

Ο ρόλος του Data Protection Officer και η χρήση της ασφάλισης cyber insurance

Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Νίκος Γεωργόπουλος, *Cyber Privacy Risks Advisor, Cromar coverholder at Lloyd's, Founding Member DPO Academy*

1. Εισαγωγικά

Τα περιστατικά παραβίασης συστημάτων και ο κυβερνοασφάλεια αποτελούν πηγή ανησυχίας για κάθε εταιρεία, δεδομένης της φύσης των πληροφοριών που διαχειρίζεται.

Όπως αποδεικνύεται από πρόσφατα περιστατικά παραβίασης συστημάτων, το πώς ένας οργανισμός χειρίζεται μια κρίση διαδραματίζει σημαντικό ρόλο στο κατά πόσο ο διευθύνων σύμβουλος και τα ανώτατα στελέχη (CIO, COO, CMO, CRO, CFO κ.λπ.) παραμένουν στη θέση τους.

Η πρόσβαση στον κυβερνοχώρο έχει δημιουργήσει νέες επιχειρηματικές ευκαιρίες για τις εταιρείες, γιατί προσφέρει τη δυνατότητα της αποτελεσματικής επικοινωνίας με τα δίκτυα διανομής και τον τελικό πελάτη, απλοποιεί τις διαδικασίες πλειουργίας τους και προσφέρει τη δυνατότητα της πρόσβασης σε νέα τμήματα της αγοράς, με προϊόντα και υπηρεσίες χαμηλότερου κόστους.

Αυτό άλλωστε είναι και το σημαντικότερο πλεονέκτημα από τη χρήση του κυβερνοχώρου. Όμως, σε αυτόν δραστηριοποιούνται και κυβερνοεγκληματίες, οι οποίοι έχουν στόχο να υποκλέψουν δεδομένα και εμπιστευτικές πληροφορίες που διατηρούν οι εταιρείες, όπως οικονομικές εκθέσεις, μισθοδοσίες υπαλλήλων, βάσεις δεδομένων πελατών, κωδικούς πρόσβασης, εμπορικά μυστικά, σχέδια του μάρκετινγκ, σχέδια δημιουργίας νέων προϊόντων και υπηρεσιών, συμβάσεις συνεργασίας με τα δίκτυα διανομής, δεδομένα υγείας, αριθμούς πιστωτικών καρτών και τραπεζικών πλογαριασμών, περιουσιακά και προσωπικά οικονομικά στοιχεία πελατών.

Επίσης, μπορούν να δημιουργηθούν προβλήματα στην ομαλή λειτουργία και διαθεσιμότητα των συστημάτων μιας εταιρείας μέσω των κυβερνοεπιθέσεων που μπορούν να οδηγήσουν σε άρνηση παροχής υπηρεσίας (DDoS) των συστημάτων εξυπηρέτησης και απλοίωση της ποιότητας των δεδομένων της εταιρείας.

Η Ευρωπαϊκή Ένωση για την προστασία των προσωπικών δεδομένων των Ευρωπαίων πολιτών δημιούργησε τον Γενικό Κανονισμό για την Προστασία των Προσωπικών Δεδομένων (GDPR), η ισχύς του οποίου ξεκινά την 25.5.2018, και σε αυτόν περιγράφονται οι υποχρεώσεις των εταιριών για την προστασία των προσωπικών δεδομένων που διατηρούν και οι συνέπειες σε περίπτωση που δεν θα καταφέρουν να διατηρήσουν την ασφάλεια των δεδομένων.

Στη συνέχεια θα αναφερθούμε συνοπτικά στον Γενικό Κανονισμό Προστασίας Δεδομένων, στον ρόλο του Data Protection Officer και στην ασφάλιση Cyber Insurance:

2. Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR)

Ο Νέος Γενικός Κανονισμός συνοπτικά απαιτεί από τις εταιρίες:

- να έχουν εκπαιδεύσει κατάλληλα το ανθρώπινο δυναμικό τους,
- να ενσωματώσουν στις διαδικασίες τους τα δικαιώματα των υποκειμένων των δεδομένων,
- να έχουν τα κατάλληλα μέτρα ασφαλείας και τις αναγκαίες πολιτικές για την προστασία των πληροφοριών,
- να έχουν τα κατάλληλα τεχνικά και οργανωτικά μέτρα που θα διασφαλίζουν τη διαθεσιμότητα της Πληροφορίας (Σχέδιο Επιχειρησιακής Συνέχειας),
- να κάνουν αναλύσεις των επιπτώσεων που μπορούν να προκύψουν πλόγω παραβίασης ιδιωτικότητας (Privacy Impact Assessment),
- να σχεδιάζουν προϊόντα και υπηρεσίες λαμβάνοντας υπόψη την προστασία της ιδιωτικότητας (Privacy by Design, Privacy by Default),
- να ενημερώνουν τις αρμόδιες αρχές εντός 72 ωρών από τον εντοπισμό συμβάντος παραβίασης συστημάτων και απώλειας δεδομένων,
- να έχουν ορίσει υπεύθυνο για την προστασία των δεδομένων (Data Protection Officer),
- να έχουν πλάνο αντιμετώπισης περιστατικών παραβίασης συστημάτων και απώλειας δεδομένων (Incident Response Plan).

Επίσης, ο νέος κανονισμός προβλέπει πρόστιμα τα οποία μπορούν να φθάσουν έως 4% του τζίρου της επιχείρησης ή 20 εκ. €, επιβάλλεται όποιο από τα δύο είναι μεγαλύτερο.

Ο νέος Κανονισμός αναμένεται να υποχρεώσει τις εταιρίες να συμμορφωθούν στα νέα δεδομένα, να προετοιμαστούν κατάλληλα επιλέγοντας προϊόντα και υπηρεσίες προστασίας των πληροφοριών που διαχειρίζονται, που θα τις βοηθήσουν να αντιμετωπίσουν αποτελεσματικά μελλοντικά περισταστικά, δημιουργώντας τις κατάλληλες συνθήκες που θα εξασφαλίσουν την ασφαλισμότητα των εταιριών και την ανάπτυξη της αγοράς του cyber insurance.

3. Ο Ρόλος του Data Protection Officer

Ο Data Protection Officer αναλαμβάνει να:

- εκπροσωπήσει την Επιχείρηση έναντι των Αρχών, Εθνικών και Ευρωπαϊκών,

- να διασφαλίσει την εναρμόνιση της πειτουργίας της επιχείρησης σε ότι αφορά τις πολιτικές πρακτικές και μεθοδολογία επεξεργασίας, αποθήκευσης και μεταφοράς Δεδομένων Προσωπικού Χαρακτήρα με το νέο αυστηρό νομοθετικό πλαίσιο και να δημιουργήσει την κατάλληλη κουλτούρα στο ανθρώπινο δυναμικό της εταιρίας,
- να προστατέψει την επιχείρηση από τους κινδύνους επιβολής των σημαντικότατων και βαρύτατων διοικητικών προτίμων που προβλέπει ο Κανονισμός τα οποία εκκινούν από 10.000.000 € ή το 2% του παγκόσμιου τζίρου εάν πρόκειται για διεθνή όμιλο και φτάνουν σε περίπτωση παράβασης βασικών διατάξεων του κανονισμού σε 20.000.000 € ή στο 4% του παγκόσμιου τζίρου.

Ο Data Protection Officer θα πρέπει να έχει τις κατάλληλες γνώσεις και δεξιότητες για να ανταποκριθεί στον ρόλο του με αποδειγμένη (πιστοποιημένη από ανεξάρτητο φορέα) γνώση και εμπειρία στη νομοθεσία και πρακτική εφαρμογή των διαδικασιών διαχείρισης προσωπικών δεδομένων, ο οποίος θα έχει εχέγγυα ανεξαρτησίας και θα αναφέρεται απευθείας στον CEO ή σε μέλος του Δ.Σ μιας εταιρίας.

4. Η αγορά των Data Protection Officers

Σύμφωνα με μελέτη του IAPP (International Association of Privacy Professionals) ο αναγκαίος αριθμός DPOs στην Ευρώπη εκτιμάται ότι θα ανέλθει σε 28.000 τουλάχιστον και αν ληφθεί υπόψη και η υποχρέωση εταιριών εκτός Ευρωπαϊκής Ένωσης οι οποίες για να προωθήσουν προϊόντα ή υπηρεσίες σε πολίτες της Ευρωπαϊκής Ένωσης θα πρέπει να έχουν ορίσει Data Protection Officers ο αριθμός αυτών εκτιμάται ότι θα ανέλθει σε 75.000 τουλάχιστον.

