ανάπτυξης, Δικτύων και Περιφερειακής Πολιτικής

Αναπληρωτής Γενικός Διευθυντής: Δρ. Γιώργος Ξηρογιάννης
Senior Advisor: Μάγκυ Αθανασιάδη
Associate Advisor: Αλέξης Νικολαΐδης

Για πληροφορίες: industrial@sev.org.gr

Είναι εμφανές ότι η **εξέλιξη των τεχνικών των κυβερνοεπιθέσεων συμβαδίζει με την εξέλιξη της τεχνολογίας**. Οι οργανισμοί πρέπει να υιοθετήσουν την αντίληψη ότι σε μεσοπρόθεσμο χρονικό ορίζοντα η ασφάλειά τους θα αντιμετωπίσει σημαντικές ψηφιακές προκλήσεις. Για το λόγο αυτό απαιτείται η έγκαιρη προετοιμασία για την άμεση και αποτελεσματική διαχείριση κακόβουλών περιστατικών, ελαχιστοποίηση των οικονομικών επιπτώσεων και επαναφορά των επιχειρησιακών λειτουργιών το συντομότερο δυνατό. Κατά συνέπεια, οι επιχειρήσεις οφείλουν να μεριμνήσουν, ώστε να πορευθούν στη νέα ψηφιακή με ένα **συνεκτικό και ισχυρό σχέδιο κυβερνοασφάλειας**, που να καλύπτει όλα τα επίπεδα και στάδια λειτουργίας τους.

Το Παρατηρητήριο Ψηφιακού Μετασχηματισμού του ΣΕΒ για την κυβερνοασφάλεια

Το Παρατηρητήριο Ψηφιακού Μετασχηματισμού του ΣΕΒ με τη συνεργασία της Deloitte, προτείνει ένα πλέγμα 35 καλών πρακτικών κυβερνοασφάλειας (ανάλυση εδώ). Επιπλέον, περιέχει έναν οδικό χάρτη προετοιμασίας για την αντιμετώπιση ψηφιακών επιθέσεων, ώστε οι επιχειρήσεις να αναβαθμίσουν την ασφάλειά τους μέσα από την απάντησή τους σε 10 κρίσιμα ερωτήματα:

Επίγνωση: περιλαμβάνει την κατανόηση και αξιολόγηση του κινδύνου και τις απαραίτητες δομές και πόρους ψηφιακής προστασίας

1. Ποιος έχει τη θέση του Υπεύθυνου Ασφάλειας Πληροφοριών (CISO); Έχει η θέση επαρκείς διοικητικές αρμοδιότητες για το σχεδιασμό και εποπτεία της κυβερνοασφάλειας;
2. Διατίθεται επαρκής προϋπολογισμός και ανθρώπινοι πόροι για θέματα κυβερνο-προστασίας;

Προστασία: λειτουργίες και συστήματα που προστατεύονται με καλές πρακτικές και δικλείδες ασφαλείας

3. Ποιες διαδικασίες της επιχείρησης βασίζονται καταλυτικά σε ψηφιακά συστήματα και πως επηρεάζεται η καθημερινή λειτουργία της επιχείρησης από προβλήματα στα συστήματα αυτά;
4. Ποια είναι τα κρίσιμα προϊόντα / υπηρεσίες / πληροφορίες / γραμμές παραγωγής / ΤΠΕ που χρήζουν προστασίας;
5. Ποιοι είναι οι νέοι κίνδυνοι που αναπτύσσονται στον κυβερνοχώρο για τις κρίσιμες διαδικασίες και συστήματα της επιχείρησης;
6. Ποιο είναι το υφιστάμενο και ποιο το επιθυμητό επίπεδο κυβερνοασφάλειας στις διαδικασίες και στα συστήματα της επιχείρησης;

Ανθεκτικότητα: με αρχιτεκτονική ψηφιακής ασφάλειας και συνεχείς προληπτικούς ελέγχους

