ΣΔΕΕ
ΣΥΝΔΕΣΜΟΣ ΔΙΚΗΓΟΡΙΚΩΝ ΕΤΑΙΡΕΙΩΝ ΕΛΛΑΔΟΣ

Οδηγός Κυβερνοασφάλειας

Πώς να προστατεύσετε αποτελεσματικά τις πληροφορίες σας με απλά και πρακτικά βήματα

Περιεχόμενα

Γιατί είναι σημαντικό να διαβάσετε αυτόν τον οδηγό

Ως δικηγορική εταιρεία, διαχειρίζεστε καθημερινά ευαίσθητες και εμπιστευτικές πληροφορίες. Αν αυτές οι πληροφορίες υποκλαπούν ή διαρρεύσουν, δεν διακυβεύεται μόνο η ασφάλεια των πελατών σας, αλλά και η φήμη και αξιοπιστία της εταιρείας σας. Δεν χρειάζονται πολύπλοκες λύσεις ή μεγάλοι προϋπολογισμοί για να βελτιώσετε σημαντικά την κυβερνοασφάλεια. Με απλά βήματα μπορείτε να καλύψετε τα πιο βασικά και κρίσιμα κενά. Τέτοια είναι τα παρακάτω.

Προφανώς η έκταση αυτού του οδηγού δεν μπορεί να υποκαταστήσει συμβουλές ειδικευμένης εταιρείας πληροφορικής ή εσωτερικού τεχνικού πληροφορικής ή και των δύο, εφόσον αυτό είναι εφικτό. Όμως, η γνώση των βασικών εννοιών θα βοηθήσει μια δικηγορική εταιρεία να βελτιώσει την καθημερινή λειτουργία της σε σχέση με τα πληροφοριακά της συστήματα, ενώ θα της δώσει τη βάση να μπορέσει ευκολότερα να αποκτήσει πιστοποιήσεις ασφαλείας ή να χειριστεί καλλίτερα ένα περιστατικό.

I. Ισχυροί Κωδικοί και Έλεγχος Πρόσβασης

Τι να κάνετε:

- Να χρησιμοποιείτε ισχυρούς, μοναδικούς κωδικούς πρόσβασης (π.χ. 12+ χαρακτήρες με γράμματα, αριθμούς και σύμβολα). Ένα passphrase είναι προτιμητέο. Μην χρησιμοποιείτε κωδικούς που μπορεί κάποιος να μαντέψει εύκολα. Για παράδειγμα, *Manos123!@#* δεν είναι καλή επιλογή. Δεν πρέπει να χρησιμοποιείτε τον ίδιο κωδικό σε άλλες προσωπικές εφαρμογές και υπηρεσίες. Μπορείτε να δημιουργήσετε ένα passphrase όπως '-ToSpitiExei4Gates' ή '"VazwdyskoloKwdiko@1285' είναι μακροί, εύκολοι να θυμηθείτε αλλά δύσκολοι να μαντέψει κάποιος άλλος.
- Να ενεργοποιήσετε διπλή ταυτοποίηση (2FA) σε email, cloud και τραπεζικές υπηρεσίες. Είναι ένας τρόπος σύνδεσης που απαιτεί περισσότερα από ένα στοιχεία ταυτοποίησης για να επιβεβαιώσει ότι είμαστε όντως εμείς που προσπαθούμε να μπούμε. Για παράδειγμα, όταν βάζουμε τον κωδικό μας και στη συνέχεια και έναν δεύτερο κωδικό που έρχεται στο κινητό μας μέσω SMS ή κάποιας σχετικής εφαρμογής π.χ. Google authenticator, Microsoft authenticator, αυτό είναι 2FA. Στις περισσότερες εφαρμογές ή υπηρεσίες θα λάβετε συνήθως αυτοματοποιημένο μήνυμα που θα σας ρωτά εάν θέλετε να ενεργοποιηθεί η διπλή ταυτοποίηση, ή αλλιώς θα μπορείτε οι ίδιοι να την ενεργοποιήσετε στα «settings» της εφαρμογής. Με τον ίδιο τρόπο θα μπορέσετε να επιλέξετε και το είδος της δεύτερης ταυτοποίησης. Οι πιο συνήθεις τέτοιοι είναι:
    - **Εφαρμογή 2FA**, όπως Google authenticator ή Microsoft

