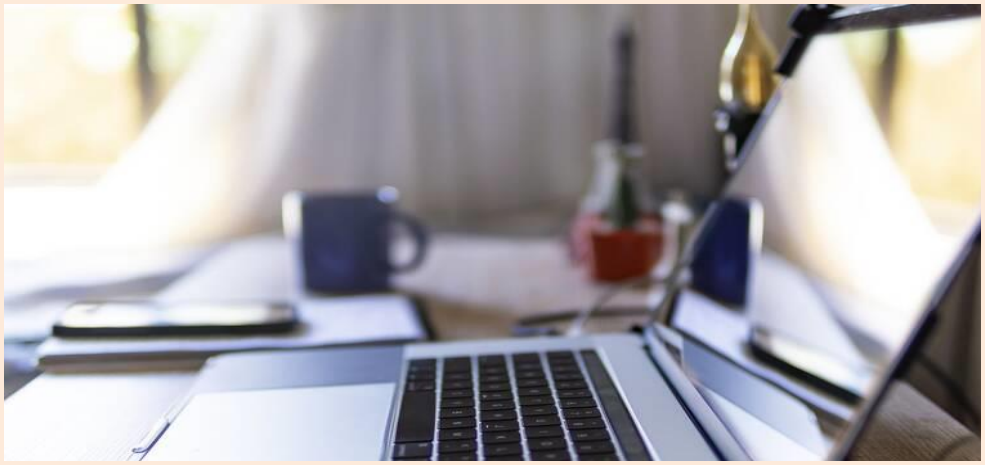
ΠΑΠΑΔΗΜΑΣ ΓΕΩΡΓΙΟΣ
ΤΕΧΝΙΚΟΣ ΑΣΦΑΛΕΙΑΣ
(ΕΞ.Υ.Π.Π) SAFE BUSINESS

Η πανδημία που αντιμετωπίζουμε θα έχει μακροχρόνιες επιπτώσεις στον τρόπο λειτουργίας των επιχειρήσεων. Οι αυξημένες ανάγκες για απομακρυσμένη πρόσβαση σε εταιρικά δεδομένα έφεραν στο προσκήνιο την ανάγκη για εκπαίδευση, σε θέματα κυβερνοασφάλειας, τόσο των τεχνικών στελεχών, όσο και ολόκληρου του ανθρώπινου δυναμικού

Είναι αναγκαίο οι εργοδότες να προσαρμοστούν όχι μόνο στις απαιτήσεις των εργαζομένων που εργάζονται από το σπίτι αυτή τη στιγμή, αλλά να δημιουργήσουν τα απαραίτητα θεμέλια ώστε η τηλεργασία να παραμείνει μία βιώσιμη εναλλακτική λύση εργασίας μακροχρόνια.

Προκειμένου να ανταποκριθούν στις νέες συνθήκες οι εταιρείες θα πρέπει να προσαρμοστούν στα νέα δεδομένα. Κάθε εταιρεία έχει διαφορετική υποδομή, οπότε δεν υπάρχει μια συνταγή για όλους», αλλά σίγουρα οι εταιρείες που ήδη επέτρεπαν την τηλεργασία έχουν μπροστά τους λιγότερα ζητήματα να αντιμετωπίσουν.

Πηγές πληροφόρησης : microsoft – Γεώργιος Μπαλαφούτης



SAFE BUSINESS S.A.
Εξωτερική Υπηρεσία Προστασίας Πρόληψης (ΕΞ.Υ.Π.Π.)