7. Ποια πρότυπα ασφαλείας πρέπει να χρησιμοποιήσει η επιχείρηση;
8. Ποιες είναι οι προτεραιότητες για την κυβερνοπροστασία της επιχείρησης, με μεσοπρόθεσμο (1 έτος) και μακροπρόθεσμο ορίζοντα (5 έτη);
9. Πως υιοθετείται μια κουλτούρα ασφαλούς χρήσης ψηφιακών συστημάτων από όλους τους εργαζόμενους;
10. Κάθε πότε γίνονται δοκιμές ανθεκτικότητας της προστασίας και κάθε πότε επικαιροποιείται η στρατηγική;

Οι απαντήσεις κάθε επιχείρησης στις παραπάνω ερωτήσεις θα τη βοηθήσουν να αποτρέψει σημαντικούς κινδύνους κυβερνοασφάλειας, εφόσον στο επόμενο στάδιο συνοδεύονται και από την εφαρμογή ενός αντίστοιχου σχεδίου, προσαρμοσμένου στις ανάγκες της. Μια τέτοια προσέγγιση, πέρα από αυξημένο επίπεδο ασφάλειας κατά τη λειτουργία της επιχείρησης, προσφέρει και ένα σημαντικό **ανταγωνιστικό πλεονέκτημα,** τόσο μέσω της διασφάλισης της εμπιστοσύνης μετόχων και πελατών στη διοίκηση της επιχείρησης, όσο και μέσα από τη μεγιστοποίηση του οφέλους των τεχνολογιών της 4ης Βιομηχανικής Επανάστασης.

Δείτε εδώ την πλήρη μελέτη και ανάλυση του παρατηρητηρίου ψηφιακού μετασχηματισμού του ΣΕΒ για την κυβερνοασφάλεια.

1. Οι νέες τεχνολογίες καθιστούν απαραίτητη την κυβερνοασφάλεια

Η 4η Βιομηχανική Επανάσταση είναι ήδη μια πραγματικότητα, στην οποία ο επιχειρηματικός κόσμος πρέπει –και οφείλει- να προσαρμοστεί. Πλέον, κομβική παράμετρος ανάπτυξης αποτελούν οι ψηφιακές καινοτομίες, οι οποίες μπορούν να δώσουν σε όσους τις υιοθετούν, βάσει ορθού προγραμματισμού, αξία και στρατηγικής σημασίας πλεονεκτήματα. Όμως, η λειτουργία των επιχειρήσεων σε ένα ψηφιακό περιβάλλον, όπου τα πάντα είναι διασυνδεδεμένα (εργαζόμενοι, τμήματα, μηχανήματα, συσκευές, πελάτες, προμηθευτές) εγκυμονεί και ψηφιακούς **κινδύνους**. Σε λύσεις Internet of Things για παράδειγμα, διακινούνται ψηφιακά μεγάλοι όγκοι δεδομένων, με αποτέλεσμα να προκύπτουν κίνδυνοι παραβίασης. Τα δίκτυα φορητών συσκευών είναι γεωγραφικά διασκορπισμένα και ανομοιογενή, χαρακτηριστικό που τα καθιστά ευάλωτα σε επιθέσεις. Ακόμα και τα chatbots που λειτουργούν με τεχνολογίες ΤΝ, μπορούν να αποτελέσουν αντικείμενα κακόβουλων επιθέσεων και να χρησιμοποιηθούν ως εργαλεία του επιτιθέμενου. Επιπλέον, η επιδημία Covid-19 επιτάχυνε σε πολύ σύντομο χρονικό διάστημα τις δράσεις ψηφιακού μετασχηματισμού προκειμένου να υλοποιηθούν νέα μοντέλα λειτουργίας και εργασίας, γεγονός που ενέτεινε τους ήδη υπάρχοντες κινδύνους.

