GDPR και Κυβερνοασφάλεια στις Επιχειρήσεις

Ένας πρακτικός οδηγός για επιχειρήσεις που επιθυμούν να συμμορφωθούν με τον Γενικό Κανονισμό Προστασίας Δεδομένων και να θωρακίσουν τα ψηφιακά τους συστήματα από σύγχρονες κυβερνοαπειλές.

Σύνδεση GDPR & Κυβερνοασφάλειας

Γιατί η προστασία δεδομένων και η ψηφιακή ασφάλεια αποτελούν δύο όψεις του ίδιου νομίσματος

Υποχρεώσεις οργανισμών

Τι οφείλουν να γνωρίζουν και να εφαρμόζουν οι επιχειρήσεις σύμφωνα με τη νομοθεσία

Στόχοι σεμιναρίου

Πρακτικές γνώσεις και εργαλεία που μπορούν να εφαρμοστούν άμεσα στο επιχειρηματικό περιβάλλον

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΤΕ
ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Τι είναι ο GDPR;

Ο **Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR – Κανονισμός ΕΕ 2016/679)** ισχύει από τον Μάιο του 2018 και αποτελεί τον πιο αυστηρό νόμο προστασίας ιδιωτικότητας παγκοσμίως. Αφορά κάθε επιχείρηση που επεξεργάζεται προσωπικά δεδομένα πολιτών της ΕΕ, ανεξάρτητα από τη χώρα εγκατάστασης.

Προστασία προσωπικών δεδομένων

Κάθε πληροφορία που ταυτοποιεί ή μπορεί να ταυτοποιήσει ένα φυσικό πρόσωπο προστατεύεται αυστηρά. Η επεξεργασία επιτρέπεται μόνο με νόμιμη βάση και για συγκεκριμένο σκοπό.

Δικαιώματα υποκειμένων

Οι πολίτες έχουν δικαίωμα πρόσβασης, διόρθωσης, διαγραφής («δικαίωμα λήθης»), φορητότητας δεδομένων και εναντίωσης στην επεξεργασία.

Υποχρεώσεις επιχειρήσεων

Οι οργανισμοί οφείλουν να τηρούν αρχεία επεξεργασίας, να ορίζουν DPO εφόσον απαιτείται, να γνωστοποιούν παραβιάσεις και να εφαρμόζουν τεχνικά και οργανωτικά μέτρα ασφαλείας.

Συχνές κυβερνοαπειλές

Οι επιχειρήσεις αντιμετωπίζουν καθημερινά μια ευρεία γκάμα ψηφιακών κινδύνων. Η γνώση των πιο κοινών απειλών είναι το πρώτο βήμα για αποτελεσματική άμυνα.

🎣 Phishing

Εξαπάτηση μέσω πλαστών email ή ιστοσελίδων που μιμούνται αξιόπιστους αποστολείς (τράπεζες, δημόσιες υπηρεσίες). Στόχος η κλοπή κωδικών ή η εγκατάσταση κακόβουλου λογισμικού. Αποτελεί την **αιτία του 91% των κυβερνοεπιθέσεων**.

🔒 Ransomware

Κακόβουλο λογισμικό που κρυπτογραφεί τα αρχεία της επιχείρησης και απαιτεί λύτρα για την αποκρυπτογράφησή τους. Μπορεί να παραλύσει ολόκληρη την επιχείρηση για ημέρες ή εβδομάδες.

📧 Business Email Compromise (BEC)

Παραποίηση ή παραβίαση εταιρικού email για να εξαπατηθούν υπάλληλοι ώστε να πραγματοποιήσουν μεταφορές χρημάτων ή να αποκαλύψουν εμπιστευτικές πληροφορίες. Προκαλεί τεράστιες οικονομικές ζημιές παγκοσμίως.

🔑 Παραβιάσεις λογαριασμών

Μη εξουσιοδοτημένη πρόσβαση σε εταιρικούς λογαριασμούς μέσω κλεμμένων διαπιστευτηρίων, brute force επιθέσεων ή επαναχρησιμοποίησης αδύναμων κωδικών. Οδηγεί σε διαρροή ευαίσθητων δεδομένων.

Ποια δεδομένα στοχεύουν οι επιτιθέμενοι;

Οι κυβερνοεγκληματίες δεν επιτίθενται τυχαία — επιλέγουν δεδομένα υψηλής αξίας που μπορούν να πωληθούν, να χρησιμοποιηθούν για εκβιασμό ή να επιτρέψουν περαιτέρω επιθέσεις. Κάθε επιχείρηση επεξεργάζεται πληροφορίες που αποτελούν πρωταρχικό στόχο.

Σύμφωνα με τον GDPR, η παραβίαση οποιουδήποτε από αυτά τα δεδομένα επιφέρει υποχρέωση γνωστοποίησης στην αρμόδια αρχή εντός 72 ωρών.

