Κυβερνοασφάλεια & πρακτικές διαχείρισης κινδύνου

Κώστας Χ. Αργυρόπουλος
General Counsel SPACE HELLAS GROUP
Chief Legal & Compliance Officer

9th Data Privacy & Protection conference
Athens May 28, 2024

SPACE

Classification ISO 27001: Public

www.space.gr

Κυβερνοασφάλεια & Τεχνητή νοημοσύνη

Η τεχνητή νοημοσύνη στην κυβερνοασφάλεια έχει δύο πλευρές, η μία από την πλευρά του επιτιθέμενου και η άλλη από την πλευρά του αμυνόμενου, του οργανισμού δηλαδή που δέχεται την επίθεση και χρησιμοποιεί εργαλεία για να είναι τα συστήματά του πιο δυναμικά και ανθεκτικά.

Το 2023 ήταν μια χρονιά με μεγάλη αύξηση στις κυβερνοεπιθέσεις παγκοσμίως και αντίστοιχα αρχή για σημαντικές επενδύσεις στην κυβερνοασφάλεια.

Το κόστος για την προστασία από κυβερνοεπιθέσεις αναμένεται να φτάσει τα 23.84 τρισ. $ έως το 2027, από 8.44 τρισ. $ το 2022.

Τα πλέον πρόσφατα στοιχεία που ανακοινώθηκαν με το Munich Security Index 2024 καταγράφουν τις κυβερνοεπιθέσεις ως το 2ο μεγαλύτερο κίνδυνο μετά τα ακραία καιρικά φαινόμενα. Σε ΗΠΑ, Κίνα και Ιαπωνία είναι στην 1η θέση και σε Ην. Βασίλειο στη 2η.

https://securityconference.org/en/munich-security-report-2024/munich-security-index-2024/

Πρακτικές προετοιμασίας

Η προετοιμασία σε μία προληπτική πολιτική για την κυβερνοασφάλεια απαιτεί:

- Να έχει γίνει κατανοητό πόσο η δομή του οργανισμού μπορεί να έχει αντίδραση στην απάντηση που θα δοθεί σε ένα περιστατικό κυβερνοεπίθεσης.
- Να έχει γίνει καταγραφή των διαφόρων κατηγοριών κυβερνοεπιθέσεων και προετοιμασία στη λήψη επιχειρηματικών αποφάσεων σε συνθήκες πολύ περιορισμένης πληροφόρησης.
- Την εξέταση του περιστατικού από την οπτική των διαφόρων επιχειρηματικών λειτουργιών οι οποίες θα επηρεαστούν από τη λήψη των αποφάσεων κατά τη διάρκεια της κυβερνοεπίθεσης, καθώς και των σεναρίων επηρεασμού των εργαζομένων, πελατών και άλλων προσώπων σε θέσεις ευθύνης.
- Εκτίμηση των συνεπειών στη φήμη του οργανισμού ως αποτέλεσμα της κυβερνοεπίθεσης και αξιολόγηση της λήψης πιθανών μέτρων για τον περιορισμό της ζημίας.

Παράγοντες επιτυχίας

- Η σωστή διαχείριση του χρόνου. Συνήθως θα πρέπει να υπολογίζουμε και αντίδραση σε πιο σύντομο χρόνο από τον απαιτούμενο.
- Η ικανότητα της διαχείρισης ανθρώπων διαφορετικών καθηκόντων στον οργανισμό.
- Η ομαδική δουλειά και στην προετοιμασία και στο στάδιο της απόφασης.

Επίπεδα διαχείρισης κίνδυνου: #1 Η ενημέρωση για το περιστατικό

- Πλήρης ενημέρωση – Διερεύνηση για τις αρχές που θα καθορίσουν την απάντησή μας.
- Με βάση την πληροφόρηση: Αναγνώριση μερικών (3-4) από τους παράγοντες κινδύνου & περιπτώσεων περιορισμού ζημίας ή μείωσης επικειμένων κινδύνων.
- Εκτίμηση των βασικών αντιδράσεων.
- Επικοινωνιακή πολιτική εντός και εκτός οργανισμού.

Επίπεδα διαχείρισης κίνδυνου:
2 Η εκτίμηση των στοιχείων από τα δεδομένα – στάδιο διαπραγμάτευσης

- Πρώτη εκτίμηση της απώλειας δεδομένων – Αξιολόγηση κινδύνου σε σχέση με τη διαπραγμάτευση.
- Ανάλυση επιπτώσεων στη στρατηγική της διαπραγμάτευσης.
- Επόμενο στάδιο επικοινωνίας με τρίτους ενδιαφερόμενους.
- Νέα επικοινωνία με εργαζομένους.
- Προετοιμασία για την υλοποίηση της διαπραγμάτευσης.

Επίπεδα διαχείρισης κίνδυνου:
3 Η αποκατάσταση – έλεγχος «παραδοτέων»

- Ανάκτηση δεδομένων – έλεγχος στο dark web.
- Σύνταξη έκθεσης – απόφαση εταιρικών οργάνων.
- Επικοινωνιακή πολιτική.

Επίπεδα διαχείρισης κίνδυνου: # 4 – Διαρροή των δεδομένων – δημοσιότητα – εκτίμηση κινδύνων

- Η εκτίμηση για την αλλαγή στρατηγικής.
- Αξιολόγηση των κινδύνων.
- Επικοινωνιακή πολιτική – ερωτήσεις & απαντήσεις.
- Ενέργειες για διατήρηση ή ανάκτηση πελατών.
- Παρουσίαση στο διοικητικό συμβούλιο – προετοιμασία εισήγησης και γνωμοδοτήσεων.

Νέες συστήματα – νέοι κίνδυνοι – Ψηφιακές ικανότητες

- Τα εργαλεία τεχνητής νοημοσύνης – η επίδραση στην κυβερνοασφάλεια.
- Οι ελλείψεις στην αγορά εξειδικευμένων επαγγελματιών.
- Σε όλα τα κράτη μέλη καταγράφεται σημαντική υστέρηση σε ειδικούς στην τεχνολογία. Αυτό εμποδίζει την ανάπτυξη και την ομαλή ενσωμάτωση των νέων εφαρμογών στις ψηφιακές τεχνολογίες. Σε περιοχές κλειδιά όπως η κυβερνοασφάλεια και η ανάλυση δεδομένων υπάρχουν σταθερά εκατοντάδες χιλιάδες κενές θέσεις.
- Το 2023, οι ελλείψεις σε εξειδικευμένο προσωπικό στην κυβερνοασφάλεια κυμάνθηκαν μεταξύ 260.000 και 500.000, ενώ η εκτίμηση είναι για ανάγκες 883.000 επαγγελματικών.
- Ο ευρωπαϊκός στόχος για το 2030 είναι να υπάρχουν 20.000.000 ειδικοί στις τεχνολογίες πληροφορικής, που θα αντιπροσωπεύουν το 10% του συνολικού εργατικού δυναμικού, με σχετική ισορροπία.

Κυβερνοασφάλεια & Διαχείριση «νέων» κινδύνων

- Όσο η τεχνητή νοημοσύνη θα ενισχύεται με νέα προϊόντα και εφαρμογές, τόσο και οι κυβερνοεπιθέσεις θα δημιουργούν νέα δεδομένα.
- Χρειάζεται ενημέρωση, εκπαίδευση, προετοιμασία και κυρίως εύκολη προσαρμογή στις νέες τεχνολογικές προοπτικές.
- Επικαιροποίηση των πολιτικών των οργανισμών τόσο για την προληπτική προσέγγιση όσο και για την αντιμετώπιση της κρίσης και τη διαχείριση των «νέων» κινδύνων.

