

Training session

Employees of small and medium enterprises

Association of Thessalian Enterprises and Industries

13/02/2025



Co-funded by
the European Union

Τι είναι η κυβερνοασφάλεια

- ❑ Η κυβερνοασφάλεια αναφέρεται στην προστασία των πληροφοριακών συστημάτων, των δεδομένων και των ψηφιακών υποδομών από απειλές, επιθέσεις και ανεπιθύμητες παρεμβάσεις. Αναφέρεται επίσης, ως ασφάλεια πληροφοριών ή ασφάλεια ΤΠ (Τεχνολογίας Πληροφοριών)
- ❑ Επίσης, η κυβερνοασφάλεια είναι η συλλογή λογισμικού, διαδικασιών και συστημάτων που προστατεύουν έναν οργανισμό από κυβερνοεπιθέσεις και διασφαλίζουν τη διαθεσιμότητα των πόρων. Η κυβερνοασφάλεια αποτελεί έναν αυξανόμενο τομέα ανησυχίας, καθώς όλο και περισσότερες εταιρείες και άτομα μπαίνουν στο διαδίκτυο. Αποτελεί ένα από τους **σημαντικότερους τομείς της παγκόσμιας αγοράς**
- ❑ Ένα καλό παράδειγμα είναι, όταν χρησιμοποιείτε τον ιστότοπο της τράπεζάς σας για να ελέγξετε το υπόλοιπό σας ή να κάνετε πληρωμές online. Αν δεν υπήρχαν μέτρα κυβερνοασφάλειας, κάποιος θα μπορούσε εύκολα να αποκτήσει πρόσβαση σε αυτές τις πληροφορίες χωρίς την άδειά σας



Λεξικό κυβερνοασφάλειας

Απειλές (Threats)

Οι απειλές αναφέρονται σε πιθανές κακόβουλες ενέργειες ή συμπεριφορές που μπορούν να προκαλέσουν ζημιά στα πληροφοριακά συστήματα, τα δεδομένα ή τις υπηρεσίες.

Ευπάθεια (Vulnerability)

Η ευπάθεια αναφέρεται σε μια αδυναμία ή έλλειψη ασφάλειας σε ένα πληροφοριακό σύστημα που μπορούν να εκμεταλλευθούν οι επιτιθέμενοι.

Επικοινωνία Κυβερνοασφάλειας

Η επικοινωνία κυβερνοασφάλειας αναφέρεται στη διασφάλιση της αποτελεσματικής επικοινωνίας μεταξύ των εμπλεκόμενων φορέων σχετικά με τα θέματα ασφάλειας.

Επίθεση (Attack)

Μια επίθεση αναφέρεται στην προσπάθεια αξιοποίησης ευπαθειών ή αδυναμιών σε ένα πληροφοριακό σύστημα με σκοπό την πρόκληση ζημιάς ή την απόκτηση παράνομης πρόσβασης.

Πολιτική Κυβερνοασφάλειας

Η πολιτική κυβερνοασφάλειας περιλαμβάνει τους κανόνες, τις διαδικασίες και τις πρακτικές που εφαρμόζονται για τη διασφάλιση της ασφάλειας στον ψηφιακό χώρο.

Συνεχόμενη Ασφάλεια (Continuous Security)

Η συνεχόμενη ασφάλεια αναφέρεται στην πρακτική συνεχούς παρακολούθησης ανάλυσης και βελτίωσης των μέτρων ασφάλειας για αντιμετώπιση σύγχρονων απειλών.



Ιστορία και εξέλιξη της κυβερνοασφάλειας (I)

Διανύοντας, πλέον, την εποχή της ψηφιοποίησης, ολοένα και περισσότεροι τομείς της σύγχρονης κοινωνίας λειτουργούν βάσει ψηφιακών τεχνολογιών. Παρόλο που τομείς όπως, η οικονομία, η υγεία και οι μεταφορές έχουν ευνοηθεί από τη ψηφιοποίηση, δεν παύουν να είναι εκτεθειμένοι σε κυβερνοαπειλές.

- ❖ Η εξέλιξη παρατηρείται από το 2004 και έπειτα. Τότε, ιδρύθηκε ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (**ENISA**), σύμφωνα με τον Κανονισμό 460/2004
- ❖ **Σκοπός** του Οργανισμού ήταν η ανάπτυξη των εθνικών στρατηγικών κυβερνοασφάλειας, καθώς και η παροχή συμβουλευτικής και λύσεων, προκειμένου τα κράτη να βελτιώσουν τις δυνατότητές τους στον τομέα αυτό, αλλά και η εφαρμογή της Πολιτικής και του Νομικού πλαισίου της Ε.Ε σε θέματα ασφάλειας δικτύου και πληροφοριών
- ❖ Οι διαφοροποιήσεις που υπάρχουν μεταξύ των κρατών-μελών, αναφορικά με τις δυνατότητές τους να διαχειριστούν συντονισμένα περιστατικά διασυνοριακών κυβερνοεπιθέσεων, οδήγησαν στη **θέσπιση ενός πλάνου έκτακτης ανάγκης**, που να περιορίζει τις επικείμενες απειλές, ή μιας ομάδας αντιμετώπισης έκτακτων αναγκών (**CERT**). Η CERT απαρτίζεται από εμπειρογνώμονες σε θέματα ψηφιακών υποδομών και υφίσταται τόσο σε επίπεδο ΕΕ, όσο και σε επίπεδο κρατών-μελών
- ❖ Σημείο καμπής για τη δράση της ΕΕ στην κυβερνοασφάλεια ήταν η έκδοση της Οδηγίας 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την **Ένωση** (NIS Directive), η οποία τέθηκε σε ισχύ το 2016, και συνέβαλε στην επίτευξη ενός κοινού υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών σε ολόκληρη την ΕΕ

IS1



IS1 Την Ευρωπαϊκή ένωση εννοούμε
Info Sthev; 2024-03-15T12:41:36.134

Ιστορία και εξέλιξη της κυβερνοασφάλειας (ι)

- ❖ Ωστόσο, **το ίδιο έτος**, τέθηκε σε ισχύ και ο **Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)**, που αντιπροσωπεύει ένα εναρμονισμένο νομικό πλαίσιο για την προστασία των προσωπικών και ιδιωτικών δεδομένων των πολιτών της ΕΕ.
- ❖ Επιπλέον, προτάθηκε η ενίσχυση της εργαλειοθήκης της Ε.Ε για τη διπλωματία στον κυβερνοχώρο, με σκοπό την αποτελεσματική πρόληψη και αντιμετώπιση κακόβουλων δραστηριοτήτων σε αυτόν, ιδίως εκείνων που επηρεάζουν τις υποδομές καίριας σημασίας και τις αξίες της ΕΕ. Μάλιστα, η **Ένωση** σκοπεύει στην ενίσχυση της συνεργασίας και των ικανοτήτων στον τομέα της κυβερνοάμυνας, αξιοποιώντας το έργο του Ευρωπαϊκού Οργανισμού Άμυνας και ενθαρρύνοντας τα κράτη-μέλη να αξιοποιήσουν πλήρως τη μόνιμη διαρθρωμένη συνεργασία τους, όπως και το Ευρωπαϊκό Ταμείο Άμυνας.
- ❖ Τέλος, η **κυβερνοασφάλεια** αποτελεί **προτεραιότητα** που αντικατοπτρίζεται και στον επόμενο μακροπρόθεσμο προϋπολογισμό της Ε.Ε (**2021-2027**), με την ίδια να προσπαθεί να διαδραματίσει ουσιαστικό ρόλο στην προώθηση ενός παγκόσμιου, ανοικτού, σταθερού και ασφαλούς κυβερνοχώρου, βασιζόμενη τόσο στις θεμελιώδεις αξίες της Ε.Ε όσο και στο κράτος δικαίου.
- ❖ Κάποιες από τις δράσεις της μπορεί να λαμβάνουν αρνητικό πρόσημο, χρειάζεται, ωστόσο, να ληφθεί υπόψη ότι η πρόοδος σε έναν τομέα όπως η κυβερνοασφάλεια απαιτεί χρόνο για να αποφέρει τα επιθυμητά αποτελέσματα, ιδιαίτερα εντός ενός πλαισίου στο οποίο χρειάζεται να γίνουν αρκετοί συμβιβασμοί μεταξύ των συμμετεχόντων.