Προσωπικά δεδομένα που στοχεύονται

Ταυτοποιητικά

Ονοματεπώνυμα, διευθύνσεις, αριθμοί ταυτότητας & ΑΦΜ

Επικοινωνία

Email, αριθμοί τηλεφώνου, λογαριασμοί κοινωνικών δικτύων

Ευαίσθητα

Ιατρικά αρχεία, διαγνώσεις, ασφαλιστικά δεδομένα υγείας

Οικονομικά

Τραπεζικοί λογαριασμοί, κάρτες πληρωμών, φορολογικά στοιχεία

Παραβίαση δεδομένων (Data Breach)

Μια **παραβίαση δεδομένων** συμβαίνει κάθε φορά που προσωπικά δεδομένα αποκαλύπτονται, χάνονται, τροποποιούνται ή καταστρέφονται χωρίς εξουσιοδότηση — είτε από κακόβουλη ενέργεια είτε από ατύχημα.

1

Τι θεωρείται παραβίαση

Hacking, κλοπή laptop με αδιόρθωτα δεδομένα, αποστολή email σε λάθος παραλήπτη, απώλεια USB, μη εξουσιοδοτημένη πρόσβαση εσωτερικού χρήστη

2

Πραγματικά παραδείγματα

Διαρροή δεδομένων πελατών από επιτίθεση ransomware, κλοπή αρχείου HR με μισθοδοσία, παραβίαση CRM από εξωτερικό συνεργάτη με αδύναμο κωδικό

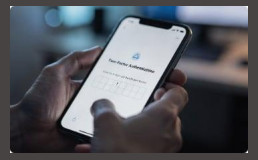
3

Επιπτώσεις για την επιχείρηση

Πρόστιμα έως **20 εκ. € ή 4% του παγκόσμιου τζίρου**, νομικές αξιώσεις, απώλεια εμπιστοσύνης πελατών και ζημία στη φήμη

Μέτρα προστασίας

Η εφαρμογή βασικών τεχνικών μέτρων μπορεί να μειώσει δραματικά τον κίνδυνο παραβίασης. Ο GDPR απαιτεί ρητά τη λήψη **«κατάλληλων τεχνικών και οργανωτικών μέτρων»** για την προστασία των δεδομένων.



Multi-Factor Authentication (MFA)

Επαλήθευση ταυτότητας με δύο ή περισσότερα βήματα. Μειώνει κατά **99,9%** τον κίνδυνο παραβίασης λογαριασμών, ακόμη και αν ο κωδικός έχει διαρρεύσει.

Κρυπτογράφηση

Μετατροπή δεδομένων σε μη αναγνώσιμη μορφή. Εφαρμόζεται στη μεταφορά δεδομένων (TLS/SSL) και στην αποθήκευση (AES-256). Ακόμη και αν κλαπούν τα δεδομένα, παραμένουν άχρηστα.

Αντίγραφα ασφαλείας (Backups)

Τακτικά backups σε απομονωμένο περιβάλλον (offline ή cloud). Ακολουθείτε τον κανόνα **3-2-1**: 3 αντίγραφα, σε 2 διαφορετικά μέσα, 1 εκτός εγκατάστασης.

Password Managers & Updates

Χρήση διαχειριστή κωδικών για μοναδικά, ισχυρά passwords ανά υπηρεσία. Ταυτόχρονα, τακτικές ενημερώσεις λογισμικού κλείνουν γνωστά κενά ασφαλείας που εκμεταλλεύονται οι επιτιθέμενοι.

Ασφαλής διαχείριση δεδομένων

Πέραν της τεχνικής προστασίας, ο GDPR απαιτεί οργανωτικές πρακτικές που διασφαλίζουν ότι τα δεδομένα συλλέγονται μόνο όταν χρειάζονται, προσβάλλονται μόνο από όσους τα χρειάζονται, και καταστρέφονται με ασφάλεια όταν δεν είναι πλέον αναγκαία.

1

Ελαχιστοποίηση δεδομένων

Συλλέγετε μόνο τα δεδομένα που είναι **απολύτως απαραίτητα** για τον εκάστοτε σκοπό. Αποφύγετε τη συλλογή «για κάθε ενδεχόμενο». Αρχή: λιγότερα δεδομένα = λιγότερος κίνδυνος.

2

Έλεγχος πρόσβασης

Εφαρμογή της αρχής **«ελάχιστης αναγκαίας πρόσβασης»** (least privilege). Κάθε υπάλληλος έχει πρόσβαση μόνο στα δεδομένα που χρειάζεται για τα καθήκοντά του.

3

Ταξινόμηση πληροφοριών

Κατηγοριοποιήστε τα δεδομένα σας (δημόσια, εσωτερικά, εμπιστευτικά, ευαίσθητα) και εφαρμόστε διαφορετικά επίπεδα προστασίας ανάλογα με την κατηγορία.