Ειδικά για την Ελλάδα η αρχική εκτίμηση για τον αριθμό των DPOs ήταν 373, η εκτίμηση αυτή βασίζονταν στο γεγονός ότι στην αρχική φάση ο Κανονισμός ζητούσε μόνο οι εταιρίες που είχαν προσωπικό άνω των 250 εργαζομένων να διαθέτουν DPO κάτι το οποίο άλλαξε και αναμένεται να αυξήσει σημαντικά τον υπολογιζόμενο αριθμό των DPOs.

5. Η ασφάλιση Cyber Insurance

Η ασφάλιση Cyber Insurance αποτελεί ένα κρίσιμο κομμάτι της στρατηγικής για τη διαχείριση των κινδύνων που πρέπει να χρησιμοποιεί κάθε εταιρία για να διαχειριστεί τον υπολοιπόμενο κίνδυνο (residual risk) που δεν μπορεί να μειώσει με την χρήση διαδικασιών και πολιτικών διαχείρισης.

Λαμβάνοντας υπόψη ότι 100% ασφάλεια δεν υπάρχει οι εταιρίες θα πρέπει να εξετάσουν την δυνατότητα μεταφοράς του κινδύνου που απομένει και δεν μπορούν να μειώσουν περαιτέρω σε ασφαλιστικά προϊόντα cyber insurance.

Ενώ η ασφάλιση δεν μπορεί να εμποδίσει ένα περιστατικό παραβίασης ασφάλειας, μπορεί εκτός από την κάλυψη των οικονομικών επιπτώσεων, να βοηθήσει στην καλύτερη υλοποίηση του πλάνου αντιμετώπισης περιστατικών (Incident Response Plan) παραβίασης συστημάτων και απώλειας προσωπικών δεδομένων παρέχοντας εξειδικευμένες ομάδες ειδικών με εμπειρία στην διαχείριση και τις απαραίτητες υποδομές όταν εμφανίζε-

ται συμβάν μειώνοντας τις επιπτώσεις της παραβίασης στους πελάτες και τη φήμη της εταιρείας.

Τα κύρια στοιχεία της ασφάλισης Cyber Insurance είναι:

- **αστική ευθύνη** έναντι τρίτων οι οποίοι υπέστησαν ζημιά λόγω απώλειας των προσωπικών τους δεδομένων από την εταιρία στην οποία τα είχαν δώσει
- **ανταπόκριση σε περιστατικά**: Έξοδα και Υπηρεσίες διαχείρισης περιστατικών παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών
- **διακοπή εργασιών** - Κάλυψη για απώλεια εσόδων λόγω διακοπής της επιχειρηματικής δραστηριότητας από περιστατικά παραβίασης συστημάτων και απώλειας εμπιστευτικών πληροφοριών,
- **κυβερνοεκβιασμός** - Κάλυψη για διαχείριση περιστατικών εκβιασμού από απειλές που μπορεί να βλάψουν ένα δίκτυο ή να οδηγήσουν σε διαρροή εμπιστευτικών πληροφοριών,
- **διοικητικά πρόστιμα**: που επιβάλλονται από τις ρυθμιστικές αρχές σε περιπτώσεις περιστατικών παραβίασης και απώλειας προσωπικών δεδομένων.

Με τη βούθεια της ασφάλισης cyber insurance οι επιχειρήσεις θα προστατεύσουν τους ισολογισμούς τους και θα διαχειριστούν αποτελεσματικά τις συνέπειες των περιστατικών αυτών.

Παραθέτουμε ένα παράδειγμα πειτουργίας ενός ασφαλιστηρίου συμβολαίου σε περίπτωση ενός περιστατικού Παραβίασης Εταιρικού Δικτύου, απώλειας δεδομένων και Εκβιασμού που συνέβη σε μια δικηγορική εταιρία:

Το δίκτυο μιας δικηγορικής εταιρίας παραβίαστηκε από hackers. Οι ευαίσθητες πληροφορίες των πελατών της ενδεχομένως βρίσκονταν σε κίνδυνο. Μέσα στα δεδομένα που χάθηκαν ήταν το σχέδιο εξαγοράς μια εταιρίας, το σχέδιο κατοχύρωσης μιας πατέντας, το σχέδιο χρηματοδότησης μιας εταιρίας μέσω venture capital και το πελατολόγιο της δικηγορικής εταιρίας.

Η δικηγορική εταιρία 48 ώρες μετά την παραβίαση του συστήματος έλαβε ένα τηλεφώνημα από εκπρόσωπο των hackers που την είχαν παραβιάσει και ζητούσαν 45 Bitcoins (50.000 €) για να μην πουλήσουν τα στοιχεία αυτά στο Darknet.

Ο εκπρόσωπος της εταιρίας που ήταν ασφαλισμένη επικοινώνησε με την ασφαλιστική της εταιρία. Μετά την επικοινωνία με την ασφαλιστική ο Incident Response Manager της ασφαλιστικής εταιρίας ανέλαβε τη διαχείριση του περιστατικού στέλνοντας ειδικούς διερεύνησης εγκλημάτων που σχετίζονται με την παραβίαση πληροφοριακών συστημάτων (Forensics Investigators) για την ανάλυση των επιπτώσεων του συμβάντος, τον περιορισμό τους και την εκτίμηση του κόστους του συμβάντος και εξειδικευμένους δικηγόρους για την αντιμετώπιση του περιστατικού.

Προσωπικά δεδομένα

Ο ρόλος του Data Protection Officer και η χρήση της ασφάλισης cyber insurance (συνέχεια)

Πιθανές οικονομικές επιπτώσεις - Καλύψεις ασφαλιστηρίου που ενεργοποιούνται

Privacy Liability Μη εξουσιοδοτημένη γνωστοποίηση προσωπικών δεδομένων και εταιρικών εμπιστευτικών πληροφοριών	
Network Security Liability - Ευθύνη της εταιρίας η οποία προκύπτει από την παραβίαση του εταιρικού δικτύου της και την αδυναμία της να το προστατεύσει αποτελεσματικά από τους hackers	
• Έξοδα υπεράσπισης και διακανονισμού των αποζημιώσεων που θα ζητήσουν τα υποκείμενα των δεδομένων ή οι εταιρίες των οποίων τα δεδομένα χάθηκαν	100.000 €
Incident Response Expenses - Έξοδα ανταπόκρισης Περιστατικού Παραβίασης • Αμοιβές ειδικών διερεύνησης εγκλημάτων που σχετίζονται με την παραβίαση πληροφοριακών συστημάτων (Forensics Investigators) για τον εντοπισμό του προβλήματος, την ανάλυση των επιπτώσεων του συμβάντος, τον περιορισμό τους και την εκτίμηση του κόστους του συμβάντος • Κόστος δημιουργίας και λειτουργίας ενός call center για να διαχειριστεί τους πελάτες της εταιρίας και να απαντά στα ερωτηματά τους • Αμοιβή Ειδικού Δημοσιών σχέσεων για να διαχειρισθεί το συμβάν στα μέσα ενημέρωσης και να υλοποιήσει το επικοινωνιακό πλάνο της εταιρίας • Έξοδα Νομικών Συμβούλων • Αμοιβή Incident response manager	44.000 € 8.000 € 12.000 € 28.000 € 8.000 €
Cyber Extortion - Ειδικοί Διαπραγματευτές για την αντιμετώπιση του περιστατικού, Δικηγόροι οι οποίοι θα εκτιμήσουν τις συνέπειες που θα προκύψουν για την εταιρία σε περίπτωση μη εξουσιοδοτημένης γνωστοποίησης, καταβολή του ποσού των λύτρων • Αμοιβή Ειδικού Διαπραγματευτή • Έξοδα Νομικών Συμβούλων • Αμοιβή Συμβούλου Πληροφοριακών συστημάτων • Καταβολή λύτρων	4.000 € 2.000 € 22.000 € 25.000 €
Συνολικό Κόστος Διαχείρισης Συμβάντος	243.000 €

Το παραπάνω παράδειγμα αφορά εταιρία που δραστηριοποιείται στο Ηνωμένο Βασίλειο, όμως τέτοια παραδείγματα συμβαίνουν καθημερινά και στην Ελλάδα.

Βλ. περισσότερα για τον Γενικό Κανονισμό και την ασφάλιση cyber insurance στη βραβευμένη από την αγορά των Lloyd's εκπαιδευτική μπραντ www.cyberinsurancequote.gr.



48 Σελίδες Χρόσιμες Πληροφορίες για Νομικούς

■ Ανεξάρτητες Αρχές ■ Αστυνομικά Τμήματα Γενικής Αστυνομικής Διεύθυνσης Αττικής ■ Αστυνομικά Τμήματα Γενικής Αστυνομικής Διεύθυνσης Αχαΐας ■ Αστυνομικά Τμήματα Γενικής Αστυνομικής Διεύθυνσης Θεσσαλονίκης ■ Αστυνομικές Αρχές
■ Ασφαλιστικά Ταμεία ■ Βουλή - Κυβερνητικό Προεδρίτο της Δημοκρατίας ■ Δικαστήρια - Υπηρεσίες Ε.Ε. ■ Δικαιοστικές Αρχές
■ Δικαστικό ένταμπο ■ Δικαιοτικές διακοπές ■ Δικηγορικοί Σύλλογοι της Επικράτειας
■ Εθνική Σχολή Δικαιοτικών Λειτουργών (Ε.Σ.Δ.Ι.) ■ Εθνικό Τυπογραφείο - Τέλη δημοσιεύσεων ασ ΦΕΚ
■ Ειρηνοδικεία της Επικράτειας ■ Εκκλησία της Ελλάδος ■ Ελληνικά Χρηματιστήρια ■ Εξαιρετές πημέρες 2016 ■ Εξωδικαστικές αμοιβές
■ Εποτολόγιο 2016 ■ Επιθεωρήσεις Εργασίας ■ Επιμελητήρια ■ Επιστημονικές Ενώσεις ■ Ιατροδικαστικές Υπηρεσίες ■ Κέντρα Διαμεσολάβησης
■ Κέντρα Εξυπηρέτησης Πολιτών (Κ.Ε.Π.) ■ Κτηματολογικά Γραφεία της χώρας ■ Απηαρχεία ■ Λοιπά Υποθηκοφυλακεία ■ Λοιπά Υπουργεία ■ Μεγαρόσημο
■ Οικονομικές Εφορίες (Δ.Ο.Υ.) ■ Οργανισμοί - Συνδικαλιστικοί Φορείς ■ Παραστάσεις σε δικαστήρια ■ Πειριφέρεια Αττικής ■ Προεισπράξεις Δικηγορικών Αμοιβών
■ Σύλλογοι Δικαιοτικών Επιμελητών της Επικράτειας ■ Συμβούλιο Δικηγορικών Συλλόγων Ε.Ε. (C.C.B.E.) ■ Συμβολαιογραφικοί Σύλλογοι της Επικράτειας
■ Σώμα Δίωξης Οικονομικού Εγκλήματος (Σ.Δ.Ο.Ε.) ■ Τόκοι ■ Τράπεζες ■ Υπηρεσία TAXIS ■ Υπηρεσίες Μεταγωγών - Σήμανση ■ Υπηρεσίες Ποινικού Μητρώου
■ Υποθηκοφυλακεία ■ Υπουργείο Δικαιοσύνης, Διαφάνεια & Ανθρωπίνων Δικαιωμάτων ■ Φυλακές - Σωφρονιστικά Καταστήματα ■ Χρήσιμα Τηλέφωνα
■ Χωροταξική κατανομή των Δικαστηρίων της Επικράτειας

Για τον έγκαιρο προγραμματισμό των υποθέσεων σας

✓ Εβδομαδιαία γραμμογράφηση ειδικά σχεδιασμένη για εξασφάλιση περισσότερου χώρου για κάθε ημέρα
✓ Ετήσιος και μηνιαίος προγραμματισμός 2017 για καλύτερη οργάνωση των υποθέσεων
✓ Προγραμματισμός δικαστηρίων για τα έτη 2018-2020
✓ Πίνακας παρακολούθησης αποφάσεων δικαστηρίων
✓ Χώρος αναγραφής σημειώσεων

Τιμή: 15 € φ.π., 20 € v.π.
Σελ. 248, Σχήμα 17x24
Ειδική τιμή κατόπιν συνεννόησεως για μαζικές παραγγελίες Δικ. Επιφεύγων & Δικηγορικών Συλλόγων