CYBER SECURITY RISKS

Το Ρυθμιστικό Πλαίσιο, οι Υποχρεώσεις Συμμόρφωσης και οι Προβλέψεις Αποτροπής Κινδύνων

Κωνσταντίνα Λόντου Παπαδημητρίου

Δικηγόρος Παρ' Αρείω Πάγω, Νομική Σύμβουλος

Ιούνιος 2023

ΕΛΛΗΝΙΚΟ ΙΝΣΤΙΤΟΥΤΟ ΑΣΦΑΛΙΣΤΙΚΩΝ ΣΠΟΥΔΩΝ
INSURANCE INSTITUTE OF GREECE
Λεωφόρος Συγγρού 106, 117 41 Αθήνα
106 Syngrou Avenue, 117 41 Athens, Greece
(+30) 210.92.19.660/684, eiasinfo@eias.gr

Περιεχόμενα

Εισαγωγή **3**

Το Ρυθμιστικό Πλαίσιο **3**

Οι Υποχρεώσεις Συμμόρφωσης **5**

Οι Προβλέψεις Αποτροπής Κινδύνων **5**

Εισαγωγή

Με τον όρο "κυβερνοασφάλεια" εννοούμε την ασφάλεια των υπολογιστών ή και την ασφάλεια της τεχνολογίας πληροφοριών δηλαδή την προστασία των συστημάτων και των δικτύων υπολογιστών από την κλοπή ή την βλάβη του υλικού, του λογισμικού ή των ηλεκτρονικών δεδομένων τους, καθώς και από τη διακοπή ή την αλλοίωση των υπηρεσιών που παρέχουν.

Έτσι στην ουσία η κυβερνοασφάλεια είναι η τέχνη προστασίας των αυτοματοποιημένων συστημάτων από κακόβουλους hacker, από μη εξουσιοδοτημένη πρόσβαση ή επίθεση, καθώς και από τυχαίες ή μη ανθρώπινες απειλές. Η ασφάλεια διαδικτύου (cybersecurity) είναι μια ευρεία και συνεχώς εξελισσόμενη περιοχή, που καλύπτει την προστασία των ψηφιακών συστημάτων και των δεδομένων από τις κυβερνοεπιθέσεις. Το ρυθμιστικό πλαίσιο, οι υποχρεώσεις συμμόρφωσης και οι προβλέψεις αποτροπής κινδύνων αποτελούν τους τρεις βασικούς πυλώνες για τη διασφάλιση της ασφάλειας διαδικτύου.

Το Ρυθμιστικό Πλαίσιο

Το ρυθμιστικό πλαίσιο για την κυβερνοασφάλεια στην Ευρωπαϊκή Ένωση (ΕΕ) είναι σύνθετο και πολυεπίπεδο. Αυτό περιλαμβάνει τόσο την ευρωπαϊκή όσο και την εθνική νομοθεσία, καθώς και έναν αριθμό άλλων κανονιστικών εργαλείων.

Το ρυθμιστικό πλαίσιο για την ασφάλεια διαδικτύου στην Ευρωπαϊκή Ένωση καθορίζεται κυρίως από τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) και την Οδηγία για την ασφάλεια των δικτύων και των πληροφοριών (NIS Directive). Ο Κανονισμός GDPR καθορίζει τα πρότυπα για την προστασία των προσωπικών δεδομένων, ενώ η Οδηγία NIS ορίζει μέτρα για ένα υψηλό επίπεδο ασφάλειας των δικτύων και των πληροφοριών σε όλη την ΕΕ. Αυτά τα νομικά εργαλεία παρέχουν τον γενικό πλαίσιο για την προστασία των πληροφοριών και την ασφάλεια των δικτύων στην ΕΕ.

Η ενωσιακή πρωτοβουλία εδράζεται καταρχάς στην ανάγκη προστασίας των συστημάτων και κυρίως του διαδικτύου που- ως αποτέλεσμα της τεχνολογικής έκρηξης των τελευταίων δεκαετιών- διαδραματίζουν ζωτικό ρόλο στην διασφάλιση της ομαλότητας στην οικονομική και κοινωνική ζωή εντός της Ε.Ε.
Εάν μάλιστα αντιπαραβάλει κανείς το θεμελιώδη ρόλο των συστημάτων και του διαδικτύου στην λειτουργία της ελεύθερης κυκλοφορίας αγαθών, υπηρεσιών και προσώπων με την ραγδαία αύξηση του μεγέθους, της συχνότητας και του αντικτύπου των συμβάντων διατάραξης της ασφάλειας μπορεί να αντιληφθεί ότι η ομαλή λειτουργία των συστημάτων αποτελεί ακρογωνιαίο λίθο για την ομαλή λειτουργία της εσωτερικής αγοράς.

Σε εθνικό επίπεδο, τα κράτη μέλη της ΕΕ έχουν την ευθύνη να εφαρμόσουν την Οδηγία NIS και τον Κανονισμό GDPR στην εθνική τους νομοθεσία. Αυτό σημαίνει ότι τα κράτη μέλη πρέπει να διαμορφώσουν τους δικούς τους κανονισμούς και να θέσουν τις δικές τους εθνικές αρχές για την εποπτεία και την εφαρμογή της νομοθεσίας για την κυβερνοασφάλεια.

Εκτός από την Ευρωπαϊκή Ένωση, υπάρχουν πολλοί άλλοι διεθνείς και εθνικοί οργανισμοί που διαμορφώνουν το ρυθμιστικό πλαίσιο για την ασφάλεια διαδικτύου. Για παράδειγμα, στις Ηνωμένες Πολιτείες, το National Institute of Standards and Technology (NIST) εκδίδει κατευθυντήριες γραμμές για την ασφάλεια των πληροφοριών και των δικτύων.

Εκτός από την Οδηγία NIS και τον Κανονισμό GDPR, υπάρχουν και άλλες σημαντικές ευρωπαϊκές και διεθνείς πρωτοβουλίες και συμφωνίες που σχετίζονται με την κυβερνοασφάλεια, όπως η Συνθήκη του Συμβουλίου της Ευρώπης για το έγκλημα του κυβερνοχώρου (Συνθήκη του Βουδαπέστης) και το πλαίσιο του ΟΗΕ για την υπεράσπιση της ειρήνης και της ασφάλειας στον κυβερνοχώρο.

Το 2018 ενσωματώθηκε στην ελληνική νομοθεσία η οδηγία 2016/1148/ΕΕ,(NIS) οποία προέβλεπε την υιοθέτηση κοινών προτύπων από τα κράτη μέλη για την επίτευξη κοινού επιπέδου ασφάλειας συστημάτων δικτύου και πληροφοριών (cyber security). Η οδηγία αυτή υιοθετήθηκε με τον ν.4577/2018 και δημιουργήθηκε η Εθνική Αρχή Κυβερνοασφάλειας, η οποία εξέδωσε την Απόφαση 1027/2019 που αφορά στις διαδικασίες και τον τρόπο εφαρμογής της οδηγίας και παρέχονται κατευθύνσεις για την ενίσχυση της Ιδιωτικότητας των πολιτών.

Στη συνέχεια, εκδόθηκε ο ν.4961/2022 που αφορά στις αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, στην ενίσχυση της ψηφιακής διακυβέρνησης, στη ψηφιακή αναβάθμιση της δημόσιας διοίκησης με στόχο τη διαμόρφωση των κατάλληλων εγγυήσεων για την διασφάλιση των δικαιωμάτων των φυσικών και νομικών προσώπων και την ενίσχυση της λογοδοσίας και της διαφάνειας κατά την χρήση συστημάτων τεχνητής νοημοσύνης. Στο πλαίσιο αυτό εξεδόθη και η ΠΕΕ195/2021, που ρυθμίζει το πλαίσιο του cyber security στις ασφαλιστικές επιχειρήσεις.

Κατά συνέπεια η εξασφάλιση των ελάχιστων κοινών απαιτήσεων ασφαλείας των συστημάτων και του διαδικτύου με σκοπό την προαγωγή της νοοτροπίας διαχείρισης των σοβαρών συμβάντων κρίθηκε απαραίτητη, διότι δεν είναι το κανονιστικό πλαίσιο, που επιβάλλει την συμμόρφωση, αλλά το πλήθος, η ένταση, ο κίνδυνος και ο αντίκτυπος που επισύρουν τα συμβάντα καθ' αυτά.
Ακόμη και αν το πλαίσιο δεν υπήρχε, η ίδια η αγορά θα αντιλαμβανόταν ότι η δημιουργία κοινών προτύπων ασφαλείας είναι ζήτημα επιβίωσης διότι οι κυβερνοεπιθέσεις θέτουν σε κίνδυνο όχι απλώς την φήμη και την προσωρινή λειτουργία τους, αλλά και την ίδια τους την υπόσταση.

Από τα παραπάνω συνάγεται ότι το νέο πλαίσιο δεν είναι μια επιπλέον επιβάρυνση, αλλά μια πρώτης τάξεως ευκαιρία για όλους να προσαρμοστούν εγκαίρως στην πραγματικότητα και κυρίως στους κινδύνους που εμφιλοχωρούν σε ένα επιχειρηματικό περιβάλλον, που διαμορφώνεται πλέον αποκλειστικά με όρους και συνθήκες διαδικτύου.

Οι Υποχρεώσεις Συμμόρφωσης

Οι επιχειρήσεις και οι οργανισμοί, που διαχειρίζονται προσωπικά δεδομένα και ψηφιακά δίκτυα έχουν σημαντικές και πολύπλοκες υποχρεώσεις συμμόρφωσης. Πρέπει να διασφαλίζουν ότι τα συστήματα και οι διαδικασίες τους συμμορφώνονται με τα πρότυπα ασφάλειας, που ορίζονται από τον Κανονισμό GDPR και την Οδηγία NIS.

Για παράδειγμα, πρέπει να υλοποιούν τεχνικά και οργανωτικά μέτρα για να διασφαλίζουν το απαραίτητο επίπεδο ασφάλειας και να προστατεύουν τα δεδομένα που επεξεργάζονται από την καταστροφή, την απώλεια, την τροποποίηση, την ανεπιθύμητη διαρροή ή την παράνομη πρόσβαση. Επίσης, πρέπει να προετοιμάζονται για περιστατικά, που αφορούν την ασφάλεια των πληροφοριών, καθώς και να αναφέρουν τις παραβιάσεις της ασφάλειας των δεδομένων στις αρμόδιες αρχές. Στα αποτελεσματικά μέτρα ασφαλείας συμπεριλαμβάνονται η προστασία των προσωπικών δεδομένων, η αναφορά περιστατικών ασφαλείας και η συμμόρφωση με τους κανονισμούς και τις πρακτικές που ορίζονται από την ΕΕ.

Οι οργανισμοί πρέπει επίσης να διασφαλίσουν ότι οι συμβάσεις τους με τρίτους, συμπεριλαμβανομένων των προμηθευτών, των υπεργολάβων και των εταίρων, συμμορφώνονται επίσης με τις απαιτήσεις για την κυβερνοασφάλεια. Αυτό μπορεί να σημαίνει την εφαρμογή συγκεκριμένων μέτρων ασφαλείας, την προστασία των προσωπικών δεδομένων και την παρακολούθηση της συμμόρφωσης των τρίτων.

Οι Προβλέψεις Αποτροπής Κινδύνων

Η πρόληψη και η αποτροπή των κινδύνων είναι ίσως ο πιο σημαντικός πυλώνας της ασφάλειας διαδικτύου**. Η εφαρμογή τεχνολογιών ασφάλειας**, όπως το firewall, τα συστήματα ανίχνευσης εισβολών, η κρυπτογράφηση και τα συστήματα προστασίας από ιούς, μπορούν να βοηθήσουν στην αποτροπή των κυβερνοεπιθέσεων. Ωστόσο, η τεχνολογία μόνη της δεν είναι αρκετή. Οι οργανισμοί πρέπει επίσης **να επενδύουν στην εκπαίδευση και την ευαισθητοποίηση των υπαλλήλων τους,** σχετικά με τις απειλές της ασφάλειας διαδικτύου. Πολλές κυβερνοεπιθέσεις, όπως τα phishing, στοχεύουν τους ανθρώπους περισσότερο από την τεχνολογία. Ως εκ τούτου, η εκπαίδευση των υπαλλήλων μπορεί να είναι μια αποτελεσματική μέθοδος προληπτικής ασφάλειας.

Επιπλέον, οι οργανισμοί πρέπει να προβαίνουν σε **διαρκείς αξιολογήσεις κινδύνου** για να αναγνωρίσουν και να αντιμετωπίσουν τις ευάλωτες πτυχές της υποδομής τους. Το προσωπικό ασφάλειας πληροφοριών πρέπει να ενημερώνεται τακτικά για τις πιο πρόσφατες **απειλές και τεχνικές επίθεσης**, ενώ πρέπει επίσης να διεξάγονται **τακτικά δοκιμές** περίπτωσης εκτάκτου ανάγκης και ασκήσεις ανάκτησης από περιστατικό, για να διασφαλίζεται η ετοιμότητα του οργανισμού.

Η αποτροπή των κινδύνων στην κυβερνοασφάλεια προϋποθέτει μια συνεχή και δυναμική προσέγγιση. Οι οργανισμοί πρέπει να διαθέτουν συστήματα και διαδικασίες που τους επιτρέπουν να αντιδρούν γρήγορα και αποτελεσματικά σε πιθανά περιστατικά ασφαλείας.

Η προσέγγιση αυτή απαιτεί επίσης την κατανόηση των τρεχόντων και των εκκρεμών απειλών και κινδύνων, καθώς και την προσαρμογή των μέτρων ασφαλείας και των στρατηγικών ανάλογα. Αυτό μπορεί να περιλαμβάνει την εφαρμογή νέων τεχνολογιών και λύσεων, όπως η τεχνητή νοημοσύνη και η μηχανική μάθηση για την αντιμετώπιση σύνθετων και εξελισσόμενων απειλών.

Η ασφάλιση των κινδύνων που προκύπτουν στον κυβερνοχώρο έχει σχεδιαστεί για να βοηθήσει τις επιχειρήσεις να αντισταθμίσουν τις δυνητικά καταστροφικές συνέπειες των εγκλημάτων στον κυβερνοχώρο, όπως κακόβουλο λογισμικό, ransomware, επιθέσεις κατανεμημένης άρνησης υπηρεσίας (DDoS) ή οποιαδήποτε άλλη μέθοδο που χρησιμοποιείται για να θέσει σε κίνδυνο ένα δίκτυο και ευαίσθητα δεδομένα. Μπορεί να καλύψει ένα ευρύ φάσμα απωλειών κινδύνου στον κυβερνοχώρο που μπορεί απροσδόκητα να προκύψουν από επιθέσεις στον κυβερνοχώρο, όπως φυσική ζημιά σε υλικό, απώλεια επιχειρηματικού εισοδήματος, νομικές αμοιβές, κόστος ανάκτησης δεδομένων και άλλα. Η ασφάλιση στον κυβερνοχώρο μπορεί να προσφέρει υποστήριξη σε επιχειρήσεις που υφίστανται ένα περιστατικό στα δίκτυα και δεδομένα τους και να τις βοηθήσει να ανακάμψουν από αυτό. Ωστόσο δεν υποκαθιστά την άμυνα της κυβερνοασφάλειας και δεν αποτρέπει την παραβίαση/επίθεση στο χώρο αυτό. Οι επιχειρήσεις πρέπει να επενδύσουν στις κατάλληλες λύσεις και πρακτικές κυβερνοασφάλειας για να μειώσουν την έκθεσή τους σε αυτούς τους κινδύνους και να πληρούν τις προϋποθέσεις για καλύτερη κάλυψη και ποσοστά.

Οι ασφαλιστικές επιχειρήσεις ασφαλίζουν τους κινδύνους αυτούς και μερικά από τα οφέλη που μπορεί να προκύψουν από την ασφάλιση των κινδύνων από τον κυβερνοχώρο είναι:

- Η βοήθεια στην επιχείρηση να ανακάμψει από τις οικονομικές απώλειες, που προκαλούνται από περιστατικά στον κυβερνοχώρο, όπως παραβιάσεις δεδομένων, επιθέσεις ransomware, διακοπή επιχείρησης, νομικές χρεώσεις και άλλα.
- Η παροχή συμβουλών με την υποστήριξη ειδικών σχετικά με τον τρόπο αντιμετώπισης και διαχείρισης ενός περιστατικού στον κυβερνοχώρο, όπως η ιατροδικαστική έρευνα, η ειδοποίηση πελατών, οι δημόσιες σχέσεις και η παρακολούθηση απειλών.

- Η βελτίωση στο επίπεδο ασφάλειας δίνοντας κίνητρα προκειμένου να υιοθετηθούν καλύτερα μέτρα και πρακτικές ασφάλειας στον κυβερνοχώρο, καθώς οι ασφαλιστικές επιχειρήσεις μπορεί να προσφέρουν χαμηλότερες τιμές ή καλύτερη ασφαλιστική κάλυψη έναντι των κινδύνων αυτών για επιχειρήσεις με ισχυρά πρότυπα ασφαλείας.
- Τέλος μπορεί να βοηθηθούν οι μέτοχοι και η διοίκηση της επιχείρησης προκειμένου να αυξήσει την επίγνωσή του για τους κινδύνους στον κυβερνοχώρο και τις συνέπειές τους για να υπάρξει καλύτερη πρόληψη και σχέδιο διαχείρισης κινδύνων στον κυβερνοχώρο. Προκειμένου να προστατευθεί η επιχείρηση από αξιώσεις ευθύνης και αγωγές τρίτων που ενδέχεται να επηρεαστούν από ένα περιστατικό στον κυβερνοχώρο, που αφορά την επιχείρηση, όπως πελάτες, συνεργάτες ή ρυθμιστικές αρχές.

Μερικοί από τους παράγοντες που μπορεί να επηρεάσουν το ασφάλιστρο είναι:

- Το μέγεθος και η φύση της επιχείρησής
- Ο τύπος και η ποσότητα των δεδομένων που αποθηκεύει και επεξεργάζεται μια επιχείρηση
- Το επίπεδο και η ποιότητα των μέτρων και των πρακτικών καθώς και η οργανωτική δομή για την κυβερνοασφάλεια
- Τα όρια κάλυψης
- Το ιστορικό αξιώσεων της επιχείρησης και του κλάδου, που υπάγεται.

Συμπερασματικά θα μπορούσε να λεχθεί ότι στην εποχή της ψηφιακής τεχνολογίας, η ασφάλεια διαδικτύου είναι απαραίτητη για την προστασία των πληροφοριών και των δικτύων. Οι οργανισμοί έχουν σημαντικές υποχρεώσεις συμμόρφωσης. Ωστόσο, για να αποτρέψουν τους κινδύνους, πρέπει επίσης να επενδύσουν στην τεχνολογία, στην εκπαίδευση και στη διαχείριση των κινδύνων. Στον κόσμο της ασφάλειας διαδικτύου, η πρόληψη είναι πάντα καλύτερη από τη θεραπεία.

Συνολικά, το ρυθμιστικό πλαίσιο, οι υποχρεώσεις συμμόρφωσης και οι προβλέψεις αποτροπής κινδύνων αποτελούν τρείς βασικούς άξονες σε επίπεδο κυβερνοασφάλειας. Η επιτυχής αντιμετώπιση των προκλήσεων στον τομέα αυτόν απαιτεί μια ολοκληρωμένη, συνεχή και δυναμική προσέγγιση.

Σε επίπεδο εφαρμογής, οι οργανισμοί πρέπει να ενσωματώσουν πολιτικές και διαδικασίες για τη διασφάλιση της κυβερνοασφάλειας. Η συμμόρφωση με τα ρυθμιστικά πλαίσια και τις πρακτικές καλύτερης διαχείρισης απαιτεί επένδυση σε ανθρώπινο δυναμικό, τεχνολογικές υποδομές και εκπαίδευση. Είναι σημαντικό οι οργανισμοί να διατηρούν επίγνωση των εξελισσόμενων απειλών και να αναθεωρούν τακτικά τις στρατηγικές ασφαλείας τους.

Οι απειλές κυβερνοασφάλειας είναι διαρκώς σε εξέλιξη και οι οργανισμοί πρέπει να διατηρούν σταθερή επαγρύπνηση για να τις αντιμετωπίσουν. Αυτό σημαίνει ότι πρέπει να εφαρμόσουν εργαλεία ανίχνευσης και προστασίας, να δημιουργήσουν συστήματα ανταπόκρισης σε περιστατικά και να καταρτίσουν το προσωπικό τους στις καλύτερες πρακτικές ασφαλείας. Είναι εξίσου σημαντικό η διοίκηση των οργανισμών να δεσμευτεί στην κυβερνοασφάλεια και να την καταστήσει προτεραιότητα.

Συνεπώς η κυβερνοασφάλεια δεν είναι μόνο ένα τεχνικό ζήτημα, αλλά και ένα ζήτημα διαχείρισης κινδύνου που απαιτεί συνεχή επαγρύπνηση, επενδύσεις και εκπαίδευση.