**(ΕΞ.Υ.Π.Π) SAFE BUSINESS Α.Ε**
**Λ. ΒΟΥΛΙΑΓΜΕΝΗΣ 39**
**16561-ΓΛΥΦΑΔΑ**
**ΤΗΛ: (+30) 2109603415**
**email:info@safebusiness.gr**
**www.safebusiness.gr**

# ΑΝΑΓΚΑΙΟΣ ΨΗΦΙΑΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ

Διαδικτυακές απάτες, κακόβουλα λογισμικά ransomware, phishing, hacking attacks. Η τηλεργασία (remote working), σε συνδυασμό με την έλλειψη πληροφόρησης, έχουν δημιουργήσει πρόσφορο έδαφος για κυβερνοεπιθέσεις εν μέσω της πανδημίας COVID-19. Ποιοι είναι οι κίνδυνοι που ελλοχεύουν και πώς μπορούμε να προστατεύσουμε επιχειρήσεις, εταιρικά δεδομένα και εργαζόμενους;

Η καινούργια πραγματικότητα της τηλεργασίας επιφέρει μια σειρά από πρωτόγνωρες προκλήσεις ασφαλείας για μικρές και μεγάλες επιχειρήσεις. Οι ιδιοκτήτες των εταιρειών βρίσκονται υπό πίεση για να διασφαλίσουν την συνέχεια και την κερδοφορία της επιχείρησης ενώ το βάρος αυτής της μετάβασης επωμίζονται οι υπεύθυνοι IT, με το κύριο μέλημα να είναι πλέον η διασφάλιση των εταιρικών δεδομένων από εξωτερικές αλλά και από εσωτερικές απειλές.

Η ξαφνική μετάβαση σε αυτό το νέο modus operandi έφερε στο προσκήνιο σημαντικά κενά που υπάρχουν στην εκπαίδευση των υπεύθυνων IT, αλλά και του γενικότερου ανθρώπινου δυναμικού σε θέματα **Cybersecurity** εφόσον όταν μιλάμε για απομακρυσμένη πρόσβαση σε εταιρικά δίκτυα και πληροφορίες τότε τα δεδομένα αλλάζουν και ξεφεύγουν από τον άμεσο έλεγχο των διαχειριστών. Με τους διαδικτυακούς απατεώνες να εκμεταλλεύονται τις αδυναμίες των συστημάτων και την αφέλεια των εργαζομένων, η ανάγκη για ενημέρωση σε θέματα κυβερνοασφάλειας και για δημιουργία υποδομών **Cyber Resilience** είναι πλέον επιτακτική.

## ΨΗΦΙΑΚΕΣ ΑΠΑΤΕΣ & ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ

**Απειλές που θέτουν σε κίνδυνο την εμπιστευτικότητα εταιρικών δεδομένων π.χ. η σύνδεση σε άγνωστα ή μη ασφαλή δίκτυα Wi-Fi μπορεί να επιτρέψει σε τρίτους, συνδεδεμένους στο ίδιο δίκτυο, να παρακολουθούν πληροφορίες που λαμβάνονται ή αποστέλλονται από συσκευές σε αυτό το δίκτυο.*

**Απειλές που θέτουν σε κίνδυνο τη διαθεσιμότητα πληροφοριών π.χ. ένα κακόβουλο λογισμικό (malware) το οποίο είναι εγκατεστημένο σε προσωπική συσκευή εργαζομένου, μπορεί να θέσει σε κίνδυνο όχι μόνο τα δεδομένα που είναι αποθηκευμένα στην συγκεκριμένη συσκευή, αλλά και οποιαδήποτε δεδομένα στα οποία έχει πρόσβαση η συσκευή αυτή.*

**Απειλές που θέτουν σε κίνδυνο την ακεραιότητα π.χ. οι πληροφορίες που είναι αποθηκευμένες σε μια συσκευή, ή ακόμα και η ίδια η συσκευή, μπορούν να κρυπτογραφηθούν από κακόβουλα λογισμικά ransomware, καθιστώντας τις κυριολεκτικά άχρηστες.*

## ΣΥΝΗΘΕΙΣ ΑΠΕΙΛΕΣ

**ΨΗΦΙΑΚΕΣ ΑΠΑΤΕΣ & ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ**

Η γραμμή μεταξύ μιας ψηφιακής απάτης και της κοινωνικής μηχανικής είναι θολή, ειδικά όταν διακυβεύονται εταιρικά συμφέροντα. Οι επιχειρησιακές απάτες δεν είναι καινούργιο φαινόμενο, ωστόσο οι ψηφιακοί ομόλογοι τους μερικές φορές έχουν ακόμη μεγαλύτερες επιπτώσεις στην λειτουργία μιας εταιρίας.