4

Ασφαλής διαγραφή

Η απλή διαγραφή αρχείων δεν αρκεί. Χρησιμοποιείτε εργαλεία **ασφαλούς καταστροφής** (data wiping, degaussing, φυσική καταστροφή μέσων) για δεδομένα που έχουν παρέλθει ο σκοπός τους.

Χρόνος αντίδρασης

72h

Το χρονικό περιθώριο που δίνει ο GDPR για γνωστοποίηση παραβίασης στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ)

Τι κάνουμε σε περίπτωση data breach;

Κάθε λεπτό μετράει. Η ύπαρξη σαφούς πλάνου αντίδρασης (Incident Response Plan) καθορίζει αν μια παραβίαση θα αντιμετωπιστεί αποτελεσματικά ή θα εξελιχθεί σε καταστροφή.

Άμεση απομόνωση

Αποσυνδέστε τα επηρεαζόμενα συστήματα από το δίκτυο για να αποτρέψετε περαιτέρω εξάπλωση. Μην απενεργοποιείτε τελείως — διατηρήστε τα για forensic ανάλυση.

Ενημέρωση IT / DPO

Ειδοποιείτε άμεσα την ομάδα IT και τον Υπεύθυνο Προστασίας Δεδομένων (DPO). Ξεκινήστε τη διαδικασία εκτίμησης της έκτασης της παραβίασης.

Καταγραφή περιστατικού

Τεκμηριώστε λεπτομερώς: τι συνέβη, πότε, ποια δεδομένα επηρεάστηκαν, πόσα άτομα θίγονται και ποιες ενέργειες ελήφθησαν.

Υποχρεώσεις γνωστοποίησης

Εντός 72 ωρών γνωστοποίηση στην ΑΠΔΠΧ. Αν υπάρχει **υψηλός κίνδυνος** για τα υποκείμενα, απαιτείται και άμεση ενημέρωσή τους χωρίς αδικαιολόγητη καθυστέρηση.

Ρόλος των εργαζομένων

Η τεχνολογία δεν αρκεί. Ο **ανθρώπινος παράγοντας** παραμένει ο πιο κρίσιμος κρίκος στην αλυσίδα κυβερνοασφάλειας — τόσο ως η πιο συχνή αιτία παραβιάσεων, όσο και ως η πιο αποτελεσματική γραμμή άμυνας όταν είναι κατάλληλα εκπαιδευμένος.

🎣 Αναγνώριση phishing

Εκπαίδευση στην αναγνώριση ύποπτων email: ελέγχετε τον αποστολέα, μη κάνετε κλικ σε άγνωστα links, επαληθεύετε αιτήματα μέσω εναλλακτικού καναλιού επικοινωνίας.

💻 Προστασία συσκευών

Κλείδωμα οθόνης σε αδράνεια, απαγόρευση USB από άγνωστες πηγές, μη χρήση προσωπικών συσκευών για εταιρικά δεδομένα χωρίς MDM λύση.

🚨 Αναφορά ύποπτων περιστατικών

Δημιουργήστε κουλτούρα όπου οι εργαζόμενοι **αναφέρουν άμεσα** ό,τι τους φαίνεται ύποπτο, χωρίς φόβο. Η έγκαιρη αναφορά μπορεί να αποτρέψει καταστροφή.

📚 Συνεχής εκπαίδευση

Τακτικά σεμινάρια, simulated phishing tests και ενημερώσεις για νέες απειλές. Η εκπαίδευση δεν είναι εφάπαξ — οι απειλές εξελίσσονται συνεχώς.

Checklist GDPR & Cybersecurity

Χρησιμοποιήστε αυτή τη λίστα ως σημείο αναφοράς για να αξιολογήσετε την τρέχουσα κατάσταση συμμόρφωσης της επιχείρησής σας. Κάθε ελλιπής τομέας αποτελεί προτεραιότητα δράσης.

- ☑ Multi-Factor Authentication (MFA) ενεργοποιημένο σε όλους τους εταιρικούς λογαριασμούς
- ☑ Ενημερωμένα λειτουργικά συστήματα και εφαρμογές — τακτική εφαρμογή patches ασφαλείας
- ☑ Τακτικά backup δεδομένων με δοκιμή αποκατάστασης (restore test) ανά τακτά διαστήματα
- ☑ Κρυπτογράφηση δεδομένων σε ηρεμία και κατά τη μεταφορά (encryption at rest & in transit)
- ☑ Πολιτικές ελέγχου πρόσβασης βάσει ρόλων — αρχή ελάχιστης αναγκαίας πρόσβασης
- ☑ Τακτική εκπαίδευση προσωπικού σε θέματα phishing, GDPR και ασφαλούς διαχείρισης δεδομένων

☐ Η συμμόρφωση με τον GDPR δεν είναι εφάπαξ ενέργεια αλλά **συνεχής διαδικασία**. Επανεξετάζετε και ενημερώνετε τα μέτρά σας τακτικά ώστε να ανταποκρίνονται στις εξελισσόμενες απειλές και νομικές απαιτήσεις.