ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΣ ΟΔΗΓΟΣ

ΤΟΥ ΔΙΕΘΝΟΥΣ ΕΜΠΟΡΙΚΟΥ ΕΠΙΜΕΛΗΤΗΡΙΟΥ (ICC)

ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

ICC ΔΙΕΘΝΕΣ ΕΜΠΟΡΙΚΟ ΕΠΙΜΕΛΗΤΗΡΙΟ (ΔΕΕ)

Ο παγκόσμιος επιχειρηματικός Οργανισμός

Το κείμενο που ακολουθεί αποτελεί μετάφραση του επίσημου οδηγού που εκδόθηκε από το Διεθνές Εμπορικό Επιμελητήριο και έγινε με τη φροντίδα του Εμπορικού και Βιομηχανικού Επιμελητηρίου Θεσσαλονίκης.

ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΣ ΟΔΗΓΟΣ

ΤΟΥ ΔΙΕΘΝΟΥΣ ΕΜΠΟΡΙΚΟΥ ΕΠΙΜΕΛΗΤΗΡΙΟΥ (ICC)

ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

Ευχαριστίες

Ο επιχειρηματικός Οδηγός του ΔΕΕ για την ασφάλεια στον κυβερνοχώρο αντλεί την έμπνευση του από τον Οδηγό για την ασφάλεια στον κυβερνοχώρο του Βελγίου, ο οποίος αποτελεί πρωτοβουλία του ΔΕΕ Βελγίου (ICC Belgium) και της Ένωσης Βελγικών Επιχειρήσεων (VBO-FEB), της EY Βελγίου (EY Belgium) και της Microsoft Βελγίου μαζί με το Βέλγικο Κέντρο Αριστείας για την αντιμετώπιση του Κυβερνοεγκλήματος (B-CCENTRE) και το Βέλγικο Ινστιτούτο Ελέγχου Συστημάτων Πληροφορικής (ISACA Belgium). Ο εν λόγω Οδηγός είχε θετική απήχηση στο Βέλγιο. Ως εκ τούτου, προτάθηκε στην Επιτροπή Ψηφιακής Οικονομίας του ΔΕΕ ως ένα πρότυπο, το οποίο θα μπορούσε να υιοθετηθεί με σκοπό να αποτελέσει έναν παγκόσμιο πόρο με την έγκριση των εμπλεκομένων επιχειρήσεων και οργανισμών.

Το ΔΕΕ αναγνωρίζει την πολύτιμη συμβολή όσων ενεπλάκησαν στην προετοιμασία και δημιουργία του Βέλγικου Οδηγού, καθώς και των μελών της Ειδικής Ομάδας για την Ασφάλεια στον Κυβερνοχώρο του ΔΕΕ που προχώρησε στη δημιουργία του παρόντος παγκόσμιου Οδηγού.

ICC Publication No. 450/1081-5
ISBN: 978-92-842-0336-9

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Πρόλογος..... 3

Διαβάστε πρώτα 4

Χρησιμοποιώντας τον Οδηγό..... 6

Βασικές αρχές ασφάλειας 8

Α. Όραμα και νοοτροπία..... 8

Β. Οργάνωση και διαδικασίες 10

Έξι βασικές δράσεις ασφάλειας..... 12

Εφαρμογή αρχών στην Πολιτική Ασφάλειας Πληροφοριών..... 16

Αυτό-αξιολόγηση ασφάλειας 20

Πηγές και αναφορές..... 37

ΠΡΟΛΟΓΟΣ

John Danilovich, Γενικός Γραμματέας του Διεθνούς Εμπορικού Επιμελητηρίου-ΔΕΕ (International Chamber of Commerce – ICC)

Το Διεθνές Εμπορικό Επιμελητήριο (ΔΕΕ) έχει μια περήφανη ιστορία εκατό περίπου ετών στην παροχή εργαλείων και αυτο-ρυθμιστικών οδηγιών σε εταιρείες με σκοπό την προώθηση των ορθών επιχειρηματικών πρακτικών. Ως ο παγκόσμιος επιχειρηματικός οργανισμός, ο κατάλογος των μελών του οποίου απαρτίζεται από εταιρείες σε όλους τους τομείς και περιφέρειες, το ΔΕΕ είναι στην ευχάριστη θέση να προσφέρει στις επιχειρήσεις ανεξαρτήτως μεγέθους σαφείς οδηγίες με σκοπό την παροχή βοήθειας σε αυτές προκειμένου να συμβάλουν στην αντιμετώπιση της όλο και πιο σοβαρής πρόκλησης της ασφάλειας στον κυβερνοχώρο.

Το ΔΕΕ είναι ένας οργανισμός που έχει ως σκοπό τη διευκόλυνση εμπορικών και επενδυτικών δραστηριοτήτων, συμπεριλαμβανομένης της ενίσχυσης της εμπιστοσύνης στη ψηφιακή οικονομία και της αύξησης των σημαντικών ευκαιριών που προσφέρει στις επιχειρήσεις, τους καταναλωτές, τις κυβερνήσεις και την κοινωνία. Η διασυνδεσιμότητα δεν έχει αλλάξει μόνο την αγορά, αλλά και τον ιστό της κοινωνίας. Τα οφέλη που απορρέουν από τη μεγαλύτερη πρόσβαση στη γνώση, την πληροφορία, τα αγαθά και τις υπηρεσίες καθίστανται εφικτά μέσω του παγκόσμιου και ανοιχτού Διαδικτύου, το οποίο πρέπει να είναι αξιόπιστο και ασφαλές. Κατά συνέπεια, κάθε στρατηγική για την ασφάλεια στον κυβερνοχώρο πρέπει να είναι ενδεδειγμένη, αιτιολογημένη και αναλογική προκειμένου να προασπίζεται τα εν λόγω οφέλη. Επειδή η ασφάλεια – όπως ακριβώς και η τελειότητα – αποτελεί ουτοπικό στόχο με πολλαπλούς συμβιβασμούς μπορεί, επίσης, να αποτελεί και ένα τρομακτικό ζήτημα. Ο φόβος ή η άγνοια μπορεί να συνιστούν εμπόδιο στη διασφάλιση εκ μέρους των επιχειρήσεων της αξιολόγησης των κινδύνων και στην ανάληψη κατάλληλων δράσεων. Ο παρών οδηγός καθιστά την επίγνωση ένα απλό σύνολο βημάτων και γκρεμίζει το φράγμα του εκφοβισμού. Το ΔΕΕ έχει εκδώσει *τον Επιχειρηματικό Οδηγό Ασφάλειας στον Κυβερνοχώρο* για να απευθυνθεί σ' ένα ευρύ κοινό έχοντας κατά νου τα πάνω από έξι εκατομμύρια μέλη του. Ο εν λόγω οδηγός προορίζεται να είναι προσβάσιμος σε ιδιοκτήτες, προσωπικό και στελέχη επιχειρήσεων και όχι μόνο σε ομάδες με εξειδίκευση στην τεχνολογία της πληροφορικής. Πρέπει, επιπλέον, να χρησιμοποιείται από κοινού με επιχειρηματικούς εταίρους στην εφοδιαστική αλυσίδα αγαθών και υπηρεσιών, καθώς και με το δημόσιο τομέα για την ενίσχυση της ανθεκτικότητας όσο το δυνατόν ευρύτερα.

Ο οδηγός θα διανεμηθεί από το παγκόσμιο δίκτυο του ΔΕΕ, το οποίο περιλαμβάνει εθνικές επιτροπές, εταιρείες-μέλη, επιχειρηματικές ενώσεις και εμπορικά επιμελητήρια, μέσω της Παγκόσμιας Ομοσπονδίας Επιμελητηρίων (WCF) του ΔΕΕ που καλύπτει πάνω 130 χώρες. Το ΔΕΕ

πιστεύει ότι η συλλογική, παγκόσμια επιχειρηματική δράση από τα δίκτυα και τους εταίρους της μπορεί να συμβάλλει καθοριστικά στη μείωση των κινδύνων του κυβερνοχώρου για τις επιχειρήσεις και την κοινωνία γενικά.

ΔΙΑΒΑΣΤΕ ΠΡΩΤΑ

Η ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΞΕΚΙΝΑΕΙ ΑΠΟ ΕΣΑΣ

Οι σύγχρονες τεχνολογίες πληροφορικής και επικοινωνιών παρέχουν τη δυνατότητα σε επιχειρήσεις ανεξαρτήτως μεγέθους να καινοτομήσουν, να κατακτήσουν νέες αγορές και να δώσουν ώθηση στην απόδοση, έτσι ώστε να επωφεληθούν οι καταναλωτές και η κοινωνία. Όλο και περισσότερο, ωστόσο, οι επιχειρηματικές πρακτικές και πολιτικές δέχονται την πρόκληση της ανάγκης προσαρμογής στον άμεσο και έμμεσο αντίκτυπο των διεισδυτικών περιβαλλόντων επικοινωνίας και της ροής πληροφοριών δικτύου που απαιτούνται στην παροχή αγαθών και υπηρεσιών. Πολλές εταιρείες υιοθετούν σύγχρονες τεχνολογίες πληροφορικής και επικοινωνιών χωρίς να συνειδητοποιούν πλήρως ότι νέα είδη κινδύνων, τα οποία προκύπτουν, θα πρέπει, κατά συνέπεια, να αποτελέσουν αντικείμενο σωστής διαχείρισης. Ο παρών οδηγός εξετάζει το εν λόγω κενό και σκιαγραφεί τον τρόπο με τον οποίο οι εταιρείες όλων των μεγεθών μπορούν να αναγνωρίσουν και να διαχειριστούν τους κινδύνους ασφάλειας στον κυβερνοχώρο.

Η αποτυχία της ασφάλειας στον κυβερνοχώρο αναφέρεται διαρκώς στον Τύπο με αναφορές για κακόβουλους παράγοντες που παραβιάζουν μικρές και μεγάλες επιχειρήσεις – φαινομενικά κατά βούληση και με ευκολία. Οι επιχειρήσεις είναι σήμερα εκτεθειμένες σε μία αυξανόμενη πηγή κινδύνων[1] όπως εγκληματικοί παράγοντες, χάκερ, κρατικοί παράγοντες και ανταγωνιστές που εκσυγχρονίζονται όλο και περισσότερο με αποτέλεσμα να εκμεταλλεύονται τις αδυναμίες των σύγχρονων τεχνολογιών πληροφορικής και επικοινωνιών. Η σύνδεση των συστημάτων πληροφορικής με διάφορες εξωτερικές συσκευές[2] αυξάνει το επίπεδο της πολυπλοκότητας και των απειλών για τα πληροφοριακά συστήματα των επιχειρήσεων. Οι επιχειρήσεις δεν αντιμετωπίζουν μόνο εξωτερικές απειλές, αλλά οφείλουν και να διαχειριστούν τους κινδύνους των εσωτερικών απειλών προς τα πληροφοριακά συστήματα τους από άτομα εντός των εταιρειών, τα οποία είναι διατεθειμένα να αλλοιώσουν δεδομένα ή να εκμεταλλευτούν επιχειρηματικούς πόρους απολαμβάνοντας την άνεση της κατοικίας τους ή της τοπικής καφετέριας. Από την πλευρά των επιχειρήσεων είναι ζωτικής σημασίας μία εταιρεία – μικρή ή μεγάλη – να είναι σε θέση να αναγνωρίζει τον κίνδυνο που απειλεί την ασφάλεια στον κυβερνοχώρο και να αντιμετωπίζει αποτελεσματικά τις απειλές για τα πληροφοριακά συστήματα. Ταυτόχρονα, οι υπεύθυνοι διοίκησης των επιχειρήσεων, συμπεριλαμβανομένων των στελεχών και των διευθυντών, πρέπει να αναγνωρίσουν ότι η διαχείριση των κινδύνων του κυβερνοχώρου είναι μία συνεχής διαδικασία κατά την οποία δεν υφίσταται ούτε πρόκειται να υπάρξει απόλυτη ασφάλεια.

Σε αντίθεση με πολλές επιχειρηματικές προκλήσεις, η διαχείριση των κινδύνων για την ασφάλεια στον κυβερνοχώρο παραμένει ένα πρόβλημα δίχως εύκολη λύση. Απαιτείται

συνεπής εφαρμογή της διαχειριστικής προσήλωσης με ανοχή στα δυσάρεστα νέα και πειθαρχία για σαφή επικοινωνία. Διαθέσιμοι είναι πολλοί εξαιρετικοί πόροι που παρέχουν περιεκτικές εξηγήσεις για κορυφαίες απειλές του κυβερνοχώρου. Το κατάλληλο, ωστόσο, υλικό για την παροχή βοήθειας στη διαχείριση των επιχειρήσεων όσον αφορά την προσέγγιση τους στην ασφάλεια του κυβερνοχώρου παραμένει δυσεύρετο. **Το παρόν έγγραφο θα βοηθήσει την επιχειρηματική διαχείριση** μικρών και μεγάλων οργανισμών **να αλληλεπιδράσει με τους διαχειριστές των τεχνολογιών πληροφορικής** και **να σταθεί οδηγός στην ανάπτυξη πρακτικών διαχείρισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο.**

1. Παραδείγματα εξωτερικών απειλών για την ασφάλεια στον κυβερνοχώρο, οι οποίες διαρκώς αυξάνονται, είναι τα κακόβουλα λογισμικά (όπως π.χ. λογισμικό εισβολών, κακόβουλοι κώδικες, exploit kits, worms, Trojans κλπ.), άρνηση υπηρεσιών, άρνηση παροχής υπηρεσιών, παραβιάσεις δεδομένων και άλλα. Για σχετικές ενημερώσεις βλ. π.χ. ENISA Threat Landscape 2014, EL 2014 στη διεύθυνση https://www.enisa.europa.eu

2. Π.χ. κινητά τηλέφωνα, μόντεμ, τερματικά πληρωμών, αυτόματες ενημερώσεις λογισμικού, βιομηχανικά συστήματα ελέγχου, αλληλεπίδραση πωλητή/καταναλωτή, καθώς και το Δίκτυο των Πραγμάτων.

Η βελτίωση της ασφάλειας στον κυβερνοχώρο μίας εταιρείας καθίσταται δυνατή μέσω μίας διαδικασίας διαχείρισης των κινδύνων – με έμφαση στη διαχείριση. Λόγω του διαρκώς μετακινούμενου τοπίου των τεχνολογιών και διανυσμάτων απειλών, τα επιχειρησιακά συστήματα πληροφορικής θα παραμένουν πάντοτε ημιτελή και δεν θα είναι ποτέ απολύτως ασφαλή. Η αποτελεσματική λειτουργία σ' ένα τόσο μεταβαλλόμενο περιβάλλον απαιτεί δέσμευση σε μία μακροπρόθεσμη προσέγγιση της διαχείρισης κινδύνων – χωρίς την ύπαρξη του τελικού σταδίου. Οι υπεύθυνοι διοίκησης των επιχειρήσεων θα παραμένουν απογοητευμένοι με τις πρωτοβουλίες ασφάλειας στον κυβερνοχώρο, εάν δεν προσεγγίσουν το εν λόγω έργο με τις κατάλληλες προσδοκίες για την επικείμενη δράση. Και χωρίς κατάλληλους περιορισμούς, οι εταιρείες μπορούν να καταναλώνουν γρήγορα όλους τους διαθέσιμους πόρους στην προσπάθεια άμβλυνσης των κινδύνων. Η προσπάθεια προσέγγισης της διαχείρισης κινδύνων για την ασφάλεια στον κυβερνοχώρο μέσω μίας διαδικασίας, η οποία επιτρέπει σε μία εταιρεία να κατανοήσει και να κατατάσσει σε σειρά προτεραιότητας ό,τι είναι σημαντικό για την εταιρεία (υλικά και πληροφοριακά στοιχεία), είναι ουσιαστικής σημασίας.

Έχει μεγάλη σημασία να γνωρίζει κανείς ότι **δίχως κατάλληλες προφυλάξεις, το Διαδίκτυο, τα επιχειρησιακά πληροφοριακά δίκτυα και οι συσκευές δεν είναι ασφαλή.** Τα σύγχρονα επιχειρησιακά πληροφοριακά συστήματα βρίσκονται στο στόχαστρο πληθώρας κακόβουλων παραγόντων. Μία χρήσιμη ιδέα για τη δημιουργία προσδοκιών όσων εμπλέκονται στη διαχείριση κινδύνων για την ασφάλεια στον κυβερνοχώρο αποτελεί μία απλή ρήση: «Εάν κάτι που έχει αξία διατίθεται στο διαδίκτυο, τίθεται σε κίνδυνο και είναι πιθανό να διαρρεύσει». Ευτυχώς, κάτι που έχει αξία για έναν κακόβουλο φορέα δεν σημαίνει ότι συμφωνεί πάντα με στοιχεία (όπως π.χ. χρήματα, επιχειρηματικά μυστικά και πληροφορίες για τους πελάτες), τα οποία θεωρούνται πολύτιμα για την εταιρεία σας. Ενώ υπάρχουν τεχνικές και διαδικασίες, οι οποίες μπορούν να βοηθήσουν να μειωθεί ο κίνδυνος διαρροής, ένας αποφασισμένος κακόβουλος φορέας επωφελείται από την αδύναμη σύνδεση των διασυνδεδεμένων συστημάτων. Υφίσταται πληθώρα δυνητικών σημείων αδυναμίας (εταιρικής, ανθρώπινης, καθώς και τεχνικής φύσεως) σε ολόκληρη την εταιρεία. Παρά την όποια καλή δουλειά των προμηθευτών τεχνολογικών προϊόντων, των παρόχων υπηρεσιών και των υπαλλήλων εντός των εταιρειών σας, δεν υφίσταται απόλυτη ασφάλεια. Ως εκ τούτου, οι διαδικασίες διαχείρισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο πρέπει να αξιολογήσουν τις μοναδικές απειλές κατά των εταιρειών σας, καθώς και τις αδυναμίες αυτών, και να τις ευθυγραμμίσουν με τα στοιχεία της εταιρείας που έχουν βασική προτεραιότητα. Παρά τις δυσοίωνες προοπτικές που περιγράφονται παραπάνω, εταιρίες κάθε μεγέθους είναι σε θέση να αναπτύξουν και να καλλιεργήσουν ουσιώδεις οργανωτικές ικανότητες με σκοπό την επιτυχή διαχείριση των κινδύνων για την ασφάλεια του κυβερνοχώρου.

- Πρώτον, τα τμήματα διοίκησης των επιχειρήσεων πρέπει να

πραγματοποιήσουν μια ανάλυση κινδύνων για την εταιρεία τους και να κατατάξουν κατά σειρά προτεραιότητας τα «περιουσιακά» εκείνα στοιχεία που χρήζουν μεγαλύτερης προστασίας.

- Δεύτερον, η ηγεσία είναι απαραίτητη ώστε να αναλάβει αναγκαία δράση και να διασφαλίσει την εφαρμογή εκ μέρους της εταιρείας ορθών πρακτικών ασφάλειας πληροφοριών.
- Τρίτον, οι εταιρίες πρέπει να είναι προετοιμασμένες να εντοπίσουν και να αντιμετωπίσουν – εσωτερικά και εξωτερικά – γεγονότα στον κυβερνοχώρο μέσω θεσμικών οργανωτικών διαδικασιών.

Οι δράσεις αντιμετώπισης θα απαιτήσουν ενισχυμένη επικοινωνία μεταξύ ομολόγων, σχετικών κυβερνητικών φορέων, πελατών ακόμα και ανταγωνιστών. Η προετοιμασία πριν από οιοδήποτε περιστατικό στον κυβερνοχώρο θα διασφαλίσει ότι το αρχικό πρόβλημα δεν επιδεινώνεται από λάθη που έγιναν κατά την απόκριση και τα οποία μπορεί να προληφθούν. Τέλος, μηχανισμοί για να αντληθούν διδάγματα από συμβάντα στον κυβερνοχώρο και να τροποποιηθούν πρακτικές κρίνονται ουσιώδεις ώστε να επιφέρουν απαραίτητες θεσμικές αλλαγές για τη γνωστοποίηση των ορθών πρακτικών διαχείρισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο σε όλη την επιχείρηση.

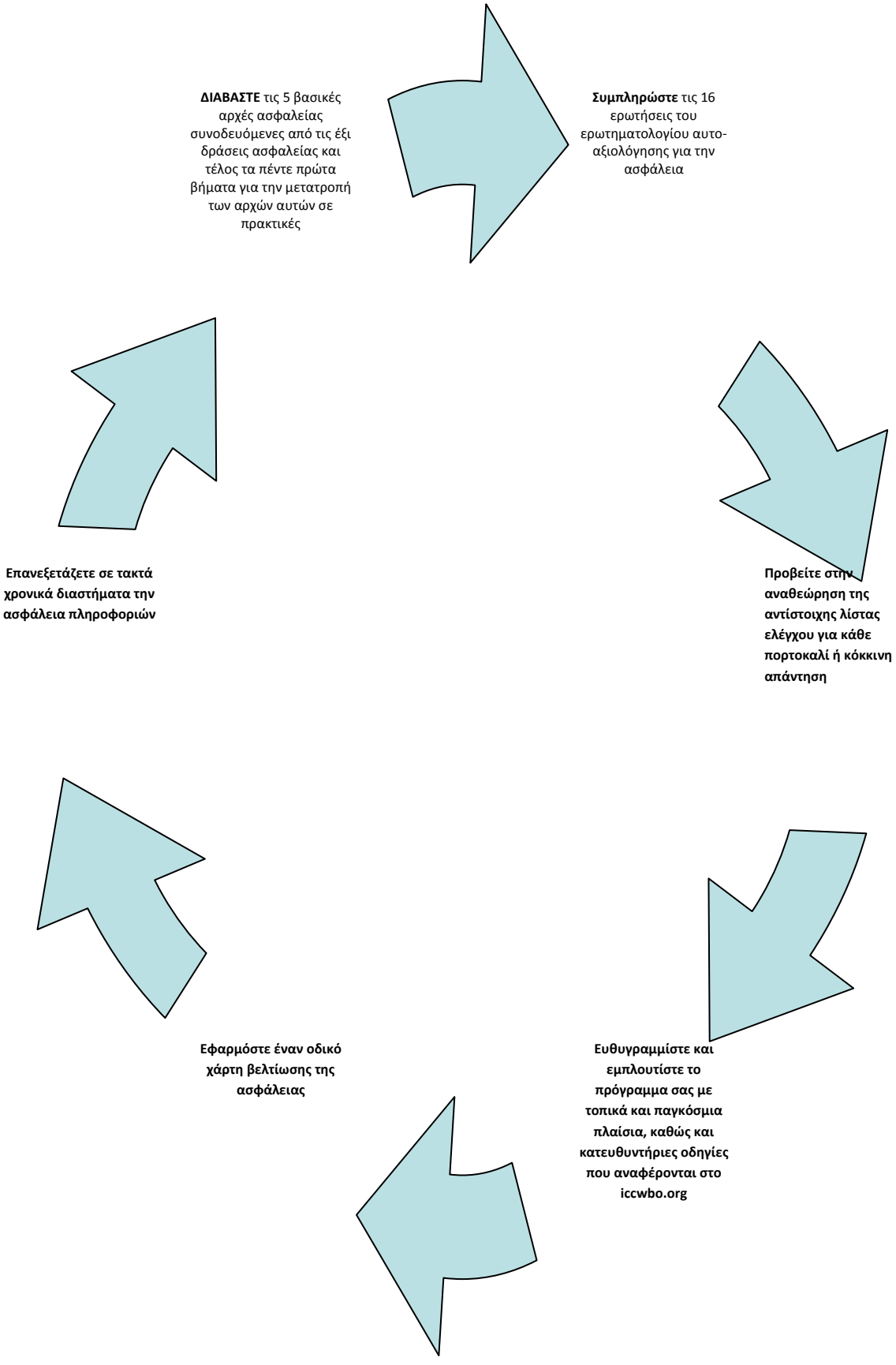
ΧΡΗΣΙΜΟΠΟΙΩΝΤΑΣ ΤΟΝ ΟΔΗΓΟ

Την τελευταία δεκαετία, κυβερνήσεις, επιχειρήσεις και ιδιώτες ανέπτυξαν πολυάριθμες πρακτικές για την αντιμετώπιση των προκλήσεων ασφάλειας πληροφοριών στον κυβερνοχώρο. Υφίστανται τόσα πολλά έγγραφα και κατευθυντήριες οδηγίες που καθίσταται δύσκολο να αναγνωρίσει κανείς τι πρέπει να πρωτοδιαβάσει και ποιο από τα εν λόγω έγγραφα είναι το πλέον κατάλληλο για την επιχείρηση σας. Το μέγεθος του διαθέσιμου υλικού είναι ιδιαιτέρως σημαντικό (με αυξημένη ακρίβεια):

- **Κατευθυντήριες γραμμές** – υψηλού επιπέδου εταιρικά οράματα, τα οποία εξετάζουν την ασφάλεια στον κυβερνοχώρο και παρέχουν έναν χάρτη για επιχειρήσεις και ιδιώτες. Παραδείγματα: Κατευθυντήριες Γραμμές του ΟΟΣΑ για την Ασφάλεια κλπ.
- **Εθνικές στρατηγικές –** Τα εν λόγω έγγραφα, τα οποία συχνά βασίζονται στις κατευθυντήριες γραμμές, διατυπώνουν μια προσέγγιση της ασφάλειας στον κυβερνοχώρο προσαρμοσμένη σ' ένα συγκεκριμένο εθνικό ή νομικό πλαίσιο. Παραδείγματα: Διεθνής Στρατηγική για την Ασφάλεια στον Κυβερνοχώρο[3], εθνικές στρατηγικές από την Ευρώπη και άλλες χώρες, κλπ.
- **Πλαίσια** – Προκειμένου οι εθνικές στρατηγικές να προχωρήσουν στο επόμενο στάδιο, τα διάφορα πλαίσια συλλέγουν έναν κατάλογο ιεραρχημένων και αξιολογημένων πηγών που βοηθούν τις επιχειρήσεις να αντιπαραβάλουν την ωριμότητα και την πρόοδο, που επιδεικνύουν στο πλαίσιο αντιμετώπισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο. Παραδείγματα: Πλαίσιο για την Ασφάλεια στον Κυβερνοχώρο του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST)[5], κλπ.
- **Πρότυπα Πρακτικής** – Έγγραφα, τα οποία καθοδηγούν και διέπουν τις οργανωτικές διαδικασίες με σκοπό τη διασφάλιση της εύρωστης και συνεκτικής λειτουργίας των ορθών πρακτικών για την ασφάλεια στον κυβερνοχώρο. Παραδείγματα: Πρότυπα διαδικασιών ISO 27001, 27002, 27032 πρότυπα διαδικασιών, πρότυπα ασφαλείας PSI, κλπ.
- **Τεχνικά πρότυπα** – Λεπτομερείς προδιαγραφές για την εφαρμογή διεπαφών για την κάλυψη συγκεκριμένων τύπων απαιτήσεων διαλειτουργικότητας. Παραδείγματα: HTTPS, AES, EMV, πρότυπα πληρωμών PCI, κλπ.

Καταρχάς, ο παρών σαφής οδηγός, ο οποίος είναι πλήρως ενημερωμένος με κατευθυντήριες οδηγίες για την ασφάλεια στον κυβερνοχώρο και εθνικές στρατηγικές από όλον τον κόσμο προσφέρει στις επιχειρήσεις ένα πρότυπο για την εξέταση του ζητήματος της online ασφάλειας – αρχής

γενομένης με ένα σύνολο **πέντε αρχών** για εταιρείες κάθε μεγέθους καθώς προσεγγίζουν τους κινδύνους για την ασφάλεια στον κυβερνοχώρο. Δεύτερον, ο παρών οδηγός προσδιορίζει **έξι βασικές δράσεις**, τις οποίες οι εταιρείες πρέπει να βεβαιωθούν ότι θα τις αναλάβουν, αντλώντας υλικό από διάφορες πηγές και ορθές πρακτικές. Ο οδηγός, εν συνεχεία, αναφέρεται στον τρόπο, **με τον οποίο οι αρχικές πέντε αρχές θα εφαρμοστούν στις πολιτικές**, με σκοπό την καθοδήγηση της ανάπτυξης δραστηριοτήτων διαχείρισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο εκ μέρους των επιχειρήσεων. Ένα διαρκώς εξελισσόμενο ψηφιακό παράρτημα με πηγές για τη συμπλήρωση των παρόντων κατευθυντήριων γραμμών χρησιμεύει ως «ζωντανή» πηγή άντλησης πληροφοριών για την παροχή περαιτέρω ειδικών συμβουλών καθώς τα εν λόγω εργαλεία αναπτύσσονται – από πρότυπα πρακτικής έως τεχνικά πρότυπα και άλλα. Ενώ απόλυτη ασφάλεια δεν υφίσταται, τα σχέδια διαχείρισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο που περιγράφονται θα βοηθήσουν τις εταιρείες να σταθούν στο ύψος των προκλήσεων της ασφάλειας πληροφοριών σε αυτό το διαρκώς μεταβαλλόμενο περιβάλλον. Δεν πρόκειται, ωστόσο, για έναν απλό Οδηγό που θα προσδώσει μεμονωμένα αξία στις επιχειρήσεις, αλλά για έναν οδηγό που πρέπει να τον κοινοποιήσουν οι επιχειρήσεις σε όλο το εύρος των ποικίλων σχέσεων τους με σκοπό την καλύτερη διασφάλιση όλων των σημείων εισόδου και ανταλλαγής με τα συστήματα και τις δραστηριότητες τους.


ΔΙΑΒΑΣΤΕ τις 5 βασικές αρχές ασφαλείας συνοδευόμενες από τις έξι δράσεις ασφαλείας και τέλος τα πέντε πρώτα βήματα για την μετατροπή των αρχών αυτών σε πρακτικές
Συμπληρώστε τις 16 ερωτήσεις του ερωτηματολογίου αυτο-αξιολόγησης για την ασφάλεια
Προβείτε στην αναθεώρηση της αντίστοιχης λίστας ελέγχου για κάθε πορτοκαλί ή κόκκινη απάντηση
Ευθυγραμμίστε και εμπλουτίστε το πρόγραμμα σας με τοπικά και παγκόσμια πλαίσια, καθώς και κατευθυντήριες οδηγίες που αναφέρονται στο iccwbo.org
Εφαρμόστε έναν οδικό χάρτη βελτίωσης της ασφάλειας
Επανεξετάζετε σε τακτά χρονικά διαστήματα την ασφάλεια πληροφοριών

ΒΑΣΙΚΕΣ ΑΡΧΕΣ ΑΣΦΑΛΕΙΑΣ

Ενώ οι προσεγγίσεις της ασφάλειας πληροφοριών μπορεί να διαφέρουν από εταιρεία σε εταιρεία ανάλογα με μία σειρά παραγόντων[6], υφίσταται μία σειρά αρχών υψηλού επιπέδου που παρέχουν πληροφορίες για την πρακτική ασφάλειας έγκυρων πληροφοριών για όλες τις εταιρείες, ανεξαρτήτως μεγέθους ή επιχειρηματικού κλάδου. Ο παρών οδηγός παρουσιάζει **πέντε βασικές αρχές** σε δύο κατηγορίες:

Α. Όραμα και νοοτροπία

Β. Οργάνωση και διαδικασίες

Οι εν λόγω αρχές συνοδεύονται από ένα σύνολο έξι σημαντικών **δράσεων ασφαλείας** και, εν συνεχεία, από **πέντε στοιχεία εκκίνησης με σκοπό την εφαρμογή των εν λόγω αρχών** και την ενίσχυση των εταιρικών πολιτικών για την ασφάλεια πληροφοριών.

Συλλογικά, οι προτεινόμενες αρχές και δράσεις του παρόντος οδηγού στοχεύουν στη βελτίωση της ανθεκτικότητας των εταιρειών απέναντι σε απειλές του κυβερνοχώρου και στον περιορισμό των διαταραχών που σχετίζονται με τις παραβιάσεις ασφαλείας.

Α. ΟΡΑΜΑ ΚΑΙ ΝΟΟΤΡΟΠΙΑ

Αρχή 1: Επικεντρωθείτε στην πληροφορία και όχι στην τεχνολογία.

Είστε η πρώτη γραμμή άμυνας της εταιρείας ενάντια στις απειλές του κυβερνοχώρου και θα βοηθήσετε στον καθορισμό της προσέγγισης της εταιρείας σας όσον αφορά στην ασφάλεια πληροφοριών. Για να γίνει αυτό, σκεφτείτε την ασφάλεια πληροφοριών με την ευρύτερή της έννοια, όχι μόνο στο πλαίσιο των τεχνολογιών πληροφορικής.

Η ασφάλεια πληροφοριών είναι ένας συνδυασμός ανθρώπων, μεθόδων και τεχνολογίας, ένα θέμα σε επίπεδο επιχειρήσεων, όχι μόνο ένα θέμα των Τεχνολογιών Πληροφορικής. Η εφαρμογή μέτρων ασφαλείας δεν θα πρέπει να περιορίζεται στα τμήματα IT, αλλά αντιθέτως να αντανακλάται απ' άκρη σ' άκρη στην εταιρία σε όλες τις υποδομές της. Το πεδίο εφαρμογής και το όραμα της ασφάλειας πληροφοριών περιλαμβάνει συνεπώς ανθρώπους, προϊόντα, μονάδες, μεθόδους, πολιτικές, διαδικασίες, συστήματα, τεχνολογίες, συσκευές, δίκτυα και πληροφορίες.

Οι άνθρωποι είναι το κλειδί. Ο καθορισμός και η διαχείριση τρωτών σημείων και απειλών των πληροφοριακών περιουσιακών στοιχείων μπορεί να είναι ένα τεράστιο έργο. Ωστόσο, με βάση την εμπειρία[7], 35% των συμβάντων ασφάλειας είναι αποτέλεσμα ανθρώπινου λάθους παρά προμελετημένες επιθέσεις. Από τα συμβάντα ασφάλειας που απομένουν, παραπάνω από τα μισά είναι αποτέλεσμα

προμελετημένης επίθεσης, η οποία **θα μπορούσε να έχει αποφευχθεί**, εάν οι άνθρωποι είχαν χειριστεί τις πληροφορίες με πιο ασφαλή τρόπο.

Εστιάστε στις προσπάθειες για την ασφάλεια, ειδικά όσον αφορά στην προστασία των πιο πολύτιμων πληροφοριών και συστημάτων σας, όπου η απώλεια της εμπιστευτικότητας, της ακεραιότητας ή της ικανότητας θα έβλαπτε σοβαρά την εταιρία σας. Αυτό δεν σημαίνει ότι άλλα πληροφοριακά περιουσιακά στοιχεία θα πρέπει να αγνοηθούν όσον αφορά στην ασφάλεια. Σημαίνει ότι μία προσέγγιση βάσει κινδύνου, που εστιάζει στα κύρια πλεονεκτήματα του οργανισμού είναι μία αποδοτική και αποτελεσματική προσέγγιση της ασφάλειας πληροφοριών στην πράξη. Την ίδια στιγμή αναγνωρίζεται ότι η εξάλειψη του κινδύνου κατά 100% είναι είτε αδύνατη είτε αχρείαστη εάν συγκριθεί με τα σχετικά κόστη.

[6] Συμπεριλαμβανομένης της φύσης της επιχείρησης, του επιπέδου των κινδύνων, των περιβαλλοντικών παραγόντων, κανονιστικών απαιτήσεων και του μεγέθους της εταιρίας, μεταξύ πολλών άλλων.

[7] ΕΥ – Παγκόσμια Έρευνα Ασφάλειας Πληροφοριών 2012 – Αγώνας για να καλυφθεί το χάσμα.

Στόχο πρέπει να αποτελεί η ανθεκτικότητα της εταιρίας στον κίνδυνο απώλειας ή καταστροφής των πληροφοριών. Οι εταιρίες υπόκεινται σε πολλούς νόμους και κανονισμούς, πολλοί από τους οποίους απαιτούν εφαρμογή κατάλληλων ελέγχων ασφαλείας. Η συμμόρφωση με τους εν λόγω νόμους, κανονισμούς και πρότυπα μπορεί να οδηγήσει σε βελτιωμένη ασφάλεια πληροφοριών. Παρ' όλα αυτά, μπορεί επίσης να οδηγήσει σε εφησυχασμό μόλις επιτευχθούν οι στόχοι συμμόρφωσης. Οι απειλές ασφαλείας αλλάζουν πολύ γρηγορότερα από τους νόμους και τους κανονισμούς, δημιουργώντας έναν κινούμενο στόχο για τις δραστηριότητες διαχείρισης των κινδύνων. Ως αποτέλεσμα, οι υπάρχουσες επιχειρηματικές πολιτικές και διαδικασίες μπορεί να καταστούν ξεπερασμένες ή απλά αναποτελεσματικές στην πράξη.

Η περιοδική αξιολόγηση της ανθεκτικότητας της εταιρίας απέναντι σε απειλές στον κυβερνοχώρο και σε τρωτά σημεία είναι ουσιώδης, ώστε να μπορεί να μετρηθεί η πρόοδος για τους στόχους διαχείρισης των κινδύνων και η προστασία των δραστηριοτήτων για την ασφάλεια στον κυβερνοχώρο. Οι δραστηριότητες αξιολόγησης μπορούν να επιτευχθούν μέσω εσωτερικών και/ή ανεξάρτητων αξιολογήσεων και ελέγχων, συμπεριλαμβανομένων μέτρων, όπως δοκιμές διείσδυσης και ανίχνευσης επιθέσεων.

Η ευθύνη για την ασφάλεια στον κυβερνοχώρο πρέπει να υπερβαίνει το τμήμα IT της εταιρείας. Τα δε ενδιαφερόμενα μέρη θα πρέπει να ασχοληθούν με τον εντοπισμό του προβλήματος, αλλά μακροπρόθεσμα επίσης και με την εφαρμογή ενός υγιούς οικοσυστήματος στον οργανισμό. Ωστόσο, η πραγματική αξία της περιοδικής επιχειρηματικής ανασκόπησης υλοποιείται όταν η διαδικασία χρησιμοποιείται για να βελτιώσει την εταιρική κουλτούρα και την νοοτροπία των υπαλλήλων απέναντι στις πρακτικές διαχείρισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο.

Η στροφή σε ανθεκτικά συστήματα πληροφορικής κρίνεται επιτακτική σε χρονικές περιόδους, κατά τις οποίες οι επιχειρήσεις υιοθετούν νέες λύσεις και συσκευές. Κατά τη διάρκεια της εν λόγω περιόδου, πρέπει να ληφθούν, όσο το δυνατόν ταχύτερα, τα κατάλληλα μέτρα ασφαλείας στη φάση της υιοθέτησης, ιδανικά για τον προσδιορισμό των επιχειρηματικών αναγκών. Μία τέτοια «σχεδιασμένη ασφάλεια» μπορεί να δώσει τη δυνατότητα στους υπαλλήλους, που προβαίνουν σε καινοτομίες εντός της εταιρείας, να στοχεύσουν στη διαχείριση των κινδύνων για την ασφάλεια πληροφοριών.

Β. ΟΡΓΑΝΩΣΗ ΚΑΙ ΔΙΑΔΙΚΑΣΙΕΣ

Αρχή 3. Να είστε έτοιμοι να ανταποκριθείτε

Ακόμα και η πιο καλά προστατευμένη επιχείρηση θα αντιμετωπίσει κάποια στιγμή μία παραβίαση ασφάλειας πληροφοριών. Ζούμε σε ένα περιβάλλον όπου το ερώτημα είναι το **πότε** και όχι το **εάν**. Επομένως, ο τρόπος με τον οποίο η επιχείρηση **ανταποκρίνεται** σε μία παραβίαση είναι το σημείο, στο οποίο **εσείς** θα αξιολογηθείτε.

Για να ελαχιστοποιηθεί ο επιχειρηματικός αντίκτυπος από περιστατικά ασφάλειας στον κυβερνοχώρο, οι επιχειρήσεις πρέπει, πέρα από τα τεχνικά μέτρα ανταπόκρισης, να αναπτύξουν σχέδια οργανωτικής ανταπόκρισης. Ένα σχέδιο ανταπόκρισης θα πρέπει να θεσπίσει κατευθυντήριες γραμμές για να βοηθήσει τους υπεύθυνους διαχείρισης να κατανοήσουν πότε θα πρέπει να εμπλέξουν ειδικευμένα τρίτα μέρη για να βοηθήσουν στον περιορισμό και την αντιμετώπιση ενός περιστατικού ασφαλείας, και πότε είναι σκόπιμο να επικοινωνήσουν με άλλα εξωτερικά μέρη (συμπεριλαμβανομένων αρχών επιβολής του νόμου ή υπηρεσίες υπό κρατική εποπτεία). Υπενθυμίζεται ότι η προσφυγή στις αρμόδιες αρχές είναι ένας τρόπος να βελτιωθεί συνολικά το τοπίο της ασφάλειας και σε ορισμένες περιπτώσεις μπορεί να είναι υποχρεωτικό, προκειμένου να αποφευχθούν τυχόν κανονιστικές παραβιάσεις και η ενδεχόμενη επιβολή προστίμων. Η επιτυχής διαχείριση ανταπόκρισης συμβάντος περιλαμβάνει μία επικοινωνιακή στρατηγική (εσωτερική και εξωτερική), η οποία μπορεί να κάνει τη διαφορά μεταξύ του να καταλήξει η επιχείρηση τίποτα περισσότερο από ένας ντροπιαστικός τίτλος στα πρωτοσέλιδα των εφημερίδων ή να αποτελέσει μία επιτυχημένη περίπτωση μελέτης στο πρόγραμμα σπουδών ενός Πανεπιστημίου.

Ενώ οι δράσεις για την εσωτερική διαχείριση κινδύνων είναι ουσιαστικές, μη ξεχνάτε επίσης να αφιερώνετε χρόνο για να έρθετε σε επαφή με ομολόγους και εταίρους όλου του επιχειρηματικού φάσματος της εταιρείας σας, την ευρύτερη επιχειρηματική κοινότητα και με τις αρχές επιβολής του νόμου, ώστε να βοηθήσετε στη διατήρηση και κατανόηση των τρεχόντων και αναδυόμενων απειλών, καθώς και να οικοδομήσετε σχέσεις, στις οποίες μπορείτε να βασιστείτε κατά τη διάρκεια ενός περιστατικού.

Αρχή 4: Επιδείξτε αρχηγική βούληση

Προκειμένου η διοίκηση των επιχειρήσεων να διαχειριστεί την ασφάλεια πληροφοριών αποτελεσματικά και αποδοτικά, πρέπει να κατανοήσει και να υποστηρίξει τις δράσεις διαχείρισης των κινδύνων ως ουσιαστικό στοιχείο για την επιτυχία της εταιρίας σας. **Εσείς** και η διευθυντική ομάδα σας θα πρέπει να εμπλακείτε εμφανώς στη διαχείριση και εποπτεία των εταιρικών σας πολιτικών διαχείρισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο. Πρέπει να διασφαλιστεί ότι οι επαρκείς πόροι – ανθρώπινοι και οικονομικοί – διοχετεύονται για την προστασία των περιουσιακών στοιχείων της εταιρίας. Ωστόσο, μόνον οι πόροι δεν επαρκούν. Ένα Τμήμα ασφάλειας πληροφοριών για επιχειρήσεις, μικρές και μεγάλες, εξουσιοδοτείται να ενεργοποιήσει την ανταπόκριση σε όλο το εύρος της εταιρίας απέναντι σε απειλές και τρωτά σημεία στον κυβερνοχώρο.

Επίσημες εκθέσεις αναφορικά με την αποτελεσματικότητα και την επάρκεια των μέτρων ασφαλείας πληροφοριών της εταιρείας πρέπει να συντάσσονται και να υποβάλλονται στο ανώτερο στέλεχος που είναι υπεύθυνο για τη διαχείριση της εταιρίας σας, και τουλάχιστον μία φορά το χρόνο στην διευθυντική ομάδα, τους ελεγκτές, και το διοικητικό συμβούλιο. Σε τακτή χρονική βάση οι εν λόγω εκθέσεις– οι οποίες βασίζονται σε διάφορους δείκτες ασφαλείας και μετρήσεις – θα συνδράμουν στην καλύτερη πληροφόρηση με σκοπό τη λήψη αποφάσεων για την πολιτική και τις επενδύσεις της ασφάλειας πληροφοριών, και θα παρέχουν σαφή εικόνα για το πόσο καλά προστατεύει η εταιρία σας τα περιουσιακά της στοιχεία.

Αν και συχνά αναφέρονται ως *ο αδύναμος κρίκος* όταν πρόκειται για την ασφάλεια πληροφοριών – εκπαιδεύστε τους ανθρώπους σας στο να γίνουν *το πολυτιμότερο περιουσιακό στοιχείο για την ορθή ασφάλεια*, αυξάνοντας την ευαισθητοποίηση στο θέμα της ασφάλειας πληροφοριών, γεγονός που θα οδηγήσει σε αποτελεσματικότερες δεξιότητες.

Αρχή 5: Ενεργείστε σύμφωνα με το όραμά σας

Η ανάγνωση απλώς του παρόντος οδηγού δεν επαρκεί. Πρέπει να μετατρέψετε σε πράξη το ξεχωριστό εταιρικό σας όραμα για τη διαχείριση των κινδύνων για την ασφάλεια στον κυβερνοχώρο με τη δημιουργία (ή την αναθεώρηση) ποικίλων πολιτικών ασφάλειας πληροφοριών. Οι εταιρικές πολιτικές ασφάλειας πληροφοριών παρέχουν μία βάση αναφοράς, η οποία θα αποτελέσει έναν οδηγό για τις δράσεις για την ασφάλεια σε ολόκληρη την εταιρεία, για όλες τις επιχειρηματικές μονάδες και το προσωπικό της, ενώ

παράλληλα θα συνδράμει στην αύξηση της ευαισθητοποίησης σε θέματα ασφαλείας σε ολόκληρη την εταιρία.

Τυπικά, ένα έγγραφο πολιτικής ασφαλείας και οι συμπληρωματικές του κατευθυντήριες γραμμές και πρότυπα συνδυάζονται σε ένα πλαίσιο πολιτικής ασφάλειας πληροφοριών, το οποίο στη συνέχεια μεταφράζεται σε φυσιολογικές επιχειρησιακές διαδικασίες. Παρ' όλα αυτά, με την αυξανόμενη αποδοχή και ένταξη τρίτων φορέων παροχής υπηρεσιών στις αλυσίδες αξιών της επιχείρησης, οι επιχειρήσεις πρέπει να κατανοήσουν τον τρόπο ροής και αλληλεξάρτησης των πληροφοριακών περιουσιακών τους στοιχείων μεταξύ διαφόρων εξωτερικών τρίτων φορέων. Εάν ένα τρίτο μέρος δεν προστατεύει επαρκώς τις πληροφορίες σας (ή τα συστήματα πληροφορικής τους, στα οποία βασίζεστε) **το δικό τους** συμβάν ασφαλείας μπορεί να αποτελέσει σοβαρή ευθύνη **για τις δικές σας** επιχειρηματικές δραστηριότητες, τη φήμη και την εμπορική αξία σας. Ενθαρρύνετε τους προμηθευτές σας να υιοθετούν, τουλάχιστον, τις πληροφορίες και τις αρχές ασφάλειας πληροφοριών που εφαρμόζονται στην εταιρία σας. Όπου δε κρίνεται απαραίτητο, να διενεργείτε ελέγχους ή να ζητείτε από τους παρόχους υπηρεσιών να σας περιγράψουν λεπτομερώς τις δικές τους πρακτικές για την ασφάλεια πληροφοριών, ώστε να λαμβάνετε επιπλέον διαβεβαίωση για τις επιχειρηματικές πρακτικές τους.

Τα τρίτα μέρη δεν αποτελούν αποκλειστικά και μόνο πηγή κινδύνων. Ορισμένοι τρίτοι φορείς μπορεί να βοηθήσουν στον περιορισμό των κινδύνων και να σας δώσουν τη δυνατότητα να επιτύχετε τους σημαντικούς σας στόχους αναφορικά με τη διαχείριση των κινδύνων για την ασφάλεια στον κυβερνοχώρο. Οι πάροχοι τεχνολογικών υπηρεσιών της πληροφορικής μπορούν να συμβάλλουν στη βελτίωση των υποδομών διαχείρισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο, μέσω αξιολογήσεων ασφαλείας και ελέγχων, καθώς και μέσω της χρήσης συσκευών για την ασφάλεια πληροφοριών, λύσεων ή υπηρεσιών, είτε επί τόπου με εξωτερική διαχείριση είτε με υποδομές Cloud[8]

[8] Οι υπηρεσίες cloud σας παρέχουν τη δυνατότητα να χρησιμοποιείτε έναν εξωτερικό πάροχο υπηρεσιών για την αποθήκευση, επεξεργασία ή διαχείριση δεδομένων μέσω ενός δικτύου, όπως π.χ. το Διαδίκτυο, με πολύ μεγάλο βαθμό ευελιξίας και παρακολούθησης σε πραγματικό χρόνο.

ΕΞΙ ΒΑΣΙΚΕΣ ΔΡΑΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

Ο παρών κατάλογος δράσεων αποτελεί ένα σύνολο πρακτικών βημάτων, τα οποία επιχειρήσεις κάθε μεγέθους μπορούν να ακολουθήσουν για να μειώσουν τους κινδύνους που σχετίζονται με συμβάντα ασφαλείας στον κυβερνοχώρο. Χωρίς να είναι απολύτως πλήρης ή εκτενής, διασφαλίζοντας, ωστόσο, ότι η επιχείρησή σας θα ασκήσει τις εν λόγω δράσεις, ο εν λόγω κατάλογος θα τοποθετήσει την εταιρεία σας σε μια πορεία προς την πλεονεκτικότητα της ασφάλειας πληροφοριών. Θα πρέπει να θυμάστε ότι η διαχείριση κινδύνων για την ασφάλεια πληροφοριών στον κυβερνοχώρο είναι μία συνεχής διαδικασία. Αφού προηγουμένως βεβαιωθείτε ότι οι εν λόγω δράσεις διεξάγονται με επιτυχία, επισκεφτείτε τη διαδικτυακή πύλη που σχετίζεται με τον παρόντα οδηγό και εντοπίστε πρότυπα και πηγές που θα σας βοηθήσουν να πραγματοποιήσετε περαιτέρω βήματα για να αυξήσετε την ανθεκτικότητα του προγράμματος ασφάλειας πληροφοριών σας.

Δράση 1: Δημιουργείστε αντίγραφα ασφαλείας πληροφοριών της επιχείρησης. Επικυρώστε τη διαδικασία επαναφοράς.

Διασφαλίστε ότι οι πληροφορίες της επιχείρησής σας είναι προστατευμένες δημιουργώντας εφεδρικά αντίγραφα– προτού η επιχείρησή σας υποστεί παραβίαση ασφαλείας, όπου οι πληροφορίες έχουν κλαπεί, μεταβληθεί, διαγραφεί ή χαθεί. Η δημιουργία μόνο αντιγράφων ασφαλείας δεν επαρκεί[9]. Η σωστή διαχείριση της διαδικασίας δημιουργίας εφεδρικών αντιγράφων περιλαμβάνει την επικύρωση του περιεχομένου των επιχειρηματικών δεδομένων και πληροφοριών που περιέχονται στα αρχεία αντιγράφων ασφαλείας, καθώς και τον έλεγχο της διαδικασίας επαναφοράς. Εάν για την αποθήκευση πληροφοριών χρησιμοποιούνται τρίτα μέρη (π.χ. υπηρεσίες cloud), διασφαλίστε ότι τα αντίγραφα ασφαλείας έχουν προβλεφθεί και για αυτές τις πληροφορίες.

Μην ξεχνάτε ότι τα φυσικά μέσα, όπως δίσκοι, κασέτες ή σκληροί δίσκοι που χρησιμοποιούνται για την αποθήκευση των δεδομένων των αντιγράφων ασφαλείας, είναι επίσης ευάλωτα στους κινδύνους. Τα μέσα δημιουργίας αντιγράφων ασφαλείας πρέπει να απολαμβάνουν το ίδιο επίπεδο προστασίας με την πηγή των δεδομένων, ιδίως σε ότι αφορά στην προσωπική ασφάλεια, εφόσον αυτά τα αντικείμενα είναι ιδιαιτέρως εύκολο να μεταφερθούν.

Δράση 2: Επικαιροποιήστε τα συστήματα τεχνολογίας της πληροφορικής

Συστήματα και λογισμικά κάθε είδους, συμπεριλαμβανομένου του εξοπλισμού δικτύων και συσκευών, θα πρέπει να επικαιροποιούνται αμέσως μόλις καθίστανται διαθέσιμες οι ενημερώσεις ασφαλείας (patches) και οι αναβαθμίσεις λογισμικών (firmware upgrades). Οι εν λόγω αναβαθμίσεις και ενημερώσεις ασφαλείας διορθώνουν τα τρωτά σημεία του συστήματος, τα οποία μπορούν να καταχραστούν οι «επιτιθέμενοι». Πολλές επιτυχημένες παραβιάσεις είναι αποτέλεσμα ευπαθειών του συστήματος, όπου οι επικαιροποιήσεις είναι διαθέσιμες, συχνά ακόμα και πάνω από ένα χρόνο πριν από το συμβάν.

[9] Η διαδικασία δημιουργίας αντιγράφων ασφαλείας είναι μια τεχνική διαδικασία, την οποία πρέπει κανείς να διαχειριστεί με ιδιαίτερη προσοχή. Για παράδειγμα, μόνο η χρήση διαφόρων ταυτόχρονα συνδεδεμένων αποθετηρίων στο ίδιο μέρος είναι αναποτελεσματική σαν διαδικασία δημιουργίας αντιγράφων ασφαλείας. Μία αποτελεσματική πολιτική δημιουργίας αντιγράφων ασφαλείας θα πρέπει να λαμβάνει υπόψη πολλαπλούς τύπους κινδύνων, συμπεριλαμβανομένων, μεταξύ άλλων, της απώλειας δεδομένων, καθώς και της απώλεια της λειτουργικής τοποθεσίας, γεγονός που προϋποθέτει τα αντίγραφα ασφαλείας να βρίσκονται off-site.

Εάν είναι δυνατό, χρησιμοποιήστε υπηρεσίες αυτόματων ενημερώσεων. Ειδικά για συστήματα ασφαλείας, όπως εφαρμογές anti-malware, εργαλεία φιλτραρίσματος διαδικτύου και συστήματα ανίχνευσης εισβολών. Οι διαδικασίες αυτόματων ενημερώσεων μπορούν να βοηθήσουν ώστε να διασφαλιστεί ότι οι χρήστες κάνουν χρήση έγκυρων ενημερώσεων ασφαλείας λογισμικού απευθείας από τον αυθεντικό πάροχο.

Δράση 3: Επενδύστε στην κατάρτιση.

Η καλλιέργεια της θεμελιώδους ευαισθητοποίησης αναφορικά με τις σοβαρές απειλές στον κυβερνοχώρο και τα ζητήματα ασφαλείας είναι ουσιώδης για το προσωπικό σε ολόκληρη την εταιρία σας και θα πρέπει να μην επαναπαύεστε. Η εκπαίδευση διασφαλίζει ότι όλο το προσωπικό, που έχει πρόσβαση στις πληροφορίες και τα συστήματα πληροφορικής, κατανοεί τις καθημερινές του υποχρεώσεις να διαχειρίζεται, να προστατεύει και να υποστηρίζει τις εταιρικές δράσεις για την ασφάλεια πληροφοριών. Χωρίς την κατάλληλη εκπαίδευση, οι υπάλληλοι μπορεί γρήγορα να μετατραπούν σε πηγή κινδύνων μέσα στην επιχείρηση, δημιουργώντας περιστατικά ασφαλείας ή τρωτά σημεία που οι αντίπαλοι μπορούν να χρησιμοποιήσουν για να παραβιάσουν τα μέτρα ασφάλειας πληροφοριών σας.

Μπορείτε να διαμορφώσετε τη νοοτροπία διαχείρισης των κινδύνων για την ασφάλεια πληροφοριών στην επιχείρησή σας. Η επένδυση στην εκπαίδευση θα ενισχύσει τα μηνύματα προς το προσωπικό για την ασφάλεια πληροφοριών της επιχείρησης σας με το πέρασμα του χρόνου και θα δημιουργήσει επιθυμητά προσόντα και δεξιότητες ασφαλείας στο προσωπικό.

Δράση 4: Παρακολουθείστε το περιβάλλον πληροφοριών σας

Οι επιχειρήσεις πρέπει να αναπτύξουν συστήματα και διαδικασίες για να διασφαλίσουν ότι θα ειδοποιηθούν σε περίπτωση εντοπισμού συμβάντος ασφαλείας πληροφοριών εντός της εταιρείας τους. Πολύ συχνά οι επιχειρήσεις δεν γνωρίζουν για τυχόν παραβιάσεις ασφαλείας. Μερικές επιχειρήσεις βιώνουν παραβιάσεις ή μολύνσεις για μήνες ή χρόνια πριν κάποιος αντιληφθεί την εισβολή. Υπάρχουν ποικίλες τεχνολογικές λύσεις που μπορεί να βοηθήσουν σε αυτό το κομμάτι, συμπεριλαμβανομένων συστημάτων ανίχνευσης και πρόληψης από εισβολές, καθώς και συστημάτων διαχείρισης συμβάντων ασφαλείας. Η απλή εγκατάσταση, ωστόσο, αυτών των λύσεων είναι ανεπαρκής. Η συνεχής παρακολούθηση και ανάλυση των εξόδων από τα εν λόγω συστήματα είναι απαραίτητη ώστε να μπορεί να επωφεληθεί κανείς από τη χρήση της τεχνολογίας.

[10] Οι τελικοί χρήστε μπορούν να βρουν γενικές πληροφορίες για την ευαισθητοποίηση για την ασφάλεια στον Κυβερνοχώρο στο www.staysafeonline.org.http://www.enisa.europa.eu/media/multimedia/material, μια πρωτοβουλία του ENISA. Έχετε το δικαίωμα να χρησιμοποιήσετε κάθε πληροφορία, βίντεο και πληροφοριακό γράφημα για εκπαιδευτικούς σκοπούς εντός της εταιρείας σας.

[11] http://www.verizonenterprise.com/DBIR/

Πολλές επιχειρήσεις ενδέχεται να μην διαθέτουν εσωτερικό εξειδικευμένο προσωπικό ή τους πόρους που απαιτούνται για την παρακολούθηση ζωτικών συστημάτων και διαδικασιών. Υπηρεσίες εσωτερικής (on-site) και εξωτερικής διαχείρισης της ασφάλειας (Managed Security Services) προσφέρονται από διάφορους παρόχους υπό τη μορφή διαφόρων επιχειρηματικών μοντέλων, συμπεριλαμβανομένης της τεχνολογίας και των υπηρεσιών cloud. Βρείτε τη σωστή εφαρμογή για την επιχείρησή σας και αναζητείστε βοήθεια από εξειδικευμένους φορείς για την παροχή συμβουλών και υποστηρικτικών υπηρεσιών για να συμπεριλάβετε τους κατάλληλους όρους στα συμβόλαια σας.

Εάν η εταιρία σας βιώνει ένα συμβάν στον κυβερνοχώρο, εξετάστε το ενδεχόμενο να αναφέρετε τη δραστηριότητα στις αρμόδιες κυβερνητικές υπηρεσίες[12] και κλαδικές ενώσεις. Η επικοινωνία με άλλους μπορεί να σας βοηθήσει να προσδιορίσετε εάν η επιχείρησή σας βιώνει ένα μεμονωμένο περιστατικό ή είναι μέρος ενός μεγαλύτερου συμβάντος στον κυβερνοχώρο[13]. Συχνά, μία τέτοια πρωτοβουλία μπορεί να έχει ως αποτέλεσμα την συγκέντρωση πληροφοριών και συμβουλών που μπορεί να βοηθήσουν την επιχείρηση να λάβει τα κατάλληλα αντίμετρα.

Δράση 5: Επίπεδα άμυνας για τη μείωση των κινδύνων

Η περιμετρική ασφάλεια δικτύου και ο παραδοσιακός έλεγχος πρόσβασης δεν επαρκούν πλέον, ιδίως όταν το εταιρικό σύστημα πληροφορικής συνδέεται με το διαδίκτυο, με παρόχους υπηρεσιών του διαδικτύου, με υπηρεσίες cloud και outsourcing, πωλητές και συνεργάτες, καθώς και φορητές συσκευές, οι οποίες βρίσκονται πέρα από τη δικαιοδοσία και τον έλεγχο της εταιρίας. Η αποτελεσματική προστασία ενάντια στους ιούς, κακόβουλα λογισμικά, συσκευές ή χάκερ απαιτεί αμυντικά μέτρα ώστε να μειωθεί ο κίνδυνος ενός συμβάντος ασφάλειας πληροφοριών. Ο συνδυασμός πολλαπλών τεχνικών[14] για την αντιμετώπιση των κινδύνων ασφάλειας στον κυβερνοχώρο μπορεί να μειώσει σημαντικά την πιθανότητα μια μικρή παραβίαση να εξελιχθεί σε ένα πραγματικό περιστατικό.

Οι πολυεπίπεδες άμυνες ασφάλειας πληροφοριών στοχεύουν στον περιορισμό του βαθμού ελευθερίας που διατίθεται στους αντιπάλους και στην αύξηση των ευκαιριών ανίχνευσης από τα συστήματα παρακολούθησης της επιχείρησης.

Η ασφάλιση κατά των κινδύνων του κυβερνοχώρου μπορεί να αποτελέσει έναν τρόπο για τις εταιρίες να περιορίσουν τις οικονομικές επιπτώσεις ενός τέτοιου συμβάντος, να διαχειριστούν αποτελεσματικά και εκ των προτέρων τυχόν έκθεση τους στον κίνδυνο, καθώς και να ενδυναμώσουν το εταιρικό σύστημα εσωτερικής διαχείρισης κινδύνων.

[12] Τα θύματα των εγκλημάτων (του κυβερνοχώρου) θα πρέπει επίσης να υποβάλουν καταγγελία σε συνεργασία με τους αξιωματούχους των αρμόδιων αρχών επιβολής του νόμου. Η τοπική αστυνομία αποτελεί συνήθως το καταλληλότερο σημείο αναφοράς παραδοσιακών εγκλημάτων. Ωστόσο, τυχόν άλλες αρχές επιβολής του νόμου ενδέχεται να εξειδικεύονται στα εγκλήματα στον κυβερνοχώρο (ηλεκτρονική πειρατεία, δολιοφθορά, κατασκοπεία).

[13] Μία επίθεση μπορεί να είναι οριζόντια (ομοειδείς εταιρίες δέχονται επίθεση) ή κάθετη (υπεργολάβοι δέχονται επίθεση). Ενδέχεται, επίσης, να αποτελεί μία απειλή ασφαλείας που στοχεύει σε συγκεκριμένο σημείο του λογισμικού ή του υλισμικού.

[14] Το φιλτράρισμα του ιστού, η προστασία από ιούς, η προληπτική προστασία από κακόβουλα λογισμικά, το τείχος προστασίας, οι ισχυρές πολιτικές ασφαλείας και η εκπαίδευση των χρηστών είναι ορισμένες μόνο από αυτές.

Δράση 6: Προετοιμαστείτε για τη στιγμή που θα συντελεστεί η παραβίαση

Η διαχείριση των κινδύνων δεν στοχεύει μόνο στη μείωση των πιθανοτήτων, αλλά και στην ελαχιστοποίηση της πιθανής ζημίας εάν προκύψει κάποιο συμβάν. Αυτό συνεπάγεται την προετοιμασία για την γρήγορη διερεύνηση του συμβάντος – διασφαλίζοντας ταυτόχρονα ότι διατίθενται επαρκείς πόροι και ότι τα συστήματα και οι διαδικασίες είναι συντονισμένα να συλλάβουν σημαντικές πληροφορίες. Εάν η παραβίαση είναι η εισχώρηση ενός κακόβουλου προγράμματος, πρέπει να εξολοθρευτεί. Η προετοιμασία επίσης συνεπάγεται την ύπαρξη ενός οργανωτικού σχεδίου με σκοπό την άμεση λήψη των ορθών αποφάσεων και τον συντονισμό των απαραίτητων δράσεων, έτσι ώστε το συμβάν να τεθεί υπό έλεγχο. Ποιος θα ανταποκριθεί και πώς; Η ομάδα σας μπορεί να διαμορφώσει το αποτέλεσμα μέσα από καλά σχεδιασμένες δράσεις και αποτελεσματική επικοινωνία.

Τέλος, η προεργασία μπορεί να ελαχιστοποιήσει κάποια από τα πλέον καταστροφικά στοιχεία μίας παραβίασης – απώλεια της λειτουργικότητας, απουσία πρόσβασης σε δεδομένα, ανικανότητα να ανακάμψει η επιχείρηση εγκαίρως. Η αδιάλειπτη λειτουργία και ο σχεδιασμός ανάκτησης ελαχιστοποιούν αυτές τις απώλειες στοχεύοντας σε προτεραιότητες και στην εκ των προτέρων προετοιμασία.

ΕΦΑΡΜΟΓΗ ΤΩΝ ΑΡΧΩΝ ΣΕ ΜΙΑ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΠΛΗΡΟΦΟΡΙΩΝ

Αρμοδιότητα της διοίκησης των επιχειρήσεων συχνά είναι η μετάφραση αρχών που παρέχονται από έγγραφα όπως το παρόν σε πολιτικές και πρακτικές που κρίνονται λογικές για την επιχείρηση. Στόχος του παρόντος κεφαλαίου είναι να καταστήσει ευκολότερη την υλοποίηση του εν λόγω καθήκοντος. Ακολουθώντας τη δομή και οργάνωση των πέντε βασικών αρχών ασφαλείας που περιγράφονται στον παρόντα Οδηγό, τα ακόλουθα στοιχεία δρουν ως σημεία έναρξης για την ανάπτυξη των εταιρικών σας πολιτικών και πρακτικών διαχείρισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο.

Εστιάστε στην πληροφορία, όχι στην τεχνολογία

- Δημιουργείστε ένα Τμήμα και προτείνετε ένα άτομο, που θα ηγείται του εν λόγω Τμήματος και θα διευκολύνει πρωτοβουλίες για την ασφάλεια πληροφοριών, ενώ η ευθύνη για την ασφάλεια θα παραμένει κατανεμημένη σε ολόκληρη την εταιρία.
- Όταν μία επιχείρηση σχεδιάζει τον τρόπο με τον οποίο θα επιτύχει τους στόχους της ασφαλείας πληροφοριών της, πρέπει να καθορίσει τα ακόλουθα:
  - Τι θα γίνει
  - Τι είδους πόροι θα χρειαστούν
  - Ποιος θα είναι υπεύθυνος
  - Πότε θα ολοκληρωθεί
  - Πότε θα αξιολογηθούν τα αποτελέσματα[15]
- Στην περίπτωση που μία επιχείρηση δεν έχει επαρκή εμπειρία εσωτερικής ασφάλειας, αναζητείστε πρόσθετες πληροφορίες και ειδικούς σε θέματα ασφαλείας στον κυβερνοχώρο που θα βοηθήσουν ώστε η ασφάλεια πληροφοριών να ενσωματωθεί στο σχέδιο της επιχειρηματικής διαδικασίας και στα συστήματα πληροφορικής.

Διαμορφώστε μία ανθεκτική νοοτροπία

- Οι δράσεις ασφάλειας πληροφοριών θα πρέπει να ευθυγραμμίζονται – και όπου είναι δυνατόν να ενσωματώνονται – σε συμφωνία με άλλες προσπάθειες ελαχιστοποίησης των κινδύνων με σκοπό τον περιορισμό της επικάλυψης πρωτοβουλιών και αρμοδιοτήτων.
- Η αποστροφή κινδύνου δεν θα πρέπει να εμποδίσει την εισαγωγή νέων τεχνολογιών. Οι προσεγγίσεις για την ασφάλεια πληροφοριών μπορεί να φέρουν μία εταιρία στη θέση να εισαγάγει νέες και καινοτόμες τεχνολογίες εκτός από την κατάκτηση των στόχων διαχείρισης των κινδύνων για την ασφάλεια στον κυβερνοχώρο.

- Βεβαιωθείτε ότι η ασφάλεια λαμβάνεται υπόψη σε κάθε ένα από όλα τα έργα τα οποία διεκπεραιώνει η επιχείρησή σας, ειδικά όταν πρόκειται για νέα έργα. Όταν η ασφάλεια συμπεριλαμβάνεται εξαρχής, με την ορθή συμμετοχή της επιχείρησης, δεν αυξάνει σημαντικά τις δαπάνες και τη διάρκεια των έργων. Όταν, όμως, η ασφάλεια προστίθεται αργότερα ή – στη χειρότερη περίπτωση – αφού έχει προκύψει κάποια παραβίαση, τότε η υπέρβαση του κόστους, οι καθυστερήσεις και άλλες επιπτώσεις είναι υψηλότερες κατά αρκετές τάξεις μεγέθους.

[15] ISO/IEC 27001:2013

...

- Καθορίστε τι είδους συσκευές – δίνοντας έμφαση σε κινητές συσκευές, όπως π.χ. αυτές του προσωπικού ή των εταίρων σας – επιτρέπεται να έχουν πρόσβαση στο δίκτυο ή/και στις πληροφορίες της εταιρείας[16] και εξετάστε τον τρόπο διαχείρισης του λογισμικού και των ρυθμίσεων ασφαλείας του εταιρικού εξοπλισμού.

- Αξιολογήστε τη διαδικασία πρόσβασης στα δεδομένα ώστε να διασφαλίσετε ότι τα συστήματα ελέγχου είναι σε ισχύ, με σκοπό την αποτελεσματικότερη διαφύλαξη του απορρήτου, της ακεραιότητας και διαθεσιμότητας των πληροφοριών.

- Οι προϊστάμενοι πρέπει να λαμβάνουν γνώση, να ελέγχουν και να επικυρώνουν τους χρήστες (εσωτερικούς και εξωτερικούς) που έχουν πρόσβαση σε εφαρμογές και δεδομένα του Τμήματος τους. Το δικαίωμα πρόσβασης αποτελεί ευθύνη. Ενέχει, ωστόσο, και κινδύνους. Ως εκ τούτου, συνίσταται ο κατάλληλος έλεγχος επί των προνομίων πρόσβασης των υπαλλήλων σε δεδομένα και πληροφοριακά συστήματα.

- Αναπτύξτε διαδικασίες υποβολής αναφορών για τυχόν απώλεια ή κλοπή εξοπλισμού και, όπου είναι δυνατόν, τη λειτουργία απομακρυσμένης διαγραφής δεδομένων με σκοπό τη διαγραφή των εταιρικών πληροφοριών από συσκευές που έχουν χαθεί ή κλαπεί.

Προετοιμαστείτε να αντιδράσετε

- Κανείς δεν είναι αλάνθαστος. Και οι εταιρείες, οι οποίες μετατρέπουν τέτοια ατυχή περιστατικά στην ασφάλεια πληροφοριών σε ευκαιρία ανοιχτής αναθεώρησης των συμβάντων ασφαλείας, μπορούν να δημιουργήσουν ένα περιβάλλον, στο οποίο οι εργαζόμενοι δεν θα φοβούνται να αναφέρουν συμβάντα που θέτουν σε κίνδυνο την ασφάλεια.

- Εξουσιοδοτήστε επιλεγμένα μέλη του προσωπικού να ανταλλάσσουν ενδεδειγμένες πληροφορίες με ομολόγους και ενδιαφερόμενα μέλη εντός του κλάδου, τόσο για τη δημιουργία βέλτιστων πρακτικών όσο και για την προειδοποίηση πιθανών μελλοντικών επιθέσεων.

- Ορίστε ένα άτομο/φορέα που θα είναι αρμόδιο για τη διασφάλιση της δέουσας προστασίας των αποδεικτικών στοιχείων, από την πρώτη κιόλας στιγμή που η εταιρεία σας θα βρεθεί αντιμέτωπη με ένα συμβάν ασφαλείας και, ειδικότερα, σε περιπτώσεις εγκλημάτων του κυβερνοχώρου[17]

- Καθορίστε πότε και πώς θα δηλώνετε τυχόν συμβάντα στην ασφάλεια πληροφοριών στις ομάδες αντιμετώπισης έκτακτης ανάγκης στον κυβερνοχώρο (γνωστές, επίσης, ως CERT), σε κυβερνητικές υπηρεσίες ή αξιωματούχους επιβολής των νόμων.

16 Οι χρήστες πρέπει να ρυθμίσουν καταλλήλως τις ρυθμίσεις ασφαλείας του κινητού τηλεφώνου για την αποτροπή εγκληματιών από την κλοπή πληροφοριών μέσω της συσκευής.

17 Κατευθυντήριες οδηγίες για την απόκτηση δεδομένων σε συμβάντα ασφαλείας για τους σκοπούς διερεύνησης από το προσωπικό ασφάλειας ΤΠΕ ή σε περίπτωση προσβολής από κακόβουλο λογισμικό διατίθενται στο διαδίκτυο: http://cert.europa.eu/cert/plainedition/en/cert_about.html

Η ηγεσία μετράει

- Το προσωπικό είναι υπόλογο για την πληροφορία και την προστασία αυτής και πρέπει να διαθέτει τη δέουσα εξουσία, πρόσβαση στην ανώτατη διοίκηση, τα εργαλεία και την εκπαίδευση, που θα το προετοιμάσει καταλλήλως για την ανάληψη των αρμοδιοτήτων του, καθώς και για τις απειλές που μπορεί να προκύψουν. [18]
- Οι μικρές επιχειρήσεις πρέπει να διαθέτουν κάποιο άτομο εντός ή εκτός της εταιρείας τους, το οποίο θα ελέγχει σε τακτά χρονικά διαστήματα την επάρκεια της ασφάλειας πληροφοριών και θα φέρει επισήμως την ευθύνη της ασφάλειας πληροφοριών.

Παρόλο που αυτό δεν αποτελεί ρόλο πλήρους απασχόλησης, είναι σημαντικό να αποδειχθεί ζωτικής σημασίας για την επιβίωση της εταιρείας.

- Σε μεγάλες επιχειρήσεις, η κατανομή καθηκόντων, ρόλων και αρμοδιοτήτων πρέπει να αποτελεί μία προσεκτική μίξη ατόμων, (εικονικών) ομάδων εργασίας και επιτροπών. Κάθε μέλος της ομάδας οφείλει να γνωρίζει πολύ καλά τις ευθύνες και τις υποχρεώσεις του. Η κατάλληλη τεκμηρίωση και επικοινωνία είναι βαρύνουσας σημασίας στην προκειμένη περίπτωση.

Δράστε με βάση το όραμα σας

- Ελέγξτε την πρόσβαση προς (και από) το εσωτερικό δίκτυο, δίνοντας προτεραιότητα στην πρόσβαση σε υπηρεσίες και πόρους που κρίνονται απαραίτητα για τις ανάγκες των επιχειρήσεων και των υπαλλήλων.[19]
- Ενισχύστε τη χρήση ισχυρών κωδικών πρόσβασης και εξετάστε το ενδεχόμενο εφαρμογής ισχυρών μεθόδων πιστοποίησης της ταυτότητας[20] που απαιτούν συμπληρωματικές πληροφορίες για την είσοδο πέρα της χρήσης κωδικού πρόσβασης.
- Χρησιμοποιήστε τη δυνατότητα κρυπτογράφησης όπου κρίνεται απαραίτητο για την ασφάλεια των δεδομένων σε αδράνεια και υπό διαβίβαση, [21]με ιδιαίτερη έμφαση στις συνδέσεις δημοσίων δικτύων και σε φορητές συσκευές όπως π.χ. σε φορητούς υπολογιστές, κλειδιά USB και έξυπνα τηλέφωνα που μπορεί εύκολα να χαθούν ή να αποτελέσουν πιθανό στόχο κλοπής.

18 Μία σημαντική απειλή, στην οποία πρέπει να εκπαιδευτούν οι υπάλληλοι, είναι η απειλή μέσω Social Engineering. Η Κοινωνική Μηχανική (Social Engineering) είναι τεχνική χειραγώγησης του κόσμου στην κατεύθυνση υλοποίησης δράσεων που αποσκοπούν στην κοινοποίηση ευαίσθητων ή εμπιστευτικών πληροφοριών.

19 Εξετάστε το ενδεχόμενο φιλτραρίσματος των υπηρεσιών και ιστοσελίδων που αυξάνουν τους κινδύνους ασφάλειας για τους εταιρικούς πόρους, για παράδειγμα ανταλλαγή αρχείων P2P και πορνογραφικές ιστοσελίδες. Οι κανόνες φιλτραρίσματος πρέπει να είναι διαφανείς σε όλους τους χρήστες στην επιχείρηση και να περιλαμβάνουν μία διαδικασία για το ξεμπλοκάρισμα εταιρικών ιστοσελίδων που ίσως έχουν ακούσια αποκλειστεί.

20 Η μέθοδος πολυπαραγοντικής πιστοποίησης της ταυτότητας (multi-factor authentication) χρησιμοποιεί έναν συνδυασμό στοιχείων, όπως “πράγματα που γνωρίζω” (π.χ. κωδικός πρόσβασης ή κωδικός PIN),”πράγματα που έχω στην κατοχή μου“(π.χ. smartcard ή SMS) και “πράγματα που είμαι” (π.χ. δακτυλικό αποτύπωμα ή σάρωση της ίριδας)

21 Για παράδειγμα, email που αποστέλλονται μέσω του διαδικτύου διαβιβάζονται συνήθως μη κρυπτογραφημένα. Οι εταιρείες θα έπρεπε να εξετάσουν το ενδεχόμενο κρυπτογράφησης της ηλεκτρονικής τους αλληλογραφίας, ειδικά όταν διαβιβάζονται ευαίσθητες πληροφορίες.

- Δημιουργήστε λεπτομερή αντίγραφα ασφαλείας και αρχειακή πολιτική εναρμονισμένη με τις νομικές και ρυθμιστικές απαιτήσεις για τη διατήρηση των πληροφοριών, συγκεκριμένα:
  - Για ποια δεδομένα έχει δημιουργηθεί αντίγραφο ασφαλείας και πώς
  - Πόσο συχνά δημιουργούνται αντίγραφα ασφαλείας δεδομένων
  - Ποιο είναι το αρμόδιο πρόσωπο για τη δημιουργία αντιγράφων ασφαλείας και την αξιολόγηση του περιεχομένου
  - Πού και πώς αποθηκεύονται τα αντίγραφα ασφαλείας
  - Ποιος έχει πρόσβαση στα εν λόγω αντίγραφα ασφαλείας
  - Πώς λειτουργούν (και δοκιμάζονται) οι διαδικασίες επαναφοράς
- Αναπτύξτε προγράμματα κατάρτισης αναφορικά με την ευαισθησία σε θέματα ασφάλειας πληροφοριών, συμπεριλαμβανομένων ζητημάτων όπως:
  - Ασφαλής και υπεύθυνη επικοινωνία
  - Χρηστή χρήση των μέσων κοινωνική δικτύωσης
  - Ασφαλής μεταφορά ψηφιακών αρχείων
  - Κατάλληλη χρήση κωδικών πρόσβασης
  - Αποφυγή απώλειας σημαντικών πληροφοριών
  - Διασφάλιση της πρόσβασης στις πληροφορίες μόνο από αρμόδια άτομα
  - Διατήρηση της προστασίας από ιούς και κακόβουλο λογισμικό
  - Ποιο πρόσωπο θα ειδοποιηθεί σε περίπτωση πιθανού συμβάντος ασφαλείας
  - Πώς να μην εξαπατηθείτε και να προδώσετε σημαντικές πληροφορίες

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

Το ακόλουθο κεφάλαιο παρουσιάζει μία εύκολη λίστα ελέγχου ως ένα εργαλείο διαχείρισης, με το οποίο η επιχείρηση θα μπορέσει να προβεί στην εσωτερική αναθεώρηση της ανθεκτικότητας της στον κυβερνοχώρο και το οποίο θα της δώσει τη δυνατότητα να θέσει τις σωστές ερωτήσεις στις ομάδες της εταιρίας που ασχολούνται με τις εν λόγω πρωτοβουλίες. Οι ερωτήσεις που τίθενται σε αυτό το «εργαλείο» μπορούν να βοηθήσουν στον εντοπισμό συγκεκριμένων ισχυρών και αδύναμων σημείων, καθώς και μεθόδων βελτίωσης στο πλαίσιο της εκάστοτε επιχείρησης.

Ταυτόχρονα, το παρόν ερωτηματολόγιο αυτό-αξιολόγησης μπορεί να χρησιμοποιηθεί ως μία λίστα ελέγχου από εταιρείες που μόλις αρχίζουν να προχωρούν στην ανάληψη πρωτοβουλιών για την ασφάλεια πληροφοριών τους και οι οποίες επιθυμούν να αξιοποιήσουν τις παρεχόμενες πληροφορίες σαν μία βάση για τον σχεδιασμό των εταιρικών δυνατοτήτων ανθεκτικότητας στον κυβερνοχώρο.

Για κάθε μία από τις ερωτήσεις που ακολουθούν, οι εταιρείες πρέπει να επιλέξουν από τις παρεχόμενες επιλογές απαντήσεων αυτήν που ανταποκρίνεται με περισσότερη ακρίβεια στις τρέχουσες πρακτικές της εταιρείας τους. Σε κάθε μία από τις απαντήσεις αντιστοιχεί ένα σύμβολο. Έτσι έχουμε:

☒ Αυτή η επιλογή αποτελεί τη λιγότερο επιθυμητή απάντηση. Η βελτίωση πρέπει να αποτελέσει προτεραιότητα για την εταιρεία σας.

! Περαιτέρω βελτίωση είναι απαραίτητη για την καλύτερη προστασία της εταιρείας σας.

☑ Αυτή η απάντηση αποτελεί το καλύτερο δείγμα ανθεκτικότητας απέναντι στις απειλές του κυβερνοχώρου.

Οι απαντήσεις που δίνονται στο ερωτηματολόγιο αντικατοπτρίζουν την αποκλειστική απόκριση του κάθε αξιολογητή. Η ύπαρξη *μίας πιο συγκεκριμένης λίστας ελέγχου κάτω από κάθε ερώτηση* αποσκοπεί στην αναγνώριση και τεκμηρίωση της κατάστασης ενός συνόλου θεμελιωδών ελέγχων της ασφάλειας πληροφοριών της εταιρείας σας. Οι πληροφορίες που συγκεντρώνονται σε αυτήν τη διαδικασία ερωτήσεων θα βοηθήσουν στην επισήμανση τυχόν κενών ή ευπαθειών στην ασφάλεια και, κατά συνέπεια, οι εταιρείες που συμβουλεύονται τον παρόντα Οδηγό θα είναι σε θέση να αναγνωρίσουν σε ποια σημεία κρίνεται αναγκαία η λήψη περαιτέρω δράσεων.

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

1

Αξιολογείτε τον τρόπο διαχείρισης των ευαίσθητων πληροφοριών εντός της εταιρίας σας;

□Χ Όχι, αλλά χρησιμοποιούμε τείχος προστασίας για να προστατευτούμε σε περίπτωση κλοπής πληροφοριών.

□! Ναι, κατανοούμε τη σημασία των πληροφοριών μας και εφαρμόζουμε γενικά μέτρα ασφαλείας.

□v Ναι, και διατηρούμε ένα μοντέλο διαβάθμισης πληροφοριών και γνωρίζουμε πού αποθηκεύονται και πού λαμβάνει χώρα η επεξεργασία των ευαίσθητων πληροφοριών μας. Εφαρμόζουμε μέτρα ασφαλείας που βασίζονται στην ευαισθησία των πληροφοριών.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Τα ευαίσθητα δεδομένα σας έχουν προσδιοριστεί και ταξινομηθεί;		
Είστε γνώστης των υποχρεώσεών σας αναφορικά με τα προσδιοριζόμενα ευαίσθητα δεδομένα;		
Τα εξαιρετικά ευαίσθητα δεδομένα βρίσκονται υπό υψηλή προστασία και είναι κρυπτογραφημένα;		
Η διαχείριση των προσωπικών ιδιωτικών δεδομένων καλύπτεται από διαδικασίες;		
Είναι σε θέση όλοι οι υπάλληλοι να αναγνωρίσουν και να προστατέψουν με τον πλέον ενδεδειγμένο τρόπο ευαίσθητα και μη ευαίσθητα δεδομένα;		

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

2

Πραγματοποιείτε αξιολογήσεις κινδύνων που να σχετίζονται με την ασφάλεια πληροφοριών;

□Χ Δεν πραγματοποιούμε αξιολογήσεις κινδύνων.

□! Πραγματοποιούμε αξιολογήσεις κινδύνων αλλά όχι συγκεκριμένα σε σχέση με ζητήματα ασφάλειας πληροφοριών.

□v Πραγματοποιούμε αξιολογήσεις κινδύνων που σχετίζονται με ζητήματα ασφάλειας πληροφοριών.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Αντιμετωπίζετε τα προβλήματα τρωτότητας προκειμένου να μεταβάλλετε το ρίσκο από υψηλό σε χαμηλό;		
Πραγματοποιείται ταυτοποίηση των περιστατικών που θα μπορούσαν να προκαλέσουν τυχόν διακοπή στις επιχειρηματικές διαδικασίες, καθώς και αξιολόγηση των επιπτώσεων από πιθανές σχετικές διακοπές;		
Διαθέτετε ένα τρέχον «Σχέδιο Επιχειρησιακής Συνέχειας», στο οποίο πραγματοποιούνται έλεγχοι και επικαιροποιήσεις σε τακτική βάση;		
Πραγματοποιείτε συχνά αξιολογήσεις κινδύνων για να επικαιροποιήσετε το επίπεδο προστασίας δεδομένων και ανάγκης πληροφόρησης;		
Είναι οι περιοχές κινδύνου αναγνωρισμένες καθ' όλη τη διάρκεια της επιχειρηματικής διαδικασίας ώστε να αποφευχθεί η διάβρωση της επεξεργασίας πληροφοριών ή η εσκεμμένη κατάχρηση;		

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

3

Σε ποιο επίπεδο εφαρμόζεται η διακυβέρνηση ασφάλειας πληροφοριών (information security governance);

□Χ Δεν υπάρχει διακυβέρνηση ασφάλειας πληροφοριών.

□! Η διακυβέρνηση ασφάλειας πληροφοριών είναι εγκατεστημένη στο τμήμα Τεχνολογίας Πληροφορικής, εφόσον εκεί διασφαλίζεται η προστασία των πληροφοριών.

□v Η διακυβέρνηση ασφάλειας πληροφοριών είναι εγκατεστημένη σε εταιρικό επίπεδο, έτσι ώστε να διασφαλιστεί ο αντίκτυπος σε ολόκληρη την εταιρία.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε

	ΝΑΙ	ΟΧΙ
Διαθέτουν τα μέλη του Διοικητικού Συμβουλίου και ο Διευθύνων Σύμβουλος προϋπολογισμό για την ασφάλεια πληροφοριών;		
Αποτελεί η ασφάλεια πληροφοριών τμήμα της υφιστάμενης διαχείρισης κινδύνων από τους διευθυντές;		
Εγκρίνει η Διοίκηση την πολιτική ασφάλειας πληροφοριών της εταιρίας και την επικοινωνεί με τον κατάλληλο τρόπο στους υπαλλήλους;		
Ενημερώνονται τακτικά τα Μέλη του Διοικητικού Συμβουλίου και η Διοίκηση για τις τελευταίες εξελίξεις στις πολιτικές ασφάλειας πληροφοριών, τα πρότυπα, τις διαδικασίες και τις κατευθυντήριες γραμμές;		
Υπάρχει τουλάχιστον ένας αρμόδιος που να αποτελεί κομμάτι των δομών διαχείρισης, και είναι υπεύθυνος για την προστασία δεδομένων και την ιδιωτικότητα των προσωπικών πληροφοριών;		

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

4

Διαθέτετε ομάδα ασφάλειας πληροφοριών ή τμήμα ειδικά επιφορτισμένο με την ασφάλεια πληροφοριών μέσα στην εταιρία σας;

□Χ Δεν διαθέτουμε ομάδα ασφάλειας πληροφοριών, ούτε συγκεκριμένους ρόλους και αρμοδιότητες αναφορικά με την ασφάλεια πληροφοριών.

□! Δεν διαθέτουμε ομάδα ασφάλειας πληροφοριών, αλλά έχουμε καθορίσει συγκεκριμένους ρόλους και αρμοδιότητες όσον αφορά στην ασφάλεια πληροφοριών μέσα στην εταιρία.

□v Διαθέτουμε ομάδα ασφάλειας πληροφοριών ή ειδικό τμήμα ασφάλειας πληροφοριών.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Υπάρχει συγκεκριμένο άτομο ή ομάδα εξειδικευμένη σε ζητήματα ασφάλειας πληροφοριών που συντονίζει τις ενδοεπιχειρησιακές γνώσεις και παρέχει βοήθεια στη διαχείριση της διαδικασίας λήψης αποφάσεων;		
Είναι ο ειδικός ή η ομάδα που ειδικεύεται σε ζητήματα ασφάλειας πληροφοριών τα αρμόδια μέλη για την αναθεώρηση και συστηματική επικαιροποίηση της πολιτικής ασφάλειας πληροφοριών βάσει σημαντικών αλλαγών ή συμβάντων;		
Διαθέτει ο ειδικός ή η ομάδα που ειδικεύεται σε ζητήματα ασφάλειας πληροφοριών επαρκή προβολή και υποστήριξη ώστε να παρεμβαίνει σε οποιαδήποτε πρωτοβουλία που σχετίζεται με τις πληροφορίες στην εταιρία;		
Υπάρχουν διαφορετικοί διαχειριστές που είναι υπεύθυνοι για ξεχωριστές κατηγορίες δεδομένων;		
Εξετάζονται τακτικά η σκοπιμότητα και η αποτελεσματικότητα της πολιτικής ασφάλειας πληροφοριών, καθώς και η επάρκεια της ομάδας ασφάλειας πληροφοριών από ανεξάρτητο σώμα ή ελεγκτή;		

5

Πώς αντιμετωπίζει η εταιρία σας κινδύνους που αφορούν την ασφάλεια πληροφοριών από προμηθευτές, οι οποίοι διαθέτουν τη δυνατότητα πρόσβασης σ' ευαίσθητες πληροφορίες σας;

□Χ Η σχέση μας με τους προμηθευτές μας βασίζεται στην αμοιβαία εμπιστοσύνη.

□! Σε ορισμένα συμβόλαια συμπεριλαμβάνουμε ρήτρες αναφορικά με την ασφάλεια πληροφοριών.

□v Θεσπίζουμε διαδικασίες για την επικύρωση της πρόσβασης των προμηθευτών μας. Επιπλέον, συγκεκριμένες κατευθυντήριες γραμμές κοινοποιούνται και υπογράφονται από τους προμηθευτές μας.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Φέρουν οι ανάδοχοι και προμηθευτές ευκρινή σήματα με τα στοιχεία ταυτότητας τους και πρόσφατη φωτογραφία;		
Διαθέτετε πολιτικές για έλεγχο του ιστορικού των αναδόχων και προμηθευτών;		
Διακόπτεται αυτόματα η πρόσβαση σε εγκαταστάσεις και πληροφοριακά συστήματα όταν ολοκληρώνεται η αποστολή ενός αναδόχου ή προμηθευτή;		
Γνωρίζουν οι προμηθευτές τον τρόπο και το πρόσωπο εντός της εταιρείας σας, στο οποίο θα απευθυνθούν σε περίπτωση απώλειας ή κλοπής πληροφοριών;		
Διασφαλίζει η εταιρία σας ότι οι προμηθευτές προβαίνουν εγκαίρως σε ενημέρωση των λογισμικών και εφαρμογών τους με τη βοήθεια των ενημερώσεων ασφαλείας (security patches);		
Ορίζονται με σαφήνεια οι απαιτήσεις ασφαλείας στις συμβάσεις σας με τους αναδόχους/προμηθευτές;		

6

Αξιολογεί η εταιρεία σας σε τακτική βάση την ασφάλεια υπολογιστών και δικτύων;

□Χ Δεν πραγματοποιούμε ελέγχους ή δοκιμές διείσδυσης για να αξιολογούμε την ασφάλεια των υπολογιστών και δικτύων μας.

□! Δεν ακολουθούμε συστηματική προσέγγιση για τη διενέργεια ελέγχων ασφαλείας και/ή δοκιμών διείσδυσης, αλλά διενεργούμε ορισμένους ελέγχους κατά περίπτωση.

□v Οι τακτικοί έλεγχοι ασφαλείας και/ή οι δοκιμές διείσδυσης αποτελούν αναπόσπαστο μέρος της προσέγγισης μας για την αξιολόγηση της ασφάλειας των υπολογιστών και δικτύων μας.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Πραγματοποιείτε ελέγχους σε τακτική βάση και τηρείτε αρχεία των αναγνωρισμένων απειλών;		
Διαθέτετε διαδικασίες για την αξιολόγηση ανθρώπινων απειλών στα συστήματα πληροφοριών σας, συμπεριλαμβανομένων τυχόν ανέντιμων συμπεριφορών, της κοινωνικής μηχανικής (social engineering) και της κατάχρησης εμπιστοσύνης;		
Απαιτεί η εταιρεία σας εκθέσεις ελέγχου ασφαλείας από τους παρόχους υπηρεσιών πληροφοριών;		
Αξιολογείται, επίσης, η χρησιμότητα κάθε είδους αποθηκευμένου στοιχείου κατά τη διενέργεια των ελέγχων ασφαλείας;		
Ελέγχετε τις διεργασίες και διαδικασίες πληροφοριών σας όσον αφορά στη συμμόρφωση με τις λοιπές υφιστάμενες πολιτικές και τα πρότυπα που τηρούνται εντός της εταιρείας σας;		

7

Όταν εισάγονται νέες τεχνολογίες, αξιολογεί η εταιρεία σας πιθανούς κινδύνους για την ασφάλεια πληροφοριών;

□Χ Η ασφάλεια πληροφοριών δεν αποτελεί μέρος της διαδικασίας εφαρμογής νέων τεχνολογιών.

□! Η ασφάλεια πληροφοριών εφαρμόζεται μόνο κατά περίπτωση στη διαδικασία εισαγωγής νέων τεχνολογιών.

□v Η ασφάλεια πληροφοριών συμπεριλαμβάνεται στη διαδικασία εφαρμογής νέων τεχνολογιών.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Όταν εξετάζετε το ενδεχόμενο εφαρμογής νέων τεχνολογιών, αξιολογείτε τις πιθανές επιπτώσεις στην υφιστάμενη πολιτική ασφάλειας πληροφοριών;		
Υπάρχουν μέτρα προστασίας για τον περιορισμό των κινδύνων κατά τη διαδικασία εφαρμογής νέων τεχνολογιών;		
Τεκμηριώνονται οι διαδικασίες εφαρμογής νέων τεχνολογιών;		
Κατά την εφαρμογή νέων τεχνολογιών, θα μπορούσε η εταιρεία σας να βασιστεί σε συνεργασίες, ώστε να καταστούν δυνατές τυχόν προσπάθειες συνεργασίας και ανταλλαγή σημαντικών πληροφοριών ασφάλειας;		
Θεωρείται συχνά η πολιτική ασφάλειας πληροφοριών της εταιρίας σας ως φραγμός στις τεχνολογικές προοπτικές;		
Διαχειρίζεται η εταιρεία σας τις νέες τεχνολογίες με τη χρήση της μεθοδολογίας ανάπτυξης συστημάτων ασφαλείας εντός του κύκλου ζωής των συστημάτων;		

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

8

Πραγματοποιείται εκπαίδευση για την ασφάλεια πληροφοριών εντός της εταιρείας σας;

□Χ Δείχνουμε εμπιστοσύνη στους υπαλλήλους μας και δεν θεωρούμε τις οδηγίες για την ασφάλεια πληροφοριών ως προστιθέμενη αξία.

□! Μόνο το προσωπικό του Τμήματος IT της εταιρείας λαμβάνει ειδική εκπαίδευση με σκοπό την ασφάλεια του περιβάλλοντος των Τεχνολογιών Πληροφορικής.

□v Διοργανώνονται τακτικές συνεδριάσεις για τη ευαισθητοποίηση όλων των υπαλλήλων μας αναφορικά με το ζήτημα ασφάλειας πληροφοριών.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Αναφέρεται σε ορισμένες από τις συνεδριάσεις το θέμα της ευαισθητοποίηση σε ζητήματα ασφάλειας πληροφοριών στο πεδίο δραστηριοτήτων των υπαλλήλων;		
Διδάσκονται οι υπάλληλοι να βρίσκονται σε επαγρύπνηση για παραβιάσεις στην ασφάλεια πληροφοριών;		
Διαθέτει η εταιρία σας οδηγίες για τους χρήστες ώστε να αναφέρουν τυχόν αδυναμίες στην ασφάλεια ή απειλές προς συστήματα ή υπηρεσίες;		
Γνωρίζουν οι υπάλληλοι πώς να διαχειρίζονται ορθά δεδομένα πιστωτικών καρτών και ιδιωτικές πληροφορίες;		
Λαμβάνουν, επίσης, χρήστες από τρίτα μέρη (όπου απαιτείται) την κατάλληλη εκπαίδευση σε ζητήματα ασφάλειας πληροφοριών, καθώς και τακτικές ενημερώσεις στις οργανωτικές πολιτικές και διαδικασίες;		

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

9

Πώς χρησιμοποιείτε τους κωδικούς πρόσβασης μέσα στην εταιρία σας;

□Χ Μοιραζόμαστε τους κωδικούς πρόσβασης με άλλους συναδέλφους και/ή δεν υφίσταται καμία πολιτική για την ασφαλή χρήση ή τη συχνή αλλαγή των κωδικών πρόσβασης.

□! Όλοι οι υπάλληλοι, συμπεριλαμβανομένης της Διοίκησης, διαθέτουν μοναδικούς κωδικούς πρόσβασης. Δεν εφαρμόζονται, ωστόσο, κανόνες πολυπλοκότητας. Η αλλαγή των κωδικών πρόσβασης είναι προαιρετική, όχι υποχρεωτική.

□v Όλοι οι υπάλληλοι, συμπεριλαμβανομένης της Διοίκησης, διαθέτουν προσωπικό κωδικό πρόσβασης, ο οποίος πρέπει να πληροί τις σαφείς απαιτήσεις κωδικού πρόσβασης και τον οποίο πρέπει να αλλάζουν σε τακτά χρονικά διαστήματα.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Έχει η εταιρεία σας καθιερώσει και επιβάλλει μία παγκοσμίως αποδεκτή πολιτική κωδικών πρόσβασης για όλα τα «περιουσιακά» στοιχεία της εταιρείας;		
Μπορείτε να βεβαιώσετε τα ακόλουθα αναφορικά με όλους τους κωδικούς πρόσβασης στην εταιρία σας; Δεν βρίσκονται αποθηκευμένοι σε αρχεία που είναι εύκολα προσβάσιμα. Δεν είναι αδύναμοι ή κενοί ή εργοστασιακοί. Δεν έχουν αλλαχθεί ποτέ ή μόνο σπανίως, ειδικά εάν πρόκειται για κινητές συσκευές.		
Αισθάνεστε καλά προστατευμένοι απέναντι σε μη εξουσιοδοτημένη φυσική πρόσβαση στα συστήματα;		
Έχουν οι χρήστες και οι ανάδοχοι επίγνωση της υποχρέωσής τους να προστατεύουν, επίσης, αφύλακτο εξοπλισμό (δηλαδή, να αποσυνδέονται [logoff]);		
Έχουν διδαχτεί οι υπάλληλοι πώς να αναγνωρίζουν κόλπα κοινωνικής μηχανικής (social engineering), με τα οποία παραπλανάται ο κόσμος, προκειμένου να κοινοποιήσει στοιχεία ασφάλειας, και γνωρίζουν πώς να αντιδράσουν σε μια τέτοια απειλή;		

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

10

Υπάρχει εταιρική πολιτική για την ορθή χρήση του διαδικτύου και των Μέσων Κοινωνικής Δικτύωσης;

□Χ Όχι, δεν υπάρχει πολιτική για την ορθή χρήση του διαδικτύου.

□! Ναι, μία πολιτική είναι διαθέσιμη σε μία κεντρική τοποθεσία που είναι προσβάσιμη σε όλους τους υπαλλήλους, την οποία, ωστόσο, δεν έχουν υπογράψει όλοι οι υπάλληλοι.

□v Ναι, μία πολιτική για την ορθή χρήση του διαδικτύου αποτελεί τμήμα των συμβάσεων/όλοι οι υπάλληλοι έχουν υπογράψει την εν λόγω πολιτική.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Υπάρχουν γενικές κατευθυντήριες γραμμές και διαδικασίες επικοινωνίας για τους υπαλλήλους στην εταιρία, συμπεριλαμβανομένης της σχέσης με τον Τύπο και τα Μέσα Κοινωνικής Δικτύωσης;		
Υπάρχει τυχόν πειθαρχική διαδικασία για τους υπαλλήλους που παραβιάζουν τις κατευθυντήριες γραμμές για την επικοινωνία της εταιρίας;		
Διαθέτετε κάποιον συγκεκριμένο διευθυντή ή ομάδα επικοινωνιών που ελέγχει το διαδίκτυο με σκοπό την αξιολόγηση των κινδύνων και της κατάστασης της ηλεκτρονικής φήμης;		
Έχει η εταιρεία σας αξιολογήσει την ευθύνη της για πράξεις των υπαλλήλων ή άλλων εσωτερικών χρηστών ή επιτιθέμενων που κάνουν κατάχρηση του συστήματος με σκοπό την τέλεση αξιόποινων πράξεων;		
Έχει λάβει η εταιρία σας μέτρα για να αποτρέψει τυχόν υπαλλήλους ή άλλους εξωτερικούς χρήστες να επιτεθούν σε άλλες τοποθεσίες;		

11

Προβαίνει η εταιρεία σας στη μέτρηση, αναφορά και παρακολούθηση (follow-up) ζητημάτων που σχετίζονται με την ασφάλεια πληροφοριών;

□Χ Δεν προβαίνουμε σε έλεγχο, αναφορά και παρακολούθηση της αποδοτικότητας και επάρκειας των μέτρων ασφαλείας που έχουν εφαρμοστεί.

□! Η εταιρεία μας έχει εφαρμόσει μεθόδους και εργαλεία για τον έλεγχο, την αναφορά και παρακολούθηση της αποδοτικότητας και επάρκειας από μία σειρά μέτρων ασφαλείας που έχουν ήδη εφαρμοστεί αλλού.

□v Η εταιρία μας έχει εφαρμόσει τις απαραίτητες μεθόδους και εργαλεία για τον έλεγχο, την αναφορά και παρακολούθηση της αποδοτικότητας και επάρκειας όλων των υπαρχόντων μέτρων ασφαλείας που ήδη έχουν εφαρμοστεί αλλού.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Τηρούνται διαδρομές ελέγχου και μητρώα σχετικά με τα συμβάντα; Έχουν ληφθεί, επίσης, δράσεις πρόληψης κατά τρόπο που το εν λόγω συμβάν να μην προκύψει ξανά;		
Διενεργεί η εταιρεία σας ελέγχους για την εκπλήρωση των κανονιστικών και νομικών απαιτήσεων (π.χ. ιδιωτικότητα των δεδομένων);		
Έχει αναπτύξει η εταιρία σας ίδια εργαλεία για να βοηθήσει το Τμήμα Διαχείρισης να αξιολογεί την κατάσταση ασφάλειας και να προσφέρει στην εταιρία τη δυνατότητα να επιταχύνει τις ικανότητες της στον περιορισμό πιθανών κινδύνων;		
Διαθέτει η εταιρεία σας οδικό χάρτη ασφάλειας πληροφοριών, που να περιλαμβάνει στόχους, αξιολόγηση προόδου και πιθανές ευκαιρίες συνεργασίας;		
Δηλώνονται οι εκθέσεις ελέγχου και τα συμβάντα στις Αρχές και σε άλλες ενδιαφερόμενες ομάδες, όπως π.χ. κλαδικές ενώσεις;		

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

12

Πώς κρατούνται ενημερωμένα τα συστήματα εντός της εταιρείας σας;

□Χ Βασιζόμαστε για την πλειονότητα των λύσεων σ' ένα αυτόματο σύστημα διαχείρισης ενημερώσεων (patch management), το οποίο προσφέρεται από τον πάροχο.

□! Οι ενημερώσεις ασφαλείας πραγματοποιούνται συστηματικά σε μηνιαία βάση.

□v Διαθέτουμε διαδικασία διαχείρισης της τρωτότητας και επιδιώκουμε διαρκώς την έγκυρη πληροφόρηση αναφορικά με πιθανές ευπάθειες (π.χ. μέσω της συνδρομής σε υπηρεσίες στέλνονται αυτόματα ειδοποιήσεις για την ύπαρξη νέων ευπαθειών) και εφαρμόζουμε ενημερώσεις που βασίζονται στους κινδύνους που μπορούν να περιοριστούν.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε

	ΝΑΙ	ΟΧΙ
Αποτελεί η ανίχνευση ευπαθειών τακτική προγραμματισμένη εργασία συντήρησης στην εταιρία σας;		
Πραγματοποιείται αναθεώρηση και έλεγχος του συστήματος εφαρμογών μετά από κάθε αλλαγή στο λειτουργικό σύστημα;		
Μπορούν οι χρήστες να ελέγχουν μόνοι τους την ύπαρξη μη ενημερωμένων εφαρμογών;		
Γνωρίζουν οι χρήστες ότι πρέπει να προβαίνουν σε διαρκή ενημέρωση του λειτουργικού συστήματος και των εφαρμογών, συμπεριλαμβανομένου και του λογισμικού ασφάλειας των κινητών τους συσκευών;		
Είναι οι χρήστες εκπαιδευμένοι ώστε να αναγνωρίζουν ένα έγκυρο μήνυμα προειδοποίησης, όπως μία άδεια για αναβάθμιση (που διαφέρει από ένα ψεύτικο μήνυμα για ύπαρξη ιών) και να ενημερώνουν κατάλληλα την ομάδα ασφαλείας εάν συμβεί κάτι κακό ή περίεργο;		

13

Πραγματοποιείται σε τακτική βάση έλεγχος και αναθεώρηση των δικαιωμάτων πρόσβασης των χρηστών σε εφαρμογές και συστήματα;

□Χ Τα δικαιώματα πρόσβασης σε εφαρμογές και συστήματα δεν αίρονται, ούτε αναθεωρούνται συχνά.

□! Τα δικαιώματα πρόσβασης σε εφαρμογές και συστήματα αίρονται μόνο στην περίπτωση αποχώρησης υπαλλήλου από την εταιρία.

□**ν**΄Έχει καθιερωθεί μία πολιτική έλεγχου της πρόσβασης με τακτικές αναθεωρήσεις των εκχωρημένων δικαιωμάτων πρόσβασης του χρήστη για όλες τις σχετικές επιχειρηματικές εφαρμογές και υποστηρικτικά συστήματα.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Περιορίζουν τυχόν πολιτικές και διαδικασίες την πρόσβαση σε ηλεκτρονικά συστήματα και εγκαταστάσεις πληροφορικής;		
Στηρίζεται η εταιρεία σας σε πολιτική απορρήτου που καταχωρεί τις πληροφορίες που συλλέγει (για παράδειγμα αναφορικά με τους πελάτες σας: ταχυδρομικές διευθύνσεις, ηλεκτρονικές διευθύνσεις, ιστορικό αναζήτησης κλπ.) και πώς τις χρησιμοποιεί;		
Καθορίζουν οι πολιτικές και οι διαδικασίες τις μεθόδους που χρησιμοποιούνται για τον έλεγχο φυσικής πρόσβασης σε ασφαλείς περιοχές, όπως ασφαλισμένες θύρες, πρόσβαση σε συστήματα ελέγχου ή παρακολούθηση με βιντεοκάμερα;		
Διακόπτεται αυτόματα η πρόσβαση σε εγκαταστάσεις και πληροφοριακά συστήματα όταν λύεται η σχέση εργασίας μελών του προσωπικού;		
Πραγματοποιείται ταξινόμηση των ευαίσθητων δεδομένων (άκρως εμπιστευτικά, ευαίσθητα, μόνο για εσωτερική χρήση); Και καταγράφονται οι χρήστες, στους οποίους παραχωρείται πρόσβαση στα εν λόγω δεδομένα;		
Αναπτύσσονται διαδικασίες για τη ρύθμιση της εξ αποστάσεως πρόσβασης στα ηλεκτρονικά συστήματα πληροφορικής της εταιρίας;		

14

Επιτρέπεται στην εταιρεία σας να χρησιμοποιήσουν οι υπάλληλοι τις προσωπικές τους συσκευές, όπως π.χ. κινητά τηλέφωνα και τάμπλετ, για να αποθηκεύσουν ή να μεταφέρουν εταιρικές πληροφορίες;

□Χ Ναι, επιτρέπεται να αποθηκεύουμε ή να μεταφέρουμε εταιρικές πληροφορίες σε προσωπικές συσκευές χωρίς την εφαρμογή επιπλέον μέτρων ασφαλείας.

□! Υπάρχει πολιτική που απαγορεύει τη χρήση προσωπικών συσκευών για την αποθήκευση ή μεταφορά εταιρικών πληροφοριών. Στην πραγματικότητα, ωστόσο, είναι πιθανόν να γίνει κάτι τέτοιο χωρίς την εφαρμογή πρόσθετων μέτρων ασφαλείας.

□v Προσωπικές συσκευές επιτρέπεται να χρησιμοποιηθούν για την αποθήκευση ή μεταφορά εταιρικών πληροφοριών μόνο μετά την εφαρμογή μέτρων ασφαλείας στην προσωπική συσκευή και/ή μετά τη χορήγηση επαγγελματικής λύσης.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Στηρίζεται η εταιρία σας σε μία ευρέως αποδεκτή πολιτική της λογικής «Φέρε τη δική σου συσκευή»;		
Είναι οι κινητές συσκευές προστατευμένες από μη εξουσιοδοτημένους χρήστες;		
Αναγνωρίζει μόνιμα το δίκτυο όλες τις συσκευές και συνδέσεις;		
Υπάρχει εγκατεστημένο λογισμικό κρυπτογράφησης σε κάθε κινητή συσκευή με σκοπό την προστασία του απορρήτου και της ακεραιότητας των δεδομένων;		
Γνωρίζετε ότι ενώ ο υπάλληλος μπορεί να είναι υπεύθυνος για μία συσκευή, η εταιρία παραμένει υπεύθυνη για τα δεδομένα;		

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

15

Έχει λάβει η εταιρεία σας μέτρα για να αποτρέψει την απώλεια αποθηκευμένων πληροφοριών;

□Χ Δεν εφαρμόζουμε διαδικασία διαθεσιμότητας/δημιουργίας αντιγράφων ασφαλείας.

□! Διαθέτουμε διαδικασία διαθεσιμότητας/δημιουργίας αντιγράφων ασφαλείας, αλλά ακόμα δεν έχουν πραγματοποιηθεί έλεγχοι επαναφοράς.

□√ Διαθέτουμε διαδικασία διαθεσιμότητας/δημιουργίας αντιγράφων ασφαλείας, η οποία περιλαμβάνει δομικές επαναφοράς/ανθεκτικότητας. Διαθέτουμε αντίγραφα ασφαλείας αποθηκευμένα και σε άλλη ασφαλή τοποθεσία ή χρησιμοποιούμε άλλες λύσεις υψηλής διαθεσιμότητας.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Υπάρχουν αρκετά μέλη του προσωπικού, τα οποία έχουν τη δυνατότητα να δημιουργήσουν ανακτήσιμα αντίγραφα ασφαλείας και αρχειακά αντίγραφα;		
Είναι ο εξοπλισμός προστατευμένος από διακοπές ηλεκτροδότησης με τη χρήση μόνιμων τροφοδοτικών ρεύματος, όπως τροφοδοτικά πολλαπλών τάσεων, αδιάλειπτα τροφοδοτικά ρεύματος (ups), εφεδρική γεννήτρια κλπ.;		
Πραγματοποιείται τακτικός έλεγχος στα μέσα δημιουργίας αντιγράφων ασφαλείας ώστε να διασφαλιστεί ότι θα μπορούσαν να ανακτηθούν εντός του χρόνου που απαιτείται για τη διαδικασία αναφοράς;		
Εφαρμόζει η εταιρία σας διαδικασία υποβολής εκθέσεων για απολεσθείσες ή κλεμμένες κινητές συσκευές;		
Έχουν λάβει οι υπάλληλοι ειδική εκπαίδευση ώστε να γνωρίζουν τι πρέπει να πράξουν σε περίπτωση που πληροφορίες διαγραφούν κατά λάθος και πώς μπορούν να ανακτήσουν πληροφορίες σε περιόδους καταστροφών;		
Έχουν εφαρμοστεί μέτρα για την προστασία τόσο του απορρήτου όσο και της ακεραιότητας των αντιγράφων ασφαλείας στην τοποθεσία αποθήκευσης;		

ΑΥΤΟ-ΑΞΙΟΛΟΓΗΣΗ ΑΣΦΑΛΕΙΑΣ

16

Είναι η εταιρία σας προετοιμασμένη να αντιμετωπίσει ένα συμβάν ασφάλειας πληροφοριών;

□Χ Δεν πρόκειται να έχουμε κανένα τέτοιο συμβάν. Σε περίπτωση, ωστόσο, που παρουσιαστεί, οι υπάλληλοί μας είναι αρκετά ικανοί να το διαχειριστούν.

□! Διαθέτουμε διαδικασίες διαχείρισης συμβάντων, χωρίς, ωστόσο, την απαραίτητη προσαρμογή ώστε να αντιμετωπιστούν τυχόν συμβάντα ασφάλειας πληροφοριών.

□ν Διαθέτουμε ειδική διαδικασία για την αντιμετώπιση συμβάντων ασφάλειας πληροφοριών, με τους απαραίτητους μηχανισμούς κλιμάκωσης και επικοινωνίας. Επιδιώκουμε να αντιμετωπίζουμε τα συμβάντα όσο το δυνατόν πιο αποτελεσματικά, ώστε να μαθαίνουμε πώς να προστατεύουμε καλύτερα τους εαυτούς μας στο μέλλον.

Οι παρακάτω ερωτήσεις παρέχονται ως μία βασική λίστα ελέγχου ασφάλειας των πληροφοριών για την εταιρία σας, με σκοπό να σας βοηθήσει να εκτιμήσετε σε ποιο σημείο της διαδικασίας βρίσκεστε.

	ΝΑΙ	ΟΧΙ
Είναι η διαδικασία που διαθέτετε σε θέση να αντιμετωπίσει διαφορετικούς τύπους συμβάντων που κυμαίνονται από την άρνηση παροχής υπηρεσιών έως την παραβίαση του απορρήτου κλπ; Και διαθέτει μεθόδους για την αντιμετώπιση αυτών των απειλών;		
Διαθέτει η εταιρία σας ένα επικοινωνιακό σχέδιο για τη διαχείριση συμβάντων;		
Γνωρίζετε ποιες Αρχές πρέπει να ειδοποιήσετε σε περίπτωση συμβάντος;		
Διαθέτει η εταιρεία σας πληροφορίες επαφών, ταξινομημένες και αναγνωρισμένες, για κάθε τύπο συμβάντος;		
Βασίζεστε σε Υπεύθυνο ενδοεπιχειρησιακής επικοινωνίας για τις επαφές με τους υπαλλήλους και τις οικογένειες αυτών;		
Εφαρμόζετε τη διαδικασία «άντλησης διδαγμάτων» ώστε να προβείτε σε βελτιώσεις στον τομέα διαχείρισης συμβάντων μετά από τυχόν συμβάν ασφάλειας πληροφοριών;		

ΠΗΓΕΣ ΚΑΙ ΑΝΑΦΟΡΕΣ

Ένα συνοδευτικό ψηφιακό παράρτημα με περαιτέρω υλικό, το οποίο περιλαμβάνει από πρότυπα πρακτικής έως τεχνικά πρότυπα, προσφέρεται με τον παρόντα Οδηγό. Βρίσκεται αναρτημένο στον διαδικτυακό τόπο www.iccwbo.org/cybersecurity. Ο διαδικτυακός τόπος περιλαμβάνει έναν κατάλογο σχετικών παγκόσμιων πλαισίων, πόρων και επαφών, ενώ σταδιακά θα παρέχονται και τοπικά πλαίσια, εφόσον διατίθενται, με τη συνδρομή των εθνικών επιτροπών και των μελών του ΔΕΕ. Πρόκειται για έναν πίνακα πηγών που διατίθεται τη χρονική στιγμή της δημοσίευσης. Υπάρχει η πρόβλεψη, ωστόσο, να αποτελέσει ένα εργαλείο που θα ενημερώνεται και θα διευρύνεται σταδιακά με το πέρασμα του χρόνου.

www.iccwbo.org/cybersecurity

Ο Οδηγός του ΔΕΕ για την ασφάλεια στον κυβερνοχώρο διατίθεται, επίσης, ηλεκτρονικά μέσω της Πύλης Πηγών μιας Στάσης, η οποία προσφέρει παγκόσμια συναφή πρότυπα και πρότυπα προσαρμοσμένα στις τοπικές ανάγκες, καθώς και πρακτικές και συμβουλές σε ζητήματα σχετικά με τεχνικές και λειτουργικές παραμέτρους της ασφάλειας πληροφοριών.

Η Πύλη σας προσφέρει:

- Τη δυνατότητα μεταφόρτωσης του επιχειρηματικού Οδηγού του ΔΕΕ για την ασφάλεια στον κυβερνοχώρο
- Μεταφρασμένες εκδόσεις του Οδηγού και/ή εκδόσεις προσαρμοσμένες στις τοπικές ανάγκες
- Συνδέσμους (links) προς διεθνώς αναγνωρισμένες ορθές πρακτικές, πρότυπα και πλαίσια
- Κατάλογο δημοσίων φορέων και οργανισμών με παγκόσμια εμβέλεια που δραστηριοποιούνται ενεργά στον τομέα του Κυβερνοχώρου και της ασφάλειας πληροφοριών
- Συνδέσμους (links) προς ένα ξεχωριστό για κάθε χώρο σύνολο πηγών, που έχει εκπονηθεί από εταιρείες, κυβερνητικές υπηρεσίες και άλλες οντότητες.

Το Διεθνές Εμπορικό Επιμελητήριο (ICC)

Το **Διεθνές Εμπορικό Επιμελητήριο [International Chamber of Commerce (ICC)]** είναι ο παγκόσμιος επιχειρηματικός οργανισμός, ένα αντιπροσωπευτικό σώμα που εκφράζει με κύρος τις επιχειρήσεις από όλους τους τομείς δραστηριοτήτων, σε κάθε μέρος του κόσμου.

Βασική αποστολή του ICC είναι η προώθηση του ελεύθερου διεθνούς εμπορίου και των επενδύσεων. Βοηθάει τις επιχειρήσεις να αντιμετωπίσουν τις προκλήσεις και τις ευκαιρίες της παγκοσμιοποίησης. Το ICC έχει την πεποίθηση ότι το εμπόριο είναι μια ισχυρή δύναμη για την ειρήνη και την ευημερία, από την ίδρυσή του στις αρχές του 20^{ου} αιώνα. Η μικρή ομάδα των εμπνευσμένων επιχειρηματιών που ίδρυσαν το ICC αποκαλέστηκαν «Οι έμποροι της ειρήνης».

Το ICC έχει τρεις κύριες δραστηριότητες: τη δημιουργία ρυθμιστικών κανόνων για τις περισσότερες επιχειρηματικές δραστηριότητες, την επίλυση διαφορών, και την υπεράσπιση της πολιτικής του ελεύθερου και θεμιτού εμπορίου. Επειδή οι επιχειρήσεις και οι ενώσεις μέλη του δραστηριοποιούνται στην διεθνή επιχειρηματική κοινότητα, το ICC έχει πρωταρχικό στόχο να καταρτίζει κανόνες που διέπουν τη διεξαγωγή των διασυνοριακών επιχειρηματικών δραστηριοτήτων. Παρά το γεγονός ότι οι κανόνες αυτοί είναι σε εθελοντική βάση, χρησιμοποιούνται καθημερινά σε χιλιάδες συναλλαγές και έχουν γίνει μέρος της δομής του διεθνούς εμπορίου.

Το ICC παρέχει επίσης βασικές υπηρεσίες, μεταξύ των οποίων είναι το Διεθνές Δικαστήριο Διαιτησίας, που είναι το κορυφαίο διαιτητικό όργανο στον κόσμο. Μια άλλη υπηρεσία είναι η Παγκόσμια Ομοσπονδία Επιμελητηρίων (WCF) του ICC, το παγκόσμιο δίκτυο των εμπορικών επιμελητηρίων, που προωθεί την αλληλεπίδραση και ανταλλαγή απόψεων και βέλτιστων πρακτικών στα επιμελητήρια. Το ICC προσφέρει επίσης εξειδικευμένη εκπαίδευση και σεμινάρια και είναι ο κορυφαίος εκδοτικός οίκος παγκοσμίως των πρακτικών και εκπαιδευτικών εργαλείων αναφοράς για τις διεθνείς επιχειρηματικές δραστηριότητες, τις τραπεζικές πρακτικές και την διαιτησία.

Επιχειρηματικοί ηγέτες και εμπειρογνώμονες που προέρχονται από τα μέλη του ICC καθορίζουν μέσω των Επιτροπών του τη στάση των επιχειρήσεων σε γενικά θέματα εμπορικής και επενδυτικής πολιτικής καθώς και σε τεχνικά και ζωτικής σημασίας ειδικά θέματα. Σε αυτά περιλαμβάνονται, μεταξύ άλλων, η καταπολέμηση της διαφθοράς, οι τραπεζικές πρακτικές, η ψηφιακή οικονομία, οι τηλεπικοινωνίες, το ηθικό μάρκετινγκ, το περιβάλλον και η ενέργεια, η πολιτική ανταγωνισμού και η πνευματική ιδιοκτησία.

Το ICC συνεργάζεται στενά με τα Ηνωμένα Έθνη, τον Παγκόσμιο Οργανισμό Εμπορίου και άλλα διακυβερνητικά φόρουμ, συμπεριλαμβανομένου του G20.

Το ICC ιδρύθηκε το 1919. Σήμερα έχει υπό την σκέπη του, πάνω από 6 εκατομμύρια μέλη-επιχειρήσεις, εμπορικά επιμελητήρια και επαγγελματικές ενώσεις σε περισσότερες από 130 χώρες. Οι Εθνικές Επιτροπές συνεργάζονται με το ICC για να αντιμετωπίσουν στις χώρες τους επιχειρηματικούς προβληματισμούς και να μεταφέρουν στις κυβερνήσεις τους τις επιχειρηματικές απόψεις που διατυπώνει το ICC.

Διεθνές Εμπορικό Επιμελητήριο (ICC)
Ο Παγκόσμιος Επιχειρηματικός Οργανισμός
33-43 avenue du Président Wilson, 75116, Παρίσι, Γαλλία
Τηλέφωνο: +33 (0)1 49 53 28 28
Φαξ: +33 (0)1 49 53 28 59
Email: icc@iccwbo.org www.iccwbo.org

Αριθμός έκδοσης: 450/1081-5
Διεθνής Πρότυπος Αριθμός Βιβλίου (ISBN): 978-92-842-0336-9