Σε αυτή τη νέα πραγματικότητα, οι επιχειρήσεις **αποτελούν συνήθη στόχο κυβερνοεπιθέσεων**. Το σύγχρονο ηλεκτρονικό έγκλημα εφαρμόζει πιο έξυπνες και πολύπλοκες τεχνικές και μεθόδους, με αποτέλεσμα να είναι αρκετά δύσκολος ο εντοπισμός των επιτιθέμενων.

Η λειτουργία μιας επιχείρησης στο σημερινό τεχνολογικό περιβάλλον απαιτεί μια ισχυρή προσέγγιση κυβερνοπροστασίας. Πλέον, οι οργανισμοί πρέπει να διαχειρίζονται κινδύνους που βρίσκονται όχι μόνο εντός, αλλά και εκτός των περιοχών ελέγχου τους.

Στην **Ελλάδα**, οι επιχειρήσεις, αν και υλοποιούν (ή σχεδιάζουν να υλοποιήσουν) δράσεις ψηφιακής μετάβασης, εν τούτοις **δεν προσδίδουν πάντα την απαιτούμενη σημασία στα θέματα ασφάλειας.** Οι κύριες αιτίες του φαινομένου εντοπίζονται στη:

- Γενικότερη έλλειψη κουλτούρας και ευαισθητοποίησης,
- Υλοποίηση μεμονωμένων ενεργειών, αντί ολιστικής προσέγγισης στο θέμα,
- Περιορισμένη στόχευση στο μέλλον, με συνέπεια να μην προβλέπονται κίνδυνοι που ενδέχεται να προκύψουν,
- Διάθεση χαμηλών προϋπολογισμών και
- Ανεπαρκή στελέχωση των τμημάτων κυβερνοασφάλειας και ανεπάρκειες στην τεχνική κατάρτιση των στελεχών.

Λαμβάνοντας υπόψη τα παραπάνω εμπόδια, η παρούσα έκδοση του Παρατηρητηρίου Ψηφιακού Μετασχηματισμού του ΣΕΒ, με τη συνεργασία της Deloitte, έχει ως σκοπό να ενημερώσει τις επιχειρήσεις για τους **κινδύνους** που αντιμετωπίζουν, τα **οφέλη** που μπορεί να έχει μια συνεκτική στρατηγική κυβερνοασφάλειας, καθώς και τα **βήματα** που πρέπει να ακολουθήσουν για να διαμορφώσουν μια ολοκληρωμένη στρατηγική.

Οι κίνδυνοι κυβερνοεπιθέσεων μεγαλώνουν διαρκώς

Οι επιχειρήσεις αποτελούν διαρκώς στόχους κυβερνοεπιθέσεων. Αθέμιτοι ανταγωνιστές, εγκληματίες του διαδικτύου, hackers, τρίτοι, ακόμα και εσωτερικοί χρήστες, ενδέχεται να εκδηλώσουν κάποιου είδους επίθεση ή παρέμβαση στα συστήματα μιας εταιρείας, εντοπίζοντας τα αδύναμα σημεία της.

Οι μέθοδοι επιθέσεων έχουν γίνει πολύπλοκες και μη αναμενόμενες, με αποτέλεσμα τακτικές του παρελθόντος, όπως η χρήση ενός μόνο περιμετρικού firewall, να μην ανταποκρίνονται στις σημερινές απειλές. Μέθοδοι όπως ransomware, phishing, τεχνικές ΤΝ, κ.ά., μπορούν να επιφέρουν σημαντικά

πλήγματα σε έναν οργανισμό, όπως αρνητική δημοσιότητα, οικονομική ζημιά, διακοπή λειτουργιών, αλλοίωση δεδομένων, διαρροή εμπιστευτικών πληροφοριών, βλάβες στη γραμμή παραγωγής, κ.λπ.