authenticator, την οποία κατεβάζετε στο κινητό σας. Αυτές συνδέονται με την υπηρεσία ή εφαρμογή για την οποία θέλετε να παράγουν τον επιπλέον κωδικό ταυτοποίησης είτε σκανάροντας ένα QR code είτε εισάγοντας έναν αριθμό που «γεννούν» οι τελευταίες. Εν συνεχεία, παράγουν συνεχώς έναν μεταβαλλόμενο αριθμό που λειτουργεί ως δεύτερος παράγοντας ταυτοποίησης. Για παράδειγμα, ας υποθέσουμε πως χρησιμοποιείτε την εφαρμογή Dropbox για την αποθήκευση αρχείων και θέλετε να ασφαλίσετε την πρόσβαση σε αυτήν με 2FA, χρησιμοποιώντας την εφαρμογή Google authenticator. Πηγαίνοντας στον υπολογιστή σας στο δικτυακό τόπο του Dropbox, στην επιλογή Settings→Security, επιλέγετε ως μέθοδο 2FA το «authenticator app», οπότε εμφανίζεται στην οθόνη ένα QR code. Αυτό το σκανάρετε με το κινητό σας μέσω της εφαρμογής Google authenticator, και το Google authenticator αρχίζει να παράγει τον μεταβαλλόμενο αριθμό που αποτελεί τον δεύτερο παράγοντα ταυτοποίησης.

- **Email.** Ο αριθμός που λειτουργεί ως δεύτερος παράγοντας ταυτοποίησης έρχεται στο email σας.
- **Κινητό.** Ο αριθμός που λειτουργεί ως δεύτερος παράγοντας ταυτοποίησης έρχεται στο κινητό σας.

<u>Προσοχή</u>: η πρόσβαση στον λογαριασμό σας είναι ιδιαίτερα δυσχερής εάν χάσετε την πρόσβαση στον δεύτερο παράγοντα ταυτοποίησης. Συνιστούμε να έχετε εναλλακτικές και να ορίσετε κάποιον άλλο εταίρο στην εταιρεία ως εναλλακτικό λήπτη επαναφοράς κωδικού.

- Να μην μοιράζεστε ποτέ κωδικούς με συναδέλφους. Αν χρειάζεται πρόσβαση άλλος, δημιουργήστε χωριστό λογαριασμό.
- Να μην χρησιμοποιείτε τους ίδιους κωδικούς για πάνω από μία εφαρμογή. Για παράδειγμα, χρησιμοποιείστε άλλον κωδικό για το email σας, άλλον για τις εφαρμογές της ΑΑΔΕ, άλλον για το ebanking και άλλον για τις πλατφόρμες Δικαστηρίων/ΔΣΑ/Ολομέλειας.
- Για να μην χρειάζεται να θυμάστε πολλούς κωδικούς, μπορείτε να χρησιμοποιήσετε μια εφαρμογή password management για το κινητό σας ή τον υπολογιστή. Κάποια παραδείγματα εφαρμογών είναι Keepass, 1Password, LastPass. Οι εφαρμογές αυτές αποθηκεύουν με ασφάλεια τα username και τους κωδικούς που χρησιμοποιείτε στις εφαρμογές ή υπηρεσίες σας, και τους επικολλούν αυτόματα όποτε χρειάζεται να τους συμπληρώσετε για να εισέλθετε σε αυτές.
- Να αλλάζετε κωδικούς εφόσον υπάρχει υποψία παραβίασης, εφόσον κάποιος κωδικός κοινοποιηθεί από λάθος σε τρίτο και σε κάθε

περίπτωση κάθε έξι μήνες ή ένα χρόνο σε κρίσιμες πλατφόρμες ή υπηρεσίες.

Για έναν δικηγόρο, ο κωδικός πρόσβασης δεν προστατεύει απλώς ένα email:

- Προστατεύει εμπιστευτικές επικοινωνίες με πελάτες (δικηγορικό απόρρητο).
- Προστατεύει προσωπικά δεδομένα και συχνά ευαίσθητα δεδομένα.
- Συνδέεται με ηλεκτρονικές καταθέσεις, προθεσμίες και διαδικασίες.

II. Ενημέρωση και Ασφάλεια Λογισμικού

Τι να κάνετε:

- Βεβαιωθείτε ότι χρησιμοποιείτε γνήσιο λογισμικό. Αυτό κατά κανόνα μπορείτε να το ελέγξετε στα settings του υπολογιστή σας ή της σχετικής εφαρμογής.
- Ενεργοποιήστε τις αυτόματες ενημερώσεις σε όλα τα προγράμματα.
- Εγκαταστήστε και να διατηρείτε ενεργό λογισμικό προστασίας (antivirus / antimalware) σε όλες τις εταιρικές συσκευές. Κάποια από τα πιο γνωστά είναι τα Norton, Bitdefender και McAfee.

