e-επιχειρηματικότητα και ασφάλεια

Γιάννης Σταματίου, Καθηγητής, Τμήμα Διοίκησης Επιχειρήσεων, Πανεπιστήμιο Πατρών

Σκοπός

Οι εξελίξεις των τελευταίων ετών στον τομέα των νέων τεχνολογιών έχουν δημιουργήσει ένα νέο ψηφιακό τοπίο επιχειρηματικών ευκαιριών και έχουν αναδείξει την ψηφιακή οικονομία (FinTech) ως κύριο πυλώνα ανάπτυξης και ευημερίας στην παγκόσμια Κοινωνία του Διαδικτύου. Είμαστε μάρτυρες μιας ταχύτατης μετάβασης από το Διαδίκτυο στο Διαδίκτυο των Πραγμάτων, από τον Παγκόσμιο Ιστό στο Web 3.0, δηλαδή την παγκόσμια γνώση κατάλληλα δομημένη για επεξεργασία από τους υπολογιστές, την απότομη εμφάνιση της Τεχνητής Νοημοσύνης στη ζωή μας, καθώς και την μετάβαση από τις καθιερωμένες υπολογιστικές υποδομές και αρχιτεκτονικές σε πιο ευέλικτες και αποδοτικές, όπως είναι το Edge Computing. Όπως είναι αναμενόμενο, όμως, κάθε τεχνολογικό επίτευγμα έχει δύο πλευρές, την πλευρά των ευκαιριών αλλά και την σκοτεινή πλευρά των κινδύνων. Και όλες οι τεχνολογίες που αναφέραμε έχουν και τις δύο πλευρές.

Στόχος της παρούσας ενότητας είναι να αναδείξει τους κινδύνους των νέων τεχνολογιών, είτε αυτές είναι ήδη καθιερωμένες είτε αναδυόμενες, καθώς και να προτείνει καλές πρακτικές αντιμετώπισης των κινδύνων αυτών. Απώτερος στόχος είναι με την υιοθέτηση των πρακτικών αυτών οι επιχειρήσεις, οι οργανισμοί αλλά και όλοι οι άνθρωποι ως χρήστες των νέων τεχνολογιών να μπορέσουν να ανταπεξέλθουν στους κινδύνους που εγκυμονεί ο κυβερνοχώρος και να χρησιμοποιήσουν τα αγαθά τους για οικονομική ανάπτυξη και ευημερία της κοινωνίας.

Προσδοκώμενα Αποτελέσματα

Μέσα από την ενασχόληση με την ενότητα αυτή, αναμένεται μία πρώτη επαφή με τα προβλήματα που δημιουργούν στους οργανισμούς και τις επιχειρήσεις οι κυβερνοεπιθέσεις καθώς και με τις βασικές στρατηγικές κυβερνοάμυνας.

Έννοιες κλειδιά

Κυβερνοεπίθεση, κυβερνοάμυνα, ψηφιακός μετασχηματισμός, κρυπτογραφία, στρατηγική κυβερνοάμυνας

Εισαγωγικές Παρατηρήσεις

Η σύντομη αυτή εισαγωγή στην κυβερνοασφάλεια αποτελείται από το παρόν κείμενο αλλά και το συνοδευτικό αρχείο παρουσίασης. Η προσπάθειά μας δεν αποσκοπεί, φυσικά, στην σε βάθος κάλυψη των θεμάτων που άπτονται του θέματος αυτού, καθώς ο διαθέσιμος χρόνος για την παρουσίαση του υλικού είναι περιορισμένος, αλλά στην παρουσίαση κάποιων βασικών στοιχείων που θα δημιουργήσουν το ενδιαφέρον για περαιτέρω διερεύνηση από

τους εκπαιδευόμενους. Ο σκοπός μας είναι να δώσουμε το έναυσμα για ανάπτυξη εγρήγορσης και συνείδησης του κινδύνου στον κυβερνοχώρο έτσι ώστε να προστατευτεί η επιχειρηματικότητα και η ανάπτυξη από τις κυβερνοαπειλές. Στο τέλος του παρόντος κειμένου παραθέτουμε δύο δραστηριότητες και ασκήσεις αυτοαξιολόγησης πολλαπλών επιλογών με τις οποίες μπορεί ο εκπαιδευόμενος να εξασκηθεί σε πρακτικά ζητήματα ασφάλειας πληροφοριακών συστημάτων και να ελέγξει την πρόοδό του όσον αφορά τα σημεία που θίγονται στο κείμενο. Είμαστε, φυσικά, στη διάθεση των εκπαιδευόμενων για οποιαδήποτε επιπρόσθετη πληροφορία ή βοήθεια περαιτέρω ενασχόλησης με το πολύ ενδιαφέρον και επίκαιρο θέμα της κυβερνοασσφάλειας, ειδικά όσον αφορά την ανάπτυξη της επιχειρηματικότητας και της ψηφιακής οικονομίας.

Ψηφιακός Μετασχηματισμός και Νέες Τεχνολογίες: ευκαιρίες και κίνδυνοι

Ο ψηφιακός μετασχηματισμός υιοθετεί μια προσέγγιση ανάπτυξης της επιχειρηματικότητας με επίκεντρο τον *πελάτη* και θεμελιωμένη στις Τεχνολογίες Πληροφορικής και Επικοινωνιών (ΤΠΕ). Ο ψηφιακός μετασχηματισμός εκτείνεται σε όλες τις πτυχές μιας επιχείρησης, από τα επιχειρηματικά της μοντέλα, τις εμπειρίες των πελατών της καθώς, επίσης, τις καθημερινές διαδικασίες και λειτουργίες της.

Ο ψηφιακός μετασχηματισμός χρησιμοποιεί τεχνικές από την τεχνητή νοημοσύνη, τον αυτοματισμό διεργασιών, τεχνολογικά συστήματα και υπηρεσίες νέφους καθώς και άλλες καθιερωμένες αλλά και αναδυόμενες νέες τεχνολογίες. Στόχος είναι να μπορέσει η επιχείρηση να αξιοποιήσει μεγάλους όγκους δεδομένων και να αναπτύξει έξυπνες ροές εργασιών, ταχύτερη και πιο ευφυή διαδικασία λήψης αποφάσεων και απόκριση, σε πραγματικό χρόνο, στις εξελίξεις και απαιτήσεις της αγοράς.

Πίσω από κάθε ψηφιακό μετασχηματισμό βρίσκονται τα *Πληροφοριακά Συστήματα*, τα οποία υποστηρίζουν όλες της φάσεις της διαδικασίας αυτής. Ένα πληροφοριακό σύστημα είναι μία οργανωμένη συλλογή τεχνολογιών και είναι υπεύθυνο για τη συλλογή, οργάνωση, επεξεργασία, αποθήκευση και διαβίβαση πληροφοριών. Υπάρχουν πολλοί και διάφοροι τύποι πληροφοριακών συστημάτων, όπως για παράδειγμα: συστήματα επεξεργασίας συναλλαγών, συστήματα υποστήριξης αποφάσεων, συστήματα διαχείρισης γνώσης, συστήματα διαχείρισης μάθησης, συστήματα διαχείρισης βάσεων δεδομένων, συστήματα αυτοματισμού κ.λπ. Ζωτικής σημασίας πάντως για τα περισσότερα πληροφοριακά συστήματα αποτελούν οι τεχνολογίες, οι οποίες συνήθως σχεδιάζονται ώστε να εκτελούν καθήκοντα υψηλών υπολογιστικών απαιτήσεων όπως η διαχείριση μεγάλου όγκου πληροφοριών, η εκτέλεση πολύπλοκων υπολογισμών, και ο έλεγχος πολλών και ταυτόχρονων διεργασιών.

Για παράδειγμα, το *Διαδίκτυο των Πραγμάτων* (Internet of Things – IoT), ως μία τεχνολογική εξέλιξη των τελευταίων ετών, περιλαμβάνει ένα πολύ μεγάλο πλήθος συσκευών κι αισθητήρων διασυνδεδέμενων μέσω του Διαδικτύου (Internet), που συλλέγουν δεδομένα από το περιβάλλον λειτουργίας τους και μπορούν να επικοινωνούν μεταξύ τους ή/και με άλλα δικτυοκεντρικά πληροφοριακά συστήματα κι εφαρμογές για την ανάλυση αυτού του τεράστιου όγκου δεδομένων. Χαρακτηριστικό παράδειγμα αυτής της περιγραφής είναι οι έξυπνες οικιακές συσκευές ή τα αυτόνομα οχήματα τα οποία προσφέρουν νέες ευκαιρίες για ανάπτυξη επιχειρηματικών ιδεών και σύγχρονων υπηρεσιών. Η ανάπτυξη του IoT προσφέρει πολλά πλεονεκτήματα και διευκολύνσεις στην καθημερινή ζωή χάρη στη δυνατότητα να ελέγχει σχεδόν τα πάντα από απόσταση

Γενικά, η σύγχρονη παγκόσμια οικονομία βασίζεται, σε μεγάλο βαθμό, στις εξελίξεις που λαμβάνουν χώρα στις σύγχρονες τεχνολογίες, οι οποίες με όλο και μικρότερο κόστος για την επιχείρηση ή τον οργανισμό, παρέχουν όλο και περισσότερες δυνατότητες για οικονομική ανάπτυξη και επιχειρηματικότητα. Ο όρος *Fintech* (Financial Technology) περιγράφει αυτήν, ακριβώς, την εξέλιξη και, σήμερα, αναφέρεται στης κύριες και αναδυόμενες τεχνολογίες που συνεισφέρουν στην παγκόσμια οικονομική ανάπτυξη.

Πιο κάτω, αναφέρονται[1] μερικές κύριες και αναδυόμενες τεχνολογίες Fintech που ήδη συμμετέχουν στην οικονομική ανάπτυξη σε μεγάλο βαθμό ή αναμένεται να διαδραματίσουν κεντρικό ρόλο στο άμεσο μέλλον.

1. Blockchain
2. Artificial Intelligence
3. The voice Technology
4. Regulation Technology
5. Robotic Process Automation
6. Internet of Things
7. The Cloud-based Approach
8. Payment Services Directive 2.0
9. Initial Public Offerings
10. Biometric Technology
11. Simplifying procedures
12. Digital banks

Όμως είναι απαραίτητο να επικεντρώσουμε το ενδιαφέρον μας και στους κινδύνους που ανακύπτουν ως αποτέλεσμα της ευρείας χρήσης των νέων τεχνολογιών όταν δεν λαμβάνονται τα κατάλληλα μέτρα διασφάλισης των συστημάτων που τις υλοποιούν. Για παράδειγμα, παρατηρούνται συνεχώς πολλά ζητήματα ασφάλειας σε συστήματα που χρησιμοποιούν συσκευές του Internet of Things, οι οποίες και αποτελούν (λόγω των περιορισμένων υπολογιστικών δυνατοτήτων τους) συχνά τον αδύναμο κρίκο στα συστήματα αυτά. Πολλές κυβερνοεπιθέσεις στοχεύουν, ακριβώς, τις συσκευές αυτές με στόχο να αποκτήσουν τον έλεγχό τους και στη συνέχεια να εξαπολύσουν, από αυτές, πιο ισχυρές επιθέσεις και σε πιο κρίσιμα υπολογιστικά συστήματα. Αντίστοιχοι κίνδυνοι υπάρχουν για κάθε τεχνολογική εξέλιξη, όπως αυτές που αναφέρθηκαν πιο πάνω.

Κατά συνέπεια, για να μπορέσουν οι οργανισμοί και οι επιχειρήσεις να αναπτυχθούν σε έναν συνεχώς εξελισσόμενο ψηφιακό κόσμο, είναι αναγκαίο να εφοδιαστούν με εργαλεία κυβερνοάμυνας και μία προσεκτικά σχεδιασμένη στρατηγική κυβερνοασφάλειας έτσι ώστε να είναι έτοιμοι να αντιμετωπίσουν το ψηφιακό έγκλημα. Και καθώς η τεχνολογία εξελίσσεται, εισάγονται και νέα είδη απειλών στον κυβερνοχώρο, ενισχύοντας τις ήδη υπάρχουσες απειλές.

Γενικά, η κοινωνία, η οικονομία και οι κρίσιμες υποδομές μας εξαρτώνται, πια, σε μεγάλο βαθμό από δίκτυα υπολογιστών και τεχνολογικές λύσεις. Οι επιθέσεις στον κυβερνοχώρο γίνονται πιο ελκυστικές και, δυνητικά, πιο καταστροφικές καθώς αυξάνεται η εξάρτηση από τις νέες τεχνολογίες. Τα θύματα των κυβερνοεπιθέσεων αυξάνονται επίσης σημαντικά και συμπεριλαμβάνουν επιχειρήσεις, οργανισμούς αλλά και φυσικά πρόσωπα. Και όσο η εξάρτηση κοινωνίας και οικονομίας αυξάνεται, τόσο θα αυξάνεται η συχνότητα, η ένταση και οι επιπτώσεις του κυβερνοεγκλήματος.

[1] https://www.linkedin.com/pulse/top-5-trends-fintech-2022-cut-kashish-pahwa/

Βασικές απαιτήσεις ασφάλειας Πληροφοριακών Συστημάτων

Ιστορικά, η ασφάλεια των πληροφοριακών συστημάτων διερευνήθηκε στις αρχές της δεκαετίας τους 1970 από στρατιωτικούς οργανισμούς στα πλαίσια της απομακρυσμένης προσπέλασης πληροφοριακών συστημάτων χωρίς τη φυσική παρουσία των χρηστών των συστημάτων στους χώρους στους οποίους ήταν εγκατεστημένα. Από τις σχετικές μελέτες προέκυψαν διάφορες καινοτόμες (για εκείνη την εποχή) ιδέες οι οποίες αποτελούν μέχρι και σήμερα θεμελιώδεις προσεγγίσεις στην κατάρτιση και εφαρμογή πολιτικών ασφαλείας. Μία τέτοια ιδέα ήταν η εύρεση της κατάλληλης ισορροπίας μεταξύ της αυστηρότητας προστασίας των πληροφορίων και της διευκόλυνσης του χρήστη στην εργασία του. Επίσης, εκείνη τη δεκαετία εμφανίστηκε και το πρώτο κακόβουλο λογισμικό, με μορφή ιού (virus), με την ονομασία Creeper στο στρατιωτικό δίκτυο υπολογιστικών συστημάτων ARPANET.