Σύμφωνα με μελέτη των Deloitte και MAPI (Manufacturer's Alliance for Productivity and Innovation):

- 4 στις 10 βιομηχανικές επιχειρήσεις τους τελευταίους 12 μήνες επηρεάστηκαν από κάποιο συμβάν ασφάλειας.
- Τα περιστατικά εκβιασμών αυξήθηκαν 35 φορές, ενώ τα περιστατικά εξαπάτησης 2,5 φορές.
- Η οικονομική ζημιά από περιστατικά ασφάλειας που σχετίζονται με δίκτυα Internet of Things ανήλθε σε €330.000 κατά μέσο όρο.
- Η οικονομική ζημιά από παραβίαση δεδομένων ανήλθε σε €7,5 εκ. κατά μέσο όρο.

2. Κυβερνοασφάλεια στο έξυπνο εργοστάσιο

Η βιομηχανία συγκαταλέγεται στους κλάδους που **απειλούνται περισσότερο από κυβερνοεπιθέσεις, στην εποχή της 4ης Βιομηχανικής Επανάστασης.** Επομένως, η μετάβαση μιας επιχείρησης στο «έξυπνο» εργοστάσιο δεν μπορεί να πραγματοποιηθεί χωρίς την ανάλογη προστασία.

Η κυβερνοασφάλεια στη βιομηχανία δεν αφορά μόνο συγκεκριμένες λειτουργίες ή τμήματα / εργαζομένους. Αντιθέτως, σχετίζεται με όλα τα επίπεδα και στάδια της βιομηχανικής μονάδας.

Πρέπει να ληφθεί υπόψη ότι στην εποχή της διασύνδεσης κάθε εργαζόμενος, ηλεκτρονική συσκευή, μηχάνημα ή τελικό προϊόν, από τη στιγμή που αποτελεί μέρος ενός διασυνδεδεμένου δικτύου, αποτελεί ταυτόχρονα και πιθανό στόχο κυβερνοεπίθεσης.

Μια βιομηχανία, προκειμένου να μεταβεί στο «έξυπνο» εργοστάσιο, πρέπει να ενοποιήσει τα συστήματα πληροφορικής και τεχνολογίας παραγωγής (IT και OT αντίστοιχα), γεγονός που συνεπάγεται μεγαλύτερη έκθεση του τομέα OT στον κυβερνοχώρο και επομένως αυξημένη πιθανότητα στοχοποίησης.

Ο συγκερασμός όμως του φυσικού και ψηφιακού μέρους του εργοστασίου αποτελεί ένα σύνθετο εγχείρημα, καθώς ενδέχεται να προκύπτουν σημαντικές διαφορές σε επίπεδο τεχνολογιών, διαδικασιών και δεξιοτήτων. Μια από τις παραμέτρους που μπορεί να δυσχεράνει τη μετάβαση σε ένα πετυχημένο μοντέλο μιας κυβερνοφυσικής μονάδας, είναι οι διαφορετικές τεχνολογίες / μηχανισμοί ασφάλειας που εφαρμόζονται στα συστήματα OT και IT. Το γεγονός αυτό, οδηγεί συχνά σε σημαντικές τροποποιήσεις, ώστε να γίνει δυνατή η υποστήριξη των μηχανισμών αυτών από τις υπάρχουσες υποδομές πληροφορικής. Όμως η διαδικασία ενοποίησης της ασφάλειας των IT και OT, ενέχει σημαντικούς κινδύνους και εμπόδια, που μπορούν να προκύψουν από:

- τον υψηλό βαθμό δυσκολίας για τη σύγκλιση των συστημάτων IT και OT (π.χ. κάποιες κρίσιμες λειτουργίες μπορεί να έχουν ανατεθεί με outsourcing σε εξωτερικούς συνεργάτες),
- το διαφορετικό τρόπο διαχείρισης κινδύνων και λειτουργίας μηχανισμών ασφαλείας,
- την προβληματική ενημέρωση του λογισμικού,
- τα απαρχαιωμένα συστήματα OT, τα οποία έχουν μεγάλο κύκλο ζωής,
- την έλλειψη σταθερότητας των υποδομών (π.χ. προβληματική λειτουργία των υφιστάμενων δικτύων και αρχιτεκτονικών στις αυξημένες ροές δεδομένων),
- λειτουργικούς περιορισμούς (π.χ. ενδεχόμενη προσωρινή παύση της γραμμής παραγωγής προκειμένου να γίνουν αλλαγές στα συστήματα OT).