⚠ *Παλαιά ή μη ενημερωμένα προγράμματα περιέχουν κενά ασφάλειας που εκμεταλλεύονται οι επιτιθέμενοι.*

III. Αντίγραφα Ασφαλείας (Backups)

Τι να κάνετε:

- Διατηρείτε τουλάχιστον ένα αντίγραφο ασφαλείας σε ξεχωριστή συσκευή (offline), για παράδειγμα σε εξωτερικό σκληρό δίσκο, και ένα αντίγραφο στο cloud (off-site) για παράδειγμα στο Google Drive του λογαριασμού σας Google ή στο OneDrive του λογαριασμού σας Microsoft. Φροντίστε να ενημερώνετε το αρχείο ασφαλείας τακτικά, π.χ. καθημερινά για τα σημαντικά αρχεία, μία φορά τον μήνα για τα λιγότερο κρίσιμα. Υπάρχουν εργαλεία backup που αυτοματοποιούν την διαδικασία και λαμβάνουν αντίγραφα ασφαλείας σε καθορισμένες χρονικές περιόδους, χωρίς κάποια ενέργεια από τον χρήστη.
- Ελέγχετε ότι τα αντίγραφα λειτουργούν και μπορούν να αποκατασταθούν. Για παράδειγμα, σε τακτική βάση δοκιμάστε δειγματοληπτικά να ανοίξετε αρχεία στο αντίγραφο ασφαλείας.
- Μην αποθηκεύετε όλα τα δεδομένα μόνο σε υπολογιστές γραφείου ή USB sticks.

- Αποσυνδέετε τον σκληρό δίσκο από το δίκτυό σας αμέσως μόλις ολοκληρωθεί η διαδικασία Backup. Κρατάτε τον δίσκο offline μέχρι το επόμενο backup. Αν είναι δυνατόν, χρησιμοποιείτε δύο σκληρούς δίσκους τους οποίους να εναλλάσσετε. Με τον τρόπο αυτό θα έχετε πάντα κάποιο μέσο offline.

⚠ *Ένα κακόβουλο λογισμικό ransomware μπορεί να σας κλειδώσει τα αρχεία. Το backup μπορεί να σας σώσει.*

IV. 🤖 Χρήση Προσωπικών Συσκευών και Εφαρμογών

Τι να κάνετε:

- Να περιορίσετε ή να μην επιτρέπετε τη χρήση προσωπικών email (π.χ. gmail, yahoo) για επαγγελματικούς σκοπούς.
- Αν επιτρέπετε προσωπικές συσκευές, να απαιτείτε τα ελάχιστα μέτρα ασφάλειας που αναφέρουμε παραπάνω.

⚠ *Οι προσωπικές συσκευές δεν έχουν συνήθως τα ίδια μέτρα ασφάλειας με τις επαγγελματικές.*

V. 🏢 Φυσική Ασφάλεια

Τι να κάνετε:

- Να εξασφαλίσετε ότι οι χώροι σας διαθέτουν πόρτες ασφαλείας, κλειδαριές, συναγερμό και κλειστό κύκλωμα τηλεόρασης CCTV.
- Να κλειδώνετε την οθόνη του υπολογιστή και τα γραφεία σας όταν φεύγετε.

⚠ *Η απώλεια υπολογιστή ή φακέλου μπορεί να οδηγήσει σε παραβίαση δεδομένων.*

VI. ✉ Ασφαλές Email

Τι να κάνετε:

- Να χρησιμοποιείτε email με domain της εταιρείας (π.χ. info@onomaetaireias.gr). Για να αποκτήσετε εταιρικό domain, μπορείτε να αγοράστε ένα όνομα χώρου (domain name) π.χ. onomaetaireias.gr από εταιρεία που λειτουργεί ως διαχειριστής και καταχωρητής domains και να δημιουργήσετε εταιρικά email μέσω παρόχου hosting ή υπηρεσίας όπως το Microsoft 365 ή το Google Workspace. Τέτοιοι διαχειριστές και καταχωρητές είναι π.χ. το papaki.gr, το dnshost.gr ή το iphost.gr. Εκεί αποκτάτε το domain name

που επιθυμείτε, εάν είναι διαθέσιμο, το ανανεώνετε και το διαχειρίζεστε. Εάν επιλέξτε μία από τις μεγάλες εταιρίες παρόχους εταιρικών email, είναι πιθανόν να μπορείτε αυτόματα, μέσα από την πλατφόρμα του καταχωρητή, να συσχετίσετε το domain name σας με την εταιρεία παρόχου email που επιλέξατε, ώστε αυτό να λειτουργήσει εύκολα. Σε αντίθετη περίπτωση, εάν δηλαδή δεν υπάρχει αυτή η αυτόματη επιλογή, θα πρέπει μάλλον να σας βοηθήσει κάποιος τεχνικός IT.

- Να αποφεύγετε την αποστολή ευαίσθητων εγγράφων χωρίς κρυπτογράφηση. Αυτό γίνεται κλειδώνοντας με κωδικό πρόσβασης τα αρχεία που στέλνετε ή χρησιμοποιώντας ασφαλείς πλατφόρμες π.χ. Microsoft OneDrive, Google Drive, Dropbox Business, για την διακίνηση των αρχείων.

⚠ *Τα δημόσια emails (gmail, yahoo) είναι πιο εύκολοι στόχοι για επιθέσεις.*

VII. Σχέδιο Αντιμετώπισης Περιστατικών Ασφάλειας

Τι να κάνετε:

- Να ορίσετε ένα πρόσωπο που θα είναι υπεύθυνος σε περίπτωση κυβερνοεπίθεσης.
- Τηρείτε βασικό σχέδιο: ποιος κάνει τι, ποιος ειδοποιείται, πώς περιορίζεται η ζημιά.
- Διατηρείτε τις οδηγίες και τα στοιχεία επικοινωνίας εκτυπωμένα και προσβάσιμα.

⚠ *Όταν "χτυπήσει" η κρίση, θα είναι αργά για να οργανωθείτε.*

VIII. Τι κερδίζετε αν εφαρμόσετε τα παραπάνω

- Ασφάλεια των πελατών και της εταιρείας σας.
- Αποφυγή προστίμων και δυσφήμισης.
- Επαγγελματική εικόνα και αξιοπιστία.
- Ηρεμία χωρίς τον φόβο διαρροής δεδομένων.

Παρακαλούμε σημειώστε ότι τίποτα στον οδηγό αυτό δεν θα πρέπει να εκληφθεί ως παρότρυνση να χρησιμοποιήσετε κάποια συγκεκριμένη υπηρεσία, εφαρμογή ή πάροχο, ή ανάληψη ευθύνης από πλευράς του ΣΔΕΕ όσον αφορά σε οποιαδήποτε υπηρεσία, εφαρμογή ή πάροχο.

IX. 🕮 Λεξιλόγιο Τεχνικών Όρων

2FA (Διπλή Ταυτοποίηση)	Μέθοδος ασφαλείας που ζητά δύο στοιχεία για είσοδο: π.χ. κωδικό + κωδικό SMS. Εναλλακτικές ονομασίες της υπηρεσίας είναι “Two step authentication” και “MFA (Multi factor authentication)”.
Antivirus / Antimalware	Πρόγραμμα που προστατεύει τον υπολογιστή από ιούς και κακόβουλο λογισμικό.
Backup (Αντίγραφο ασφαλείας)	Αντίγραφο των αρχείων που κρατάμε ξεχωριστά για να τα επαναφέρουμε αν χαθούν.
Cloud	Αποθήκευση δεδομένων σε απομακρυσμένους υπολογιστές μέσω Internet (π.χ. Google Drive, OneDrive).
Domain name	Το όνομα ενός ιστότοπου, π.χ. onomaetaireias.gr, που αντιπροσωπεύει την επιχείρησή σας online.
Passphrase	Μακροσκελής φράση-κωδικός, συνδυασμός λέξεων, αριθμών και συμβόλων για αυξημένη ασφάλεια.
Phishing	Μέθοδος εξαπάτησης μέσω ψεύτικων emails ή μηνυμάτων που προσπαθούν να αποσπάσουν προσωπικά στοιχεία.
Ransomware	Κακόβουλο λογισμικό που κλειδώνει τα αρχεία σας και ζητά λύτρα για να τα ξεκλειδώσει.
Update (Ενημέρωση)	Εγκατάσταση νέας έκδοσης προγράμματος για διόρθωση λαθών και ενίσχυση ασφάλειας.