Η εξέλιξη των κυβερνοεπιθέσεων

Η κυβερνοασφάλεια γεννήθηκε όταν οι πρώτοι υπολογιστές μπόρεσαν να δικτυωθούν και να μεταφέρουν πληροφορίες μεταξύ τους. Αυτό δε συνέβη μέχρι τη δεκαετία του 1950 δηλαδή όταν αναπτύχθηκαν τα πρώτα δίκτυα υπολογιστών και μόντεμ. Μόλις τη δεκαετία του **1960**, η **κυβερνοασφάλεια άρχισε να παίρνει τη μορφή**, με την οποία είναι γνωστή σήμερα. Η δημιουργία του διαδικτύου ήρθε το 1969, όταν η Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων του Πενταγώνου (ARPA) κατάφερε να στείλει ένα μήνυμα από το Πανεπιστήμιο της Καλιφόρνιας στο Ερευνητικό Κέντρο του Στάνφορντ.

Η έλευση του κακόβουλου λογισμικού

Η ιδέα της κυβερνοασφάλειας θα ξεκινούσε εκείνη τη στιγμή και το πρόγραμμα που ανέπτυξε ο Ray Tomlinson θα θεωρούνταν το πρώτο antivirus. Τη δεκαετία του 1980 παρατηρήθηκε έκρηξη κακόβουλων προγραμμάτων, τα οποία πολλαπλασιάστηκαν με γεωμετρική πρόοδο. Ως απάντηση, το 1987 ο John McAfee ίδρυσε την McAfee και λάνσαρε το λογισμικό Virus Scan, σηματοδοτώντας την εμπορική ύπαρξη των antivirus.



Μην ξεχνάμε το WannaCry

Στις αρχές της δεκαετίας του 2000, οι επιθέσεις ransomware άρχισαν να εμφανίζονται σε όλο και πιο εξελιγμένη μορφή. Ήταν το 2017 όταν σημειώθηκε η κυβερνοεπίθεση γνωστή ως WannaCry: μια κρατικά χρηματοδοτούμενη επίθεση που εξαπλώθηκε διεθνώς. Σήμερα αποτελεί σημαντικό κίνδυνο λόγω των ολοένα και πιο εξελιγμένων μεθόδων που χρησιμοποιεί και των συνεπαγόμενων ζημιών και σοβαρών οικονομικών απωλειών που συνεπάγεται.



Το πραγματικό Y2K: Loveletter

Η νέα χιλιετία ξεκίνησε με τον φόβο που δημιούργησε το πρόβλημα Y2K: ότι τα υπολογιστικά συστήματα ήταν ελαττωματικά επειδή οι ημερομηνίες στα προγράμματα παρέλειπαν την εκατονταετηρίδα. Φοβούνταν ότι με την αλλαγή της χιλιετίας όλες οι ημερομηνίες θα ήταν λάθος και αυτό θα οδηγούσε σε αποτυχίες και σοβαρές ζημιές σε όλες τις χώρες. Αυτό επρόκειτο να αλλάξει με τον περιβόητο ιό Loveletter phishing, ο οποίος θα εξαπλωνόταν μέσα σε μόλις πέντε ώρες σε υπολογιστές στην Ασία, την Ευρώπη και την Αμερική.

Το μέλλον της τεχνητής νοημοσύνης είναι εδώ

- ❖ Τα τελευταία χρόνια παρατηρήθηκε αύξηση της πολυπλοκότητας των επιθέσεων στον κυβερνοχώρο και των επιθέσεων ransomware, με νέα μέσα φορέων επίθεσης να αυξάνονται, από τις επιθέσεις στην αλυσίδα εφοδιασμού έως την τεχνητή νοημοσύνη. Δυστυχώς, όλοι οι ειδικοί του κλάδου προβλέπουν την αναπόφευκτη αύξηση των κυβερνοεπιθέσεων και των νέων μέσων phishing σε όλο τον κόσμο, με τις διασυνδεδεμένες επιχειρήσεις και την κοινωνία μας.
- ❖ Όσον αφορά την Ελλάδα ένας οργανισμός δέχεται επίθεση κατά μέσο όρο 871 φορές την εβδομάδα τους τελευταίους 6 μήνες, με κορυφαίο κακόβουλο λογισμικό να είναι το Emotet.
- ❖ Η τεχνητή νοημοσύνη σηματοδοτεί ένα σημείο καμπής στην εξέλιξη των κυβερνοεπιθέσεων, καθώς αυτού του είδους η τεχνολογία επιτρέπει στις απειλές να είναι πιο συχνές, ταχύτερες και πιο αποτελεσματικές. Τεχνικές όπως το deepfake καταφέρνουν να υποδύονται αξιόπιστα σχετικές ταυτότητες και εταιρείες για την κλοπή πληροφοριών, οι επιθέσεις phishing γίνονται όλο και πιο πειστικές, και νέες παραλλαγές ransomware και κακόβουλου λογισμικού αναπτύσσονται ταχύτατα και είναι οικονομικά πιο αποδοτικές. Καθώς οι τεχνικές των κυβερνοεγκλημάτων εξελίσσονται με ταχείς ρυθμούς, η ασφάλεια στον κυβερνοχώρο χρησιμοποιεί επίσης την τεχνητή νοημοσύνη για να βελτιώσει τις αμυντικές μεθόδους της, ώστε να συμβαδίζει.

Πως αντιμετωπίζεται η κυβερνοασφάλεια σήμερα (ι)

- ❖ Από τα πλέον νευραλγικά κομμάτια του ψηφιακού μετασχηματισμού των χρηματοοικονομικών υπηρεσιών η αντιμετώπιση των διαδικτυακών απειλών χρειάζεται ιδιαίτερη προσοχή, ενώ είναι πολλές και σημαντικές οι προδιαγραφές που πρέπει να τηρούνται, για την πρόληψη κινδύνων.
- ❖ Η πανδημία έφερε μεγάλες ανατροπές, εξαναγκάζοντάς μας να περάσουμε από τον offline στον online κόσμο πάμπολλες δραστηριότητες. Η βίαιη, λόγω της COVID-19, επιτάχυνση του ψηφιακού μετασχηματισμού είχε τα καλά της, αλλά βέβαια είχε (κι έχει ακόμα) τους κινδύνους της. Ένας από τους μεγαλύτερους, που ίσως ακόμα να μην έχουμε δει σε πλήρη ανάπτυξη, αλλά η πρόγνωση που πήραμε ως τώρα προμηνύει πολλά, είναι σίγουρα η κυβερνοασφάλεια, ειδικά στον χώρο της οικονομίας.
- ❖ Με δεδομένο, μάλιστα, ότι το 2020 αποδείχθηκε η χειρότερη χρονιά στην ιστορία, όσον αφορά στις παραβιάσεις δεδομένων, μάλλον δικαιολογούνται οι ειδήμονες του κλάδου να υποστηρίζουν πως **«η κυβερνοασφάλεια είναι σήμερα το πιο σημαντικό πρόβλημα στην ψηφιακή οικονομία»**.
- ❖ Οι κίνδυνοι караδοκούν και είναι πολλοί. Το τοπίο σε θέματα αντιμετώριων στον χώρο της κυβερνοασφάλειας μένει κατά πολύ το ίδιο. Σε πολύ μεγαλύτερο βαθμό αυξάνουν οι χρήστες, όπως προείπαμε, με την απειρία να τους οδηγεί συχνά σε αβίαστα συμπεριφορικά σφάλματα που διευκολύνουν τις παραβιάσεις δεδομένων.
- ❖ Οι απανταχού κυβερνήσεις πρέπει να επιμείνουν στη δίκαιη κατανομή και την προστασία των πολιτών και των δεδομένων τους, κάτι που ήδη γίνεται σε κάποιες χώρες (πχ. Κίνα, Ινδία, Φινλανδία κ.ά). Ο μεν ιδιωτικός τομέας θα πρέπει να αφεθεί ελεύθερος να αναλάβει επιχειρηματικές πρωτοβουλίες, όμως, και οι κυβερνήσεις από την πλευρά τους θα πρέπει να διασφαλίσουν οφέλη για όλους και να διαχειριστούν τους κινδύνους.