Σήμερα, κατά το σχεδιασμό ασφαλών πολιτικών διαχείρισης των πληροφοριακών συστημάτων και νέων τεχνολογιών, γενικότερα, ενσωματώνονται διαδικασίες όχι μόνο τεχνικής φύσης αλλά και διοικητικές οι οποίες και θα πρέπει να συμβαδίζουν, κάθε φορά, με τις τρέχουσες ηθικές και κοινωνικές αντιλήψεις καθώς και τις επιταγές της νομοθεσίας, εθνικής και ευρωπαϊκής. Οι πολιτικές αυτές έχουν μοναδικό στόχο την προφύλαξη των πληροφοριακών συστημάτων ενός οργανισμού από κάθε στοχευμένη κυβερνοαπειλή.

Βασικός άξονας κάθε πολιτικής ασφάλειας είναι ο εντοπισμός και η κατηγοριοποίηση των πληροφοριών καθώς και των πόρων του υπολογιστικού συστήματος και του οργανισμού ανάλογα με την κρισιμότητά τους και τον κίνδυνο στον οποίο εκτίθενται. Η πολιτική ασφάλειας πρέπει, επίσης, να λαμβάνει υπόψιν όλους τους εμπλεκόμενους στη χρήση και τη λειτουργία ενός πληροφοριακού συστήματος. Οι εμπλεκόμενοι είναι, συνήθως, οι χρήστες και διαχειριστές, τα διευθυντικά στελέχη και οι πελάτες του οργανισμού.

Οι βασικές απαιτήσεις ασφάλειας που πρέπει να διατυπώνονται με σαφήνεια σε μία πολιτική ασφάλειας ενός οργανισμού και να ικανοποιούνται από κάθε πληροφοριακό σύστημά του είναι οι εξής:

- Ακεραιότητα (Integrity): Είναι πολύ σημαντικό τα δεδομένα του πληροφοριακού συστήματος να διατηρούνται σε μία γνωστή και έγκυρη κατάσταση χωρίς να υποστούν οποιουδήποτε είδους τροποποίηση, αφαίρεση ή προσθήκη από άτομα εντός και εκτός του οργανισμού που δεν έχουν την αντίστοιχη εξουσιοδότηση. Κατά συνέπεια, θα πρέπει να αποτρέπεται αυστηρά η πρόσβαση στα δεδομένα του πληροφοριακού συστήματος από μη εξουσιοδοτημένα άτομα.

- Διαθεσιμότητα (Availability): Τα δεδομένα, τα πληροφοριακά υποσυστήματα, τα δίκτυα και οι υπολογιστικοί πόροι ενός οργανισμού θα πρέπει να είναι στη διάθεση των χρηστών τους ανά πάσα στιγμή και για οσοδήποτε χρονικό διάστημα απαιτείται. Οι πιο συχνές περιπτώσεις μη διαθεσιμότητας των πόρων ενός πληροφοριακού συστήματος ανακύπτουν μετά από επιτυχημένες επιθέσεις DDoS (Distributed Denial of Service). Τέτοιες επιθέσεις έχουν στόχο την υπερφόρτωση των υπολογιστικών συστημάτων ενός οργανισμού από τους επιτιθέμενους με στόχο να τεθούν εκτός λειτουργίας διάφορες υπηρεσίες ενός οργανισμού προς τους χρήστες.

- Εμπιστευτικότητα (Confidentiality): Κάθε πληροφορία που είναι αποθηκευμένη σε ένα πληροφοριακό σύστημα ή που αποστέλλεται μέσω δικτυακών υποδομών δεν θα πρέπει να αποκαλύπτεται σε μη εξουσιοδοτημένα άτομα. Η εμπιστευτικότητα

επιτυγχάνεται, κυρίως, με χρήση προηγμένων κρυπταλγορίθμων, όπως θα δούμε στη συνέχεια.

- Πιστοποίηση και Αυθεντικότητα (authentication): Εδώ αναφερόμαστε στην πιστοποίηση οντοτήτων (entity authentication ή identification) και την πιστοποίηση δεδομένων (data authentication). Στην πρώτη περίπτωση διασφαλίζουμε ότι κάθε οντότητα στο πληροφοριακό σύστημα είναι, πραγματικά, αυτή που ισχυρίζεται ότι είναι. Στη δεύτερη περίπτωση διασφαλίζουμε τη εγκυρότητα της θέσης και της χρονικής στιγμής της δημιουργίας των δεδομένων καθώς και την εγκυρότητα των ίδιων των δεδομένων.

- Μη αποποίηση ευθύνης (non-repudiation): Κανένας χρήστης, είτε αυτός είναι αποστολέας είτε παραλήπτης δεδομένων, δεν μπορεί να αποποιηθεί πράξεις που έχει διενεργήσει σε δεδομένα όπως είναι, για παράδειγμα, η δημιουργία των δεδομένων ή κάποιες αλλαγές σε αυτά. Ένας από τους πιο διαδεδομένους αλλά και ταυτόχρονα αποτελεσματικούς τρόπους επίτευξης της μη αποποίησης ευθύνης είναι η χρήση των *ψηφιακών υπογραφών*.

Κυβερνοεπιθέσεις

Στην ετήσια αναφορά της ENISA (European Network and Information Security Agency) του 2022 για τις 15 σημαντικότερες κυβερνοαπειλές[2], βρίσκουμε στην 1η θέση (όπως και σχεδόν όλα τα τελευταία χρόνια) το *κακόβουλο λογισμικό* (malware) με ένα ευρύ φάσμα διαφορετικών εκδοχών του.

Πολλοί ειδικοί στην κυβερνοάμυνας επιβεβαιώνουν τα ευρήματα της ENISA ότι το κακόβουλο λογισμικό (malware) είναι ο πιο συχνά χρησιμοποιούμενος τρόπος παραβίασης της ασφάλειας ενός πληροφοριακού συστήματος και, κατά συνέπεια, η πιο σημαντική απειλή. Το κακόβουλο λογισμικό, ως έννοια, αναφέρεται σε μια ευρεία κατηγορία λογισμικών επίθεσης που μεταφορτώνονται σε ένα υπολογιστικό σύστημα, κατά κανόνα χωρίς τη γνώση του νόμιμου χρήστη του συστήματος, έτσι ώστε να θέσουν σε κίνδυνο το σύστημα προς όφελος του επιτιθέμενου. Παραδείγματα κακόβουλου λογισμικού αποτελούν οι Ιοί (Virus), τα Σκουλήκια (worm), οι Δούρειοι Ίπποι (Trojans), το Κατασκοπευτικό Λογισμικό (Spyware) και το Κακόβουλο Λογισμικό που ζητά Λύτρα για την «απελευθέρωση» ενός υπολογιστικού συστήματος (Ransomware).

Το κακόβουλο λογισμικό μολύνει τα συστήματα με διάφορους τρόπους όπως, για παράδειγμα, εξαπατώντας τους χρήστες έτσι ώστε να ανοίξουν μολυσμένα αρχεία συνημμένα σε μηνύματα ηλεκτρονικού ταχυδρομείου ή δελεάζοντάς τους να επισκεφθούν ιστότοπους διάδοσης κακόβουλου λογισμικού. Επίσης, το κακόβουλο λογισμικό μπορεί να φορτωθεί σε μια μονάδα USB που έχει εισαχθεί σε μια μολυσμένη συσκευή και στη συνέχεια να μολύνει κάθε άλλο σύστημα στο οποίο, στη συνέχεια, εισάγεται αυτή η συσκευή.

Άλλες συχνά εμφανιζόμενες κυβερνοεπιθέσεις είναι και οι εξής:

Επιθέσεις από το διαδίκτυο (web based attacks): Πρόκειται για απειλές που στοχεύουν απευθείας στο χρήστη μέσω εκμετάλλευσης αδυναμιών στους φυλλομετρητές (browsers), καθώς και στα συστήματα διαχείρισης περιεχομένου (content management systems).

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

Κυριότερα είδη επιθέσεων αυτής της κατηγορίας αποτελούν τα browser exploits, drive-by downolads, watering hole attacks κ.α.

Phishing: Κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου ή τηλεφωνικές συνδιαλλαγές, οι οποίες αποσκοπούν στο να παραπλανήσουν τους χρήστες και να αποκαλύψουν εμπιστευτικές πληροφορίες.

Επιθέσεις σε διαδικτυακές εφαρμογές (web application attacks): Επιθέσεις που στοχεύουν σε διαδικτυακές εφαρμογές (web applications). Οι εν λόγω εφαρμογές λόγω της καθολικής χρήσης τους στην προσφορά περιεχομένου αποτελούν στόχο πολλαπλών ειδών επιθέσεων, με κυριότερες τα cross-site scripting (XSS), SQL injection, path traversal, local file inclusion κ.α.

Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου: Αναφερόμενες και ως SPAM, αυτές οι επιθέσεις περιλαμβάνουν την αποστολή ανεπιθύμητης αλληλογραφίας σε χρήστες. Η εν λόγω αλληλογραφία χαρακτηρίζεται από το πολύ μικρό κόστος αποστολής των μηνυμάτων, την ενόχληση που προκαλεί στους χρήστες, αλλά και την εν δυνάμει μετεξέλιξη των μηνυμάτων σε απειλή phishing.

Επιθέσεις άρνησης υπηρεσίας (Denial of Service – DoS attacks): Επιθέσεις κατά τις οποίες μεγάλος όγκος διαδικτυακής κίνησης στοχεύει σε μια υπηρεσία, με σκοπό να καταστεί αδύνατο από τα συστήματα να εξυπηρετήσουν νόμιμα αιτήματα. Ουσιαστικά, εκμεταλλεύονται την πεπερασμένη χωρητικότητα συστημάτων και δικτύων, ώστε να καταστήσουν αδύνατη την παροχή υπηρεσιών (απώλεια διαθεσιμότητας).

Κλοπή ταυτότητας χρήστη (identity theft): Ο επιτιθέμενος αποκτά δεδομένα προσωπικού χαρακτήρα του χρήστη (passwords, social security numbers κ.α.), με αποτέλεσμα την ιδιοποίηση της ταυτότητας του χρήστη (impersonation) και με σκοπό το οικονομικό όφελος (αγορές προϊόντων μέσω πιστωτικών καρτών, παράνομη επιστροφή φόρου κ.λπ.) εις βάρος του.

Παραβιάσεις προσωπικών δεδομένων: Επιθέσεις οι οποίες αποσκοπούν στη διαρροή, αλλοίωση ή μη διαθεσιμότητα προσωπικών δεδομένων. Σύμφωνα με τον Κανονισμό της Ε.Ε. 2016/679, τέτοιου είδους επιθέσεις νοούνται ως παραβιάσεις δεδομένων προσωπικού χαρακτήρα οι οποίες χρήζουν άμεσης αντιμετώπισης.

Εσωτερικές απειλές (insider threat): Απειλές που προέρχονται από στελέχη Φορέων που εργάζονται ή εργάζονταν σε έναν Οργανισμό, καθώς και εξωτερικών συνεργατών, οι οποίοι κατέχουν εσωτερική πληροφόρηση σχετικά με τις πρακτικές ασφάλειας, τα υπολογιστικά συστήματα και τα δεδομένα του Οργανισμού. Οι εν λόγω απειλές μπορούν να οδηγήσουν σε πλήθος επιθέσεων που περιγράφονται στην παρούσα ενότητα, συνήθως με πολύ μεγάλο αντίκτυπο για τον Φορέα και είναι εξαιρετικά δύσκολο να διαγνωσθούν ή/και αντιμετωπισθούν.

Botnets: Δίκτυα τα οποία αποτελούνται από υπολογιστικές συσκευές ανυποψίαστων χρηστών που έχουν μολυνθεί με κακόβουλο λογισμικό και ελέγχονται κεντρικά από κάποιον επιτιθέμενο, προκειμένου να χρησιμοποιηθούν ομαδικά στην αποστολή μηνυμάτων ανεπιθύμητης αλληλογραφίας, σε επιθέσεις άρνησης υπηρεσίας, σε cryptojacking, κλπ.

Φυσικές απειλές: Απειλές που στοχεύουν στην καταστροφή ή αλλοίωση ή κλοπή εξοπλισμού, με απώτερο στόχο την διαρροή ή/και καταστροφή δεδομένων ή την άρνηση υπηρεσίας.

Διαρροή δεδομένων: Διαρροή δεδομένων σε μη εξουσιοδοτημένους χρήστες. Τα δεδομένα μπορεί να περιλαμβάνουν οικονομικά στοιχεία, πατέντες, δεδομένα με κατοχυρωμένα πνευματικά δικαιώματα, πλάνα στρατηγικής ανάπτυξης κλπ.

Λογισμικό λύτρων (ransomware): Κακόβουλο λογισμικό (malware) το οποίο κρυπτογραφεί τα δεδομένα του πληροφοριακού συστήματος, για την αποκρυπτογράφηση των οποίων ο επιτιθέμενος απαιτεί λύτρα (συνήθως σε μορφή κρυπτονομίσματος).

Ηλεκτρονική κατασκοπία: Κατασκοπία μέσω του κυβερνοχώρου, η οποία μπορεί να περιλαμβάνει χρήση εξειδικευμένων εργαλείων για την άντληση στοιχείων ή/και χρήση συνδυασμού των προαναφερθέντων απειλών. Συνήθως αυτή η μορφή επίθεσης αναφέρεται ως «στοχευμένη», λόγω του ότι οι επιτιθέμενοι έχουν πολύ συγκεκριμένους στόχους, με απώτερο στόχο την υποκλοπή ευαίσθητων, για τον οργανισμό, πληροφοριών.