Αν δεν διευθετηθούν τα παραπάνω ζητήματα, το «έξυπνο» εργοστάσιο, όντας μια μονάδα που ενσωματώνει διαφορετικά περιβάλλοντα και τεχνολογίες (μηχανολογικά – ψηφιακά), μπορεί να εμφανίσει σημαντικές ευπάθειες / αδύναμα σημεία, σε τομείς όπως: μοντέλα σχεδιασμού παραγωγής, συστήματα προγραμματισμού ποσότητας υλικών (MRP), τεχνολογίες 3D printing, διαδικασίες Robotic Process Automation, προληπτική συντήρηση, κ.ά.

4. 10 βήματα για ένα ολιστικό σχέδιο κυβερνοασφάλειας

Η επιχείρηση πρέπει να λάβει υπόψη τις ευκαιρίες, αλλά και τους κινδύνους που ενδέχεται να προκύψουν από την υιοθέτηση disruptive τεχνολογιών. Στα πλαίσια αυτά, αφενός πρέπει να σταθμίσει τις ανάγκες υιοθέτησης καινοτομιών που είναι απαραίτητες για την ανάπτυξή της και αφετέρου να προσδιορίσει τις ανάγκες προστασίας που θα προκύψουν, τόσο από τις υπάρχουσες, όσο και τις επερχόμενες απειλές. Επομένως, χρειάζεται να καταρτίσει ένα ολιστικό σχέδιο κυβερνοασφάλειας, ακολουθώντας τα εξής βασικά βήματα:

1. **Κατανομή ρόλων και δημιουργία ομάδας για την κατάρτιση του σχεδίου.** Αρχικά, η επιχείρηση πρέπει να θεσπίσει τη θέση του Υπεύθυνου Ασφάλειας Πληροφοριών (CISO), ο οποίος αποτελεί μέλος της Διοίκησης, αλλά και σύμβουλο της Εκτελεστικής Διοίκησης σε θέματα τεχνολογίας και ασφάλειας πληροφοριών και δεδομένων. Ακολούθως, σχηματίζεται μια ομάδα η οποία θα αναλάβει το σχεδιασμό και εποπτεία του πλάνου κυβερνοασφάλειας της επιχείρησης, με τη συμμετοχή της Εκτελεστικής Διοίκησης (C-Suite), του Υπεύθυνου Ασφάλειας Πληροφοριών και στελεχών του τμήματος IT (π.χ. Υπεύθυνος Ασφάλειας Πληροφοριακών Συστημάτων (IT Security Officer)). Τέλος, δημιουργείται το τμήμα κυβερνοασφάλειας, το οποίο ο CISO στελεχώνει με τις κατάλληλες δεξιότητες.
2. **Εξέταση του μοντέλου λειτουργίας.** Η ομάδα σχεδιασμού ξεκινάει την κατάρτιση του πλάνου κυβερνοασφάλειας με την καταγραφή και κατανόηση του τρόπου με τον οποίο λειτουργεί η επιχείρηση, των διαδικασιών που χρησιμοποιεί και των στόχων που έχουν τεθεί.
3. **Αξιολόγηση του υφιστάμενου επιπέδου κυβερνοασφάλειας.** Για κάθε μια από τις διαδικασίες που καταγράφονται στο προηγούμενο βήμα, προσδιορίζεται ο βαθμός προστασίας τους από επιθέσεις και επομένως η ωριμότητα του τωρινού επιπέδου κυβερνοασφάλειας της επιχείρησης. Με τον τρόπο αυτό, εντοπίζονται πιθανά κενά (breaches) στην ασφάλεια του οργανισμού, και γενικότερα τομείς για βελτίωση του επιπέδου προστασίας.Το βήμα αυτό, μπορεί να υλοποιηθεί είτε ενδοεπιχειρησιακά, είτε από εξωτερικούς εξειδικευμένους συμβούλους.
4. **Διερεύνηση και αξιολόγηση των υφιστάμενων και αναπτυσσόμενων κινδύνων και απειλών στον κυβερνοχώρο.** Απαραίτητη προϋπόθεση κατάρτισης της στρατηγικής για μια αποτελεσματική κυβερνοασφάλεια, αποτελεί η εξέταση του εξωτερικού περιβάλλοντος, με τον εντοπισμό των απειλών στον κυβερνοχώρο και των συνεπειών που ενδέχεται να έχουν στην επιχείρηση. Για να αποτυπωθεί σωστά ο χάρτης με τις πηγές προέλευσης και τη φύση των κινδύνων και απειλών, πρέπει να διερευνηθεί προσεκτικά το περιβάλλον στο οποίο λειτουργεί η επιχείρηση. Ενδεικτικά, να καταγραφούν / προσδιοριστούν: οι πελάτες, οι προμηθευτές, διάφοροι τρίτοι με τους οποίους έχουν καταρτιστεί συνεργασίες, οι κυριότεροι ανταγωνιστές, οι απειλές που αντιμετωπίζουν οι ανταγωνιστές ή τους έχουν επηρεάσει στο παρελθόν, ποιοι θα μπορούσαν να επωφεληθούν από μια επίθεση στα συστήματα της επιχείρησης και τη διακοπή της λειτουργίας της, οι μέθοδοι που χρησιμοποιούν κυρίως οι επιτιθέμενοι, τα κίνητρά τους, κ.λπ.
5. **Προσδιορισμός των αγαθών στρατηγικής σημασίας που πρέπει να προστατευθούν.** Η ομάδα κυβερνοπροστασίας καθορίζει ποια είναι τα σημαντικότερα αγαθά (assets) της επιχείρησης που είναι περισσότερο έκθετα σε κυβερνοεπιθέσεις, ή επιθέσεις εκ των έσω, και επομένως προκύπτουν ανάγκες προστασίας τους. Τα αγαθά είναι: διαδικασίες, πληροφοριακά συστήματα, συσκευές, τεχνολογικός & μηχανολογικός εξοπλισμός, ανθρώπινο δυναμικό που εργάζεται σε ενδεχομένως στοχοποιημένες θέσεις ευθύνης, πληροφορίες και δεδομένα.
6. **Ανάπτυξη πλαισίου και προτύπων διαχείρισης της κυβερνοασφάλειας.** Πριν την κατάρτιση του στρατηγικού σχεδίου, η ομάδα κυβερνοπροστασίας καθορίζει το υποστηρικτικό

πλαίσιο διαχείρισης της κυβερνοασφάλειας που θα χρησιμοποιηθεί. Πρόκειται για τις μεθοδολογίες και πρότυπα που χρησιμοποιούνται για την αξιολόγηση της ανθεκτικότητας ενός οργανισμού σε θέματα κυβερνοασφάλειας και τη διαχείριση των κινδύνων που προκύπτουν. Τα πιο γνωστά πρότυπα που εφαρμόζονται διεθνώς είναι τα ISO 2700x, NIST και IRAM2.