**+ EMAIL SCAMS**

Η διασφάλιση των λογαριασμών ηλεκτρονικού ταχυδρομείου είναι καίριας σημασίας για κάθε επιχείρηση. Το ηλεκτρονικό ταχυδρομείο ήταν και παραμένει το πιο κοινό κανάλι μετάδοσης απειλών όπως **ransomware** και **phishing.**

Ο εργαζόμενος εξ'αποστάσεως είναι πιο πιθανό να ανοίξει ένα (τυχαίο) email με τίτλο "Πληρωμή τιμολογίου" ή να κατεβάσει ένα συνημμένο αρχείο PDF που θα μολύνει με λογισμικό ransomware την συσκευή του και κατ' επέκταση ολόκληρο το δίκτυο.

**+ ΗΛΕΚΤΡΟΝΙΚΟ "ΨΑΡΕΜΑ"**

Το ηλεκτρονικό "ψάρεμα" (phishing) είναι μια από τις συχνότερες εταιρικές κυβερνοαπειλές. Ένα email που μπορεί φαινομενικά να έχει σταλεί από μια εταιρεία που γνωρίζετε ή εμπιστεύεστε όπως π.χ. μια τράπεζα, ένα ιστότοπο κοινωνικής δικτύωσης, μια εφαρμογή διαδικτυακών πληρωμών ή ένα διαδικτυακό κατάστημα, παροτρύνει τον χρήστη να πατήσει σε έναν σύνδεσμο ή να ανοίξει ένα συνημμένο αρχείο. Οι απατεώνες ουσιαστικά με αυτό το τρόπο θέλουν να εξαπατήσουν τους χρήστες ώστε να καταχωρήσουν εμπιστευτικά στοιχεία όπως κωδικούς για λογαριασμούς email, προσωπικούς κωδικούς πρόσβασης σε εταιρικά δίκτυα ή και κωδικούς για τραπεζικούς λογαριασμούς.

Τόσες πολλές φαινομενικά «άκακες» κινήσεις κρύβουν ψηφιακούς κινδύνους που μπορούν να στοιχίσουν ακριβά εάν δεν δοθεί εξαρχής η απαιτούμενη προσοχή.

## ΑΠΑΡΑΙΤΗΤΑ ΕΡΓΑΛΕΙΑ

Η τηλεργασία απαιτεί συγκεκριμένα εργαλεία τα οποία διασφαλίζουν την ομαλή σύνδεση εξ αποστάσεως:

**+ Δημόσια & Ιδιωτικά δίκτυα**

Ασφαλή δίκτυα είναι δίκτυα στα οποία έχουν εφαρμοστεί μέτρα ασφαλείας για να αποτρέπεται η σύνδεση μη-εξουσιοδοτημένων χρηστών ή εισβολέων. Στην περίπτωση των ιδιωτικών οικιακών δικτύων, είναι σημαντικό ο δρομολογητής Wi-Fi (wi-fi router) να διαθέτει ισχυρό κωδικό πρόσβασης και να γίνεται συχνά έλεγχος των συσκευών που συνδέονται με αυτό.

Τα δημόσια δίκτυα είναι πολύ χρήσιμα όταν χρειαστεί να εργαστούμε σε δημόσιους χώρους όπως καφετέριες, ξενοδοχεία ή σε οποιονδήποτε άλλο δημόσιο χώρο και είναι συνήθως ανοιχτά δίκτυα. Ως εκ τούτου, δεν έχουν περιοριστικά μέτρα ασφαλείας, ένας χάκερ μπορεί εύκολα να υποκλέψει δεδομένα που μεταφέρονται στο συγκεκριμένο δίκτυο. Επομένως, εάν χρειαστεί σύνδεση σε δημόσια δίκτυα, θα ήταν καλό να αποφύγετε τη πρόσβαση σε εμπιστευτικές πληροφορίες.

**+ VPN**

Το εικονικό ιδιωτικό δίκτυο (VPN) χρησιμοποιεί τεχνολογίες κρυπτογράφησης για να παρέχει ασφαλή απομακρυσμένη πρόσβαση σε ένα δίκτυο, με τέτοιο τρόπο ώστε να εμποδιστεί η διάδοση εμπιστευτικών πληροφοριών σε μη εξουσιοδοτημένους τρίτους. Είναι σημαντικό να παρέχεται στους υπαλλήλους σύνδεση μέσω VPN για απομακρυσμένη πρόσβαση σε εταιρικά δίκτυα και δεδομένα.

**+ Αυξημένος έλεγχος πρόσβασης**

Ένας ισχυρός κωδικός πρόσβασης είναι ο απλούστερος τρόπος να προστατέψετε τις συσκευές σας, αν και οι περισσότερες συσκευές παρέχουν πλέον και βιομετρικά σύστημα ελέγχου ταυτότητας. Συστήνεται ανεπιφύλακτα ένα επιπρόσθετο μέτρο ασφαλείας όπως ο έλεγχος ταυτότητας δύο παραγόντων (Two factor authentication – 2FA).

Ο σκοπός του 2FA είναι να αποτρέψει την πρόσβαση στους λογαριασμούς και τις συσκευές σας, σε περιπτώσεις που ο κωδικός πρόσβασής σας έχει παραβιαστεί από κάποιο κακόβουλο λογισμικό ή κάποιας μορφής ψηφιακή απάτη. Ουσιαστικά εκτός από το όνομα χρήστη και τον κωδικό πρόσβασης ( username & password), απαιτείται επιπρόσθετος έλεγχος για να δοθεί πρόσβαση: ένας κωδικός ασφαλείας μέσω SMS, ένα hard token, μια εφαρμογή ελέγχου ταυτότητας ή ακόμη και ένα κλειδί USB.

**+ Κρυπτογράφηση**

Καθημερινά μεταφέρονται εκατομμύρια πληροφορίες από και προς πολλαπλές συσκευές, είτε αυτές είναι εμπιστευτικά email, εταιρικά αρχεία, πιστοποιητικά ή πληροφορίες για λογαριασμούς. Αυτές οι πληροφορίες συνήθως αποθηκεύονται στις εσωτερικές μνήμες διαφόρων συσκευών, σε διακομιστές cloud ή και σε φορητούς δίσκους. Εάν μια συσκευή χτυπηθεί από hackers, κλαπεί ή χαθεί, διακυβεύονται εμπιστευτικές πληροφορίες.

Η κρυπτογράφηση είναι ένα πολύ χρήσιμο εργαλείο για την προστασία αποθηκευμένων δεδομένων. Με απλά λόγια, πρόκειται για την μετατροπή των πληροφοριών σε μία ακατανόητη μορφή με τη χρήση κρυπτογραφικού αλγορίθμου, ώστε να μην μπορούν να διαβαστούν από κανέναν εκτός αυτών που έχουν τα συγκεκριμένα κλειδιά.

**+ Mail Security**

Είδαμε ότι κατά την τηλεργασία, οι πιο συνήθεις κυβερνοαπειλές είναι αυτές που χρησιμοποιούν το ηλεκτρονικό ταχυδρομείο ως κανάλι πρόσβασης. Η ενίσχυση της προστασίας των λογαριασμών ηλεκτρονικών ταχυδρομείων και η βαθύτερη ανάλυση των εγγράφων και άλλων αρχείων που είναι συνημμένα σε email είναι πρωταρχικής σημασίας.

**+ Εφεδρικά Αντίγραφα**

Έχουμε δώσει πληροφορίες για την προστασία δεδομένων σε περιπτώσεις κυβερνοεπίθεσης, απώλειας ή κλοπής μιας συσκευής. Είναι εξίσου σημαντικό να υπάρχουν εναλλακτικοί τρόποι πρόσβασης σε τυχόν χαμένα δεδομένα, ώστε στην εσχάτη περίπτωση που δεν θα υπάρχει πιθανότητα ανάκτησης, να μπορούμε να συνεχίσουμε απρόσκοπτα την εργασία μας.

Για αυτό το λόγο, θα πρέπει να δημιουργούνται συχνά εφεδρικά αντίγραφα αρχείων τα οποία θα είναι δύσκολο να αναπαραχθούν εάν χαθούν. Αυτό ισχύει ειδικά για προσωπικά έγγραφα, εκθέσεις, έρευνες, λογιστικά φύλλα, παρουσιάσεις ή και φωτογραφίες.

**+ Συνδυαστικές λύσεις ασφαλείας**

Είναι απαραίτητο τα πιο πάνω εργαλεία να συνδυαστούν με ένα προενεργό σύστημα ανίχνευσης απειλών, μια ολοκληρωμένη λύση ασφαλείας. Ο λόγος για τον οποίο μιλάμε για μια ολοκληρωμένη λύση, και όχι μόνο για ένα λογισμικό “antivirus”, είναι γιατί πλέον δεν είναι αρκετός ο εντοπισμός ενός κακόβουλου κώδικα. Οι περιεκτικές λύσεις ασφαλείας περιλαμβάνουν μια σειρά από εργαλεία τα οποία εντοπίζουν διάφορους τύπους απειλών, όπως οι μη ασφαλείς συνδέσεις, οι πλαστοί ιστότοποι και πολλές άλλες μορφές πιθανών κινδύνων.

## Πώς μπορεί ένας χρήστης να προστατευτεί;

Αν η εταιρεία σου παρέχει laptop, τότε πρέπει να κάνεις ό,τι θα έκανες κι από το γραφείο. Βεβαιώσου πως κάνεις αντίγραφα ασφαλείας ευαίσθητων δεδομένων, το λογισμικό και το antivirus είναι ενημερωμένο, δεν ανοίγεις ύποπτα συνημμένα και συνδέσμους και δεν επισκέπτεσαι επισφαλείς ιστοσελίδες.

Δεν χρησιμοποιείς στικάκια USB για μεταφορά εταιρικών δεδομένων ή τουλάχιστον βεβαιώνεσαι πως είναι κρυπτογραφημένο το στικάκι σε περίπτωση απώλειάς του.

Δεν χρησιμοποιείς μη-εγκεκριμένες εξωτερικές υπηρεσίες για μεταφορά εταιρικών δεδομένων (προσωπικό Dropbox, κτλ). Αυτή η χρήση μη-εγκεκριμένης τεχνολογίας λέγεται **Shadow IT** και σε περίπτωση απώλειας δεδομένων ο υπάλληλος φέρει την ευθύνη».

Εννοείται πως κλειδώνεις τον υπολογιστή όταν απομακρύνεσαι από αυτόν, ειδικά αν έχεις παιδιά, διότι δεν ξέρεις ποιος μπορεί να κάνει κάτι λάθος κατά την απουσία σου. Επίσης, αυτές τις ημέρες πολλοί δουλεύουν περισσότερες ώρες απ' όσο συνήθως, κι ο διαχωρισμός μεταξύ δουλειάς/διαλείμματος/ξεκούρασης δεν είναι ευδιάκριτος.

Απόφυγε τη χρήση εταιρικού υπολογιστή για προσωπική εργασία ή αναζητήσεις. Ό,τι δημιουργείς χρησιμοποιώντας τον εταιρικό υπολογιστή, είναι στη δικαιοδοσία της εταιρείας να το παρακολουθήσει.

Επίσης, ό,τι πνευματική ιδιοκτησία δημιουργήσεις χρησιμοποιώντας τον εταιρικό υπολογιστή, νομικά ανήκει στην εταιρεία.

Να μην εγκαταστείς προγράμματα αμφιβόλου προελεύσεως και «σπασμένο» λογισμικό