Cryptojacking: Τεχνικές που χρησιμοποιούν την υπολογιστική ισχύ του υπολογιστή του θύματος με σκοπό την εξόρυξη (mining) κρυπτονομισμάτων (κυρίως το bitcoin). Καθώς η εξόρυξη των κρυπτονομισμάτων είναι, ενεργειακά, δαπανηρή διαδικασία, το θύμα επωμίζεται το (συχνά πολύ υψηλό) κόστος της εξόρυξης και το κέρδος αυτής το καρπώνεται ο επιτιθέμενος.

Τεχνικές άμυνας

Ασφάλεια περιμέτρου

Κάποιες προσεγγίσεις που έχουν ως στόχο να μετριαστούν οι επιθέσεις που επιχειρούν να διεισδύσουν σε ένα πληροφοριακό σύστημα διασπείροντας, για παράδειγμα, κακόβουλο λογισμικό, βασίζονται στην επιβολή *περιμετρικής ασφάλειας*. Αντί να προστατεύει κάθε περιουσιακό στοιχείο, η περιμετρική αμυντική στρατηγική έχει χρησιμοποιηθεί κυρίως για να βάλει ένα τείχος (firewall) έξω από όλους τους εσωτερικούς πόρους για να προστατεύσει τα πάντα μέσα από οποιαδήποτε ανεπιθύμητη εισβολή από έξω.

Η εργαλειοθήκη ενός περιμετρικού αμυντικού μηχανισμού συμπεριλαμβάνει λογισμικό τείχους προστασίας (Firewall) για έλεγχο εισερχόμενων και εξερχόμενων αιτημάτων σύνδεσης, εφαρμογές εντοπισμού και απενεργοποίησης κακόβουλου λογισμικού ιούς καθώς και συστήματα ανίχνευσης και αναχαίτισης προσπαθειών εισβολής. Κάθε κίνηση που προέρχεται από έξω παρακολουθείται και εξετάζεται για να διασφαλιστεί ότι δεν υπάρχει κακόβουλο λογισμικό που διεισδύει στους εσωτερικούς πόρους. Η γενική αποδοχή αυτού του περιμετρικού μοντέλου υπεράσπισης έχει συμβεί επειδή είναι πολύ πιο εύκολο και φαινομενικά λιγότερο δαπανηρό να ασφαλιστεί μία περίμετρος από ότι είναι να εξασφαλιστεί ένας μεγάλος όγκος εφαρμογών ή μεγάλος αριθμός εσωτερικών δικτύων. Για να δοθεί πιο συγκεκριμένη πρόσβαση σε ορισμένες εσωτερικές πηγές, οι μηχανισμοί ελέγχου πρόσβασης έχουν χρησιμοποιηθεί σε συνδυασμό με τον περιμετρικό αμυντικό μηχανισμό.

Το firewall δεν είναι ένα απλό πρόγραμμα, αλλά ένα σύνολο από επί μέρους συστατικά, κανόνες και πρακτικές. Η συνήθης διαδικασία είναι ότι όλη η κίνηση από εσωτερικά προς εξωτερικά και αντίστροφα πρέπει να διέρχεται μέσα από το firewall. Ανάλογα με το μοντέλο υλοποίησης ενός firewall έχουμε τις εξής κατηγορίες:

- **Software Based:** Αποτελεί λογισμικό που τρέχει σε έναν υπολογιστή.

- **Hardware Based:** Είναι μια εξειδικευμένη συσκευή η οποία δρα σαν πύλη ασφαλείας σε ένα δίκτυο.
- **Cloud Hosted:** Πάροχοι υπηρεσιών ασφάλειας προσφέρουν λύσεις firewall οι οποίοι φιλοξενούνται σε υπολογιστικό νέφος.

Όσον αφορά τα πλεονεκτήματα και τα μειονεκτήματα των firewall, μπορούμε να πούμε τα εξής:

ΕΙΔΟΣ firewall	ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Packet Filtering Firewall	• Μία απλή συσκευή μπορεί να χρησιμοποιηθεί για όλο το δίκτυο • Αποδοτικός και γρήγορος • Οικονομικός • Ελάχιστη επίδραση στους πόρους του δικτύου	• Δεν μπορεί να επέμβει σε επίπεδο εφαρμογής. • Παραμετροποιείται δύσκολα • Δεν έχει δυνατότητες όπως πιστοποίηση σύνδεσης • Ευάλωτος σε επιθέσεις spoofing • Οι κανόνες είναι δύσκολοι στην δημιουργία και διαχείρισή τους
Circuit-Level Firewall	• Σχετικά οικονομικός • Καλύτερη διαχείριση κίνησης από τους application-level • Εύκολος στη ρύθμιση • Ελάχιστη επίδραση στη τελική εμπειρία χρήστη	• Προστατεύει δικτυακές συνδέσεις και όχι ξεχωριστά πακέτα • Είναι αδύνατο το φιλτράρισμα περιεχομένου. • Πρέπει να συνδυαστεί με άλλες τεχνικές για να είναι αποδοτικός
Application-Level Firewall	• Μπορεί να ανιχνεύσει επιθέσεις που δεν είναι ορατές στα κατώτερα επίπεδα του μοντέλου OSI • Προστατεύει την ανωνυμία του χρήστη • Πραγματοποιεί καλύτερους ελέγχους ασφάλειας	• Απαιτητικός στη ρύθμιση • Μπορεί να έχει αρνητική επίδραση στην απόδοση του δικτύου
Stateful Inspection Firewall	• Ικανός για αποτρέπει επιθέσεις που βασίζονται σε ευπάθειες των πρωτοκόλλων. • Μπορεί να αποτρέπει επιθέσεις DOS	• Υψηλές απαιτήσεις για την ρύθμισή του. • Υψηλό κόστος πόρων για την επεξεργασία • Δεν υποστηρίζει πιστοποιημένες συνδέσεις

Next Generation Firewall	• Παρέχει όλες τις λειτουργίες firewall, συνδυασμένες με συστήματα ανίχνευσης και προειδοποίησης. • Παρακολούθηση των πρωτοκόλλων δικτύου μέσω του application layer. • Δυνατότητα τήρησης αρχείων ημερολογίου.	• Υψηλό κόστος • Υψηλή απαίτηση σε επεξεργαστική ισχύ • Αρνητική επίδραση στην απόδοση του δικτύου

Honeypots

Τα συστήματα honeypot, χρησιμοποιούνται ευρέως ως συμπληρωματική πρακτική στην τεχνολογία IPDS, αλλά μπορούν να ρυθμιστούν και αυτόνομα. Μπορούν να οριστούν ως τα συστήματα που χρησιμοποιούνται για να παρασύρουν εισβολείς ή κακόβουλους χρήστες μακριά από τα κύρια συστήματα. Έχουν σχεδιαστεί με σκοπό να αποσπάσουν την προσοχή των επιτιθέμενων από κρίσιμα συστήματα και να αποκτήσουν πληροφορίες σχετικά με την κακόβουλη δραστηριότητά τους.

Τα honeypots περιέχουν παραπλανητικές πληροφορίες, ώστε να φαίνονται σημαντικές. Το σύστημα είναι μπορεί να καταγράφει συμβάντα, να παρακολουθεί κίνηση, τις προσβάσεις και τη δραστηριότητα που πραγματοποιείται. Με αυτό τον τρόπο όποιος έχει πρόσβαση στο honeypot χαρακτηρίζεται ύποπτος. Ουσιαστικά πρόκειται για παγίδα, καθώς έχει σχεδιαστεί για να δελεάσει και να παγιδέψει τον επιτιθέμενο.

Εφόσον όλα τα δεδομένα καταγράφονται, στη συνέχεια αναλύονται για να ανιχνευτούν νέα μοτίβα επίθεσης που αποτελούν απειλή για ζωτικούς πόρους. Τα honeypots προφανώς δεν είναι χρήσιμα αν δεν υπάρξει επίθεση.

Τα χαρακτηριστικά των συστημάτων honeypot είναι:

- Παίζουν σημαντικό ρόλο στην πρόληψη των επιθέσεων και κακόβουλων δραστηριοτήτων.
- Βελτιώνουν τον χρόνο ανίχνευσης μιας επίθεσης και τον χρόνο απόκρισης.
- Εξάγουν συμπεράσματα σχετικά με το προφίλ συμπεριφοράς μιας επίθεσης και την συμπεριφορά του συστήματος απέναντι σε αυτή.
- Καταγράφουν όλες τις δραστηριότητες
- Μπορούν να αναπτυχθούν σε φυσικό σύστημα ή να ρυθμιστούν εικονικά
- Από τη στιγμή που δεν χρησιμοποιούνται από κοινούς χρήστες αναμένεται να έχουν μηδενικούς ψευδείς συναγερμούς.

Όσον αφορά τα πλεονεκτήματα και τα μειονεκτήματα των honeypots, μπορούμε να αναφέρουμε τα εξής, επιγραμματικά:

ΠΛΕΟΝΕΚΤΗΜΑΤΑ	ΜΕΙΟΝΕΚΤΗΜΑΤΑ
Data Value ✓ Συλλέγουν δεδομένα τα οποία έχουν μεγάλη αξία.	**Narrow Field of View**

✓ Τα δεδομένα είναι υψηλής ποιότητας και η ανάλυση των δεδομένων είναι εύκολη	✓ Καταγράφουν μόνο την κακόβουλη δραστηριότητα που εξαπολύεται εναντίον τους.
Resources ✓ Δεν απαιτούν υψηλή επεξεργαστική ισχύ καθώς τα συστήματα δεν πραγματοποιούν καμία άλλη επεξεργασία. ✓ Είναι οικονομικά για την υλοποίηση τους.	**Fingerprinting** ✓ Μπορούν να αναγνωριστούν από έμπειρους επιτιθέμενους καθώς έχουν συγκεκριμένα χαρακτηριστικά και συμπεριφορές.
Simplicity ✓ Εύκολα στη ρύθμιση ✓ Εύκολα στη χρήση	**Risk** ✓ Μπορούν να χρησιμοποιηθούν σαν πλατφόρμα για επίθεση στο κανονικό σύστημα. ✓ Απλούστερα honeypot μικρότερο το ρίσκο.
Return of Investment ✓ Η αξία τους αντανακλάται στο γεγονός ότι ανιχνεύουν γρήγορα τις επιθέσεις. ✓ Αντανακλούν το επίπεδο ασφαλείας του συνολικού συστήματος.	
Reduce false positives ✓ Έχουν μηδενικούς ψευδείς συναγερμούς	

Λογισμικά Antivirus

Είναι ο πλέον διαδεδομένος τρόπος προστασίας για την ανίχνευση και απομάκρυνση ιών και, γενικότερα, κακόβουλου λογισμικού που προσβάλλει έναν υπολογιστή. Λειτουργούν, συνήθως, με δύο τρόπους: είτε σαρώνουν προγράμματα και αρχεία όταν εισέρχονται στην συσκευή και συγκρίνουν τα αποτελέσματα με γνωστούς ιούς είτε σαρώνουν προγράμματα που προϋπάρχουν με τον ίδιο σκοπό.

Επίσης, μπορούν να εκτελούνται σε πραγματικό χρόνο και να ελέγχουν κατά την εκτέλεση ενός προγράμματος ή όταν ανοίγει ένα αρχείο από το αποθηκευτικό μέσο.

Κρυπτογραφία

Ένας από τους πιο σημαντικούς κλάδους της επιστήμης των υπολογιστών που στοχεύει στην προστασία των συναλλαγών και των προσωπικών δεδομένων είναι η *κρυπτογραφία*. Η κρυπτογραφία στοχεύει στη σχεδίαση και υλοποίηση συστημάτων λογισμικού ή και υλικού τα οποία μετασχηματίζουν μία χρήσιμη και εμπιστευτική πληροφορία σε τέτοια μορφή η οποία να είναι κατανοητή μόνο από τον αποστολέα και τον νόμιμο παραλήπτη, ενώ ταυτόχρονα να είναι ακατανόητη (και συνεπώς χωρίς αξία) σε οποιαδήποτε μη εξουσιοδοτημένη οντότητα.

Η κρυπτογραφία εμφανίστηκε αρχικά, τουλάχιστον από όσα γνωρίζουμε μέχρι σήμερα, στην εποχή των αρχαίων Αιγυπτίων (2.000 π.Χ.), παίζοντας ένα πολύ σημαντικό ρόλο καθ' όλη τη διάρκεια της ιστορίας. Ειδικότερα στον 2ο παγκόσμιο πόλεμο, τόσο οι Γερμανοί όσο και οι Ιάπωνες κατάφεραν να αναπτύξουν κρυπτογραφικές μηχανές όπως η Enigma και η Purple Machine αντίστοιχα. Αξίζει να σημειωθεί ότι αργότερα πολύπλοκες κρυπτογραφικές μέθοδοι

επικοινωνίας αναπτύχθηκαν από λαθρεμπόρους, αλλά και στη συνέχεια ακόμη πιο πολύπλοκες αναπτύχθηκαν από μυστικές υπηρεσίες κυβερνήσεων. Τέλος, στις μέρες μας, η ανάγκη για κρυπτογραφημένα μηνύματα είναι πολύ μεγάλη, αρκεί μόνο να συλλογιστούμε πόσο απαραίτητο μας είναι πολλές φορές το γεγονός να ανταλλάσσουμε πληροφορίες μέσω διαδικτύου. Για παράδειγμα, η μεταφορά χρηματικών ποσών από ένα λογαριασμό σε έναν άλλο, που πλέον γίνεται εύκολα μέσω διαδικτύου, επιθυμούμε να γίνεται με τέτοιο τρόπο ώστε να είναι αδύνατο οι δύο αριθμοί λογαριασμών να γίνουν γνωστοί σε κάποιον τρίτο. Κάθε κρυπτογραφικό σύστημα θα πρέπει να έχει τέτοιες ιδιότητες, ώστε να παρέχεται η επιθυμητή ασφάλεια στους χρήστες. Τη σημαντικότητα των συγκεκριμένων ιδιοτήτων θα προσπαθήσουμε να παρουσιάσουμε στο παρακάτω παράδειγμα.