7. **Κατάρτιση στρατηγικής κυβερνοασφάλειας.** Μετά τη χαρτογράφηση του εσωτερικού και εξωτερικού περιβάλλοντος και την επιλογή του πλαισίου διαχείρισης, καταρτίζεται η στρατηγική κυβερνοασφάλειας, με τη συμμετοχή της Διοίκησης, σε συμφωνία όμως με τη γενικότερη επιχειρησιακή στρατηγική και το μοντέλο λειτουργίας της επιχείρησης. Λαμβάνεται υπόψη το υφιστάμενο επίπεδο ωριμότητας της ασφάλειας, αλλά και το επίπεδο που θέλει να φτάσει η επιχείρηση. Προτείνεται η κατάρτιση στρατηγικής με δύο χρονικούς ορίζοντες: μεσοπρόθεσμα (1 έτος) και μακροπρόθεσμα (5 έτη). Περιέχονται: διαδικασίες, πόροι, τεχνολογίες, στόχος (σε ποιο επίπεδο κυβερνοασφάλειας επιθυμεί η επιχείρηση να φτάσει), προϋπολογισμός.
8. **Υιοθέτηση κουλτούρας κυβερνοασφάλειας.** Η ομάδα σχεδιασμού κυβερνοπροστασίας, στα πλαίσια της εφαρμογής της στρατηγικής, αναλαμβάνει την υλοποίηση προγραμμάτων ευαισθητοποίησης, ώστε όλα τα επίπεδα της επιχείρησης να είναι ενήμερα σε θέματα κυβερνοπροστασίας και σε ετοιμότητα. Π.χ. πρόγραμμα εκπαίδευσης του προσωπικού, υιοθέτηση ρόλων και αρμοδιοτήτων σε κάθε τμήμα.
9. **Ανάπτυξη και εφαρμογή σχεδίου ανθεκτικότητας.** Το σχέδιο ανθεκτικότητας περιλαμβάνει συστηματικές δοκιμές σε ελεγχόμενο περιβάλλον, για να αξιολογείται η αποτελεσματικότητα των συστημάτων ασφάλειας και να βελτιώνεται συνεχώς το επίπεδο προστασίας. Περιλαμβάνει: σχεδιασμό σεναρίων για επιθέσεις που ενδέχεται να συμβούν και ενεργειών αντιμετώπισής τους, δοκιμαστικά σχέδια αντιμετώπισης περιστατικών, π.χ. προσομοίωση περιστατικών ασφάλειας (war gaming), προσομοίωση ρεαλιστικών επιθέσεων από ανεξάρτητη εταιρεία, χωρίς τη γνώση της ομάδας αντιμετώπισης (red teaming). Κατά τη διεξαγωγή των προσομοιώσεων, συμμετέχουν τα μέλη της ομάδας κυβερνοασφάλειας που ασχολούνται με τη διαχείριση κρίσεων.
10. **Περιοδικός έλεγχος.** Το σχέδιο ανθεκτικότητας πρέπει να ελέγχεται και να επικαιροποιείται τουλάχιστον μια φορά το χρόνο, ώστε να διαπιστώνεται ο βαθμός αποτελεσματικής λειτουργίας του. Λαμβάνονται υπόψη τόσο οι αλλαγές στο περιβάλλον της επιχείρησης, όσο και νέοι κίνδυνοι ή απειλές που ενδέχεται να έχουν προκύψει.

Η πλήρης ανάλυση του παρατηρητηρίου ψηφιακού μετασχηματισμού του ΣΕΒ, εδώ.