IS1

IS1 Αυξάνουν ή αυξάνονται??
Info Sthev; 2024-03-15T12:55:37.207

Πως αντιμετωπίζεται η κυβερνοασφάλεια σήμερα (II)

Πολλά χρηματοπιστωτικά ιδρύματα εφαρμόζουν λύσεις και τεχνολογίες **FinTech** για την ανάπτυξη και τη βελτίωση των υπηρεσιών τους που αφορούν σε πληρωμές, δάνεια, ασφάλιση, αποταμιεύσεις και επενδύσεις, κι έτσι οι καταναλωτές έχουν πλέον πρόσβαση σε όλο και περισσότερες ηλεκτρονικές συναλλαγές. Ωστόσο, ο ψηφιακός μετασχηματισμός των χρηματοοικονομικών υπηρεσιών εγείρει ολοένα και περισσότερους κινδύνους κυβερνοεπιθέσεων.

- Κύριο μέλημα του χρηματοπιστωτικού τομέα θα πρέπει να αποτελεί η προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των καταναλωτών, καθώς και η ασφάλεια των ηλεκτρονικών συναλλαγών.
- Επιβάλλεται, επομένως, η ανάπτυξη και λειτουργία ψηφιακών συστημάτων παροχής χρηματοπιστωτικών υπηρεσιών με έμφαση στην ασφάλεια, καθώς και η εφαρμογή αυστηρού νομικού πλαισίου που θα θέτει σημαντικές εγγυήσεις ασφάλειας, ώστε να εξασφαλιστεί η εμπιστοσύνη στις ηλεκτρονικές συναλλαγές.
- Η μη συμμόρφωση των εταιρειών με το κανονιστικό πλαίσιο έχει ως συνέπεια υψηλά πρόστιμα και, λόγω αυτού, οι εταιρείες αναζητούν λύσεις, ώστε να μειωθεί αυτός ο κίνδυνος. Ωστόσο, η ραγδαία εξέλιξη της τεχνολογίας και η αύξηση των κυβερνοεπιθέσεων συχνά δημιουργεί κενά στο θεσμικό πλαίσιο και απαιτεί τη συνεχή αναπροσαρμογή του. Η διατήρηση ίσων κανόνων ανταγωνισμού μεταξύ των υφιστάμενων τραπεζών και των νέων εταιρειών FinTech, έτσι ώστε να διατηρείται η οικονομική σταθερότητα, παραμένει μεγάλη πρόκληση. Αυστηρή προτεραιότητα του θεσμικού πλαισίου είναι η προστασία των καταναλωτών, ιδίως όσον αφορά στην ιδιωτικότητα και την ασφάλεια στον κυβερνοχώρο, κι αυτό αποδείχτηκε με τη θέσπιση του κανονισμού GDPR.
- Προς αυτή την κατεύθυνση, κάθε νέα εταιρεία οφείλει να κατανοεί τους κινδύνους στους οποίους εκθέτει τους πελάτες της, καθώς και τους άλλους συμμετέχοντες στο χρηματοπιστωτικό σύστημα και να συμμορφώνεται πλήρως με τους ισχύοντες κανονισμούς.

Σημασία της κυβερνοασφάλειας για τις μικρομεσαίες επιχειρήσεις

- Η περίοδος της πανδημίας επιτάχυνε τη χρήση υπηρεσιών Διαδικτύου και τεχνολογικών εργαλείων από πολλές ΜμΕ, που συμπεριέλαβαν στον τρόπο λειτουργίας τους μεταξύ άλλων χρήση υπηρεσιών cloud, τηλεργασία, αλλά και τη βελτίωση των διαδικτυακών υπηρεσιών τους.
- Ωστόσο, όλες οι ηλεκτρονικές διαδικασίες ενέχουν και υψηλότερο ρίσκο ως προς την ασφάλεια, αν δεν τηρηθούν σωστά όλα τα απαραίτητα μέτρα πρόληψης. 25 εκατομμύρια ΜμΕ δραστηριοποιούνται σήμερα στην Ευρωπαϊκή Ένωση και απασχολούν περισσότερους από 100 εκατομμύρια εργαζόμενους, είναι σημαντικό να δίνεται βαρύτητα σε ζητήματα ασφάλειας. Ένα σοβαρό περιστατικό κυβερνοεπίθεσης μπορεί να θέσει σε κίνδυνο μία επιχείρηση, προκαλώντας σημαντική οικονομική ζημιά ή διαρρέοντας ευαίσθητες πληροφορίες.
- Παρ' όλα αυτά, οι κυβερνοεπιθέσεις εξακολουθούν να μην θεωρούνται σημαντικός κίνδυνος από μεγάλο αριθμό ΜμΕ, καθώς παραμένει η πεποίθηση ότι τα περιστατικά στον κυβερνοχώρο στοχεύουν μόνο μεγαλύτερους οργανισμούς. Η μελέτη αποκαλύπτει ότι οι επιθέσεις phishing είναι από τα πιο κοινά περιστατικά στον κυβερνοχώρο στα οποία είναι πιθανό να εκτεθούν οι ΜμΕ, μαζί με επιθέσεις ransomware, κλεμμένους φορητούς υπολογιστές, αλλά και "απάτες του CEO" (όπου ο απατεώνας στέλνει μηνύματα υποδύομενος υψηλόβαθμο στέλεχος της επιχείρησης).
- Η Ελλάδα έχει δημοσιεύσει από τα τέλη του 2020 την Εθνική Στρατηγική Κυβερνοασφάλειας (2020-2025), η οποία περιλαμβάνει σειρά δράσεων που καλύπτει όλους τους σημαντικούς και κρίσιμους τομείς .



Μορφές κυβερνοεπιθέσεων

❖ Μη καταχωρημένο λογισμικό

Είναι προγράμματα που χρησιμοποιεί στην καθημερινότητά του ένας χρήστης (Java, Adobe Reader κ.α.) και οι εταιρίες στην προσπάθειά τους να καλύπτουν τα κενά ασφαλείας, προχωρούν στην έκδοση νεότερων ενημερώσεων των λογισμικών τους.

❖ Ηλεκτρονικό ψάρεμα (phishing)

Πρόκειται για πλαστή οντότητα που υποδύεται μία αξιόπιστη και αυθεντική όπου σκοπό έχει να αποσπάσει πληροφορίες από τον χρήστη. Η επιτυχία του ηλεκτρονικού ψαρέματος στηρίζεται στην έλλειψη γνώσεων του θύματος, στην έλλειψη προσοχής του θύματος και στην οπτική εξαπάτηση.

❖ Ransomware

Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που μπορεί να κλειδώσει μια συσκευή ή να κρυπτογραφήσει το περιεχόμενό της, εμποδίζοντας τον χρήστη από την πρόσβαση στα προσωπικά του αρχεία με σκοπό την καταβολή λύτρων.

❖ Σκουλήκια (Network-traveling Worms)

Ένας ιός τύπου σκουληκιού αντιγράφει τον εαυτό του σε άλλους υπολογιστές, προκαλώντας υπερφόρτωση δικτύου ή εγκαθιστώντας επιβλαβές λογισμικό ιού. Αυτοί οι ιοί ενδέχεται να διαγράψουν αρχεία, ή να κλέψουν πολύτιμες πληροφορίες.



Συνέπειες κυβερνοεπιθέσεων

❖ Οικονομικό κόστος των κυβερνοεπιθέσεων

Οι απατεώνες χρησιμοποιούν ιστοσελίδες και email "ψαρέματος" με κακόβουλους συνδέσμους και συνημμένα για να κλέψουν τραπεζικά στοιχεία ή να εκβιάσουν οργανισμούς. Το **2020, το ετήσιο κόστος του κυβερνοεγκλήματος για την παγκόσμια οικονομία έφτασε τα 5,5 τρις ευρώ, ποσό διπλάσιο από εκείνο του 2015**

❖ Επιπτώσεις στη Δημοκρατία

Η ζημιά που προκαλείται από τις κυβερνοεπιθέσεις δεν αφορά μόνο την οικονομία και το χρηματοπιστωτικό σύστημα, αλλά επηρεάζει τα δημοκρατικά θεμέλια της Ε.Ε και απειλεί τις βασικές λειτουργίες της κοινωνίας. Για παράδειγμα, η **παραπληροφόρηση** είναι ένα από τα εργαλεία κυβερνοεπιθέσεων.

❖ Επιπτώσεις στις βασικές υπηρεσίες και στους τομείς καίριας σημασίας

Βασικές υπηρεσίες και τομείς καίριας σημασίας, όπως οι μεταφορές και η υγεία, εξαρτώνται όλο και περισσότερο από τη ψηφιακή τεχνολογία. Η εξάρτηση αυτή, σε συνδυασμό με τη διασύνδεση των υλικών αντικειμένων με το διαδίκτυο των πραγμάτων, μπορεί να έχει άμεσες συνέπειες, καθιστώντας την κυβερνοασφάλεια ζήτημα ζωής και θανάτου. Παράδειγμα αποτελούν οι κυβερνοεπιθέσεις έναντι νοσοκομείων, τα οποία αναγκάστηκαν να αναβάλλουν επείγουσες χειρουργικές επεμβάσεις, ή οι επιθέσεις έναντι δικτύων παροχής ενέργειας και νερού που απειλούν τη λειτουργία υπη

IS1



IS1 Υπερβολική σαν λέξη για παρουσίαση.
Info Sthev; 2024-03-15T13:02:14.377

Ασφαλής χρήση του διαδικτύου

- ❖ Το διαδίκτυο είναι ένας καινούριος κόσμος και για πολλούς πρωτόγνωρος. Προσφέρει διαδραστικότητα, έντονη εναλλαγή εικόνων και συναισθημάτων. Είναι μια εικονική κοινωνία, η οποία διαμορφώνεται παράλληλα με την πραγματικότητα.
- ❖ Η ασφάλεια του σπιτιού μας όμως, στο οποίο βρίσκεται ο υπολογιστής, μπορεί να μας οδηγήσει στο να μην αντιληφθούμε την απειλή καθώς ο κίνδυνος δεν είναι άμεσος και ορατός.
- ❖ Η γνώση των κανόνων ασφάλειας, η ανάπτυξη κριτικής και αντιληπτικής ικανότητας και η ικανότητα αναγνώρισης των κινδύνων είναι βασικά εφόδια για την ασφαλή πλοήγησή στο διαδίκτυο.
- ❖ Τα προσωπικά δεδομένα, όπως το ονοματεπώνυμο, η ηλικία, η κατοικία, το επάγγελμα, η εκπαίδευση, η οικονομική και οικογενειακή κατάσταση κατάσταση, χρησιμοποιούνται σε καθημερινή βάση καθώς περιηγούμαστε στο διαδίκτυο.



Κάποιες χρήσιμες συμβουλές ...

- Για κάθε σημαντικό λογαριασμό σας, φροντίζετε να χρησιμοποιείτε πάντα **μεγάλους και μοναδικούς κωδικούς**, αποτελούμενους από **αριθμούς, γράμματα και σύμβολα**
- **Μην** αποστέλλεται τους κωδικούς σας με email και μην τους μοιράζεστε με τρίτους
- Βάζετε **password recovery options** (επιλογές ανάκτησης κωδικού πρόσβασης) και κρατάτε τα ενημερωμένα
- **Αποφύγετε** οτιδήποτε ύποπτο. Μην απαντάτε σε περίεργα emails και μηνύματα και μη συμπληρώνετε τα στοιχεία σας (προσωπικές πληροφορίες, αριθμούς πιστωτικών καρτών, κωδικούς κ.ο.κ.) σε όλες τις ιστοσελίδες που σου το ζητούν
- Να **αναφέρετε** το παράνομο και καταχρηστικό περιεχόμενο που συναντάτε
- **Ελέγχετε** συχνά τις ρυθμίσεις ασφαλείας και ιδιωτικότητάς σας και καθορίστε πώς και με ποιους θέλετε να μοιράζεστε το περιεχόμενο σας



- Λαμβάνετε υπόψιν τη διαδικτυακή σας εικόνα, σκεπτόμενος πάντα καλά πριν από τη δημοσίευση ντροπιαστικού ή ακατάλληλου περιεχομένου
- Φροντίζετε να **διατηρείτε το λειτουργικό σύστημα** και τον **browser** σας **ενημερωμένα**
- Κατά την εγκατάσταση, **εξασφαλίζετε** πάντοτε ότι οι πηγές σας είναι **αξιόπιστες**
- **Προσέχετε** πού κάνετε sign in
- Αν η διεύθυνση σας **ξεκινά από https://**, τα δεδομένα σας προστατεύονται καλύτερα.
- **Κλειδώστε** πάντα **την οθόνη** του υπολογιστή, του tablet ή του smartphone σου μετά τη χρήση ή επίλεξε να κλειδώνει αυτόματα.



Κυβερνοασφάλεια και ελληνικές επιχειρήσεις

- Το 1/3 των Ελληνικών εταιρειών αναφέρει περιστατικά κυβερνοεπίθεσης ή κυβερνοεγκλήματος ουσιαστικά δείχνοντας την ανάγκη για λήψη μέτρων που θα διασφαλίσουν τη συνέχιση της εύρυθμης λειτουργία τους.
- Σύμφωνα με έρευνα που διενήργησε η Metron Analysis οι επιθέσεις στις ελληνικές εταιρείες αφορούν, κατά κύριο λόγο, παραπλανητικά emails και δευτερευόντως κακόβουλο λογισμικό ή χακάρισμα κοινωνικών δικτύων και emails, ενώ ελάχιστα σχετίζονται με παραβίαση προσωπικών δεδομένων πελατών.
- Στην ίδια έρευνα αναφέρεται ότι σχεδόν 4 στις 10 επιχειρήσεις θεωρούν ότι ήταν πολύ/αρκετά σοβαρή η κυβερνοεπίθεση που δέχθηκαν ενώ, σε κάθε περίπτωση, η αίσθηση κινδύνου παραμένει, καθώς 2 στις 3 επιχειρήσεις θεωρούν ότι είναι πολύ/αρκετά πιθανό να επαναληφθεί στο μέλλον κάποιου είδους κυβερνοεπίθεση.



- Το ψηφιακό έγκλημα δείχνει να απειλεί σημαντικά τις ελληνικές εταιρείες με τον κίνδυνο των κυβερνοεπιθέσεων, να βαίνει κλιμακούμενος στην Ελλάδα, με τη συντριπτική πλειονότητα των επιχειρήσεων να διαπιστώνει ότι οι κίνδυνοι στον κυβερνοχώρο αυξάνονται με την πάροδο του χρόνου.
- Συνολικά, περισσότερες από 8 στις 10 εταιρείες στην Ελλάδα (83%) πιστεύουν ότι το διαδίκτυο εγκυμονεί κινδύνους για τη λειτουργία τους. Μάλιστα, η συντριπτική πλειονότητα (82%) εκφράζει την άποψη ότι οι κίνδυνοι που αντιμετωπίζουν σήμερα είναι αυξημένοι σε σχέση με πέντε χρόνια νωρίτερα. Πάντως, παρόλα αυτά, μόλις 1 στις 5 εταιρείες (21%) έχει απευθυνθεί στη Δίωξη Ηλεκτρονικού Εγκλήματος για θέματα ασφάλειας στο Διαδίκτυο.
- Προκειμένου να αποφύγουν παρόμοιους κινδύνους οι εταιρείες έχουν αρχίσει να «θωρακίζονται» με συστήματα κυβερνοασφάλειας ενώ ακόμα μεγαλύτερη κινητικότητα παρατηρείται στο ελληνικό δημόσιο και τους δημόσιους οργανισμούς που έχουν πληγεί σημαντικά από περιστατικά κυβερνοεπιθέσεων.



Νόμος για την κυβερνοασφάλεια

- Το Υπουργείο Ψηφιακής Διακυβέρνησης συνέταξε **νόμο** με τίτλο «Εθνική Αρχή Κυβερνοασφάλειας και λοιπές διατάξεις», το οποίο προβλέπει τη σύσταση Νομικού Προσώπου Δημοσίου Δικαίου με την επωνυμία «Εθνική Αρχή Κυβερνοασφάλειας».
- Βασικός **στόχος** της νέας «Εθνικής Αρχής Κυβερνοασφάλειας» θα είναι ο συντονισμός και η υλοποίηση της Εθνικής Στρατηγικής για την Κυβερνοασφάλεια, καθώς και η αποτελεσματική πρόληψη και διαχείριση κυβερνοεπιθέσεων στην Ελλάδα, ώστε να επιτευχθεί ένα υψηλό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών στον δημόσιο και στον ιδιωτικό τομέα.



LET'S PLAY





mecys.eu



Co-funded by
the European Union

Training session

Employees of small and medium enterprises

Association of Thessalian Enterprises and Industries

27/03/2025



Co-funded by
the European Union

Τι είναι η κυβερνοασφάλεια

- ❑ Η κυβερνοασφάλεια αναφέρεται στην προστασία των πληροφοριακών συστημάτων, των δεδομένων και των ψηφιακών υποδομών από απειλές, επιθέσεις και ανεπιθύμητες παρεμβάσεις. Αναφέρεται επίσης, ως ασφάλεια πληροφοριών ή ασφάλεια ΤΠ (Τεχνολογίας Πληροφοριών)
- ❑ Επίσης, η κυβερνοασφάλεια είναι η συλλογή λογισμικού, διαδικασιών και συστημάτων που προστατεύουν έναν οργανισμό από κυβερνοεπιθέσεις και διασφαλίζουν τη διαθεσιμότητα των πόρων. Η κυβερνοασφάλεια αποτελεί έναν αυξανόμενο τομέα ανησυχίας, καθώς όλο και περισσότερες εταιρείες και άτομα μπαίνουν στο διαδίκτυο. Αποτελεί ένα από τους **σημαντικότερους τομείς της παγκόσμιας αγοράς**
- ❑ Ένα καλό παράδειγμα είναι, όταν χρησιμοποιείτε τον ιστότοπο της τράπεζάς σας για να ελέγξετε το υπόλοιπό σας ή να κάνετε πληρωμές online. Αν δεν υπήρχαν μέτρα κυβερνοασφάλειας, κάποιος θα μπορούσε εύκολα να αποκτήσει πρόσβαση σε αυτές τις πληροφορίες χωρίς την άδειά σας



Λεξικό κυβερνοασφάλειας

Απειλές (Threats)

Οι απειλές αναφέρονται σε πιθανές κακόβουλες ενέργειες ή συμπεριφορές που μπορούν να προκαλέσουν ζημιά στα πληροφοριακά συστήματα, τα δεδομένα ή τις υπηρεσίες.

Ευπάθεια (Vulnerability)

Η ευπάθεια αναφέρεται σε μια αδυναμία ή έλλειψη ασφάλειας σε ένα πληροφοριακό σύστημα που μπορούν να εκμεταλλευθούν οι επιτιθέμενοι.

Επικοινωνία Κυβερνοασφάλειας

Η επικοινωνία κυβερνοασφάλειας αναφέρεται στη διασφάλιση της αποτελεσματικής επικοινωνίας μεταξύ των εμπλεκόμενων φορέων σχετικά με τα θέματα ασφάλειας.

Επίθεση (Attack)

Μια επίθεση αναφέρεται στην προσπάθεια αξιοποίησης ευπαθειών ή αδυναμιών σε ένα πληροφοριακό σύστημα με σκοπό την πρόκληση ζημιάς ή την απόκτηση παράνομης πρόσβασης.

Πολιτική Κυβερνοασφάλειας

Η πολιτική κυβερνοασφάλειας περιλαμβάνει τους κανόνες, τις διαδικασίες και τις πρακτικές που εφαρμόζονται για τη διασφάλιση της ασφάλειας στον ψηφιακό χώρο.

Συνεχόμενη Ασφάλεια (Continuous Security)

Η συνεχόμενη ασφάλεια αναφέρεται στην πρακτική συνεχούς παρακολούθησης ανάλυσης και βελτίωσης των μέτρων ασφάλειας για αντιμετώπιση σύγχρονων απειλών.



Ιστορία και εξέλιξη της κυβερνοασφάλειας (I)

Διανύοντας, πλέον, την εποχή της ψηφιοποίησης, ολοένα και περισσότεροι τομείς της σύγχρονης κοινωνίας λειτουργούν βάσει ψηφιακών τεχνολογιών. Παρόλο που τομείς όπως, η οικονομία, η υγεία και οι μεταφορές έχουν ευνοηθεί από τη ψηφιοποίηση, δεν παύουν να είναι εκτεθειμένοι σε κυβερνοαπειλές.

- ❖ Η εξέλιξη παρατηρείται από το 2004 και έπειτα. Τότε, ιδρύθηκε ο Οργανισμός της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών (**ENISA**), σύμφωνα με τον Κανονισμό 460/2004
- ❖ **Σκοπός** του Οργανισμού ήταν η ανάπτυξη των εθνικών στρατηγικών κυβερνοασφάλειας, καθώς και η παροχή συμβουλευτικής και λύσεων, προκειμένου τα κράτη να βελτιώσουν τις δυνατότητές τους στον τομέα αυτό, αλλά και η εφαρμογή της Πολιτικής και του Νομικού πλαισίου της Ε.Ε σε θέματα ασφάλειας δικτύου και πληροφοριών
- ❖ Οι διαφοροποιήσεις που υπάρχουν μεταξύ των κρατών-μελών, αναφορικά με τις δυνατότητές τους να διαχειριστούν συντονισμένα περιστατικά διασυνοριακών κυβερνοεπιθέσεων, οδήγησαν στη **θέσπιση ενός πλάνου έκτακτης ανάγκης**, που να περιορίζει τις επικείμενες απειλές, ή μιας ομάδας αντιμετώπισης έκτακτων αναγκών (**CERT**). Η CERT απαρτίζεται από εμπειρογνώμονες σε θέματα ψηφιακών υποδομών και υφίσταται τόσο σε επίπεδο ΕΕ, όσο και σε επίπεδο κρατών-μελών
- ❖ Σημείο καμπής για τη δράση της ΕΕ στην κυβερνοασφάλεια ήταν η έκδοση της Οδηγίας 2016/1148 σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την **Ένωση** (NIS Directive), η οποία τέθηκε σε ισχύ το 2016, και συνέβαλε στην επίτευξη ενός κοινού υψηλού επιπέδου ασφάλειας των συστημάτων δικτύου και πληροφοριών σε ολόκληρη την ΕΕ

IS1



IS1 Την Ευρωπαϊκή ένωση εννοούμε
Info Sthev; 2024-03-15T12:41:36.134

Ιστορία και εξέλιξη της κυβερνοασφάλειας (ι)

- ❖ Ωστόσο, **το ίδιο έτος**, τέθηκε σε ισχύ και ο **Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)**, που αντιπροσωπεύει ένα εναρμονισμένο νομικό πλαίσιο για την προστασία των προσωπικών και ιδιωτικών δεδομένων των πολιτών της ΕΕ.
- ❖ Επιπλέον, προτάθηκε η ενίσχυση της εργαλειοθήκης της Ε.Ε για τη διπλωματία στον κυβερνοχώρο, με σκοπό την αποτελεσματική πρόληψη και αντιμετώπιση κακόβουλων δραστηριοτήτων σε αυτόν, ιδίως εκείνων που επηρεάζουν τις υποδομές καίριας σημασίας και τις αξίες της ΕΕ. Μάλιστα, η **Ένωση** σκοπεύει στην ενίσχυση της συνεργασίας και των ικανοτήτων στον τομέα της κυβερνοάμυνας, αξιοποιώντας το έργο του Ευρωπαϊκού Οργανισμού Άμυνας και ενθαρρύνοντας τα κράτη-μέλη να αξιοποιήσουν πλήρως τη μόνιμη διαρθρωμένη συνεργασία τους, όπως και το Ευρωπαϊκό Ταμείο Άμυνας.
- ❖ Τέλος, η **κυβερνοασφάλεια** αποτελεί **προτεραιότητα** που αντικατοπτρίζεται και στον επόμενο μακροπρόθεσμο προϋπολογισμό της Ε.Ε (**2021-2027**), με την ίδια να προσπαθεί να διαδραματίσει ουσιαστικό ρόλο στην προώθηση ενός παγκόσμιου, ανοικτού, σταθερού και ασφαλούς κυβερνοχώρου, βασιζόμενη τόσο στις θεμελιώδεις αξίες της Ε.Ε όσο και στο κράτος δικαίου.
- ❖ Κάποιες από τις δράσεις της μπορεί να λαμβάνουν αρνητικό πρόσημο, χρειάζεται, ωστόσο, να ληφθεί υπόψη ότι η πρόοδος σε έναν τομέα όπως η κυβερνοασφάλεια απαιτεί χρόνο για να αποφέρει τα επιθυμητά αποτελέσματα, ιδιαίτερα εντός ενός πλαισίου στο οποίο χρειάζεται να γίνουν αρκετοί συμβιβασμοί μεταξύ των συμμετεχόντων.

Η εξέλιξη των κυβερνοεπιθέσεων

Η κυβερνοασφάλεια γεννήθηκε όταν οι πρώτοι υπολογιστές μπόρεσαν να δικτυωθούν και να μεταφέρουν πληροφορίες μεταξύ τους. Αυτό δε συνέβη μέχρι τη δεκαετία του 1950 δηλαδή όταν αναπτύχθηκαν τα πρώτα δίκτυα υπολογιστών και μόντεμ. Μόλις τη δεκαετία του **1960**, η **κυβερνοασφάλεια άρχισε να παίρνει τη μορφή**, με την οποία είναι γνωστή σήμερα. Η δημιουργία του διαδικτύου ήρθε το 1969, όταν η Υπηρεσία Προηγμένων Ερευνητικών Προγραμμάτων του Πενταγώνου (ARPA) κατάφερε να στείλει ένα μήνυμα από το Πανεπιστήμιο της Καλιφόρνιας στο Ερευνητικό Κέντρο του Στάνφορντ.

Η έλευση του κακόβουλου λογισμικού

Η ιδέα της κυβερνοασφάλειας θα ξεκινούσε εκείνη τη στιγμή και το πρόγραμμα που ανέπτυξε ο Ray Tomlinson θα θεωρούνταν το πρώτο antivirus. Τη δεκαετία του 1980 παρατηρήθηκε έκρηξη κακόβουλων προγραμμάτων, τα οποία πολλαπλασιάστηκαν με γεωμετρική πρόοδο. Ως απάντηση, το 1987 ο John McAfee ίδρυσε την McAfee και λάνσαρε το λογισμικό Virus Scan, σηματοδοτώντας την εμπορική ύπαρξη των antivirus.



Μην ξεχνάμε το WannaCry

Στις αρχές της δεκαετίας του 2000, οι επιθέσεις ransomware άρχισαν να εμφανίζονται σε όλο και πιο εξελιγμένη μορφή. Ήταν το 2017 όταν σημειώθηκε η κυβερνοεπίθεση γνωστή ως WannaCry: μια κρατικά χρηματοδοτούμενη επίθεση που εξαπλώθηκε διεθνώς. Σήμερα αποτελεί σημαντικό κίνδυνο λόγω των ολοένα και πιο εξελιγμένων μεθόδων που χρησιμοποιεί και των συνεπαγόμενων ζημιών και σοβαρών οικονομικών απωλειών που συνεπάγεται.



Το πραγματικό Y2K: Loveletter

Η νέα χιλιετία ξεκίνησε με τον φόβο που δημιούργησε το πρόβλημα Y2K: ότι τα υπολογιστικά συστήματα ήταν ελαττωματικά επειδή οι ημερομηνίες στα προγράμματα παρέλειπαν την εκατονταετηρίδα. Φοβούνταν ότι με την αλλαγή της χιλιετίας όλες οι ημερομηνίες θα ήταν λάθος και αυτό θα οδηγούσε σε αποτυχίες και σοβαρές ζημιές σε όλες τις χώρες. Αυτό επρόκειτο να αλλάξει με τον περιβόητο ιό Loveletter phishing, ο οποίος θα εξαπλωνόταν μέσα σε μόλις πέντε ώρες σε υπολογιστές στην Ασία, την Ευρώπη και την Αμερική.

Το μέλλον της τεχνητής νοημοσύνης είναι εδώ

- ❖ Τα τελευταία χρόνια παρατηρήθηκε αύξηση της πολυπλοκότητας των επιθέσεων στον κυβερνοχώρο και των επιθέσεων ransomware, με νέα μέσα φορέων επίθεσης να αυξάνονται, από τις επιθέσεις στην αλυσίδα εφοδιασμού έως την τεχνητή νοημοσύνη. Δυστυχώς, όλοι οι ειδικοί του κλάδου προβλέπουν την αναπόφευκτη αύξηση των κυβερνοεπιθέσεων και των νέων μέσων phishing σε όλο τον κόσμο, με τις διασυνδεδεμένες επιχειρήσεις και την κοινωνία μας.
- ❖ Όσον αφορά την Ελλάδα ένας οργανισμός δέχεται επίθεση κατά μέσο όρο 871 φορές την εβδομάδα τους τελευταίους 6 μήνες, με κορυφαίο κακόβουλο λογισμικό να είναι το Emotet.
- ❖ Η τεχνητή νοημοσύνη σηματοδοτεί ένα σημείο καμπής στην εξέλιξη των κυβερνοεπιθέσεων, καθώς αυτού του είδους η τεχνολογία επιτρέπει στις απειλές να είναι πιο συχνές, ταχύτερες και πιο αποτελεσματικές. Τεχνικές όπως το deepfake καταφέρνουν να υποδύονται αξιόπιστα σχετικές ταυτότητες και εταιρείες για την κλοπή πληροφοριών, οι επιθέσεις phishing γίνονται όλο και πιο πειστικές, και νέες παραλλαγές ransomware και κακόβουλου λογισμικού αναπτύσσονται ταχύτατα και είναι οικονομικά πιο αποδοτικές. Καθώς οι τεχνικές των κυβερνοεγκλημάτων εξελίσσονται με ταχείς ρυθμούς, η ασφάλεια στον κυβερνοχώρο χρησιμοποιεί επίσης την τεχνητή νοημοσύνη για να βελτιώσει τις αμυντικές μεθόδους της, ώστε να συμβαδίζει.

Πως αντιμετωπίζεται η κυβερνοασφάλεια σήμερα (ι)

- ❖ Από τα πλέον νευραλγικά κομμάτια του ψηφιακού μετασχηματισμού των χρηματοοικονομικών υπηρεσιών η αντιμετώπιση των διαδικτυακών απειλών χρειάζεται ιδιαίτερη προσοχή, ενώ είναι πολλές και σημαντικές οι προδιαγραφές που πρέπει να τηρούνται, για την πρόληψη κινδύνων.
- ❖ Η πανδημία έφερε μεγάλες ανατροπές, εξαναγκάζοντάς μας να περάσουμε από τον offline στον online κόσμο πάμπολλες δραστηριότητες. Η βίαιη, λόγω της COVID-19, επιτάχυνση του ψηφιακού μετασχηματισμού είχε τα καλά της, αλλά βέβαια είχε (κι έχει ακόμα) τους κινδύνους της. Ένας από τους μεγαλύτερους, που ίσως ακόμα να μην έχουμε δει σε πλήρη ανάπτυξη, αλλά η πρόγνωση που πήραμε ως τώρα προμηνύει πολλά, είναι σίγουρα η κυβερνοασφάλεια, ειδικά στον χώρο της οικονομίας.
- ❖ Με δεδομένο, μάλιστα, ότι το 2020 αποδείχθηκε η χειρότερη χρονιά στην ιστορία, όσον αφορά στις παραβιάσεις δεδομένων, μάλλον δικαιολογούνται οι ειδήμονες του κλάδου να υποστηρίζουν πως **«η κυβερνοασφάλεια είναι σήμερα το πιο σημαντικό πρόβλημα στην ψηφιακή οικονομία»**.
- ❖ Οι κίνδυνοι караδοκούν και είναι πολλοί. Το τοπίο σε θέματα αντιμετώριων στον χώρο της κυβερνοασφάλειας μένει κατά πολύ το ίδιο. Σε πολύ μεγαλύτερο βαθμό αυξάνουν οι χρήστες, όπως προείπαμε, με την απειρία να τους οδηγεί συχνά σε αβίαστα συμπεριφορικά σφάλματα που διευκολύνουν τις παραβιάσεις δεδομένων.
- ❖ Οι απανταχού κυβερνήσεις πρέπει να επιμείνουν στη δίκαιη κατανομή και την προστασία των πολιτών και των δεδομένων τους, κάτι που ήδη γίνεται σε κάποιες χώρες (πχ. Κίνα, Ινδία, Φινλανδία κ.ά). Ο μεν ιδιωτικός τομέας θα πρέπει να αφεθεί ελεύθερος να αναλάβει επιχειρηματικές πρωτοβουλίες, όμως, και οι κυβερνήσεις από την πλευρά τους θα πρέπει να διασφαλίσουν οφέλη για όλους και να διαχειριστούν τους κινδύνους.

IS1

IS1

Αυξάνουν ή αυξάνονται??

Info Sthev; 2024-03-15T12:55:37.207

Πως αντιμετωπίζεται η κυβερνοασφάλεια σήμερα (II)

Πολλά χρηματοπιστωτικά ιδρύματα εφαρμόζουν λύσεις και τεχνολογίες **FinTech** για την ανάπτυξη και τη βελτίωση των υπηρεσιών τους που αφορούν σε πληρωμές, δάνεια, ασφάλιση, αποταμιεύσεις και επενδύσεις, κι έτσι οι καταναλωτές έχουν πλέον πρόσβαση σε όλο και περισσότερες ηλεκτρονικές συναλλαγές. Ωστόσο, ο ψηφιακός μετασχηματισμός των χρηματοοικονομικών υπηρεσιών εγείρει ολοένα και περισσότερους κινδύνους κυβερνοεπιθέσεων.

- Κύριο μέλημα του χρηματοπιστωτικού τομέα θα πρέπει να αποτελεί η προστασία των προσωπικών δεδομένων και της ιδιωτικότητας των καταναλωτών, καθώς και η ασφάλεια των ηλεκτρονικών συναλλαγών.
- Επιβάλλεται, επομένως, η ανάπτυξη και λειτουργία ψηφιακών συστημάτων παροχής χρηματοπιστωτικών υπηρεσιών με έμφαση στην ασφάλεια, καθώς και η εφαρμογή αυστηρού νομικού πλαισίου που θα θέτει σημαντικές εγγυήσεις ασφάλειας, ώστε να εξασφαλιστεί η εμπιστοσύνη στις ηλεκτρονικές συναλλαγές.
- Η μη συμμόρφωση των εταιρειών με το κανονιστικό πλαίσιο έχει ως συνέπεια υψηλά πρόστιμα και, λόγω αυτού, οι εταιρείες αναζητούν λύσεις, ώστε να μειωθεί αυτός ο κίνδυνος. Ωστόσο, η ραγδαία εξέλιξη της τεχνολογίας και η αύξηση των κυβερνοεπιθέσεων συχνά δημιουργεί κενά στο θεσμικό πλαίσιο και απαιτεί τη συνεχή αναπροσαρμογή του. Η διατήρηση ίσων κανόνων ανταγωνισμού μεταξύ των υφιστάμενων τραπεζών και των νέων εταιρειών FinTech, έτσι ώστε να διατηρείται η οικονομική σταθερότητα, παραμένει μεγάλη πρόκληση. Αυστηρή προτεραιότητα του θεσμικού πλαισίου είναι η προστασία των καταναλωτών, ιδίως όσον αφορά στην ιδιωτικότητα και την ασφάλεια στον κυβερνοχώρο, κι αυτό αποδείχτηκε με τη θέσπιση του κανονισμού GDPR.
- Προς αυτή την κατεύθυνση, κάθε νέα εταιρεία οφείλει να κατανοεί τους κινδύνους στους οποίους εκθέτει τους πελάτες της, καθώς και τους άλλους συμμετέχοντες στο χρηματοπιστωτικό σύστημα και να συμμορφώνεται πλήρως με τους ισχύοντες κανονισμούς.

Σημασία της κυβερνοασφάλειας για τις μικρομεσαίες επιχειρήσεις

- Η περίοδος της πανδημίας επιτάχυνε τη χρήση υπηρεσιών Διαδικτύου και τεχνολογικών εργαλείων από πολλές ΜμΕ, που συμπεριέλαβαν στον τρόπο λειτουργίας τους μεταξύ άλλων χρήση υπηρεσιών cloud, τηλεργασία, αλλά και τη βελτίωση των διαδικτυακών υπηρεσιών τους.
- Ωστόσο, όλες οι ηλεκτρονικές διαδικασίες ενέχουν και υψηλότερο ρίσκο ως προς την ασφάλεια, αν δεν τηρηθούν σωστά όλα τα απαραίτητα μέτρα πρόληψης. 25 εκατομμύρια ΜμΕ δραστηριοποιούνται σήμερα στην Ευρωπαϊκή Ένωση και απασχολούν περισσότερους από 100 εκατομμύρια εργαζόμενους, είναι σημαντικό να δίνεται βαρύτητα σε ζητήματα ασφάλειας. Ένα σοβαρό περιστατικό κυβερνοεπίθεσης μπορεί να θέσει σε κίνδυνο μία επιχείρηση, προκαλώντας σημαντική οικονομική ζημιά ή διαρρέοντας ευαίσθητες πληροφορίες.
- Παρ' όλα αυτά, οι κυβερνοεπιθέσεις εξακολουθούν να μην θεωρούνται σημαντικός κίνδυνος από μεγάλο αριθμό ΜμΕ, καθώς παραμένει η πεποίθηση ότι τα περιστατικά στον κυβερνοχώρο στοχεύουν μόνο μεγαλύτερους οργανισμούς. Η μελέτη αποκαλύπτει ότι οι επιθέσεις phishing είναι από τα πιο κοινά περιστατικά στον κυβερνοχώρο στα οποία είναι πιθανό να εκτεθούν οι ΜμΕ, μαζί με επιθέσεις ransomware, κλεμμένους φορητούς υπολογιστές, αλλά και “απάτες του CEO” (όπου ο απατεώνας στέλνει μηνύματα υποδύομενος υψηλόβαθμο στέλεχος της επιχείρησης).
- Η Ελλάδα έχει δημοσιεύσει από τα τέλη του 2020 την Εθνική Στρατηγική Κυβερνοασφάλειας (2020-2025), η οποία περιλαμβάνει σειρά δράσεων που καλύπτει όλους τους σημαντικούς και κρίσιμους τομείς .



Μορφές κυβερνοεπιθέσεων

❖ Μη καταχωρημένο λογισμικό

Είναι προγράμματα που χρησιμοποιεί στην καθημερινότητά του ένας χρήστης (Java, Adobe Reader κ.α.) και οι εταιρίες στην προσπάθειά τους να καλύπτουν τα κενά ασφαλείας, προχωρούν στην έκδοση νεότερων ενημερώσεων των λογισμικών τους.

❖ Ηλεκτρονικό ψάρεμα (phishing)

Πρόκειται για πλαστή οντότητα που υποδύεται μία αξιόπιστη και αυθεντική όπου σκοπό έχει να αποσπάσει πληροφορίες από τον χρήστη. Η επιτυχία του ηλεκτρονικού ψαρέματος στηρίζεται στην έλλειψη γνώσεων του θύματος, στην έλλειψη προσοχής του θύματος και στην οπτική εξαπάτηση.

❖ Ransomware

Το Ransomware είναι ένας τύπος κακόβουλου λογισμικού που μπορεί να κλειδώσει μια συσκευή ή να κρυπτογραφήσει το περιεχόμενό της, εμποδίζοντας τον χρήστη από την πρόσβαση στα προσωπικά του αρχεία με σκοπό την καταβολή λύτρων.

❖ Σκουλήκια (Network-traveling Worms)

Ένας ιός τύπου σκουληκιού αντιγράφει τον εαυτό του σε άλλους υπολογιστές, προκαλώντας υπερφόρτωση δικτύου ή εγκαθιστώντας επιβλαβές λογισμικό ιού. Αυτοί οι ιοί ενδέχεται να διαγράψουν αρχεία, ή να κλέψουν πολύτιμες πληροφορίες.



Συνέπειες κυβερνοεπιθέσεων

❖ Οικονομικό κόστος των κυβερνοεπιθέσεων

Οι απατεώνες χρησιμοποιούν ιστοσελίδες και email "ψαρέματος" με κακόβουλους συνδέσμους και συνημμένα για να κλέψουν τραπεζικά στοιχεία ή να εκβιάσουν οργανισμούς. Το **2020, το ετήσιο κόστος του κυβερνοεγκλήματος για την παγκόσμια οικονομία έφτασε τα 5,5 τρις ευρώ, ποσό διπλάσιο από εκείνο του 2015**

❖ Επιπτώσεις στη Δημοκρατία

Η ζημιά που προκαλείται από τις κυβερνοεπιθέσεις δεν αφορά μόνο την οικονομία και το χρηματοπιστωτικό σύστημα, αλλά επηρεάζει τα δημοκρατικά θεμέλια της Ε.Ε και απειλεί τις βασικές λειτουργίες της κοινωνίας. Για παράδειγμα, η **παραπληροφόρηση** είναι ένα από τα εργαλεία κυβερνοεπιθέσεων.

❖ Επιπτώσεις στις βασικές υπηρεσίες και στους τομείς καίριας σημασίας

Βασικές υπηρεσίες και τομείς καίριας σημασίας, όπως οι μεταφορές και η υγεία, εξαρτώνται όλο και περισσότερο από τη ψηφιακή τεχνολογία. Η εξάρτηση αυτή, σε συνδυασμό με τη διασύνδεση των υλικών αντικειμένων με το διαδίκτυο των πραγμάτων, μπορεί να έχει άμεσες συνέπειες, καθιστώντας την κυβερνοασφάλεια ζήτημα ζωής και θανάτου. Παράδειγμα αποτελούν οι κυβερνοεπιθέσεις έναντι νοσοκομείων, τα οποία αναγκάστηκαν να αναβάλλουν επείγουσες χειρουργικές επεμβάσεις, ή οι επιθέσεις έναντι δικτύων παροχής ενέργειας και νερού που απειλούν τη λειτουργία υπη

IS1



IS1 Υπερβολική σαν λέξη για παρουσίαση.
Info Sthev; 2024-03-15T13:02:14.377

Ασφαλής χρήση του διαδικτύου

- ❖ Το διαδίκτυο είναι ένας καινούριος κόσμος και για πολλούς πρωτόγνωρος. Προσφέρει διαδραστικότητα, έντονη εναλλαγή εικόνων και συναισθημάτων. Είναι μια εικονική κοινωνία, η οποία διαμορφώνεται παράλληλα με την πραγματικότητα.
- ❖ Η ασφάλεια του σπιτιού μας όμως, στο οποίο βρίσκεται ο υπολογιστής, μπορεί να μας οδηγήσει στο να μην αντιληφθούμε την απειλή καθώς ο κίνδυνος δεν είναι άμεσος και ορατός.
- ❖ Η γνώση των κανόνων ασφάλειας, η ανάπτυξη κριτικής και αντιληπτικής ικανότητας και η ικανότητα αναγνώρισης των κινδύνων είναι βασικά εφόδια για την ασφαλή πλοήγησή στο διαδίκτυο.
- ❖ Τα προσωπικά δεδομένα, όπως το ονοματεπώνυμο, η ηλικία, η κατοικία, το επάγγελμα, η εκπαίδευση, η οικονομική και οικογενειακή κατάσταση κατάσταση, χρησιμοποιούνται σε καθημερινή βάση καθώς περιηγούμαστε στο διαδίκτυο.



Κάποιες χρήσιμες συμβουλές ...

- Για κάθε σημαντικό λογαριασμό σας, φροντίζετε να χρησιμοποιείτε πάντα **μεγάλους και μοναδικούς κωδικούς**, αποτελούμενους από **αριθμούς, γράμματα και σύμβολα**
- **Μην** αποστέλλεται τους κωδικούς σας με email και μην τους μοιράζεστε με τρίτους
- Βάζετε **password recovery options** (επιλογές ανάκτησης κωδικού πρόσβασης) και κρατάτε τα ενημερωμένα
- **Αποφύγετε** οτιδήποτε ύποπτο. Μην απαντάτε σε περίεργα emails και μηνύματα και μη συμπληρώνετε τα στοιχεία σας (προσωπικές πληροφορίες, αριθμούς πιστωτικών καρτών, κωδικούς κ.ο.κ.) σε όλες τις ιστοσελίδες που σου το ζητούν
- Να **αναφέρετε** το παράνομο και καταχρηστικό περιεχόμενο που συναντάτε
- **Ελέγχετε** συχνά τις ρυθμίσεις ασφαλείας και ιδιωτικότητάς σας και καθορίστε πώς και με ποιους θέλετε να μοιράζεστε το περιεχόμενο σας



- Λαμβάνετε υπόψιν τη διαδικτυακή σας εικόνα, σκεπτόμενος πάντα καλά πριν από τη δημοσίευση ντροπιαστικού ή ακατάλληλου περιεχομένου
- Φροντίζετε να **διατηρείτε το λειτουργικό σύστημα** και τον **browser** σας **ενημερωμένα**
- Κατά την εγκατάσταση, **εξασφαλίζετε** πάντοτε ότι οι πηγές σας είναι **αξιόπιστες**
- **Προσέχετε** πού κάνετε sign in
- Αν η διεύθυνση σας **ξεκινά από https://**, τα δεδομένα σας προστατεύονται καλύτερα.
- **Κλειδώστε** πάντα **την οθόνη** του υπολογιστή, του tablet ή του smartphone σου μετά τη χρήση ή επίλεξε να κλειδώνει αυτόματα.



Κυβερνοασφάλεια και ελληνικές επιχειρήσεις

- Το 1/3 των Ελληνικών εταιρειών αναφέρει περιστατικά κυβερνοεπίθεσης ή κυβερνοεγκλήματος ουσιαστικά δείχνοντας την ανάγκη για λήψη μέτρων που θα διασφαλίσουν τη συνέχιση της εύρυθμης λειτουργία τους.
- Σύμφωνα με έρευνα που διενήργησε η Metron Analysis οι επιθέσεις στις ελληνικές εταιρείες αφορούν, κατά κύριο λόγο, παραπλανητικά emails και δευτερευόντως κακόβουλο λογισμικό ή χακάρισμα κοινωνικών δικτύων και emails, ενώ ελάχιστα σχετίζονται με παραβίαση προσωπικών δεδομένων πελατών.
- Στην ίδια έρευνα αναφέρεται ότι σχεδόν 4 στις 10 επιχειρήσεις θεωρούν ότι ήταν πολύ/αρκετά σοβαρή η κυβερνοεπίθεση που δέχθηκαν ενώ, σε κάθε περίπτωση, η αίσθηση κινδύνου παραμένει, καθώς 2 στις 3 επιχειρήσεις θεωρούν ότι είναι πολύ/αρκετά πιθανό να επαναληφθεί στο μέλλον κάποιου είδους κυβερνοεπίθεση.



- Το ψηφιακό έγκλημα δείχνει να απειλεί σημαντικά τις ελληνικές εταιρείες με τον κίνδυνο των κυβερνοεπιθέσεων, να βαίνει κλιμακούμενος στην Ελλάδα, με τη συντριπτική πλειονότητα των επιχειρήσεων να διαπιστώνει ότι οι κίνδυνοι στον κυβερνοχώρο αυξάνονται με την πάροδο του χρόνου.
- Συνολικά, περισσότερες από 8 στις 10 εταιρείες στην Ελλάδα (83%) πιστεύουν ότι το διαδίκτυο εγκυμονεί κινδύνους για τη λειτουργία τους. Μάλιστα, η συντριπτική πλειονότητα (82%) εκφράζει την άποψη ότι οι κίνδυνοι που αντιμετωπίζουν σήμερα είναι αυξημένοι σε σχέση με πέντε χρόνια νωρίτερα. Πάντως, παρόλα αυτά, μόλις 1 στις 5 εταιρείες (21%) έχει απευθυνθεί στη Δίωξη Ηλεκτρονικού Εγκλήματος για θέματα ασφάλειας στο Διαδίκτυο.
- Προκειμένου να αποφύγουν παρόμοιους κινδύνους οι εταιρείες έχουν αρχίσει να «θωρακίζονται» με συστήματα κυβερνοασφάλειας ενώ ακόμα μεγαλύτερη κινητικότητα παρατηρείται στο ελληνικό δημόσιο και τους δημόσιους οργανισμούς που έχουν πληγεί σημαντικά από περιστατικά κυβερνοεπιθέσεων.



Νόμος για την κυβερνοασφάλεια

- Το Υπουργείο Ψηφιακής Διακυβέρνησης συνέταξε **νόμο** με τίτλο «Εθνική Αρχή Κυβερνοασφάλειας και λοιπές διατάξεις», το οποίο προβλέπει τη σύσταση Νομικού Προσώπου Δημοσίου Δικαίου με την επωνυμία «Εθνική Αρχή Κυβερνοασφάλειας».
- Βασικός **στόχος** της νέας «Εθνικής Αρχής Κυβερνοασφάλειας» θα είναι ο συντονισμός και η υλοποίηση της Εθνικής Στρατηγικής για την Κυβερνοασφάλεια, καθώς και η αποτελεσματική πρόληψη και διαχείριση κυβερνοεπιθέσεων στην Ελλάδα, ώστε να επιτευχθεί ένα υψηλό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών στον δημόσιο και στον ιδιωτικό τομέα.



LET'S PLAY





mecys.eu



Co-funded by
the European Union