Έστω ότι η Alice επιθυμεί να μεταφέρει χρήματα από έναν δικό της τραπεζικό λογαριασμό σε έναν τραπεζικό λογαριασμό του Bob μέσω διαδικτύου (η Alice και ο Bob είναι δύο δημοφιλείς χαρακτήρες στα παραδείγματα χρήσης κρυπτογραφικών συστημάτων που παραθέτουν τα βιβλία). Η Alice, φυσικά, επιθυμεί η συγκεκριμένη επικοινωνία να είναι εμπιστευτική, έτσι ώστε κανένας τρίτος να μην μπορέσει να λάβει γνώση τόσο των δύο αριθμών λογαριασμού όσο και του μεταφερόμενου χρηματικού ποσού. Από την άλλη πλευρά, ο Bob θα πρέπει, επίσης, να λάβει το μήνυμα πιστοποιημένο, ότι δηλαδή αυτό προέρχεται πράγματι από την Alice. Και οι δύο πλευρές (Alice και Bob) θα πρέπει, επιπρόσθετα, να είναι βέβαιες ότι η ακεραιότητα του μηνύματος διατηρείται, όπως για παράδειγμα ότι το μεταφερόμενο χρηματικό ποσό δε δύναται να αλλαχθεί από κάποιον τρίτο κατά τη διαδικασία. Τέλος, ο Bob επιθυμεί την μη αποποίηση ευθύνης από την Alice, δηλαδή η Alice να μην μπορεί να ισχυριστεί, αργότερα, ότι δεν έδωσε την εντολή μεταφοράς του χρηματικού ποσού. Όλα αυτά τα σενάρια είναι αντιπροσωπευτικά για την κρυπτογραφία η οποία έχει για αυτά τις κατάλληλες λύσεις.

Ειδικότερα, *κρυπτογράφηση* ονομάζεται η διαδικασία εκείνη κατά την οποία ένα απλό κείμενο (plain text) μετατρέπεται σε ένα κρυπτογραφημένο κείμενο (cipher text). Ενώ αποκρυπτογράφηση είναι η ακριβώς αντίστροφη διαδικασία. Και οι δύο αυτές διαδικασίες πραγματοποιούνται με τη χρήση κλειδιών κρυπτογράφησης και αποκρυπτογράφησης αντίστοιχα. Ο αποστολέας κρυπτογραφεί ένα μήνυμα χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης μαζί με το αντίστοιχο κλειδί κρυπτογράφησης και στη συνέχεια στέλνει το κρυπτογραφημένο, πλέον, μήνυμα στον παραλήπτη. Εκείνος με τη σειρά του, αποκρυπτογραφεί το μήνυμα χρησιμοποιώντας έναν αλγόριθμο αποκρυπτογράφησης και το κλειδί αποκρυπτογράφησης. Στην μεταξύ επικοινωνία των δύο χρηστών, είναι πιθανόν να προσπαθήσει να παρέμβει με κακόβουλο τρόπο μία τρίτη οντότητα. Αυτή η οντότητα στην κρυπτογραφία αποκαλείται *υποκλοπέας* (interceptor), *ωτακουστής* (eavesdropper) ή απλά *επιτιθέμενος* (attacker). Η διαδικασία που εκτελεί ο υποκλοπέας ονομάζεται κρυπτανάλυση. Συνεπώς, κρυπτανάλυση είναι η διαδικασία εκείνη κατά την οποία ο υποκλοπέας μελετά το κρυπτογραφημένο μήνυμα και προσπαθεί με διάφορες τεχνικές και μεθόδους και χωρίς φυσικά να διαθέτει το κλειδί αποκρυπτογράφησης, να εξάγει την αρχική πληροφορία (ή μέρος αυτής) του κρυπτογραφημένου μηνύματος. Η έννοια της κρυπτολογίας περιλαμβάνει μαζί την έννοια της κρυπτογραφίας και της κρυπτανάλυσης.

Πολύ συχνά στα κρυπτογραφημένα μηνύματα ορίζεται ένα Έμπιστο Τρίτο Μέλος (Trusted Third Party - TTP). Ο ρόλος του μέλους αυτού είναι η επίλυση διαφωνιών μεταξύ των υπολοίπων χρηστών του συστήματος ή ακόμα και η διευκόλυνση της μεταξύ τους επικοινωνίας. Το Έμπιστο Τρίτο Μέλος διακρίνεται σε λειτουργικά έμπιστο (functionally trusted) και σε άνευ όρων έμπιστο (unconditionally trusted). Λειτουργικά έμπιστο μέλος

θεωρείται ένα TTP το οποίο είναι έμπιστο για να λύσει διαφωνίες μεταξύ των χρηστών, αλλά δεν μπορεί να έχει πρόσβαση στα μυστικά κλειδιά τους. Ένα TTP μέλος θεωρείται άνευ όρων έμπιστο μέλος μόνον εφόσον όλοι οι χρήστες του κρυπτογραφημένου συστήματος μπορούν να το εμπιστευθούν από κάθε άποψη, όπως για παράδειγμα να είναι γνώστης όλων των μυστικών κλειδιών των χρηστών.

Τέλος, αξίζει να σημειωθεί ότι η ασφάλεια του συστήματος εξαρτάται μόνο από την μυστικότητα των κλειδιών αποκρυπτογράφησης, μιας και οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης που χρησιμοποιούνται είναι γνωστοί σε όλους. Από αυτό και μόνο το γεγονός, είναι φανερό ότι η διανομή και διαχείριση των κλειδιών αποκρυπτογράφησης αποτελεί ένα από τα πιο βασικά και δύσκολα προβλήματα της επιστήμης της κρυπτογραφίας.

Τα κρυπτογραφικά συστήματα διαχωρίζονται σε δύο είδη με βάση τα κλειδιά αποκρυπτογράφησης. Έτσι έχουμε τις εξής δύο μεγάλες κατηγορίες:

- Τα συμμετρικά (symmetric) ή συμβατικά (conventional) κρυπτογραφικά συστήματα, και
- τα μη συμμετρικά (asymmetric) ή δημόσιου κλειδιού (public key) κρυπτογραφικά συστήματα.

Ένα κρυπτογραφικό σύστημα ονομάζεται συμμετρικό όταν το κλειδί αποκρυπτογράφησής του μπορεί εύκολα να υπολογιστεί από το αντίστοιχο κλειδί κρυπτογράφησης. Στην πληθώρα των περιπτώσεων των συμβατικών κρυπτογραφικών συστημάτων, τα δύο κλειδιά είναι ίδια. Αντίστοιχα, ένα κρυπτογραφικό σύστημα ονομάζεται δημοσίου κλειδιού όταν το κλειδί αποκρυπτογράφησής του υπολογίζεται δύσκολα (υπολογιστικά) από το αντίστοιχο κλειδί κρυπτογράφησης.

Είναι πλέον σαφές ότι η ασφάλεια όλων των κρυπτογραφικών συστημάτων βασίζεται στην μυστικότητα του κλειδιού αποκρυπτογράφησης, το οποίο και δεν πρέπει να αποκαλυφθεί σε κανένα άλλον, πέραν των πιστοποιημένων χρηστών του κρυπτογραφικού συστήματος. Έτσι, για να θεωρείται ένα συμβατικό (συμμετρικό) κρυπτογραφικό σύστημα ασφαλές, να είναι δηλαδή ο δίαυλος επικοινωνίας των χρηστών του ασφαλής, θα πρέπει τόσο το κλειδί αποκρυπτογράφησης όσο και το κλειδί κρυπτογράφησης να είναι μυστικά. Αυτό το γεγονός από μόνο του αποτελεί ένα σημαντικό μειονέκτημα των συμβατικών κρυπτογραφικών συστημάτων. Αντίθετα, κάτι τέτοιο δεν απαιτείται για την ασφάλεια των κρυπτογραφικών συστημάτων δημοσίου κλειδιού.

Στα κρυπτογραφικά συστήματα δημοσίου κλειδιού, οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης είναι με τέτοιο τρόπο σχεδιασμένοι ώστε τα αντίστοιχα κλειδιά, κρυπτογράφησης και αποκρυπτογράφησης, να είναι διαφορετικά μεταξύ τους. Η επιτυχία, και συνεπώς η ασφάλεια, αυτού του είδους των κρυπτογραφικών συστημάτων βασίζεται στο ότι παρά το γεγονός ότι το δημόσιο κλειδί κρυπτογράφησης είναι γνωστό σε όλους, ο υπολογισμός του κλειδιού αποκρυπτογράφησης είναι δύσκολος έως αδύνατος. Στα συστήματα αυτά, δημόσιο κλειδί καλείται το κλειδί κρυπτογράφηση, που είναι σε όλους γνωστό και ιδιωτικό κλειδί καλείται το άλλο κλειδί, το κλειδί αποκρυπτογράφησης.

Σύμφωνα με όλα τα παραπάνω, αυτό που προσδίδει ασφάλεια στα κρυπτογραφικά συστήματα δημοσίου κλειδιού είναι στην ουσία η δυσκολία που παρουσιάζεται στην επίλυση ενός μαθηματικού προβλήματος. Πιο συγκεκριμένα, η εξακρίβωση του ιδιωτικού κλειδιού με βάση το δημόσιο κλειδί, αλλά και κάποιες ακόμα παραμέτρους του συστήματος

είναι ένα τρομερά δύσκολο υπολογιστικά πρόβλημα. Όσο πιο δυσεπίλυτο το πρόβλημα αυτό, τόσο πιο αποδοτικό και ασφαλές είναι το κρυπτογραφικό σύστημα.

Τακτική λήψη Αντιγράφων Ασφαλείας (Backup)

Η λήψη αντιγράφων ασφαλείας είναι απαραίτητη καθώς επιτρέπει την προστασία των δεδομένων και των εφαρμογών μιας επιχείρησης με ένα δομημένο τρόπο. Αυτά λαμβάνονται σύμφωνα με την πολιτική της επιχείρησης και την κρισιμότητα των δεδομένων που προστατεύουν. Υπάρχει πληθώρα λύσεων backup - restore ανάλογα με το μέγεθος και την πολυπλοκότητα του εταιρικού περιβάλλοντος. Πολλές είναι βέβαια οι επιχειρήσεις που προτιμούν να υλοποιούν το backup δεδομένων στο υπολογιστικό νέφος (cloud), για ακόμη μεγαλύτερη προστασία αυτών. Σε αυτές τις περιπτώσεις είναι απαραίτητη και η χρήση μεθόδων κρυπτογράφησης καθώς ο κίνδυνος να υποπέσουν ευαίσθητα δεδομένα σε λάθος χέρια είναι αυξημένος.

Ανωνυμοποίηση

Η ανωνυμοποίηση (αγγλικά: anonymization) αφορά στην επεξεργασία πληροφοριών με σκοπό την προστασία των προσωπικών δεδομένων και της ιδιωτικότητας. Κατά τη διαδικασία της ανωνυμοποίησης αφαιρούνται προσωπικά στοιχεία από σύνολα δεδομένων, ώστε τα άτομα που περιγράφουν τα δεδομένα να παραμένουν μη αναγνωρίσιμα, ανώνυμα, και να μη μπορούν να ταυτοποιηθούν με κανένα τρόπο, άμεσα ή έμμεσα.

Ψευδονυμοποίηση

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τρόπο ώστε τα δεδομένα να μη μπορούν πλέον να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο.

Σχέδιο Ασφαλείας

Το Σχέδιο Ασφαλείας (Security Plan) είναι το επιχειρησιακό έγγραφο στο οποίο περιγράφονται τα οργανωτικά και τεχνικά μέτρα, καθώς και τα μέτρα φυσικής ασφαλείας που εφαρμόζονται και πρόκειται να εφαρμοστούν για την κάλυψη των βασικών αρχών και κανόνων ασφαλείας που αναφέρονται στην πολιτική ασφαλείας, καθώς και οι απαραίτητες ενέργειες για την υλοποίησή τους. Αφορά τόσο αυτοματοποιημένα, όσο και μη αυτοματοποιημένα συστήματα διαχείρισης και επεξεργασίας δεδομένων και πρέπει να εφαρμόζεται με ακρίβεια για την προστασία των προσωπικών δεδομένων, ευαίσθητων και μη, που τηρούνται από τον υπεύθυνο επεξεργασίας. Το Σχέδιο αυτό υπόκειται σε τακτικές επισκοπήσεις και αναθεωρήσεις, δεδομένης της ραγδαίας ανάπτυξης τεχνολογικών λύσεων και της εφαρμογής τους στα πληροφοριακά συστήματα.

Το Σχέδιο Ασφαλείας αποτελείται από την περιγραφή του συστήματος επεξεργασίας προσωπικών δεδομένων, του υπευθύνου επεξεργασίας, τα οργανωτικά και τεχνικά μέτρα ασφαλείας, καθώς και τα μέτρα φυσικής ασφάλειας που υπάρχουν. Ακόμα, περιλαμβάνει το πλάνο υλοποίησης των μέτρων ασφαλείας και την περιγραφή των διαδικασιών συνεχούς επισκόπησης και αναθεώρησης του σχεδίου ασφαλείας.

Παρόν και μέλλον στην κυβερνοασφάλεια

Κάθε τεχνολογική εξέλιξη, εκτός από τις θετικές της πλευρές, μπορεί να αποτελέσει και μία ακόμη ευκαιρία για να δράσουν οι κυβερνοεγκληματίες. Ειδικότερα τα τελευταία χρόνια, έχει υπάρξει αλματώδης ανάπτυξη σε πολλούς τεχνολογικούς τομείς με αντίστοιχη δημιουργία ευκαιριών για καινοτομία και επιχειρηματικότητα. Πιο κάτω, αναφέρουμε μερικούς από αυτούς τους τομείς μαζί με τα σημεία προσοχής όσον αφορά το κυβερνοέγκλημα:

Edge computing: ως Edge Computing (υπολογισμός στις «παρυφές» ενός κατανεμημένου υπολογιστικού συστήματος) αναφέρεται η αποκεντρωμένη και κατανεμημένη επεξεργασία δεδομένων στις «παρυφές» (edge) ενός διαδικτυωμένου πληροφοριακού συστήματος. Το Edge Computing είναι μια ανοικτή, κατανεμημένη αρχιτεκτονική IT, η οποία χαρακτηρίζεται από μια αποκεντρωμένη απόδοση επεξεργασίας. Έτσι το Edge Computing δεν αποτελεί μόνο τη βάση για το Mobile Computing, αλλά και για τις τεχνολογίες του Internet of Things (IoT). Στην πράξη στα πλαίσια του Edge Computing γίνεται επεξεργασία δεδομένων απευθείας σε μια (κινητή) συσκευή, ένα τοπικό PC ή Server, χωρίς να μεσολαβεί μεταφορά τους σε κέντρο υπολογιστών. Η μεγάλη αδυναμία του edge computing, όμως, είναι στηρίζεται σε υπολογισμούς που παρέχουν μεγάλες ομάδες συσκευών σχετικά περιορισμένων δυνατοτήτων που είναι απομακρυσμένες από τους ισχυρούς servers του συστήματος. Κατά συνέπεια, υπάρχουν πολλά ευάλωτα σημεία στις συσκευές αυτές και ο μεγάλος αριθμός τους απλά διευρύνει την επιφάνεια επιφάνειας επιθέσεων (attack surface) δηλαδή τα σημεία από τα οποία μπορεί να πραγματοποιηθεί προσπάθεια παραβίασης της ασφάλειας του συστήματος.