Οικονομικά Στοιχεία Μελών ΣΕΒ

ΕΝΕΡΓΗΤΙΚΟ
€311 δισ.
63% συνόλου*

ΙΔΙΑ ΚΕΦΑΛΑΙΑ
€55 δισ.
45% συνόλου*

ΠΩΛΗΣΕΙΣ
€72 δισ.
42% συνόλου*

ΠΡΟ ΦΟΡΩΝ ΚΕΡΔΗ
€4,2 δισ.**
38% συνόλου**

ΕΡΓΑΖΟΜΕΝΟΙ
216.000
10% συνόλου ασφαλισμένων στον ΕΦΚΑ

ΜΙΣΘΟΙ
€5,2 δισ.
18% συνόλου***

ΑΣΦΑΛΙΣΤΙΚΕΣ ΕΙΣΦΟΡΕΣ
€2,2 δισ.
23% συνόλου***

ΦΟΡΟΣ ΕΠΙ ΚΕΡΔΩΝ
€1,3 δισ.
29% συνόλου****

* 19.910 δημοσιευμένοι ισολογισμοί χρήσης 2018 που περιλαμβάνονται στη βάση της ICAP.
** Σύνολο κερδών κερδοφόρων επιχειρήσεων.
*** % επί του συνόλου τακτικών αποδοχών (χωρίς bonus και υπερωρίες) / ασφαλιστικών εισφορών ασφαλισμένων στον ΕΦΚΑ.
**** % επί του συνόλου εσόδων από φόρο εισοδήματος νομικών προσώπων.

Όραμα

Οραματιζόμαστε την Ελλάδα ως τη χώρα, που κάθε πολίτης του κόσμου θα θέλει και θα μπορεί να επισκεφθεί, να ζήσει και να επενδύσει.
Οραματιζόμαστε μια ανοιχτή, κοινωνικά υπεύθυνη και οικονομικά φιλελεύθερη χώρα-μέλος της Ευρωπαϊκής Ένωσης, που προτάσσει την ισχυρή ανάπτυξη ως παράγοντα κοινωνικής συνοχής. Θέλουμε μια Ελλάδα δυναμικό κέντρο της ευρωπαϊκής περιφέρειας, με στέρεους θεσμούς, ελκυστικό κοινωνικό και οικονομικό περιβάλλον, που προάγει τις εξαγωγές, την καινοτόμο επιχειρηματικότητα, την παραγωγή και τις ποιοτικές υπηρεσίες, τη βιώσιμη ανάπτυξη, τη γνώση, τη συνοχή, τις ίσες ευκαιρίες και το κράτος δικαίου.

Αποστολή

Ηγεσία & Γνώση

Ο ΣΕΒ διαδραματίζει ηγετικό ρόλο στον μετασχηματισμό της Ελλάδας σε μια παραγωγική, εξωστρεφή και ανταγωνιστική οικονομία, ως ανεξάρτητος και υπεύθυνος εκπρόσωπος της ιδιωτικής οικονομίας.

Κοινωνικός Εταίρος

Ο ΣΕΒ, ως κοινωνικός εταίρος που πιστεύει στη λειτουργία των θεσμών, προωθεί στα αρμόδια όργανα της Πολιτείας και της Ε.Ε. τις απόψεις και θέσεις της επιχειρηματικής κοινότητας.

Ισχυρός Εκπρόσωπος

Ο ΣΕΒ διαμορφώνει θέσεις, αναλύσεις και προτάσεις πολιτικής για την οικονομία, τη βιομηχανία, την καινοτομία, την απασχόληση, την παιδεία και τις εργασιακές δεξιότητες, τον κοινωνικό διάλογο, τη βιώσιμη ανάπτυξη, την εταιρική υπευθυνότητα.

Φορέας Δικτύωσης

Ο ΣΕΒ δικτυώνει τα μέλη του μεταξύ τους & με τα κέντρα αποφάσεων (εγχώρια και διεθνή), με στόχο τη δημιουργία προστιθέμενης αξίας.

ΣΕΒ
Σύγχρονες Επιχειρήσεις, Σύγχρονη Ελλάδα

ΣΕΒ σύνδεσμος επιχειρήσεων και βιομηχανιών

Ξενοφώντος 5, 105 57 Αθήνα
T: 211 5006 000
F: 210 3222 929
E: info@sev.org.gr
www.sev.org.gr

SEV Hellenic Federation of Enterprises

168, Avenue de Cortenbergh
B-1000 Bruxelles
T: +32 (0) 2 662 26 85
E: kdiamantouros@sev.org.gr

ΑΚΟΛΟΥΘΗΣΤΕ ΜΑΣ ΣΤΑ ΜΕΣΑ ΚΟΙΝΩΝΙΚΗΣ ΔΙΚΤΥΩΣΗΣ