Εισηγήσεις 2024

- «Ψηφιακός μετασχηματισμός και διοίκηση. Ευρωπαϊκές ευκαιρίες και προκλήσεις», Διαδικτυακή εκδήλωση της Ευρωπαϊκής Έδρας Jean Monnet "Citizen Europe" του Πανεπιστημίου Αιγαίου, στο πλαίσιο της δράσης της «Απογεύματα της Ευρώπης», Εισήγηση με θέμα: «Τεχνητή νοημοσύνη και δημόσιες συμβάσεις», 17 Μαΐου 2024.
- «Τεχνολογίες τεχνητής νοημοσύνης – κυβερνοασφάλεια – προστασία δεδομένων προσωπικού χαρακτήρα – κανόνες διακυβέρνησης», Συμμετοχή στην ενότητα «AI & προσωπικά δεδομένα», «Practitioners perspective», 10ο συνέδριο «Δικαίου Τεχνολογίας & Επικοινωνιών», Νομική Βιβλιοθήκη, 13 Μαρτίου 2024.
- «Making smart choices in selecting AI tools for the right purpose» - Συμμετοχή στην ενότητα «Legal Components of AI Tools: Comparative Analysis», The GenAI Summit, 29 Φεβρουαρίου – 2 Μαρτίου 2024.
- «Πολιτικές κυβερνοασφάλειας και τεχνητής νοημοσύνης στην εταιρική διακυβέρνηση», Corporate Governance & Compliance Forum – Leveraging Good Governance for Business Success, Διοργάνωση BOUSSIAS, 14 Φεβρουαρίου 2024.

Εισηγήσεις 2023

- «Μπορεί η τεχνητή νοημοσύνη να πετύχει καλύτερα αποτελέσματα από τους διαχειριστές;» - Συμμετοχή στην ενότητα με εισήγηση για το νομικό πλαίσιο της τεχνητής νοημοσύνης, ΣΥΝΔΕΣΜΟΣ ΕΠΕΝΔΥΤΩΝ ΚΑΙ ΔΙΑΔΙΚΤΥΟΥ, 21ο ΕΠΕΝΔΥΤΙΚΟ & ΧΡΗΜΑΤΙΣΤΗΡΙΑΚΟ ΣΥΝΕΔΡΙΟ, Γενικός τίτλος: «ΕΠΕΝΔΥΣΕΙΣ, στην εποχή της Τεχνητής Νοημοσύνης και της Κλιματικής Αλλαγής», 9 Δεκεμβρίου 2023.
- «M&A Roundtable Greece 2023» - Συμμετοχή για την αγορά πληροφορικής με εισήγηση για την Τεχνητή Νοημοσύνη και την Κυβερνοασφάλεια, διοργάνωση της MASOUROS ATTORNEYS AT LAW, διοργάνωση «THE LEGAL 500», 1 Δεκεμβρίου 2023.
- «Ευρωπαϊκή Οικονομία και Κοινωνία. Η σημασία των δημοσίων συμβάσεων», Διαδικτυακή εκδήλωση της Ευρωπαϊκής Έδρας Jean Monnet "Citizen Europe" του Πανεπιστημίου Αιγαίου, στο πλαίσιο της δράσης της «Απογεύματα της Ευρώπης», 24 Νοεμβρίου 2023.
- «Ethics & Governance in Legal Practice» - LAW IN ACTION 2023, 24 Οκτωβρίου 2023.
- «Integrating Advanced LLMs in Legal Practice: ChatGPT and the Next Steps in Digitalisation» - European General Counsel Forum, ECLA's 40th anniversary, Φρανκφούρτη, 19 Σεπτεμβρίου 2023.
- «Predictive Analysis in Law», Συμμετοχή στο roundtable της δικηγορικής εταιρείας «ΚΟΥΤΑΛΙΔΗΣ», 15ο ΠΑΝΕΛΛΗΝΙΟ ΣΥΝΕΔΡΙΟ ΔΙΚΗΓΟΡΩΝ ΝΟΜΙΚΩΝ ΥΠΗΡΕΣΙΩΝ – «Η Νομική Υπηρεσία στην Εποχή του ESG & του ChatGPT», Νομική Βιβλιοθήκη, Ζάππειο Μέγαρο, 13 Ιουνίου 2023.

Empowering

Your Digital Transformation Journey

Thank you for your attention

www.space.gr