IoT (Internet of Things): όπως αναφέραμε νωρίτερα, το IoT μπορεί να θεωρηθεί ως μια παγκόσμια διαδικτυωμένη υποδομή που αποτελείται από δεκάδες δισεκατομμυρίων συνδεδεμένες συσκευές που βασίζονται σε πολύ διαφορετικές τεχνολογίες, έχουν δυνατότητες συλλογής και επεξεργασίας δεδομένων μέσω αισθητήρων, και μπορούν να αποστέλλουν και να λαμβάνουν δεδομένα με διάφορες τεχνολογίες ασύρματων και ενσύρματων δικτύων. Όμως η εμφάνιση, στο υπολογιστικό τοπίο συσκευών κάθε είδους, μεγέθους και δυνατοτήτων με, συνήθως, μικρή έως ανύπαρκτη άμυνα απέναντι σε κυβερνοεπιθέσεις. Οι συσκευές αυτές, όπως είναι οι ασύρματες κάμερες, οι αισθητήρες θερμοκρασίας και θέσης (GPS), οι έξυπνες συσκευές σπιτιού και οι διαδικτυωμένες οικιακές συσκευές, έχουν πολλές καταγεγραμμένες ευπάθειες όπως, για παράδειγμα, ενσωματωμένους σε αυτές κωδικούς ασφαλούς επικοινωνίας οι οποίοι μπορούν να υποκλαπούν με μεγάλη ευκολία και γενικά είναι ευάλωτες σε επιθέσεις. Συνήθως, οι επιτιθέμενοι δημιουργούν από αυτές τις συσκευές bots, τα οποία είναι δίκτυα συσκευών που είναι υπό τον έλεγχο των επιτιθέμενων και που χρησιμοποιούνται για κυβερνοεπιθέσεις μεγάλης κλίμακας (attack amplification), όπως είναι οι επιθέσεις DDos (Distributed Denial of Service) σε κρίσιμες υποδομές ή διαδικτυακές υπηρεσίες.

Web 3.0: Μια άλλη εξέλιξη που αρχίζει να αποδεικνύει τα οφέλη της στο πλαίσιο του σημερινού διαδικτύου είναι ο Σημασιολογικός Ιστός ή Web3.0. Ο Σημασιολογικός Ιστός είναι η επόμενη γενιά του διαδικτύου στον οποίο οι πληροφορίες είναι επεξεργάσιμες από μηχανές και αυτοματοποιημένες υπηρεσίες που μπορούν να ανακτήσουν, να εξαγάγουν και να συνδυάσουν πληροφορίες από το διαδίκτυο. Στοχεύει στην ενσωμάτωση σημασιολογίας, δηλαδή «νοήματος», στα δεδομένα όπου μέσα από αυτή τη διαδικασία, ορίζεται η δομή και το «νόημα» των περιεχόμενων των ιστοσελίδων. Δημιουργώντας ένα περιβάλλον, όπου ειδικά σχεδιασμένες εφαρμογές μπορούν, αυτόνομα, να ερευνήσουν το διαδίκτυο για

δεδομένα και πληροφορίες και να συνάγουν, αυτόματα, συμπεράσματα και νέα γνώση χωρίς ανθρώπινη παρέμβαση. Ο κίνδυνος εδώ εμφανίζεται από το ότι στον Παγκόσμιο Ιστό θα υπάρχει, σταδιακά, στα πλαίσια της εξέλιξης του Web 3.0 ανυπολόγιστος αριθμών πληροφοριών και «ανώνυμων» ιχνών όλων των χρηστών του ιστού δομημένα για επεξεργασία από υπερυπολογιστές με στόχο την εξαγωγή συμπερασμάτων και υπολογισμό νέας γνώσης με βάση την προηγούμενα. Με αυτό τον τρόπο, πολλοί άνθρωποι αλλά και οργανισμοί απειλούνται με αποκάλυψη ευαίσθητων ή απόρρητων πληροφοριών και δεδομένων που ενώ δεν είναι άμεσα αποθηκευμένα στον Παγκόσμιο Ιστό, συνάγονται ως αποτέλεσμα της επεξεργασίας της υπάρχουσας πληροφορίας από του υπολογιστές.

Τεχνητή Νοημοσύνη (Artificial Intelligence – AI): Ως *Τεχνητή Νοημοσύνη* (AI) χαρακτηρίζουμε κάθε ευφυή συμπεριφορά ή εκτέλεση μιας εργασίας που επιδεικνύεται από μηχανές (υπολογιστικά συστήματα), σε αντίθεση με τη νοημοσύνη που επιδεικνύεται από ζώντες οργανισμούς, κυρίως τους ανθρώπους. Παραδείγματα τέτοιων εργασιών συμπεριλαμβάνουν την αναγνώριση ομιλίας, την τεχνητή όραση, τη μετάφραση μεταξύ δύο (φυσικών) γλωσσών, καθώς και άλλες εργασίες στις οποίες υπερέχουν των μηχανών οι ζώντες οργανισμοί, κυρίως οι άνθρωποι. Παραδείγματα εφαρμογών τεχνητής νοημοσύνης συμπεριλαμβάνουν τις προηγμένες μηχανές αναζήτησης ιστού (για παράδειγμα το Google Search), τα συστήματα συστάσεων για περιεχόμενο (recommendation systems – που χρησιμοποιούνται από το YouTube, το Amazon και το Netflix, για παράδειγμα), την κατανόηση της ανθρώπινης ομιλίας (για παράδειγμα το Siri και η Alexa), τα αυτόνομα οχήματα (π.χ. Waymo), τα συστήματα παραγωγής κειμένων και συνομιλίας ή άλλα δημιουργικά εργαλεία (ChatGPT καθώς και δημιουργία έργων τέχνης), αυτοματοποιημένη λήψη αποφάσεων και μεγάλες επιδόσεις σε στρατηγικά παίγνια (όπως το σκάκι και το Go). Η Τεχνητή Νοημοσύνη ήδη χρησιμοποιείται, κυρίως στην μορφή Deep Learning νευρωνικών δικτύων, για τον εντοπισμό μοτίβων κυβερνοεπιθέσεων σε δεδομένα δικτύων έτσι ώστε να γίνεται έγκαιρα ο εντοπισμός κακόβουλων προσπαθειών. Όμως και ο ψηφιακός υπόκοσμος χρησιμοποιεί, όλο και περισσότερο, μεθόδους της Τεχνητής Νοημοσύνης για να ανιχνεύσει και να επιλέξει, «έξυπνα», στόχους και να εξαπολύσει «έξυπνες» επιθέσεις που αποφεύγουν τον εντοπισμό. Επιπρόσθετα, οι μέθοδοι της Τεχνητής Νοημοσύνης χρησιμοποιούνται για την παραγωγή και διασπορά αληθοφανών ψεύτικων ειδήσεων (fake news) αλλά και την δημιουργία παραποιημένων φωτογραφιών με στόχο την παραπλάνηση αλλά και την αμαύρωση της υπόληψης των θυμάτων.

Γενικά, οι απειλές μπορούν να κατηγοριοποιηθούν ανάλογα με την επικινδυνότητά τους ως εξής:

Επίπεδο κινδύνου απειλών	Χαρακτηριστικά απειλών	Τελικός στόχος απειλών	Στρατηγική αποφυγής απειλών
Μέσου κινδύνου απειλές	• Οι κυβερνοεγκληματίες υποκλέπτουν ταυτότητες (προφίλ) και χρήματα • Χρησιμοποιούν διάφορες τεχνικές • Συχνά, Botnets και Bot Herders	Στοχεύουν σε άτομα ή άλλες οντότητες (π.χ. εταιρίες) με στόχο υποκλοπή προσωπικών ή εταιρικών δεδομένων, προφίλ, και χρηματικών ποσών (π.χ. Ransomware)	Αυστηρή εφαρμογή και επιβολή αναγνωρισμένων καλών πρακτικών στην ασφάλεια πληροφοριακών συστημάτων
Χαμηλού κινδύνου απειλές	• Μέσω κοινού Διαδικτύου (Surface Web) • «Θόρυβος»/Μικροεισβολές/ Πρόκληση εκνευρισμού • Απειλές εναντίον κάθε χρήστη • Χωρίς, συνήθως, τεχνικό βάθος ή τεχνολογική καινοτομία, όμως με βάση μία τακτική επίθεσης • worms, viruses, script kiddie hackers για να προσελκύσουν την προσοχή	Συνήθως στόχος είναι η πρόκληση θορύβου γύρω από την επίθεση – δεν στοχεύουν σε συγκεκριμένους στόχους ύστερα από μία διαδικασία επιλογής με βάση κάποια κριτήρια	

Επίπεδο κινδύνου απειλών	Χαρακτηριστικά απειλών	Τελικός στόχος απειλών	Στρατηγική αποφυγής απειλών
Υψηλού κινδύνου απειλές	• Προέρχονται από επιθετικές και «διάχυτες» υψηλού κίνητρου και υψηλών οικονομικών ή άλλων πόρων • Πολλαπλοί τρόπου επίθεσης (attack vectors) όπως email, social media, και εκμετάλλευσης εμπιστοσύνης • Χρήση zero-day attacks και εκμετάλλευση ευπαθειών αδύναμων συσκευών (κυρίως IoT) • Καλούνται, συχνά, Advanced Persistent Threats (APTs)	Επίθεση σε εθνικές οικονομίες ή πολιτικές, προπαγάνδα, βιομηχανική κατασκοπεία, κλοπή πνευματικής ιδιοκτησίας, ακτιβισμός (hacktivists, WikiLeaks κ.λπ.)	Ετοιμότητα Εθνικής Κυβερνοασφάλειας και Εθνική Στρατηγική Αντιμετώπισης Απειλών και Επιθέσεων που συμπεριλαμβάνουν τα εξής, τουλάχιστον, μέσα: ❑ Τεχνικά ❑ Εθνική Τεχνογνωσία ❑ Εθνικές Δομές Πληροφοριακών Συστημάτων και Τηλεπικοινωνιών ❑ Νομικά (π.χ. GDPR) ❑ Υψηλή ετοιμότητα σε κάθε κυβερνητική δομή – άμεση αντίδραση

Οι απειλές που περιγράψαμε σε αυτή την ενότητα ανήκουν στην κατηγορία υψηλού κινδύνου και πρέπει να υπάρχει στρατηγική αντιμετώπισής τους για το παρόν αλλά και το μέλλον, καθώς θα εξελίσσονται παράλληλα με τις τεχνολογικές εξελίξεις.

Εκτός από αυτές τις εξελίξεις, έχουμε την αλματώδη αύξηση των ομάδων κυβερνοεγκληματιών από τους οποίους προέρχονται οι *Προηγμένες Επίμονες Απειλές* ή APTs από τα αρχικά Advanced Persistent Threats. Αυτές οι ομάδες στοχεύουν στην οργανωμένη και επίμονη εφαρμογή ενός ευρέως φάσματος κακόβουλου λογισμικού και διάφορων προηγμένων τεχνικών εισβολής σε επιλεγμένους στόχους, συνήθως επιχειρηματικούς ή κυβερνητικούς.

Τα κύρια χαρακτηριστικά των APTs είναι τα εξής:

Προηγμένες (Advanced)

- Οι επιτιθέμενοι χρησιμοποιούν μια μεγάλη γκάμα τεχνολογιών εισβολής και κακόβουλου λογισμικού, συμπεριλαμβανομένης της ανάπτυξης προσαρμοσμένου λογισμικού, αν αυτό κριθεί απαραίτητο
- Τα επιμέρους τμήματα του λογισμικού δεν είναι υποχρεωτικά προηγμένα από τεχνικής άποψης, ωστόσο είναι προσεκτικά διαλεγμένα ώστε να ταιριάζουν με τον επιλεγμένο στόχο

Επίμονες (Persistent)

- Οι επιθέσεις εξαπολύονται με αμείωτη ένταση και για μεγάλο χρονικό διάστημα εναντίον του επιλεγμένου στόχου ώστε να μεγιστοποιηθεί η πιθανότητα επιτυχίας
- Μπορεί να εφαρμοστούν σταδιακά διάφορες επιθέσεις μέχρι να παραβιαστεί ο στόχος

Απειλές (Threats)

- Οι απειλές για τους επιλεγμένους στόχους είναι το αποτέλεσμα της πρόθεσης των οργανωμένων, ικανών και καλά χρηματοδοτούμενων επιτιθέμενων να παραβιάσουν τους ειδικά επιλεγμένους στόχους τους
- Η ενεργή συμμετοχή του ανθρώπινου παράγοντα στη διαδικασία αυξάνει πολύ το επίπεδο της απειλής σε σύγκριση με το επίπεδο απειλών που προκύπτουν από αυτοματοποιημένα εργαλεία επίθεσης, καθώς και την πιθανότητα επιτυχούς έκβασης της επίθεσης

Όσον αφορά τον σκοπό των APTs, ποικίλει από την κλοπή πνευματικής ιδιοκτησίας ή δεδομένων που σχετίζονται με την ασφάλεια και τις υποδομές έως τη διακοπή της λειτουργίας των φυσικών υποδομών. Οι τεχνικές που χρησιμοποιούνται συμπεριλαμβάνουν την κοινωνική μηχανική, το ηλεκτρονικό «καμάκωμα» (spear-phishing) μέσω email, και τις κρυφές λήψεις (drive-by-downloads) από επιλεγμένους εκτεθειμένους ιστότοπους τους οποίους είναι πιθανό να επισκεφθεί το προσωπικό του οργανισμού που έχει μπει στο στόχαστρο του επιτιθέμενου. Η κύρια πρόθεση των APTs είναι να μολύνουν τον στόχο με εξελιγμένο κακόβουλο λογισμικό μέσω πολλών μηχανισμών εξάπλωσης και απελευθέρωσης φορτίων εκτέλεσης του λογισμικού αυτού. Μόλις οι ομάδες αυτές αποκτήσουν για πρώτη φορά πρόσβαση στα συστήματα του οργανισμού-στόχου, χρησιμοποιούν και άλλα εργαλεία επίθεσης προκειμένου να διατηρήσουν και να επεκτείνουν την πρόσβασή τους.

Προς μία αποτελεσματική πανευρωπαϊκή και εθνική στρατηγική κυβερνοασφάλειας

Η κοινωνία της πληροφορίας και η ψηφιακή διακυβέρνηση προσφέρει τεράστιες ευκαιρίες και δίνει λύσεις σε πολλές από τις προκλήσεις που αντιμετωπίζει η Ευρώπη, εκθέτει όμως την οικονομία και την κοινωνία σε κυβερνοαπειλές. Η τάση αυτή πρόκειται να ενισχυθεί περαιτέρω στο μέλλον, καθώς αναμένεται ότι έως το 2024 δεκάδες δισεκατομμύρια συσκευές παγκοσμίως θα είναι συνδεδεμένες με το διαδίκτυο των πραγμάτων.

Η κυβερνοασφάλεια περιλαμβάνει τις δραστηριότητες που απαιτούνται για την προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών των εν λόγω συστημάτων και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων.

Υπό το πρίσμα αυτών των προκλήσεων στον τομέα της κυβερνοασφάλειας, η ΕΕ αναπτύσσει δράση σε διάφορα μέτωπα, προκειμένου:

- να ενισχύσει την κυβερνοανθεκτικότητα
- να καταπολεμήσει το κυβερνοέγκλημα
- να ενισχύσει την κυβερνοδιπλωματία
- να ενδυναμώσει την κυβερνοάμυνα
- να τονώσει την έρευνα και την καινοτομία
- να προστατεύσει τις υποδομές ζωτικής σημασίας

Η ανάπτυξη ισχυρότερης δράσης στο πεδίο της κυβερνοασφάλειας, με στόχο να οικοδομηθεί ένας ανοικτός και ασφαλής κυβερνοχώρος, μπορεί να αυξήσει την εμπιστοσύνη των πολιτών στα ψηφιακά εργαλεία και υπηρεσίες.

Στρατηγική της ΕΕ για την κυβερνοασφάλεια

Τον Δεκέμβριο του 2020 η Ευρωπαϊκή Επιτροπή και η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) παρουσίασαν μια νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια. Στόχος της στρατηγικής αυτής είναι να ενισχυθεί η ανθεκτικότητα της Ευρώπης απέναντι στις κυβερνοαπειλές και να μπορέσουν να ωφεληθούν πλήρως όλοι οι πολίτες και οι επιχειρήσεις από έγκυρες και αξιόπιστες υπηρεσίες και ψηφιακά εργαλεία. Η νέα στρατηγική περιλαμβάνει συγκεκριμένες προτάσεις για τη χρήση κανονιστικών και επενδυτικών μέσων καθώς και μέσων πολιτικής.

Στις 22 Μαρτίου 2021, το Συμβούλιο ενέκρινε συμπεράσματα σχετικά με τη στρατηγική κυβερνοασφάλειας, υπογραμμίζοντας ότι η κυβερνοασφάλεια είναι αναγκαία για μια ανθεκτική, πράσινη και ψηφιακή Ευρώπη. Οι υπουργοί της ΕΕ έθεσαν ως βασικό στόχο την επίτευξη στρατηγικής αυτονομίας με διατήρηση μιας ανοικτής οικονομίας. Στο πλαίσιο αυτό περιλαμβάνεται η ενίσχυση της ικανότητας για αυτόνομες επιλογές στον τομέα της κυβερνοασφάλειας με σκοπό να ενισχυθεί ο ηγετικός ρόλος της ΕΕ στον ψηφιακό τομέα και οι στρατηγικές της ικανότητες.

Η ΕΕ επεξεργάζεται επίσης δύο νομοθετικές προτάσεις με στόχο την αντιμετώπιση των υφιστάμενων και μελλοντικών κινδύνων εντός και εκτός διαδικτύου:

- μια επικαιροποιημένη οδηγία για την καλύτερη προστασία των συστημάτων δικτύου και πληροφοριών
- μια νέα οδηγία για την ανθεκτικότητα των κρίσιμων οντοτήτων

Οι ευρωπαϊκές χώρες καταλαμβάνουν 18 από τις 20 κορυφαίες θέσεις στον παγκόσμιο δείκτη κυβερνοασφάλειας. Η αξία της αγοράς της ΕΕ στον τομέα της κυβερνοασφάλειας εκτιμάται σε περισσότερα από 130 δισ. € και αυξάνεται με ρυθμό 17% ετησίως. Η ΕΕ διαθέτει περισσότερες από 60.000 εταιρείες κυβερνοασφάλειας και περισσότερα από 660 κέντρα υψηλής εξειδίκευσης στον τομέα της κυβερνοασφάλειας.

Ειδικότερα, η ΕΕ έχει ιδρύσει τον ENISA. Ο νέος Οργανισμός της ΕΕ για την Κυβερνοασφάλεια βασίζεται στις δομές του φορέα τον οποίο διαδέχτηκε, δηλαδή του Οργανισμού της Ευρωπαϊκής Ένωσης για την Ασφάλεια Δικτύων και Πληροφοριών, διαθέτει όμως ενισχυμένο

ρόλο και μόνιμη εντολή. Επίσης έχει υιοθετήσει το ίδιο αρκτικόλεξο (ENISA). Ο φορέας παρέχει στήριξη στα κράτη μέλη, τα θεσμικά όργανα της ΕΕ και λοιπούς ενδιαφερόμενους φορείς για την αντιμετώπιση κυβερνοεπιθέσεων

Οδηγία για τα συστήματα δικτύου και πληροφοριών

Η οδηγία για την ασφάλεια των συστημάτων δικτύου και πληροφοριών (ΣΔΠ) θεσπίστηκε το 2016 και αποτελεί το πρώτο νομοθετικό μέτρο εμβέλειας Ευρωπαϊκής Ένωσης με στόχο την ενίσχυση της συνεργασίας μεταξύ των κρατών μελών όσον αφορά το κρίσιμο ζήτημα της κυβερνοασφάλειας. Θεσπίζει υποχρεώσεις ασφάλειας για τους φορείς εκμετάλλευσης βασικών υπηρεσιών (σε ζωτικούς τομείς όπως η ενέργεια, οι μεταφορές, η υγεία και ο χρηματοοικονομικός κλάδος) και για τους παρόχους ψηφιακών υπηρεσιών (διαδικτυακές αγορές, μηχανές αναζήτησης και υπηρεσίες υπολογιστικού νέφους).

Τον Δεκέμβριο του 2020 η Ευρωπαϊκή Επιτροπή πρότεινε αναθεωρημένη οδηγία για τα ΣΔΠ (ΣΔΠ2) προς αντικατάσταση της οδηγίας του 2016. Η νέα πρόταση ανταποκρίνεται στο εξελισσόμενο τοπίο των απειλών και λαμβάνει υπόψη τον ψηφιακό μετασχηματισμό της κοινωνίας μας, τον οποίο έχει επιταχύνει η κρίση της COVID-19.

Οι νέοι κανόνες είναι οι εξής:

- θα ορίζουν αυστηρότερες υποχρεώσεις ασφάλειας για τις εταιρείες
- θα καλύπτουν την ασφάλεια των αλυσίδων εφοδιασμού
- θα θεσπίζουν αυστηρότερα εποπτικά μέτρα για τις εθνικές αρχές
- θα ενισχύουν περαιτέρω την ανταλλαγή πληροφοριών και τη συνεργασία

Η πρόταση συζητείται επί του παρόντος στους κόλπους του Συμβουλίου.

Καταπολέμηση του κυβερνοεγκλήματος

Όπως συζητήσαμε νωρίτερα, το κυβερνοέγκλημα λαμβάνει διάφορες μορφές και πολλά κοινά εγκλήματα διευκολύνονται από τον κυβερνοχώρο. Για παράδειγμα, οι εγκληματίες μπορούν:

- να αποκτούν τον έλεγχο προσωπικών συσκευών χρησιμοποιώντας κακόβουλο λογισμικό
- να κλέβουν ή να παραβιάζουν προσωπικά δεδομένα και διανοητική ιδιοκτησία για τη διάπραξη διαδικτυακής απάτης
- να χρησιμοποιούν διαδικτυακές πλατφόρμες και μέσα κοινωνικής δικτύωσης για να διανέμουν παράνομο περιεχόμενο
- να χρησιμοποιούν το «σκοτεινό δίκτυο» (darknet) για να πωλούν παράνομα προϊόντα και να παρέχουν υπηρεσίες αθέμιτης παρείσφρησης (hacking)

Ορισμένες μορφές κυβερνοεγκλήματος, όπως η σεξουαλική εκμετάλλευση παιδιών στο διαδίκτυο, προκαλούν σοβαρή βλάβη στα θύματά τους.

Στους κόλπους της Europol έχει δημιουργηθεί ένα ειδικευμένο Ευρωπαϊκό Κέντρο για το Κυβερνοέγκλημα, το οποίο βοηθά τις χώρες της ΕΕ να ερευνούν ηλεκτρονικά εγκλήματα και να εξαρθρώνουν εγκληματικά δίκτυα γνωστό ως EMPACT. Η EMPACT (European

Multidisciplinary Platform Against Criminal Threats) είναι μια πρωτοβουλία ασφάλειας που καθοδηγείται από τα κράτη μέλη της ΕΕ για τον εντοπισμό, την ιεράρχηση και την αντιμετώπιση των απειλών που δημιουργεί το οργανωμένο και σοβαρό διεθνές έγκλημα.

Αντιμετώπιση κυβερνοεπιθέσεων

Το σχέδιο δράσης της EMPACT (European Multidisciplinary Platform Against Criminal Threats) για τις κυβερνοεπιθέσεις στοχεύει στην πάταξη εγκληματικών δραστηριοτήτων που σχετίζονται με επιθέσεις κατά συστημάτων πληροφοριών, ιδίως όσων ακολουθούν το επιχειρηματικό μοντέλο «crime-as-a-service» —όπου το έγκλημα μετατρέπεται σε υπηρεσία που μπορεί κανείς να προμηθευτεί— και λειτουργούν ως παράγοντες διευκόλυνσης του διαδικτυακού εγκλήματος.

Καταπολέμηση της απάτης στις πληρωμές χωρίς μετρητά

Η απάτη και η πλαστογραφία που σχετίζονται με τα μέσα πληρωμής πλην των μετρητών συνιστούν σοβαρή απειλή για την ασφάλεια της ΕΕ και αποφέρουν σημαντικό εισόδημα στο οργανωμένο έγκλημα. Επιπλέον, αυτού του είδους η απάτη πλήττει την εμπιστοσύνη των καταναλωτικού κοινού στην ασφάλεια των ψηφιακών τεχνολογιών.

Το ειδικό σχέδιο δράσης της EMPACT θέτει στο στόχαστρο τους εγκληματίες που εμπλέκονται σε δραστηριότητες απάτης και παραχάραξης που αφορούν μέσα πληρωμής πλην των μετρητών, συμπεριλαμβανομένης της μεγάλης κλίμακας απάτης με κάρτες πληρωμής και των αναδυόμενων απειλών για άλλα μέσα πληρωμής πλην των μετρητών.

Βελτίωση της ασφάλειας των παιδιών στο διαδίκτυο

Η Ευρωπαϊκή Επιτροπή σκοπεύει να προτείνει νέα νομοθεσία το 2021 για την αντιμετώπιση της σεξουαλικής κακοποίησης και εκμετάλλευσης παιδιών στο διαδίκτυο. Εντωμεταξύ, η ΕΕ επεξεργάζεται προσωρινούς κανόνες που θα επιτρέψουν στους παρόχους υπηρεσιών ηλεκτρονικού ταχυδρομείου και υπηρεσιών ανταλλαγής μηνυμάτων μέσω του ιστού να συνεχίσουν να ανιχνεύουν περιεχόμενο σεξουαλικής κακοποίησης παιδιών στο διαδίκτυο, μέχρι να υπάρξει μόνιμη νομοθετική ρύθμιση.

Το ειδικό σχέδιο δράσης της EMPACT στοχεύει στην καταπολέμηση της σεξουαλικής κακοποίησης και της σεξουαλικής εκμετάλλευσης παιδιών, συμπεριλαμβανομένης της παραγωγής και διάδοσης υλικού κακοποίησης παιδιών.

Δικαιοσύνη και επιβολή του νόμου

Οι κανόνες και οι πολιτικές της ΕΕ καλύπτουν επίσης άλλες πτυχές της καταπολέμησης του κυβερνοεγκλήματος και του εγκλήματος γενικότερα οι οποίες άπτονται της δικαιοσύνης και της επιβολής του νόμου, όπως η πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία, η κρυπτογράφηση και η διατήρηση δεδομένων.

Πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία

Οι εγκληματίες εκμεταλλεύονται την ψηφιακή τεχνολογία για να διαπράττουν αδικήματα και να αποκρύπτουν παράνομες δραστηριότητες. Ως εκ τούτου, οι υπηρεσίες επιβολής του νόμου και οι δικαστικές αρχές βασίζονται όλο και περισσότερο για τις ποινικές έρευνες και διώξεις τους σε ηλεκτρονικά αποδεικτικά στοιχεία, όπως τα SMS, τα μηνύματα ηλεκτρονικού ταχυδρομείου και οι εφαρμογές ανταλλαγής μηνυμάτων.

Κρυπτογράφηση

Η ΕΕ προσπαθεί να καθιερώσει έναν δυναμικό διάλογο με τον κλάδο της τεχνολογίας, προκειμένου να βρεθεί η σωστή ισορροπία ανάμεσα στη συνεχιζόμενη χρήση ισχυρής κρυπτογραφικής τεχνολογίας και στην κατοχύρωση της εξουσίας των υπηρεσιών επιβολής του νόμου και της δικαιοσύνης να λειτουργούν με τους ίδιους όρους που ισχύουν για τη λειτουργία τους εκτός του διαδικτύου.

Διατήρηση δεδομένων

Για την αποτελεσματική καταπολέμηση του εγκλήματος σήμερα, είναι σημαντικό οι πάροχοι υπηρεσιών να διατηρούν ορισμένα δεδομένα τα οποία μπορούν να κοινοποιούνται υπό ορισμένες αυστηρές προϋποθέσεις με σκοπό την πάταξη του εγκλήματος. Ωστόσο, η διατήρηση δεδομένων μπορεί να παραβιάζει ατομικά θεμελιώδη δικαιώματα, ιδίως τα δικαιώματα της ιδιωτικότητας και της προστασίας των προσωπικών δεδομένων.

Ενίσχυση της κυβερνοδιπλωματίας

Η Ευρωπαϊκή Ένωση και τα κράτη μέλη της προωθούν δυναμικά έναν ανοικτό, ελεύθερο, σταθερό και ασφαλή κυβερνοχώρο, όπου θα εξασφαλίζεται πλήρως ο σεβασμός των ανθρωπίνων δικαιωμάτων, των θεμελιωδών ελευθεριών και του κράτους δικαίου, με στόχο την κοινωνική σταθερότητα, την οικονομική μεγέθυνση, την ευημερία καθώς και την ακεραιότητα της ελευθερίας και της δημοκρατικότητας των κοινωνιών.

Η ΕΕ καταβάλλει σημαντικές προσπάθειες για την προστασία της από κυβερνοαπειλές προερχόμενες από τρίτες χώρες, ιδίως μέσω της ανάπτυξης κοινής διπλωματικής αντίδρασης με την ονομασία «εργαλειοθήκη για τη διπλωματία στον κυβερνοχώρο». Η αντίδραση αυτή περιλαμβάνει διπλωματική συνεργασία και διάλογο, προληπτικά μέτρα κατά των κυβερνοεπιθέσεων και κυρώσεις.

Η στρατηγική της ΕΕ για την κυβερνοασφάλεια, την οποία ενέκριναν η Ευρωπαϊκή Επιτροπή και η ΕΥΕΔ τον Δεκέμβριο του 2020, ενισχύει τη διπλωματική αντίδραση της ΕΕ στις κυβερνοεπιθέσεις.

Κυρώσεις για την καταπολέμηση των κυβερνοεπιθέσεων

Τον Μάιο του 2019 το Συμβούλιο θέσπισε πλαίσιο που επιτρέπει στην ΕΕ να επιβάλλει στοχευμένες κυρώσεις ως μέσο αποτροπής και αντίδρασης σε κυβερνοεπιθέσεις που συνιστούν εξωτερική απειλή για την ίδια ή τα κράτη μέλη της.

Πιο συγκεκριμένα, το πλαίσιο αυτό επιτρέπει για πρώτη φορά στην ΕΕ να επιβάλλει κυρώσεις σε πρόσωπα ή οντότητες που ευθύνονται για κυβερνοεπιθέσεις ή απόπειρες κυβερνοεπιθέσεων, παρέχουν οικονομική, τεχνική ή υλική υποστήριξη για την πραγματοποίηση τέτοιων επιθέσεων ή εμπλέκονται με άλλους τρόπους σε αυτές. Είναι επίσης δυνατή η επιβολή κυρώσεων σε άλλα συνδεόμενα πρόσωπα ή οντότητες.

Τα περιοριστικά μέτρα περιλαμβάνουν την απαγόρευση μετακίνησης προς την ΕΕ και την δέσμευση περιουσιακών στοιχείων φυσικών και νομικών προσώπων. Οι πρώτες κυρώσεις για κυβερνοεπιθέσεις επιβλήθηκαν στις 30 Ιουλίου 2020.

Προστασία των δικτύων 5G

Τα δίκτυα 5G είναι ζωτικής σημασίας όχι μόνο για την ψηφιακή επικοινωνία αλλά και για κρίσιμους τομείς όπως η ενέργεια, οι μεταφορές, οι τραπεζικές υπηρεσίες και η υγεία. Έχει συνεπώς καθοριστική σημασία για την κοινωνία μας να εξασφαλιστεί η ανθεκτικότητα των δικτύων 5G.

Με τα παγκόσμια έσοδα από το 5G να εκτιμώνται σε 225 δισ. € το 2025, οι τεχνολογίες 5G αποτελούν βασικό μοχλό για την ανταγωνιστικότητα της Ένωσης στην παγκόσμια αγορά και η κυβερνοασφάλειά τους είναι ζωτικής σημασίας για την εξασφάλιση της στρατηγικής αυτονομίας της Ένωσης.

Τον Ιανουάριο του 2020 η ΕΕ κατέληξε σε συμφωνία για μια εργαλειοθήκη με στόχο τον προσδιορισμό μιας πιθανής κοινής δέσμης μέτρων για τον μετριασμό των κύριων κινδύνων κυβερνοασφάλειας των δικτύων 5G και για την παροχή καθοδήγησης.

Η κυβερνοασφάλεια στην Ελλάδα

Με την απόφαση 34368/7-12-2020 του υπουργού ψηφιακής διακυβέρνησης εγκρίθηκε η Εθνική Στρατηγική Κυβερνοασφάλειας 2020 – 2025 (δείτε το έγγραφο ΑΔΑ: 6ΙΒΕ46ΜΤΛΠ-ΦΜ5 στην ψηφιακή υπηρεσία «Διαύγεια»).

Το όραμα:

«Ένα σύγχρονο και ασφαλές ψηφιακό περιβάλλον πληροφοριακών και δικτυακών υποδομών, εφαρμογών και υπηρεσιών προς όφελος της οικονομικής και κοινωνικής ευημερίας, με την εγγύηση της προστασίας των θεμελιωδών δικαιωμάτων των πολιτών, την ανάπτυξη κουλτούρας ασφαλούς χρήσης των ψηφιακών υπηρεσιών και εφαρμογών, και την επαύξηση της εμπιστοσύνης των πολιτών και επιχειρήσεων στις ψηφιακές τεχνολογίες.»

Ως βασικά στοιχεία του οράματος μπορούμε να αναφέρουμε τα εξής:

- Η οικοδόμηση ενός σύγχρονου ψηφιακού περιβάλλοντος: Ένα ψηφιακό περιβάλλον που επιτρέπει τη διαρκή ανάπτυξη και ενσωμάτωση των νέων τεχνολογιών και καινοτομιών στην ψηφιακή εποχή.
- Το υψηλό επίπεδο κυβερνοασφάλειας: Σε όλο το φάσμα των πληροφοριακών υποδομών, εφαρμογών και υπηρεσιών, προσαρμοσμένο στις διαρκώς μεταβαλλόμενες προκλήσεις και απαιτήσεις
- Η προστασία των θεμελιωδών δικαιωμάτων: Ιδίως των προσωπικών δεδομένων, της διαφύλαξης της ιδιωτικότητας, της ανάπτυξης της προσωπικότητας, της ισότητας και της συμμετοχής στην ψηφιακή κοινωνία
- Η ανάπτυξη κουλτούρας ασφαλούς χρήσης: Υπό την έννοια της ψηφιακής παιδείας, της διαρκούς ενημέρωσης και ευαισθητοποίησης στους κινδύνους και τις παγίδες των νέων τεχνολογιών
- Η επαύξηση της εμπιστοσύνης στην ψηφιακή διακυβέρνηση: Ως το βασικό επίτευγμα ενός ασφαλούς ψηφιακού περιβάλλοντος, δηλ. η αξιοποίηση των νέων τεχνολογιών σε όλο το φάσμα της κοινωνικής και οικονομικής ζωής προς όφελος των πολιτών και των επιχειρήσεων και της κοινωνικοοικονομικής ευημερία.

Σε ένα πρώτο επίπεδο, αξιοποιούνται τα αποτελέσματα της ανάλυσης των στρατηγικών προτεραιοτήτων, ώστε να διαμορφωθούν πέντε (5) συνολικά εμβληματικοί στόχοι ανάπτυξης του στρατηγικού σχεδιασμού, οι οποίοι καλύπτουν και τους δεκαπέντε ειδικούς στόχους ανάπτυξης στρατηγικής του ENISA για τα κράτη μέλη της Ε.Ε., ως εξής:

ΣΤΡΑΤΗΓΙΚΟΙ ΣΤΟΧΟΙ	ΚΑΛΥΠΤΟΜΕΝΟΙ ΣΤΟΧΟΙ ENISA ΓΙΑ ΚΡΑΤΗ ΜΕΛΗ
1. Ένα λειτουργικό σύστημα διακυβέρνησης	Ανάπτυξη εθνικών σχεδίων έκτακτης ανάγκης στον κυβερνοχώρο
	Συμμετοχή σε διεθνείς συνεργασίες
	Θεσμοθέτηση της συνεργασίας μεταξύ κυβερνητικών οργανισμών
2. Θωράκιση κρίσιμων υποδομών, ασφάλεια και νέες τεχνολογίες	Προστασία κρίσιμων δεδομένων και πληροφοριών
	Θέσπιση βασικών μέτρων ασφαλείας
	Εξισορρόπηση μεταξύ των απαιτήσεων ασφάλειας και της προστασίας της ιδιωτικότητας
3. Βελτιστοποίηση διαχείρισης περιστατικών, καταπολέμηση του κυβερνοεγκλήματος και προστασία της ιδιωτικότητας	Καθιέρωση μηχανισμών αναφοράς συμβάντων
	Καθιέρωση ικανότητας έγκαιρης αντιμετώπισης συμβάντων
	Αντιμετώπιση του εγκλήματος στον κυβερνοχώρο
4. Ένα σύγχρονο επενδυτικό περιβάλλον με έμφαση στην προαγωγή της Έρευνας και Ανάπτυξης	Προώθηση της Έρευνας και Ανάπτυξης
	Παροχή κινήτρων στον ιδιωτικό τομέα για επενδύσεις σε μέτρα ασφαλείας
	Αξιοποίηση Συμπράξεων Δημόσιου και Ιδιωτικού τομέα (ΣΔΙΤ)
5. Ανάπτυξη ικανοτήτων (capacity building), προαγωγή της ενημέρωσης και ευαισθητοποίησης	Ενίσχυση της ευαισθητοποίησης και εγρήγορσης των χρηστών
	Οργάνωση ασκήσεων ασφάλειας στον κυβερνοχώρο
	Ενίσχυση των προγραμμάτων κατάρτισης και εκπαίδευσης

Για κάθε έναν από τους ανωτέρω στρατηγικούς στόχους αναπτύσσονται ειδικοί στόχοι, οι οποίοι αποσκοπούν στην εξειδίκευση και καλύτερη διαχείριση του στρατηγικού πλαισίου (cascade effect). Οι ειδικοί στόχοι εξειδικεύονται, περαιτέρω, σε δραστηριότητες, οι οποίες καλύπτουν όλο το φάσμα της αναγνώρισης, πρόληψης και προστασίας, αποτροπής και ανάκαμψης από κυβερνοεπιθέσεις.

Μερικές πρακτικές δράσεις άμυνας απέναντι στις κυβερνοεπιθέσεις

Πέρα από τις πανευρωπαϊκές και εθνικές στρατηγικές κυβερνοάμυνας, υπάρχουν μερικές πρακτικές κατευθύνσεις οι οποίες μπορούν να θωρακίσουν, σε σημαντικό βαθμό, τα πληροφοριακά συστήματα που χρησιμοποιούμε καθημερινά. Αυτές οι κατευθύνσεις συμπεριλαμβάνουν τις εξής:

- Ανάλυση και αποτίμηση κινδύνων με χρήση τυπικών, ημι-τυπικών και άτυπων μεθόδων
- Καθορισμός πολιτικών, διαδικασιών, και τεχνικών ασφάλειας
- Διαχείριση/έλεγχος εγκατάστασης και ρύθμισης συσκευών και λογισμικού (ειδικότερα σε συσκευές IoT)
- Καθορισμός στρατηγικής αντιμετώπισης επιθέσεων και περιστατικών παραβίασης ασφάλειας
- Ενημέρωση και εκπαίδευση γύρω από την ασφάλεια πληροφοριακών συστημάτων
- Ασφάλεια φυσικών υποδομών
- Ασφάλεια προσωπικού
- Συνεχής επιτήρηση
- Μηχανισμοί ελέγχου πρόσβασης
- Μηχανισμοί ταυτοποίησης (biometrics, tokens, passwords)
- Μηχανισμοί καταγραφής και ελέγχου (logging και auditing)
- Τεχνικές κρυπτογράφησης και ανωνυμοποίησης δεδομένων
- Ασφάλεια περιμέτρου (cloud και edge)
- Συστήματα ανίχνευσης/αντιμετώπισης εισβολών (και σε συσκευές IoT)
- Πρωτόκολλα καθορισμού και ελέγχου παραμέτρων ασφάλειας
- Διαρκώς ενημερωμένα λογισμικά προστασίας (Anti-viral, anti-spyware, anti-spam software)
- Χρήση secure tokens, σε περίπτωση που οι απαιτήσεις ασφάλειας είναι υψηλές

Οι αντίπαλοι επιτίθενται στον πιο αδύναμο κρίκο ... Ποιος είναι ο δικός μας;

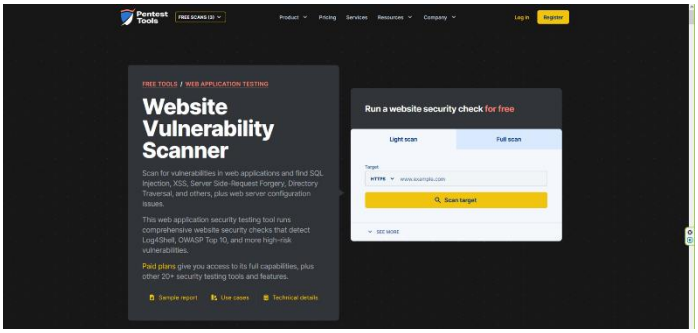
Δραστηριότητα 1

Περιγραφή: Εντοπισμός αδυναμιών εξυπηρετητών με δωρεάν διαδικτυακά εργαλεία

Χρόνος: 60 λεπτά

Στόχος: Να μπορούν οι εκπαιδευόμενοι να ανιχνεύουν ευάλωτα σημεία εξυπηρετητών με χρήση δωρεάν διαδικτυακών εργαλείων

Στην ιστοσελίδα https://pentest-tools.com/website-vulnerability-scanning/website-scanner θα βρείτε ένα εργαλείο ανίχνευσης ευάλωτων σημείων εξυπηρετητών, με αρχική οθόνη την εξής:



Πειραματιστείτε με διάφορες διευθύνσεις υπηρεσιών του διαδικτύου και δείτε τις αναφορές που εμφανίζει το εργαλείο. Προσπαθήστε να εντοπίσετε τα ευάλωτα σημεία που αναφέρονται και να βρείτε, με αναζήτηση στο διαδίκτυο, τις απειλές που αυτά ενέχουν.

Δραστηριότητα 2
Περιγραφή: Διαπίστωση ασφάλειας εξυπηρετητών μέσω των ψηφιακών πιστοποιητικών τους – διαπίστωση χρήσης του πρωτοκόλλου ασφαλούς επικοινωνίας SSL/TLS **Χρόνος**: 60 λεπτά **Στόχος**: Να μπορούν οι εκπαιδευόμενοι να επιβεβαιώνουν την ταυτότητα ενός εξυπηρετητή μέσα από τα στοιχεία του ψηφιακού του πιστοποιητικού 1. Σε έναν browser, πληκτρολογήστε το όνομα του site που σας ενδιαφέρει με https στην αρχή (κρυπτογράφηση), για παράδειγμα, https://www.upatras.gr 2. Επάνω στον browser, στη γραμμή διεύθυνσης θα σας εμφανίσει το https και το λουκέτο – χαρακτηριστικό του SSL, με πράσινο χρώμα. 3. Κάντε κλικ επάνω στο λουκέτο και επιλέξτε Connection Secure και μετά More Information. Στο νέο παράθυρο διαλόγου που θα εμφανιστεί, επιλέξτε Security και μετά View Certificate 4. Στο νέο παράθυρο διαλόγου, εμφανίζονται οι ημερομηνίες έναρξης και λήξης του πιστοποιητικού που έχετε εγκαταστήσει. ΣΗΜΕΙΩΣΗ: Τις παραπάνω πληροφορίες μπορείτε να τις δείτε για όλα τα site που επισκέπτεστε, καθώς είναι πληροφορία που εμφανίζει ο browser.

Σύνοψη

Στην ψηφιακή εποχή που διανύουμε, οι βασικοί πυλώνες ανάπτυξης είναι οι καινοτομίες στο που προκύπτουν από τις ραγδαίες τεχνολογικές εξελίξεις. Αυτές οι καινοτομίες θα παρέχουν στις επιχειρήσεις και στους οργανισμούς τις ευκαιρίες που θα οδηγήσουν στην ανάπτυξή και στην ανταγωνιστικότητά τους σε ένα γρήγορα μεταβαλλόμενο ψηφιακό οικονομικό και κοινωνικό περιβάλλον. Ένας σημαντικός παράγοντας της ανάπτυξης αυτής, όμως, είναι και η επιβίωση σε ένα, επίσης, διαρκώς εξελισσόμενο τοπίο κυβερνοεπιθέσεων οι οποίες γίνονται όλο και πιο απειλητικές και καταστροφικές για την επιχειρηματικότητα.

Στην ενότητα αυτή παρουσιάσαμε τα προβλήματα που μπορούν να δημιουργήσουν οι κυβερνοεπιθέσεις καθώς και κάποιες στρατηγικές αντιμετώπισής τους με στόχο είτε την αποφυγή τους ή, τουλάχιστον, την μετρίαση των επιπτώσεών τους στους οργανισμούς και τις επιχειρήσεις. Πιστεύουμε ότι η επόμενη γενιά που θα στηρίξει την ψηφιακή επιχειρηματικότητα και οικονομία θα πρέπει να είναι έτοιμη να ανταπεξέλθει και στις προκλήσεις του κυβερνοεγκλήματος, τουλάχιστον να έχει συνείδηση του κινδύνου και εγρήγορση για την αποτελεσματική αντιμετώπισή του.

Ασκήσεις αυτό-αξιολόγησης

1) Τα πιο κάτω είναι βασικοί πυλώνες του Ηλεκτρονικού Εμπορίου εκτός από έναν:

α. Ηλεκτρονικές πληρωμές

β. Κρυπτογραφία

γ. Διαδίκτυο

δ. Κάρτες ανάληψης μετρητών

2) Η ασφάλεια της κρυπτογραφίας πρέπει να στηρίζεται στο εξής:

α. Την κατάλληλη επιλογή κλειδιού (μήκος και ποιότητα)

β. Να διατηρείται μυστικός ο κρυπταλγόριθμος

γ. Να διατηρείται μυστικό το δημόσιο κλειδί

δ. Να τρέχει ο κρυπταλγόριθμος σε υλικό και όχι σε λογισμικό

3) Τα ηλεκτρονικά πιστοποιητικά βασίζονται κυρίως

α. Στην κρυπτογραφία δημόσιου κλειδιού

β. Στην κρυπτογραφία διαμοιραζόμενου κλειδιού

γ. Σε ψηφιοποιημένες (ως εικόνες, μέσω scanner) υπογραφές

δ. Σε συναρτήσεις κατακερματισμού (hash functions)

4) Η κρυπτογραφία δημόσιου κλειδιού χρησιμοποιείται για όλα τα πιο κάτω εκτός από ένα:

α. Ταυτοποίηση προσώπων

β. Ηλεκτρονικές υπογραφές

γ. Αποστολή κρυπτογραφημένων μηνυμάτων

δ. Τον εντοπισμού κακόβουλου λογισμικού σε αρχεία

5) Ένα βασικό χαρακτηριστικό της συμμετρικής κρυπτογράφησης είναι και το εξής:

α. Επιτυγχάνει χαμηλότερες ταχύτητες κρυπτογράφησης από την μη συμμετρική κρυπτογράφηση.

β. Κρυπταναλύεται εύκολα και, γι’ αυτό, δεν χρησιμοποιείται σε εφαρμογές ηλεκτρονικού εμπορίου.

γ. Τα επικοινωνούντα μέρη μοιράζονται το ίδιο κλειδί κρυπτογράφησης/αποκρυπτογράφησης.

δ. Τα επικοινωνούντα μέρη δεν μοιράζονται το ίδιο κλειδί κρυπτογράφησης/αποκρυπτογράφησης αλλά έχουν διαφορετικά κλειδιά το καθένα.

6) Η ψηφιακή/ηλεκτρονική υπογραφή είναι:

α. Η ψηφιοποιημένη (ως εικόνα), χειρόγραφη υπογραφή ενός ατόμου.

β. Ένα ζεύγος αριθμών, ο ένας αντίστροφος του άλλου, με τον έναν εκ των οποίων μετασχηματίζεται (υπογράφεται) το μήνυμα ενώ με τον άλλον πιστοποιείται η γνησιότητα της υπογραφής.

γ. Ένας αριθμός με τον οποίο μετασχηματίζεται (υπογράφεται) το μήνυμα και με τον οποίο, επίσης, πιστοποιείται η γνησιότητα της υπογραφής.

δ. Ένα ζεύγος αλγορίθμων συμμετρικής και μη συμμετρικής κρυπτογράφησης ο ένας εκ των οποίων «υπογράφει» το μήνυμα ενώ ό άλλος πιστοποιεί την γνησιότητα της υπογραφής.

7) Για το firewall ισχύουν όλα τα πιο κάτω εκτός από ένα:

α. Το firewall απλοποιεί τη διαχείριση ασφάλειας ενός οργανισμού, αφού ο έλεγχος προσπέλασης στο δίκτυο επικεντρώνεται κυρίως σε αυτό το σημείο.

β. Το firewall εφαρμόζει έλεγχο προσπέλασης από και προς το Διαδίκτυο.

γ. Το firewall προστατεύει τους χρήστες και το δίκτυο ενός οργανισμού από το κακόβουλο λογισμικό (π.χ. ιούς).

δ. Το firewall προσφέρει αποτελεσματική καταγραφή της δραστηριότητας στο δίκτυο ενός οργανισμού.

8) Η τιμή hash για ένα αρχείο διευκολύνει την εξής λειτουργία:

α. Την ταυτοποίηση του αποστολέα του αρχείου.

β. Τον έλεγχο ακεραιότητας του αρχείου.

γ. Τον έλεγχο γνησιότητας του αρχείου.

δ. Τον εντοπισμού κακόβουλου λογισμικού σε αυτό.

9) Η χρήση του πρωτοκόλλου SSL./TLS στις συναλλαγές μας είναι απαραίτητη διότι:

α. Χωρίς την ενεργοποίηση του SSL/TLS δεν μπορούν να λειτουργήσουν οι browsers (φυλλομετρητές) του υπολογιστή μας.

β. Με το SSL/TLS γίνεται καλύτερη αναζήτηση προϊόντων στο Διαδίκτυο.

γ. Το Διαδίκτυο δεν εξασφαλίζει την έγκαιρη παράδοση των μηνυμάτων που διακινούνται στις συναλλαγές.

δ. Το Διαδίκτυο δεν διασφαλίζει το απόρρητο των δεδομένων των συναλλαγών.

10) Ένα βασικό χαρακτηριστικό της μη συμμετρικής κρυπτογράφησης είναι και το εξής:

α. Επιτυγχάνει υψηλότερες ταχύτητες κρυπτογράφησης από την συμμετρική κρυπτογράφηση.

β. Κρυπταναλύεται εύκολα και δεν χρησιμοποιείται συχνά σε εφαρμογές ηλεκτρονικού εμπορίου.

γ. Τα επικοινωνούντα μέρη δεν μοιράζονται το ίδιο κλειδί κρυπτογράφησης/αποκρυπτογράφησης αλλά έχουν διαφορετικά κλειδιά το καθένα.

δ. Τα επικοινωνούντα μέρη μοιράζονται το ίδιο κλειδί κρυπτογράφησης/αποκρυπτογράφησης.

Αναφορές

Stallings, W. (2012). Κρυπτογραφία και Ασφάλεια Δικτύων. Εκδόσεις ΙΩΝ.

Γκρίτζαλης Σ., Κάτσικας Σ., Χρυσικόπουλος Β., & Burmester Μ (επιμελητές συλλογικού τόμου). (2011). Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές. Εκδόσεις Παπασωτηρίου.

Χρηματοδότηση

Το παρόν εκπαιδευτικό υλικό (κείμενο, εικόνες, διαγράμματα, κλπ.) έχει αναπτυχθεί στο πλαίσιο της Πράξης «Υποστήριξη Δράσεων Στήριξης της Επιχειρηματικότητας, Καινοτομίας και Ωρίμανσης για την Αξιοποίηση της Ερευνητικής Δραστηριότητας και των Νέων Προϊόντων και Υπηρεσιών που αναπτύσσονται στο Πανεπιστήμιο Πατρών» - «ΜΕΤΩΝ, MIS 5132546».

Η πράξη «ΜΕΤΩΝ» υλοποιείται στο πλαίσιο του Ε.Π. «ΑΝΑΠΤΥΞΗ ΑΝΘΡΩΠΙΝΟΥ ΔΥΝΑΜΙΚΟΥ, ΕΚΠΑΙΔΕΥΣΗ & ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από Εθνικούς πόρους.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

Επιχειρησιακό Πρόγραμμα
Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Διά Βίου Μάθηση
Ειδική Υπηρεσία Διαχείρισης
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΣΠΑ 2014-2020
ανάπτυξη - εργασία - αλληλεγγύη

Σημειώματα

Σημείωμα Ιστορικού Εκδόσεων Έργου

Το παρόν έργο αποτελεί την έκδοση 1.0

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης

Ως **Μη Εμπορική** ορίζεται η χρήση:

- που δεν περιλαμβάνει άμεσο ή έμμεσο οικονομικό όφελος από την χρήση του έργου, για το διανομέα του έργου και αδειοδόχο
- που δεν περιλαμβάνει οικονομική συναλλαγή ως προϋπόθεση για τη χρήση ή πρόσβαση στο έργο
- που δεν προσπορίζει στο διανομέα του έργου και αδειοδόχο έμμεσο οικονομικό όφελος (π.χ. διαφημίσεις) από την προβολή του έργου σε διαδικτυακό τόπο

Ο δικαιούχος μπορεί να παρέχει στον αδειοδόχο ξεχωριστή άδεια να χρησιμοποιεί το έργο για εμπορική χρήση, εφόσον αυτό του ζητηθεί.

Διατήρηση Σημειωμάτων

Οποιαδήποτε αναπαραγωγή ή διασκευή του υλικού θα πρέπει να συμπεριλαμβάνει:

- το Σημείωμα Αναφοράς
- το Σημείωμα Αδειοδότησης
- τη δήλωση Διατήρησης Σημειωμάτων
- το Σημείωμα Χρήσης Έργων Τρίτων (εφόσον υπάρχει)

μαζί με τους συνοδευόμενους υπερσυνδέσμους.

Σημείωμα Χρήσης Έργων Τρίτων

Το Έργο αυτό κάνει χρήση των ακόλουθων έργων: