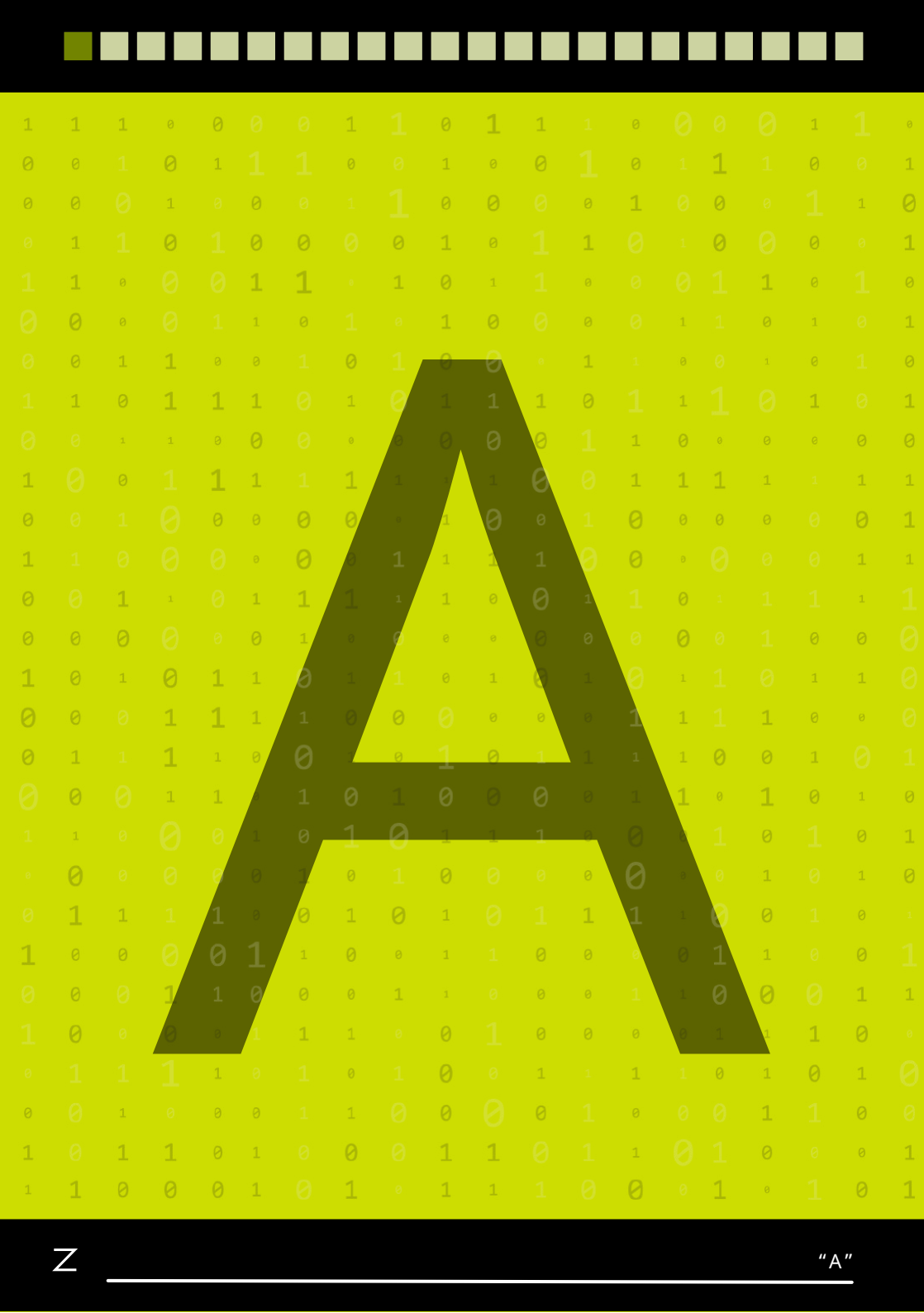
Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ'ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή του OeAD-GmbH. Ούτε η Ευρωπαϊκή Ένωση ούτε η χορηγούσα αρχή μπορούν να θεωρηθούν υπεύθυνες για αυτές. Αριθμός έργου: 2023-1-AT01-KA220-ADU-000157050

Εδώ θα βρείτε την περιγραφή κάθε άγνωστου όρου που συναντήσατε στο ηλεκτρονικό βιβλίο DataGame ή που μπορεί να συναντήσετε στις μελλοντικές σας προσπάθειες στον τομέα της ιδιωτικότητας και της προστασίας των δεδομένων. Ένα Γλωσσάριο είναι πολύ χρήσιμο όταν μπαίνετε σε αυτά τα νερά.

Και ναι, το παίρνουμε όντως τόσο σοβαρά ώστε να αισθανόμαστε την ανάγκη να εξηγήσουμε τον όρο "Διαδίκτυο".

. . . Κι αν έρχεστε από άλλον πλανήτη;


A

Έλεγχος πρόσβασης - Μηχανισμοί και πολιτικές που ρυθμίζουν ποιος μπορεί να βλέπει ή να χρησιμοποιεί πόρους σε ένα υπολογιστικό περιβάλλον.

Λίστα ελέγχου πρόσβασης (ACL) - Μια λίστα δικαιωμάτων που επισυνάπτεται σε ένα αντικείμενο και καθορίζει ποιοι χρήστες ή συστήματα επιτρέπεται να έχουν πρόσβαση σε αυτό και ποιες ενέργειες μπορούν να εκτελέσουν.

Διαχείριση πρόσβασης - Η διαδικασία διαχείρισης της πρόσβασης των χρηστών σε πόρους και δεδομένα εντός ενός οργανισμού.

Λογοδοσία - Η αρχή ότι ένας οργανισμός ή ένα άτομο είναι υπεύθυνος για τις πράξεις και τις αποφάσεις του, ιδίως όσον αφορά το απόρρητο και την ασφάλεια των δεδομένων.

Active Directory - Μια υπηρεσία της Microsoft για τη διαχείριση των δικαιωμάτων και της πρόσβασης σε δικτυακούς πόρους εντός ενός περιβάλλοντος τομέα.

Λογαριασμός διαχειριστή - Ένας λογαριασμός χρήστη με αυξημένα προνόμια που επιτρέπει τη διαχείριση των ρυθμίσεων του συστήματος και των λογαριασμών χρηστών.

Advanced Encryption Standard (AES) - Ένας συμμετρικός αλγόριθμος κρυπτογράφησης που χρησιμοποιείται ευρέως για την ασφάλεια δεδομένων και θεωρείται ιδιαίτερα ασφαλής και αποδοτικός.

Advanced Persistent Threat (APT) - Παρατεταμένη και στοχευμένη επίθεση στον κυβερνοχώρο, όπου ο επιτιθέμενος αποκτά μη εξουσιοδοτημένη πρόσβαση σε ένα δίκτυο και παραμένει απαρατήρητος για παρατεταμένο χρονικό διάστημα.

Adware - Λογισμικό που εμφανίζει ή κατεβάζει αυτόματα διαφημιστικό υλικό (συχνά ανεπιθύμητο) όταν ο χρήστης βρίσκεται στο διαδίκτυο.

Ανίχνευση ανωμαλιών - Η διαδικασία εντοπισμού ασυνήθιστων μοτίβων ή αποκλίσεων από την κανονική συμπεριφορά που μπορεί να υποδεικνύουν απειλή για την ασφάλεια.

Ανωνυμοποίηση - Η διαδικασία αφαίρεσης πληροφοριών προσωπικής ταυτοποίησης από σύνολα δεδομένων, έτσι ώστε τα άτομα να μην μπορούν να αναγνωριστούν εύκολα.

Anti-Malware - Λογισμικό σχεδιασμένο για τον εντοπισμό, την πρόληψη και την αφαίρεση κακόβουλου λογισμικού, συμπεριλαμβανομένων ιών, σκουληκιών και spyware.

Antiphishing - Τεχνικές και εργαλεία που χρησιμοποιούνται για την αποτροπή επιθέσεων phishing, οι οποίες επιχειρούν να εξαπατήσουν άτομα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες.

Ασφάλεια API - Η πρακτική της διασφάλισης των διεπαφών προγραμματισμού εφαρμογών για την αποτροπή μη εξουσιοδοτημένης πρόσβασης και παραβίασης δεδομένων.

Ασφάλεια εφαρμογών - Η πρακτική της προστασίας των εφαρμογών από απειλές και ευπάθειες καθ' όλη τη διάρκεια του κύκλου ζωής τους.

Ευπάθεια εφαρμογής - Μια αδυναμία σε μια εφαρμογή που μπορεί να αξιοποιηθεί από επιτιθέμενους για να παραβιάσουν την ασφάλεια ή να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα.

Λευκή λίστα εφαρμογών - Ένα μέτρο ασφαλείας που επιτρέπει την εκτέλεση μόνο εγκεκριμένων εφαρμογών σε ένα σύστημα, αποκλείοντας όλες τις άλλες.

Ασύμμετρη κρυπτογράφηση - Ένας τύπος κρυπτογράφησης που χρησιμοποιεί ένα ζεύγος κλειδιών (δημόσιο και ιδιωτικό) για την ασφαλή μετάδοση δεδομένων, όπου το ένα κλειδί κρυπτογραφεί τα δεδομένα και το άλλο κλειδί τα αποκρυπτογραφεί.

Τεχνητή νοημοσύνη (ΤΝ) στην ασφάλεια - Η χρήση τεχνολογιών ΤΝ για τη βελτίωση των μέτρων ασφαλείας, όπως η ανίχνευση απειλών, η αξιολόγηση κινδύνων και η αντιμετώπιση περιστατικών.

Διαχείριση περιουσιακών στοιχείων - Η διαδικασία διαχείρισης και διασφάλισης των φυσικών και ψηφιακών περιουσιακών στοιχείων ενός οργανισμού, συμπεριλαμβανομένου του υλικού, του λογισμικού και των δεδομένων.

Επιφάνεια επίθεσης - Η συνολική περιοχή ή το σύνολο των σημείων εισόδου σε ένα σύστημα ή δίκτυο που θα μπορούσαν να αξιοποιηθούν από επιτιθέμενους.

Φορέας επίθεσης - Η μέθοδος ή το μονοπάτι που χρησιμοποιούν οι επιτιθέμενοι για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα ή δίκτυο.

Έλεγχος - Συστηματική εξέταση ενός συστήματος ή μιας διαδικασίας για τη διασφάλιση της συμμόρφωσης με τις πολιτικές ασφαλείας και τον εντοπισμό περιοχών για βελτίωση.

Audit Log - Μια λεπτομερής καταγραφή των συμβάντων του συστήματος, συμπεριλαμβανομένων των ενεργειών των χρηστών και των αλλαγών του συστήματος, που χρησιμοποιείται για την παρακολούθηση της ασφάλειας και τη συμμόρφωση.

Audit Trail - Μια χρονολογική καταγραφή γεγονότων, ενεργειών ή αλλαγών σε ένα σύστημα που βοηθά στην παρακολούθηση και τον έλεγχο των δραστηριοτήτων των χρηστών.

Αυθεντικοποίηση - Η διαδικασία επαλήθευσης της ταυτότητας ενός χρήστη ή ενός συστήματος, συχνά μέσω κωδικών πρόσβασης, βιομετρικών στοιχείων ή άλλων μεθόδων.

Αυθεντικοποίηση Token - Ένα ψηφιακό αντικείμενο που χρησιμοποιείται για την απόδειξη της ταυτότητας ενός χρήστη και την παροχή ασφαλούς πρόσβασης σε ένα σύστημα, συχνά με τη μορφή συσκευής υλικού ή κώδικα που βασίζεται σε λογισμικό.

Εξουσιοδότηση - Η διαδικασία προσδιορισμού του κατά πόσον ένας χρήστης ή ένα σύστημα έχει το δικαίωμα πρόσβασης ή εκτέλεσης ορισμένων ενεργειών σε έναν πόρο.

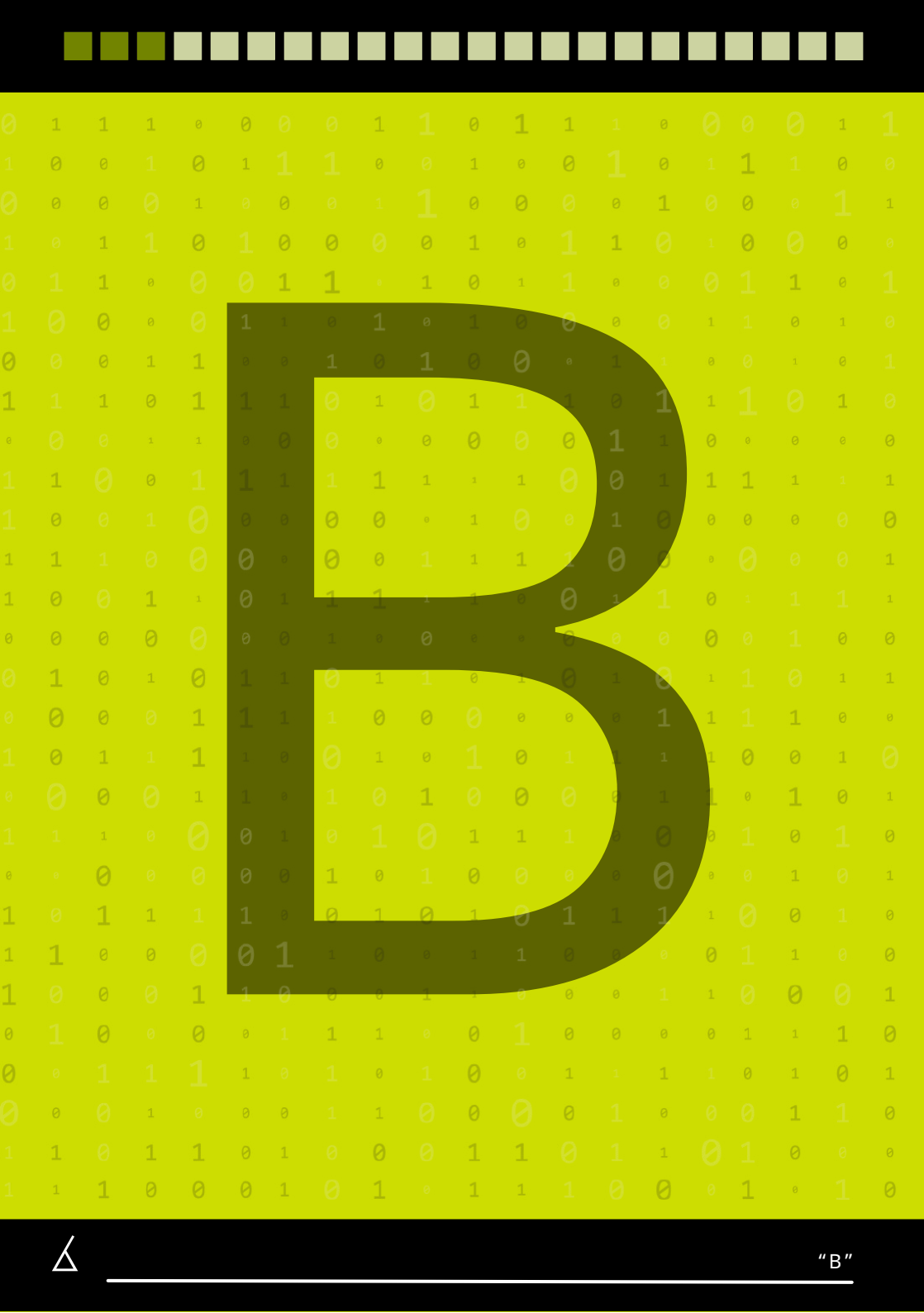
Πρωτόκολλο εξουσιοδότησης – Ένα σύνολο κανόνων και διαδικασιών για τον καθορισμό και την επιβολή δικαιωμάτων πρόσβασης σε πόρους και εκτέλεσης ενεργειών.

Automated Backup – Μια διαδικασία δημιουργίας αντιγράφων ασφαλείας που προγραμματίζεται και εκτελείται αυτόματα, μειώνοντας την ανάγκη για χειροκίνητη παρέμβαση.

Αυτοματοποιημένη ανίχνευση απειλών – Η χρήση αυτοματοποιημένων εργαλείων και τεχνολογιών για τον εντοπισμό και την αντιμετώπιση πιθανών απειλών ασφαλείας σε πραγματικό χρόνο.

Διαθεσιμότητα – Η διασφάλιση ότι τα δεδομένα και οι πόροι είναι προσβάσιμα στους εξουσιοδοτημένους χρήστες όταν χρειάζεται, μέρος της τριάδας CIA (Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα) στην ασφάλεια πληροφοριών.

Αρχιτεκτονική μηδενικής εμπιστοσύνης – Ένα μοντέλο ασφάλειας που υποθέτει ότι κανένα δίκτυο, συσκευή ή χρήστης δεν είναι εξ ορισμού αξιόπιστο και ότι η πρόσβαση χορηγείται μόνο μετά από συνεχή επαλήθευση της ταυτότητας και της κατάστασης ασφαλείας.


B

Backdoor – Μια κρυφή ή μη εξουσιοδοτημένη μέθοδος πρόσβασης σε ένα σύστημα ή δίκτυο, η οποία συχνά δημιουργείται από επιτιθέμενους ή κακόβουλο λογισμικό για την παράκαμψη των συνήθων ελέγχων ασφαλείας.

Δημιουργία αντιγράφου ασφαλείας – Ένα αντίγραφο δεδομένων ή αρχείων συστήματος που αποθηκεύεται ξεχωριστά για την αποφυγή απώλειας σε περίπτωση βλάβης ή συμβάντος απώλειας δεδομένων.

Δημιουργία αντιγράφων ασφαλείας και ανάκτηση – Διαδικασίες και τεχνολογίες που χρησιμοποιούνται για τη δημιουργία αντιγράφων ασφαλείας δεδομένων και την επαναφορά τους σε περίπτωση απώλειας ή καταστροφής δεδομένων.

Κρυπτογράφηση αντιγράφων ασφαλείας – Η πρακτική της κρυπτογράφησης δεδομένων αντιγράφων ασφαλείας για τη διασφάλιση της εμπιστευτικότητάς τους και την αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Συχνότητα δημιουργίας αντιγράφων ασφαλείας – Το χρονικό διάστημα στο οποίο εκτελούνται τα αντίγραφα ασφαλείας, το οποίο μπορεί να κυμαίνεται από ωριαία έως ετήσια, ανάλογα με την κρισιμότητα των δεδομένων.

Ακεραιότητα αντιγράφων ασφαλείας – Η διαβεβαίωση ότι τα δεδομένα αντιγράφων ασφαλείας είναι πλήρη, ακριβή και αξιόπιστα και δεν έχουν αλλοιωθεί ή καταστραφεί.

Πολιτική αντιγράφων ασφαλείας – Ένα σύνολο κατευθυντήριων γραμμών και διαδικασιών για τη δημιουργία, τη διαχείριση και την αποκατάσταση αντιγράφων ασφαλείας ώστε να διασφαλίζεται η ακεραιότητα και η διαθεσιμότητα των δεδομένων.

Λύση αντιγράφων ασφαλείας – Ένα ολοκληρωμένο σύστημα ή υπηρεσία που έχει σχεδιαστεί για τη δημιουργία, την αποθήκευση και τη διαχείριση αντιγράφων ασφαλείας ώστε να διασφαλίζεται η προστασία και η ανάκτηση δεδομένων.

Δοκιμή αντιγράφων ασφαλείας – Η διαδικασία τακτικής επαλήθευσης της αποτελεσματικότητας και της αξιοπιστίας των διαδικασιών δημιουργίας αντιγράφων ασφαλείας για να διασφαλιστεί ότι τα δεδομένα μπορούν να αποκατασταθούν με επιτυχία όταν χρειαστεί.

Βασική ασφάλεια – Το ελάχιστο επίπεδο μέτρων και πρακτικών ασφαλείας που απαιτούνται για την προστασία των περιουσιακών στοιχείων και των δεδομένων ενός οργανισμού από γνωστές απειλές και ευπάθειες.

Ανίχνευση με βάση τη συμπεριφορά – Μια προσέγγιση ασφάλειας που εντοπίζει απειλές αναλύοντας μοτίβα συμπεριφοράς και όχι βασιζόμενη αποκλειστικά σε γνωστές υπογραφές ή μοτίβα.

Behavioral Analytics – Η ανάλυση μοτίβων συμπεριφοράς χρηστών και συστημάτων για τον εντοπισμό ανωμαλιών και πιθανών απειλών ασφαλείας.

Βιομετρική πιστοποίηση – Μέθοδος επαλήθευσης της ταυτότητας με βάση μοναδικά βιολογικά χαρακτηριστικά, όπως δακτυλικά αποτυπώματα, αναγνώριση προσώπου ή σαρώσεις ίριδας.

Συστήματα βιομετρικού ελέγχου ταυτότητας – Συστήματα που χρησιμοποιούν βιομετρικά δεδομένα (π.χ. δακτυλικά αποτυπώματα, αναγνώριση προσώπου) για την επαλήθευση και τον έλεγχο ταυτότητας των χρηστών.

Βιομετρικά δεδομένα – Πληροφορίες σχετικά με τα μοναδικά βιολογικά χαρακτηριστικά ενός ατόμου, που χρησιμοποιούνται για σκοπούς ελέγχου ταυτότητας και ταυτοποίησης.

Βιομετρική επαλήθευση – Η διαδικασία επιβεβαίωσης της ταυτότητας ενός ατόμου με τη χρήση βιομετρικών χαρακτηριστικών, όπως δακτυλικά αποτυπώματα, φωνή ή μοτίβα ίριδας.

Biohacking – Η πρακτική της χρήσης βιολογικών τεχνικών και τεχνολογιών για τη βελτίωση ή τη χειραγώγηση των ανθρώπινων ικανοτήτων, η οποία μπορεί να εγείρει ανησυχίες για την προστασία της ιδιωτικής ζωής και την ασφάλεια.

Μαύρη λίστα – Ένας κατάλογος οντοτήτων ή διευθύνσεων IP στις οποίες απαγορεύεται η πρόσβαση σε ένα σύστημα ή δίκτυο λόγω γνωστής κακόβουλης συμπεριφοράς ή κινδύνων για την ασφάλεια.

Black Hat – Όρος που χρησιμοποιείται για να περιγράψει χάκερ ή επαγγελματίες ασφαλείας που χρησιμοποιούν τις δεξιότητές τους για κακόβουλους σκοπούς, όπως η κλοπή δεδομένων ή η διατάραξη συστημάτων.

Black Hat SEO – Κακόβουλες τεχνικές που χρησιμοποιούνται για την ανήθικη χειραγώγηση της κατάταξης στις μηχανές αναζήτησης, οι οποίες μπορούν να χρησιμοποιηθούν για τη διανομή κακόβουλου λογισμικού ή για επιθέσεις phishing.

Blockchain – Μια αποκεντρωμένη τεχνολογία ψηφιακού βιβλίου που καταγράφει τις συναλλαγές σε πολλούς υπολογιστές, ενισχύοντας την ασφάλεια και τη διαφάνεια.

Ασφάλεια blockchain – Τα μέτρα και τα πρωτόκολλα που εφαρμόζονται για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της ασφάλειας των συναλλαγών και των δεδομένων blockchain.

Μπλε ομάδα – Η ομάδα που είναι υπεύθυνη για την υπεράσπιση και την ασφάλεια των συστημάτων και των δικτύων ενός οργανισμού έναντι κυβερνοεπιθέσεων και άλλων απειλών ασφαλείας.

Ανίχνευση bot – Τεχνικές και εργαλεία που χρησιμοποιούνται για τον εντοπισμό και τον αποκλεισμό αυτοματοποιημένων bots που ενδέχεται να χρησιμοποιηθούν για κακόβουλους σκοπούς, όπως η απόσπαση δεδομένων ή η εξαπόλυση επιθέσεων.

Ανίχνευση και μετριασμός bot – Στρατηγικές και εργαλεία που χρησιμοποιούνται για τον εντοπισμό και την αντιμετώπιση κακόβουλων bots που ενδέχεται να θέσουν σε κίνδυνο την ασφάλεια των δεδομένων ή να διαταράξουν τις υπηρεσίες.

Botnet – Ένα δίκτυο παραβιασμένων υπολογιστών ή συσκευών που ελέγχεται από έναν κακόβουλο παράγοντα, το οποίο συχνά χρησιμοποιείται για συντονισμένες επιθέσεις ή για τη διάδοση κακόβουλου λογισμικού.

Επώνυμο κακόβουλο λογισμικό – Κακόβουλο λογισμικό που έχει σχεδιαστεί για να μιμείται νόμιμο λογισμικό ή υπηρεσίες, χρησιμοποιώντας συχνά γνωστή επωνυμία ή ονόματα για να εξαπατήσει τους χρήστες.

Παραβίαση – Ένα περιστατικό κατά το οποίο πραγματοποιείται μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη δεδομένων, που ενδεχομένως θέτει σε κίνδυνο το απόρρητο και την ασφάλεια των δεδομένων.

Ανίχνευση παραβίασης – Τεχνικές και εργαλεία που χρησιμοποιούνται για τον έγκαιρο εντοπισμό και την αντιμετώπιση μη εξουσιοδοτημένης πρόσβασης ή παραβίασης δεδομένων.

Γνωστοποίηση παραβίασης – Η διαδικασία ενημέρωσης των επηρεαζόμενων ατόμων και των αρμόδιων αρχών σχετικά με μια παραβίαση δεδομένων, όπως απαιτείται από κανονισμούς και νόμους.

Brute Force Attack – Ένας τύπος κυβερνοεπίθεσης όπου ο επιτιθέμενος δοκιμάζει συστηματικά όλους τους πιθανούς συνδυασμούς κωδικών πρόσβασης ή κλειδιών κρυπτογράφησης έως ότου βρεθεί ο σωστός.

Απομόνωση προγράμματος περιήγησης – Μια τεχνική ασφαλείας που απομονώνει τη δραστηριότητα περιήγησης στο διαδίκτυο από το υπόλοιπο σύστημα για την αποτροπή μολύνσεων από κακόβουλο λογισμικό και παραβιάσεων δεδομένων.

Ασφάλεια προγράμματος περιήγησης – Μέτρα και πρακτικές που αποσκοπούν στην προστασία των προγραμμάτων περιήγησης στο διαδίκτυο από απειλές ασφαλείας, όπως κακόβουλο λογισμικό, phishing και παραβιάσεις δεδομένων.

Buffer Overflow – Μια ευπάθεια που εμφανίζεται όταν ένα πρόγραμμα γράφει περισσότερα δεδομένα σε ένα buffer από όσα μπορεί να χωρέσει, επιτρέποντας δυνητικά σε έναν εισβολέα να εκτελέσει αυθαίρετο κώδικα.

Buffer Zone – Ένα μέτρο ασφαλείας που δημιουργεί μια προστατευμένη περιοχή γύρω από ένα κρίσιμο σύστημα ή δίκτυο για την αποτροπή μη εξουσιοδοτημένης πρόσβασης ή επιθέσεων.

Επιχειρηματικός συνεργάτης – Πρόσωπο ή οντότητα που εκτελεί ορισμένες λειτουργίες ή δραστηριότητες για λογαριασμό καλυπτόμενης οντότητας, οι οποίες συνεπάγονται τη χρήση ή αποκάλυψη προστατευόμενων πληροφοριών υγείας.

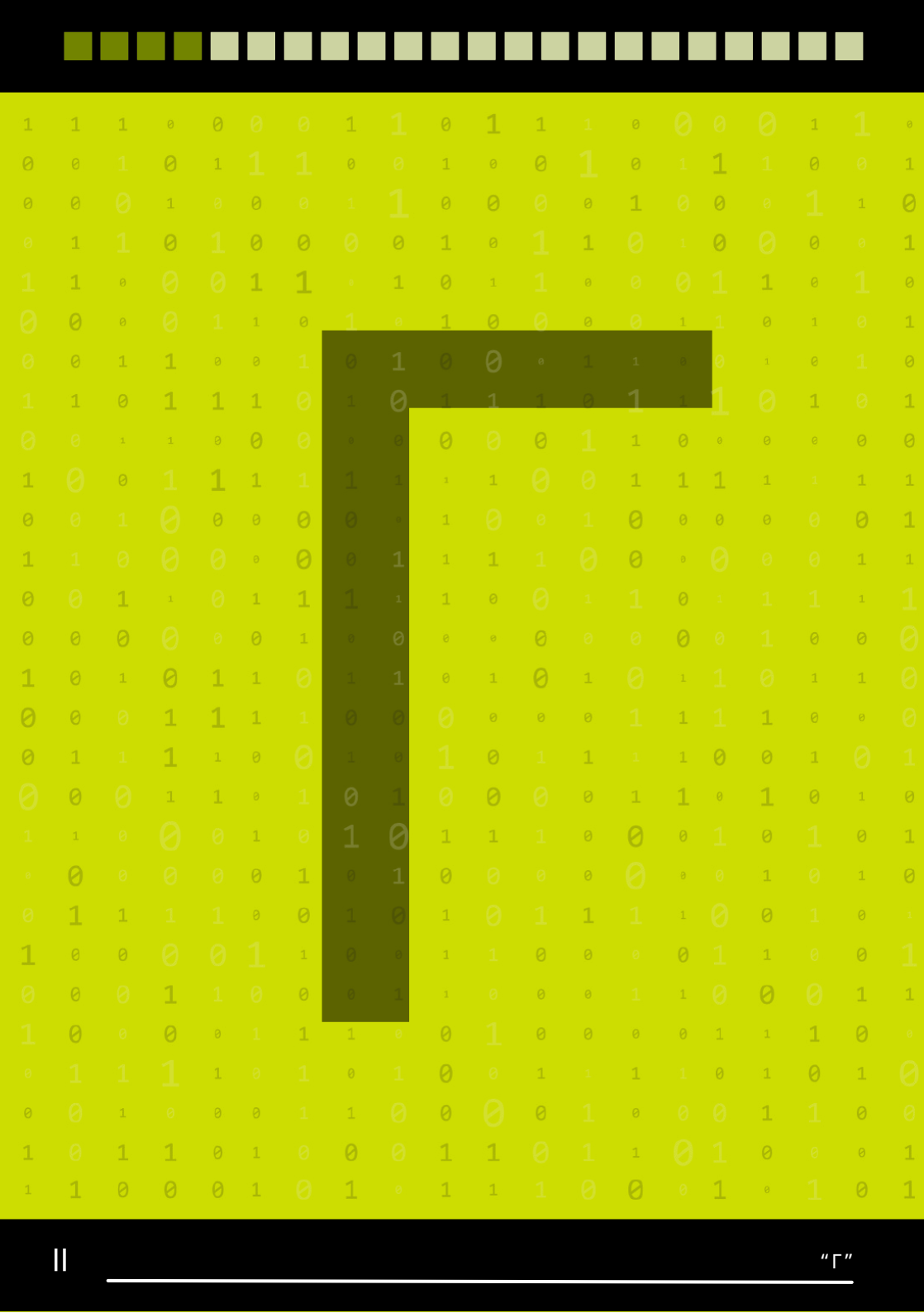
Συμφωνία επιχειρηματικού συνεργάτη (BAA) – Μια σύμβαση μεταξύ ενός παρόχου υγειονομικής περίθαλψης και ενός τρίτου παρόχου υπηρεσιών που περιγράφει τον τρόπο με τον οποίο ο τρίτος θα προστατεύει τις ευαίσθητες πληροφορίες υγείας σύμφωνα με τον HIPAA.

Σχεδιασμός επιχειρησιακής συνέχειας (BCP) – Η διαδικασία δημιουργίας συστημάτων και διαδικασιών που διασφαλίζουν ότι οι κρίσιμες επιχειρηματικές λειτουργίες μπορούν να συνεχιστούν κατά τη διάρκεια και μετά από μια διαταραχή.

Εξωτερίκευση επιχειρηματικών διαδικασιών (BPO) - Η πρακτική σύναψης συμβάσεων με τρίτους παρόχους υπηρεσιών για τη διεκπεραίωση ορισμένων επιχειρηματικών λειτουργιών, η οποία απαιτεί προσεκτική διαχείριση του απορρήτου και της ασφάλειας των δεδομένων.

Διαχείριση επιχειρηματικών κινδύνων - Η διαδικασία εντοπισμού, αξιολόγησης και μετριασμού των κινδύνων που θα μπορούσαν να επηρεάσουν τις επιχειρηματικές λειτουργίες, συμπεριλαμβανομένων των κινδύνων κυβερνοασφάλειας και απορρήτου δεδομένων.

Παράκαμψη - Ενέργεια ή μέθοδος που χρησιμοποιείται για την παράκαμψη μέτρων ή ελέγχων ασφαλείας, συχνά για την απόκτηση μη εξουσιοδοτημένης πρόσβασης ή την εκμετάλλευση τρωτών σημείων.



Μελέτες περίπτωσης – Λεπτομερής εξέταση συγκεκριμένων περιπτώσεων ή σεναρίων που σχετίζονται με τις προκλήσεις και τις λύσεις για το απόρρητο των δεδομένων.

Αρχή Πιστοποιητικών (CA) – Μια οντότητα που εκδίδει ψηφιακά πιστοποιητικά που χρησιμοποιούνται για την επαλήθευση της αυθεντικότητας ιστότοπων, λογισμικού και επικοινωνιών.

Certified Information Systems Security Professional (CISSP) – Μια παγκοσμίως αναγνωρισμένη πιστοποίηση για επαγγελματίες στον τομέα της ασφάλειας των πληροφοριών που επιδεικνύουν εξειδίκευση σε διάφορους τομείς της ασφάλειας στον κυβερνοχώρο.

Cloud Computing – Η παροχή υπολογιστικών υπηρεσιών μέσω του διαδικτύου, συμπεριλαμβανομένης της αποθήκευσης, της επεξεργασίας και των εφαρμογών, η οποία απαιτεί ισχυρά μέτρα ασφαλείας.

Κρυπτογράφηση νέφους – Η διαδικασία κρυπτογράφησης δεδομένων που αποθηκεύονται ή μεταδίδονται μέσω υπηρεσιών νέφους για την προστασία τους από μη εξουσιοδοτημένη πρόσβαση.

Ασφάλεια νέφους – Το σύνολο πολιτικών, τεχνολογιών και ελέγχων που αποσκοπούν στην προστασία δεδομένων, εφαρμογών και συστημάτων που φιλοξενούνται σε περιβάλλοντα νέφους.

Συμμόρφωση – Τήρηση νόμων, κανονισμών, προτύπων και πολιτικών που σχετίζονται με την προστασία δεδομένων και την ασφάλεια στον κυβερνοχώρο.

Έλεγχος συμμόρφωσης – Συστηματική εξέταση της συμμόρφωσης ενός οργανισμού με τους νόμους, τους κανονισμούς και τις εσωτερικές πολιτικές προστασίας δεδομένων.

Διαχείριση συμμόρφωσης – Η διαδικασία διασφάλισης ότι ένας οργανισμός πληροί τις νομικές και κανονιστικές υποχρεώσεις του σχετικά με το απόρρητο και την ασφάλεια των δεδομένων.

Εμπιστευτικότητα – Η αρχή της διασφάλισης ότι οι πληροφορίες είναι προσβάσιμες μόνο σε όσους έχουν εξουσιοδοτηθεί να έχουν πρόσβαση, προστατεύοντάς τες από μη εξουσιοδοτημένη αποκάλυψη.

Συμφωνία εμπιστευτικότητας – Μια νομική σύμβαση στην οποία τα μέρη συμφωνούν να διατηρήσουν ορισμένες πληροφορίες απόρρητες και να μην τις αποκαλύψουν σε μη εξουσιοδοτημένα άτομα.

Configuration Management – Η διαδικασία διαχείρισης και διατήρησης των ρυθμίσεων και διαμορφώσεων του συστήματος για τη διασφάλιση της ασφάλειας και της συμμόρφωσης.

Συναίνεση – Η εκούσια συμφωνία ενός ατόμου για την επεξεργασία των προσωπικών του δεδομένων για συγκεκριμένους σκοπούς.

Ασφάλεια εμπορευματοκιβωτίων – Η πρακτική της διασφάλισης εφαρμογών σε εμπορευματοκιβώτια και των σχετικών δεδομένων και ρυθμίσεων για την αποτροπή μη εξουσιοδοτημένης πρόσβασης και τρωτών σημείων.

Φιλτράρισμα περιεχομένου – Η πρακτική του αποκλεισμού ή της άδειας πρόσβασης σε συγκεκριμένους τύπους περιεχομένου σε ένα δίκτυο ή σύστημα για την προστασία των χρηστών από επιβλαβές ή ακατάλληλο υλικό.

Συνεχής παρακολούθηση – Η συνεχής διαδικασία αξιολόγησης και ανάλυσης συμβάντων ασφαλείας και τρωτών σημείων για τον εντοπισμό και την αντιμετώπιση απειλών σε πραγματικό χρόνο.

Ελεγχόμενη πρόσβαση – Η πρακτική του περιορισμού της πρόσβασης σε συστήματα, δεδομένα ή πόρους μόνο σε εξουσιοδοτημένα άτομα ή οντότητες.

Cookie – Ένα μικρό κομμάτι δεδομένων που αποθηκεύεται στη συσκευή ενός χρήστη από ένα πρόγραμμα περιήγησης ιστού, το οποίο χρησιμοποιείται για την παρακολούθηση της δραστηριότητας και των προτιμήσεων του χρήστη.

Cookies – Μικρά κομμάτια δεδομένων που αποθηκεύονται στη συσκευή ενός χρήστη από έναν ιστότοπο και χρησιμοποιούνται για την παρακολούθηση της δραστηριότητας και των προτιμήσεων του χρήστη.

Διασυνοριακές μεταφορές δεδομένων – Η διακίνηση δεδομένων σε διεθνή σύνορα, η οποία μπορεί να απαιτεί συμμόρφωση με ειδικούς κανονισμούς.

Cross-Site Scripting (XSS) – Μια ευπάθεια σε διαδικτυακές εφαρμογές που επιτρέπει στους επιτιθέμενους να εισάγουν κακόβουλα σενάρια σε ιστοσελίδες που προβάλλονται από άλλους χρήστες.

Κρυπτογραφικό κλειδί – Μια πληροφορία που χρησιμοποιείται σε κρυπτογραφικούς αλγορίθμους για την κρυπτογράφηση ή αποκρυπτογράφηση δεδομένων.

Κρυπτογραφία – Η πρακτική της χρήσης μαθηματικών αλγορίθμων για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων, εξασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητά τους.

Cryptojacking – Η μη εξουσιοδοτημένη χρήση των υπολογιστικών πόρων κάποιου άλλου για την εξόρυξη κρυπτονομισμάτων.

Κρίσιμα δεδομένα – Πληροφορίες που είναι απαραίτητες για τις λειτουργίες ενός οργανισμού και απαιτούν αυξημένη προστασία λόγω της ευαισθησίας τους.

Κρίσιμες υποδομές – Τα βασικά συστήματα και περιουσιακά στοιχεία που είναι ζωτικής σημασίας για τις λειτουργίες ενός οργανισμού και των οποίων η διακοπή θα μπορούσε να έχει σημαντικές συνέπειες.

Επίθεση στον κυβερνοχώρο – Προσπάθεια χάκερ ή κακόβουλων φορέων να διαταράξουν, να βλάψουν ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή δίκτυα υπολογιστών.

Ασφάλεια εμπορευματοκιβωτίων – Η πρακτική της διασφάλισης εφαρμογών σε εμπορευματοκιβώτια και των σχετικών δεδομένων και ρυθμίσεων για την αποτροπή μη εξουσιοδοτημένης πρόσβασης και τρωτών σημείων.

Φιλτράρισμα περιεχομένου – Η πρακτική του αποκλεισμού ή της άδειας πρόσβασης σε συγκεκριμένους τύπους περιεχομένου σε ένα δίκτυο ή σύστημα για την προστασία των χρηστών από επιβλαβές ή ακατάλληλο υλικό.

Συνεχής παρακολούθηση – Η συνεχής διαδικασία αξιολόγησης και ανάλυσης συμβάντων ασφαλείας και τρωτών σημείων για τον εντοπισμό και την αντιμετώπιση απειλών σε πραγματικό χρόνο.

Ελεγχόμενη πρόσβαση – Η πρακτική του περιορισμού της πρόσβασης σε συστήματα, δεδομένα ή πόρους μόνο σε εξουσιοδοτημένα άτομα ή οντότητες.

Cookie – Ένα μικρό κομμάτι δεδομένων που αποθηκεύεται στη συσκευή ενός χρήστη από ένα πρόγραμμα περιήγησης ιστού, το οποίο χρησιμοποιείται για την παρακολούθηση της δραστηριότητας και των προτιμήσεων του χρήστη.

Cookies – Μικρά κομμάτια δεδομένων που αποθηκεύονται στη συσκευή ενός χρήστη από έναν ιστότοπο, τα οποία χρησιμοποιούνται για την παρακολούθηση της δραστηριότητας και των προτιμήσεων του χρήστη.

Διασυνοριακές μεταφορές δεδομένων – Η διακίνηση δεδομένων σε διεθνή σύνορα, η οποία μπορεί να απαιτεί συμμόρφωση με ειδικούς κανονισμούς.

Cross-Site Scripting (XSS) – Μια ευπάθεια σε διαδικτυακές εφαρμογές που επιτρέπει στους επιτιθέμενους να εισάγουν κακόβουλα σενάρια σε ιστοσελίδες που προβάλλονται από άλλους χρήστες.

Κρυπτογραφικό κλειδί – Μια πληροφορία που χρησιμοποιείται σε κρυπτογραφικούς αλγορίθμους για την κρυπτογράφηση ή αποκρυπτογράφηση δεδομένων.

Κρυπτογραφία – Η πρακτική της χρήσης μαθηματικών αλγορίθμων για την κρυπτογράφηση και αποκρυπτογράφηση δεδομένων, εξασφαλίζοντας την εμπιστευτικότητα και την ακεραιότητά τους.

Cryptojacking – Η μη εξουσιοδοτημένη χρήση των υπολογιστικών πόρων κάποιου άλλου για την εξόρυξη κρυπτονομισμάτων.

Κρίσιμα δεδομένα – Πληροφορίες που είναι απαραίτητες για τις λειτουργίες ενός οργανισμού και απαιτούν αυξημένη προστασία λόγω της ευαισθησίας τους.

Κρίσιμες υποδομές – Τα βασικά συστήματα και περιουσιακά στοιχεία που είναι ζωτικής σημασίας για τις λειτουργίες ενός οργανισμού και των οποίων η διακοπή θα μπορούσε να έχει σημαντικές συνέπειες.

Επίθεση στον κυβερνοχώρο – Προσπάθεια χάκερ ή κακόβουλων φορέων να διαταράξουν, να βλάψουν ή να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε συστήματα ή δίκτυα υπολογιστών.

Αντιμετώπιση περιστατικών στον κυβερνοχώρο – Η διαδικασία διαχείρισης και αντιμετώπισης ενός περιστατικού κυβερνοασφάλειας για τον μετριασμό των επιπτώσεών του και την αποτροπή περαιτέρω ζημιών.

Cyber Insurance – Ένα είδος ασφάλισης που έχει σχεδιαστεί για την προστασία των οργανισμών από τις οικονομικές επιπτώσεις των κυβερνοεπιθέσεων, των παραβιάσεων δεδομένων και άλλων περιστατικών κυβερνοασφάλειας.

Cyber Law – Το σύνολο των νόμων και κανονισμών που διέπουν τις δραστηριότητες που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, τη**ν προστασία των δεδομένων και τις ψηφιακές επικοινωνίες.**

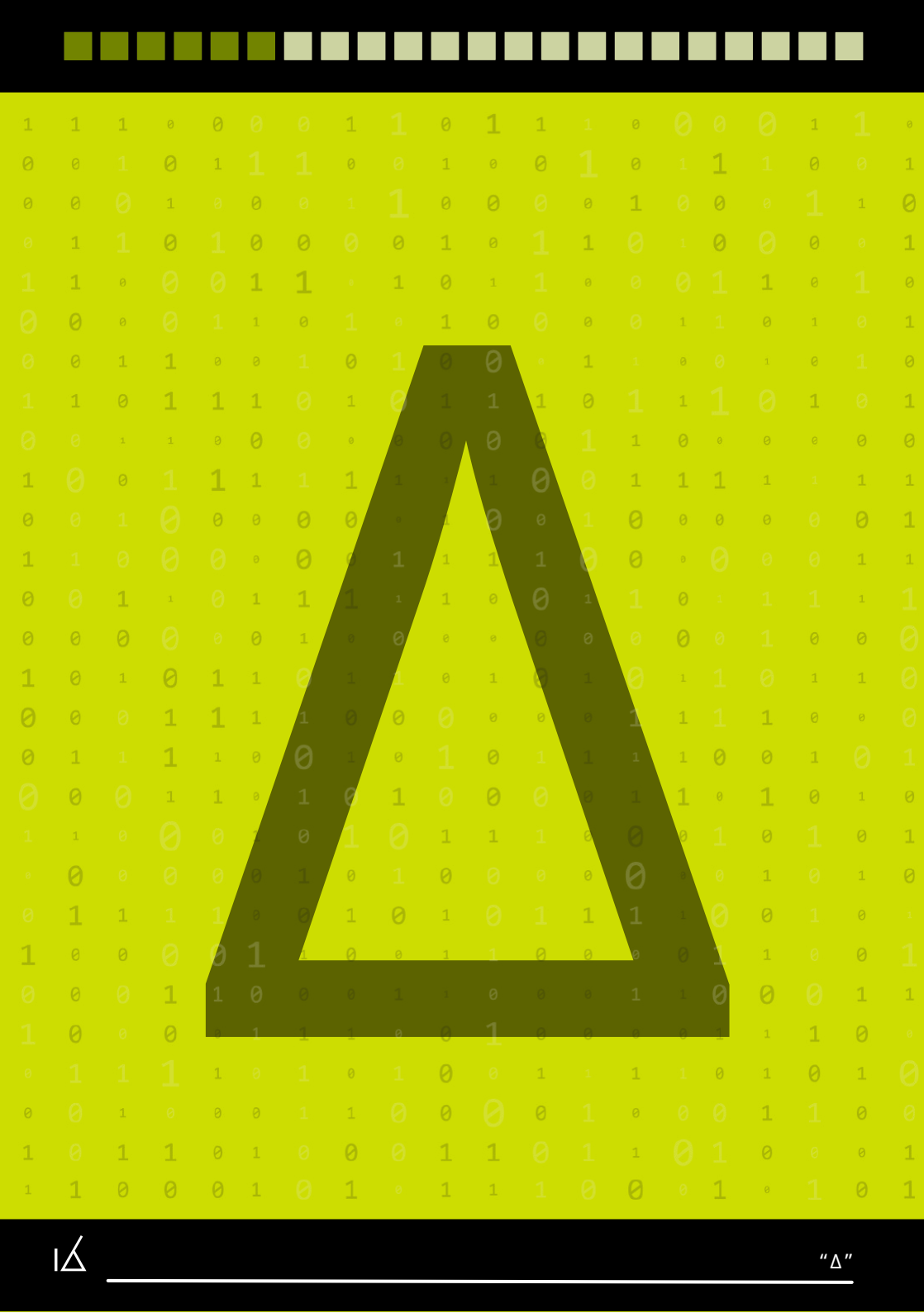
Ανθεκτικότητα στον κυβερνοχώρο – Η ικανότητα ενός οργανισμού να αντέχει και να ανακάμπτει από επιθέσεις στον κυβερνοχώρο και άλλες διαταραχές, διατηρώντας παράλληλα βασικές λειτουργίες.

Κυβερνοασφάλεια – Η πρακτική της προστασίας συστημάτων, δικτύων και δεδομένων από ψηφιακές επιθέσεις, κλοπές και ζημιές.

Πλαίσιο κυβερνοασφάλειας – Ένα σύνολο κατευθυντήριων γραμμών και βέλτιστων πρακτικών που έχουν σχεδιαστεί για να βοηθούν τους οργανισμούς να διαχειρίζονται και να μειώνουν τους κινδύνους κυβερνοασφάλειας.

Πολιτικές κυβερνοασφάλειας – Κατευθυντήριες γραμμές και κανόνες που έχουν σχεδιαστεί για την προστασία των ψηφιακών περιουσιακών στοιχείων ενός οργανισμού από απειλές στον κυβερνοχώρο.

Απειλή στον κυβερνοχώρο – Πιθανή ή πραγματική κακόβουλη επίθεση ή δραστηριότητα που στοχεύει τα πληροφοριακά συστήματα ή τα δεδομένα ενός οργανισμού.



Ημερολόγια πρόσβασης σε δεδομένα – Αρχεία σχετικά με το ποιος είχε πρόσβαση σε δεδομένα, πότε και ποιες ενέργειες έγιναν.

Ακρίβεια δεδομένων – Ο βαθμός στον οποίο τα δεδομένα αναπαριστούν σωστά το αντικείμενο ή την έννοια του πραγματικού κόσμου που προορίζονται να μοντελοποιήσουν.

Συγκέντρωση δεδομένων – Η διαδικασία συνδυασμού δεδομένων από πολλαπλές πηγές για την ανάλυση και την εξαγωγή χρήσιμων πληροφοριών.

Εργαλεία συγκέντρωσης δεδομένων – Τεχνολογίες που χρησιμοποιούνται για τον συνδυασμό δεδομένων από διάφορες πηγές για ανάλυση και υποβολή εκθέσεων.

Ανωνυμοποίηση δεδομένων – Η διαδικασία μετατροπής προσωπικών δεδομένων έτσι ώστε το άτομο στο οποίο αναφέρονται τα δεδομένα να μην μπορεί πλέον να ταυτοποιηθεί.

Παραβίαση δεδομένων – Ένα περιστατικό κατά το οποίο ευαίσθητες, εμπιστευτικές ή προστατευόμενες πληροφορίες αποκτούν πρόσβαση, αποκαλύπτονται ή κλέβονται από μη εξουσιοδοτημένα άτομα.

Γνωστοποίηση παραβίασης δεδομένων – Η απαίτηση ενημέρωσης των επηρεαζόμενων ατόμων και των αρμόδιων αρχών όταν συμβαίνει παραβίαση δεδομένων, η οποία συχνά διέπεται από κανονισμούς όπως ο ΓΚΠΔ.

Κανονισμοί κοινοποίησης παραβίασης δεδομένων – Νόμοι που απαιτούν από τους οργανισμούς να ενημερώνουν τα θιγόμενα άτομα και τις ρυθμιστικές αρχές σε περίπτωση παραβίασης δεδομένων.

Ταξινόμηση δεδομένων – Η διαδικασία οργάνωσης των δεδομένων σε κατηγορίες με βάση την ευαισθησία και τη σημασία τους για τη διασφάλιση των κατάλληλων ελέγχων ασφαλείας.

Συλλογή δεδομένων – Η διαδικασία συλλογής δεδομένων από διάφορες πηγές για ανάλυση ή επεξεργασία.

Έλεγχος συμμόρφωσης δεδομένων – Αξιολόγηση που διενεργείται για να διασφαλιστεί ότι οι πρακτικές χειρισμού δεδομένων ανταποκρίνονται στα νομικά και κανονιστικά πρότυπα.

Υπεύθυνος επεξεργασίας δεδομένων – Μια οντότητα που καθορίζει τους σκοπούς και τα μέσα επεξεργασίας προσωπικών δεδομένων, όπως ορίζεται από τους νόμους περί προστασίας δεδομένων, όπως ο ΓΚΠΔ.

Καταστροφή δεδομένων – Η διαδικασία μόνιμης διαγραφής ή καταστροφής δεδομένων ώστε να διασφαλίζεται ότι δεν μπορούν να ανακτηθούν ή να ανακατασκευαστούν.

Κρυπτογράφηση δεδομένων – Η διαδικασία μετατροπής αναγνώσιμων δεδομένων σε κωδικοποιημένη μορφή που μπορεί να διαβαστεί μόνο από εξουσιοδοτημένους χρήστες με το σωστό κλειδί αποκρυπτογράφησης.

Πρότυπα κρυπτογράφησης δεδομένων – Πρωτόκολλα και κατευθυντήριες γραμμές για την κρυπτογράφηση δεδομένων ώστε να διασφαλίζεται η ασφάλειά τους.

Διακυβέρνηση δεδομένων – Ένα πλαίσιο για τη διαχείριση της διαθεσιμότητας, της χρηστικότητας, της ακεραιότητας και της ασφάλειας των δεδομένων σε έναν οργανισμό μέσω πολιτικών, διαδικασιών και ελέγχων.

Διαχείριση δεδομένων – Η διαχείριση των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους, συμπεριλαμβανομένης της συλλογής, της αποθήκευσης, της μεταφοράς και της διαγραφής, σύμφωνα με τα πρότυπα ασφάλειας και προστασίας της ιδιωτικής ζωής.

Ακεραιότητα δεδομένων – Η ακρίβεια και η συνέπεια των δεδομένων καθ' όλη τη διάρκεια του κύκλου ζωής τους, διασφαλίζοντας ότι παραμένουν αναλλοίωτα κατά τη μεταφορά ή την αποθήκευση.

Διαρροή δεδομένων – Η μη εξουσιοδοτημένη διαβίβαση ευαίσθητων δεδομένων από το εσωτερικό ενός οργανισμού σε εξωτερικό ή μη εξουσιοδοτημένο παραλήπτη.

Διαχείριση κύκλου ζωής δεδομένων – Η διαδικασία διαχείρισης δεδομένων από τη δημιουργία και την αποθήκευση έως τη διαγραφή ή την αρχειοθέτηση.

Απώλεια δεδομένων – Η τυχαία ή κακόβουλη καταστροφή ή διαγραφή δεδομένων, η οποία μπορεί να συμβεί λόγω βλαβών υλικού, κυβερνοεπιθέσεων ή ανθρώπινου λάθους.

Πρόληψη απώλειας δεδομένων (DLP) – Ένα σύνολο εργαλείων και διαδικασιών που έχουν σχεδιαστεί για τον εντοπισμό και την πρόληψη της μη εξουσιοδοτημένης χρήσης, μεταφοράς ή αποκάλυψης ευαίσθητων δεδομένων.

Κάλυψη δεδομένων – Η διαδικασία απόκρυψης συγκεκριμένων δεδομένων εντός ενός συνόλου δεδομένων για την προστασία ευαίσθητων πληροφοριών, διατηρώντας παράλληλα τη δυνατότητα χρήσης τους για εξουσιοδοτημένους σκοπούς.

Ελαχιστοποίηση δεδομένων – Η αρχή της συλλογής και διατήρησης μόνο της ελάχιστης ποσότητας προσωπικών δεδομένων που είναι αναγκαία για ένα συγκεκριμένο σκοπό, μειώνοντας τους κινδύνους για την προστασία της ιδιωτικής ζωής.

Φορητότητα δεδομένων – Η δυνατότητα μεταφοράς προσωπικών δεδομένων από έναν οργανισμό σε άλλον.

Δικαιώματα φορητότητας δεδομένων – Το δικαίωμα των ατόμων να αποκτούν και να επαναχρησιμοποιούν τα προσωπικά τους δεδομένα σε διάφορες υπηρεσίες.

Επεξεργασία δεδομένων – Οι εργασίες που εκτελούνται σε δεδομένα, συμπεριλαμβανομένης της συλλογής, αποθήκευσης, τροποποίησης και διαγραφής.

Αρχές επεξεργασίας δεδομένων – Βασικές αρχές που διέπουν τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της νομιμότητας, της δικαιοσύνης και της διαφάνειας.

Προστασία δεδομένων – Τα νομικά και τεχνικά μέτρα που αποσκοπούν στην προστασία των προσωπικών και ευαίσθητων δεδομένων από μη εξουσιοδοτημένη πρόσβαση, χρήση ή αποκάλυψη.

Αρχή Προστασίας Δεδομένων (ΑΠΔ) – Ρυθμιστικός φορέας αρμόδιος για την εποπτεία της εφαρμογής των νόμων περί προστασίας δεδομένων, όπως ο ΓΚΠΔ.

Εκτίμηση αντικτύπου προστασίας δεδομένων (DPIA) – Μια διαδικασία εκτίμησης κινδύνου που χρησιμοποιούν οι οργανισμοί για να αξιολογήσουν τους δυνητικούς κινδύνους προστασίας της ιδιωτικής ζωής που συνδέονται με την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Υπεύθυνος προστασίας δεδομένων (DPO) – Ένα άτομο που διορίζεται για να επιβλέπει και να διασφαλίζει τη συμμόρφωση με τους νόμους και τις πρακτικές προστασίας δεδομένων και να διασφαλίζει τον ορθό χειρισμό των δεδομένων προσωπικού χαρακτήρα.

Ποιότητα δεδομένων – Το μέτρο της ακρίβειας, της πληρότητας και της αξιοπιστίας των δεδομένων.

Data Redaction – Η διαδικασία επεξεργασίας ή συσκότισης ευαίσθητων πληροφοριών σε ένα έγγραφο πριν από την κοινοποίησή του, για την προστασία της ιδιωτικής ζωής ή της εμπιστευτικότητας.

Κατοικία δεδομένων – Η φυσική τοποθεσία στην οποία αποθηκεύονται τα δεδομένα, η οποία μπορεί να έχει επιπτώσεις στη συμμόρφωση με τους νόμους περί προστασίας δεδομένων ανάλογα με τη δικαιοδοσία.

Διατήρηση δεδομένων – Οι πολιτικές και οι πρακτικές για την αποθήκευση δεδομένων για ένα συγκεκριμένο χρονικό διάστημα πριν από τη διαγραφή ή την αρχειοθέτησή τους.

Πολιτική διατήρησης δεδομένων – Μια επίσημη κατευθυντήρια γραμμή που ορίζει πόσο καιρό ένας οργανισμός διατηρεί δεδομένα και τη διαδικασία για την ασφαλή διαγραφή τους όταν δεν χρειάζονται πλέον.

Καθαρισμός δεδομένων – Η διαδικασία ασφαλούς διαγραφής ή καταστροφής δεδομένων από ένα σύστημα για να αποτραπεί η ανάκτησή τους.

Ασφάλεια δεδομένων – Τα προστατευτικά μέτρα που λαμβάνονται για την προστασία των δεδομένων από μη εξουσιοδοτημένη πρόσβαση, αλλοίωση ή κλοπή, εξασφαλίζοντας την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητά τους.

Παραβίαση ασφάλειας δεδομένων – Περιστατικό κατά το οποίο λαμβάνει χώρα μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, αλλοίωση ή καταστροφή δεδομένων, θέτοντας σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητά τους.

Κυριαρχία δεδομένων – Η έννοια ότι τα δεδομένα υπόκεινται στους νόμους και τους κανονισμούς της χώρας όπου αποθηκεύονται.

Λύσεις αποθήκευσης δεδομένων – Τεχνολογίες και μέθοδοι που χρησιμοποιούνται για την ασφαλή αποθήκευση δεδομένων, συμπεριλαμβανομένων φυσικών επιλογών και επιλογών που βασίζονται στο υπολογιστικό νέφος.

Υποκείμενο δεδομένων – Ένα άτομο του οποίου τα προσωπικά δεδομένα υποβάλλονται σε επεξεργασία από έναν οργανισμό, όπως ορίζεται από κανονισμούς προστασίας δεδομένων όπως ο ΓΚΠΔ.

Αίτημα πρόσβασης υποκειμένου δεδομένων (DSAR) – Ένα αίτημα που υποβάλλεται από ένα άτομο σε έναν οργανισμό για πρόσβαση στα δεδομένα προσωπικού χαρακτήρα που κατέχει γι' αυτό, σύμφωνα με τους νόμους περί προστασίας δεδομένων.

Αιτήματα πρόσβασης υποκειμένου δεδομένων (DSAR) – Αιτήματα που υποβάλλονται από ιδιώτες για πρόσβαση στα προσωπικά τους δεδομένα που κατέχει ένας οργανισμός.

Tokenisation δεδομένων – Η διαδικασία αντικατάστασης ευαίσθητων δεδομένων με μοναδικά σύμβολα αναγνώρισης ή "tokens" που διατηρούν βασικές πληροφορίες χωρίς να εκθέτουν τα αρχικά δεδομένα.

Μεταφορά δεδομένων – Μετακίνηση δεδομένων από ένα σύστημα ή μια τοποθεσία σε ένα άλλο, η οποία μπορεί να συνεπάγεται συμμόρφωση με τους νόμους περί προστασίας δεδομένων.

Συμφωνία μεταφοράς δεδομένων (DTA) – Ένα νομικό έγγραφο που περιγράφει τους όρους και τις προϋποθέσεις για τη μεταφορά δεδομένων μεταξύ οργανισμών, διασφαλίζοντας τη συμμόρφωση με τους κανονισμούς προστασίας της ιδιωτικής ζωής και της ασφάλειας.

Χρήση δεδομένων – Ο τρόπος με τον οποίο τα δεδομένα που συλλέγονται εφαρμόζονται σε έναν οργανισμό, μεταξύ άλλων για ανάλυση, υποβολή εκθέσεων και λήψη αποφάσεων.

Επικύρωση δεδομένων – Η διαδικασία διασφάλισης ότι τα δεδομένα είναι ακριβή, πλήρη και έγκυρα πριν από την επεξεργασία ή τη χρήση τους.

Διαγραφή δεδομένων – Η διαδικασία ασφαλούς διαγραφής δεδομένων από συσκευές αποθήκευσης για την αποφυγή ανάκτησης, που χρησιμοποιείται συχνά κατά τον παροπλισμό ή την ανακύκλωση υλικού.

Deep Packet Inspection (DPI) – Μια μέθοδος παρακολούθησης δικτύου που εξετάζει το περιεχόμενο των πακέτων δεδομένων καθώς περνούν από ένα σημείο ελέγχου, που χρησιμοποιείται συχνά για τον εντοπισμό και τον μετριασμό των απειλών.

Επίθεση άρνησης υπηρεσίας (DoS) – Μια κυβερνοεπίθεση κατά την οποία ο επιτιθέμενος κατακλύζει ένα δίκτυο ή μια υπηρεσία με υπερβολικές αιτήσεις, καθιστώντας την μη διαθέσιμη στους νόμιμους χρήστες.

Ψηφιακό πιστοποιητικό – Ένα ηλεκτρονικό έγγραφο που χρησιμοποιείται για την απόδειξη της ταυτότητας ενός ιστότοπου ή ενός χρήστη, το οποίο χρησιμοποιείται συχνά σε συνδυασμό με την κρυπτογράφηση για την ασφάλεια των διαδικτυακών επικοινωνιών.

Ψηφιακό αποτύπωμα – Το ίχνος δεδομένων που αφήνει πίσω του ένα άτομο όταν χρησιμοποιεί ψηφιακές πλατφόρμες.

Digital Forensics – Η διαδικασία συλλογής, ανάλυσης και διατήρησης ψηφιακών αποδεικτικών στοιχείων από υπολογιστές, δίκτυα και συσκευές κατά τη διερεύνηση εγκλημάτων ή περιστατικών στον κυβερνοχώρο.

Ψηφιακή ταυτότητα – Ένα σύνολο χαρακτηριστικών και διαπιστευτηρίων που καθορίζουν την ταυτότητα ενός χρήστη στις ψηφιακές αλληλεπιδράσεις, που συχνά επαληθεύονται μέσω μεθόδων ελέγχου ταυτότητας, όπως κωδικοί πρόσβασης ή βιομετρικά στοιχεία.

Ψηφιακή υπογραφή – Μια ηλεκτρονική, κρυπτογραφική υπογραφή που χρησιμοποιείται για την επαλήθευση της αυθεντικότητας και της ακεραιότητας ενός μηνύματος, εγγράφου ή συναλλαγής.

Disaster Recovery (DR) – Ένα σχέδιο και μια διαδικασία για την αποκατάσταση των συστημάτων και των δεδομένων ΤΠ μετά από μια σημαντική διαταραχή ή καταστροφή, εξασφαλίζοντας την επιχειρησιακή συνέχεια.

Distributed Denial of Service (DDoS) Attack – Ένας τύπος κυβερνοεπίθεσης όπου πολλαπλά συστήματα κατακλύζουν έναν στόχο με πλημμύρα κυκλοφορίας, προκαλώντας διακοπές υπηρεσιών.

DNS Spoofing – Ένας τύπος κυβερνοεπίθεσης όπου ένας χάκερ υποκλέπτει και τροποποιεί τα ερωτήματα DNS για να ανακατευθύνει τους χρήστες σε κακόβουλους ιστότοπους εν αγνοία τους.

Σύστημα ονομάτων τομέα (DNS) – Το ιεραρχικό σύστημα που χρησιμοποιείται για τη μετάφραση ονομάτων τομέα (π.χ. www. example.com) σε διευθύνσεις IP, καθιστώντας δυνατή την πλοήγηση στο διαδίκτυο.

Domain-based Message Authentication, Reporting & Conformance (DMARC) – Πρωτόκολλο ελέγχου ταυτότητας ηλεκτρονικού ταχυδρομείου που χρησιμοποιείται για την προστασία από την πλαστογράφηση και το phishing με την επαλήθευση του τομέα του αποστολέα.

Drive-by Download – Ένας τύπος κυβερνοεπίθεσης όπου κακόβουλο λογισμικό μεταφορτώνεται αυτόματα στη συσκευή ενός χρήστη χωρίς τη συγκατάθεσή του, συνήθως με την επίσκεψη ενός παραβιασμένου ιστότοπου.

Dual-Factor Authentication (2FA) – Μια διαδικασία ασφαλείας που απαιτεί δύο ξεχωριστές μορφές ταυτοποίησης (π.χ. έναν κωδικό πρόσβασης και ένα δακτυλικό αποτύπωμα) για την επαλήθευση της ταυτότητας ενός χρήστη.

Dumpster Diving – Μια φυσική απειλή για την ασφάλεια κατά την οποία οι επιτιθέμενοι ψάχνουν σε πεταμένα υλικά, όπως έγγραφα σε χαρτί ή παλιό υλικό, για να βρουν ευαίσθητες πληροφορίες.

Υποκλοπή – Η πράξη της κρυφής ακρόασης ιδιωτικών επικοινωνιών, συνήθως μέσω μη ασφαλών δικτύων, για τη συλλογή ευαίσθητων πληροφοριών.

E-discovery (Ηλεκτρονική ανακάλυψη) – Η διαδικασία εντοπισμού, συλλογής και παραγωγής ηλεκτρονικά αποθηκευμένων πληροφοριών (ESI) για νομικές διαδικασίες ή έρευνες.

Email Authentication (Αυθεντικοποίηση ηλεκτρονικού ταχυδρομείου) – Τεχνικές που χρησιμοποιούνται για την επαλήθευση της γνησιότητας των μηνυμάτων ηλεκτρονικού ταχυδρομείου, διασφαλίζοντας ότι προέρχονται από νόμιμες πηγές και δεν είναι πλαστά.

Κρυπτογράφηση ηλεκτρονικού ταχυδρομείου – Η διαδικασία κρυπτογράφησης μηνυμάτων ηλεκτρονικού ταχυδρομείου για την προστασία του περιεχομένου τους από μη εξουσιοδοτημένη πρόσβαση κατά τη μεταφορά ή σε κατάσταση ηρεμίας.

Φιλτράρισμα ηλεκτρονικού ταχυδρομείου – Εργαλεία βασισμένα σε λογισμικό ή υλικό που χρησιμοποιούνται για τον αποκλεισμό ή την επισήμανση ανεπιθύμητων ή ύποπτων μηνυμάτων ηλεκτρονικού ταχυδρομείου, όπως spam ή απόπειρες phishing.

Email Spoofing – Μια τεχνική κυβερνοεπίθεσης κατά την οποία ο αποστολέας ενός email πλαστογραφεί τη διεύθυνση αποστολέα για να το κάνει να φαίνεται ότι προέρχεται από νόμιμη πηγή.

Ασφάλεια ενσωματωμένων συστημάτων – Η πρακτική της διασφάλισης των στοιχείων υλικού και λογισμικού ενσωματωμένων συστημάτων, τα οποία είναι εξειδικευμένα συστήματα υπολογιστών εντός μεγαλύτερων συστημάτων (π.χ. ιατρικές συσκευές, αυτοκίνητα).

Κρυπτογράφηση – Η διαδικασία μετατροπής αναγνώσιμων δεδομένων (απλό κείμενο) σε μη αναγνώσιμη μορφή (κρυπτογραφημένο κείμενο) για την προστασία τους από μη εξουσιοδοτημένη πρόσβαση, συνήθως αναστρέψιμη μόνο με ένα κλειδί αποκρυπτογράφησης.

Τελικό σημείο – Κάθε συσκευή που είναι συνδεδεμένη σε ένα δίκτυο, όπως υπολογιστές, smartphones ή συσκευές IoT, οι οποίες μπορεί να είναι ευάλωτες σε κινδύνους ασφαλείας και επιθέσεις.

Endpoint Detection and Response (EDR) – Μια λύση κυβερνοασφάλειας που παρακολουθεί και συλλέγει συνεχώς δεδομένα από τα τελικά σημεία (π.χ. υπολογιστές, κινητές συσκευές) για τον εντοπισμό και την αντιμετώπιση πιθανών απειλών ασφαλείας.

Κρυπτογράφηση τελικού σημείου – Η χρήση τεχνικών κρυπτογράφησης σε συσκευές τελικού σημείου (π.χ. φορητοί υπολογιστές, κινητά τηλέφωνα) για την προστασία ευαίσθητων δεδομένων που αποθηκεύονται ή μεταδίδονται από αυτές τις συσκευές.

Ασφάλεια τελικών σημείων – Η πρακτική της διασφάλισης των τελικών σημείων (συσκευών) από απειλές στον κυβερνοχώρο, χρησιμοποιώντας εργαλεία όπως λογισμικό προστασίας από ιούς, τείχη προστασίας και συστήματα πρόληψης εισβολών.

Enhanced Security Administrative Environment (ESAE) – Ένα αποκλειστικό, απομονωμένο περιβάλλον διαχείρισης που έχει σχεδιαστεί για την προστασία από επιθέσεις με προνομιακούς λογαριασμούς σε ευαίσθητα δίκτυα ή δίκτυα υψηλού κινδύνου.

Enterprise Information Security Architecture (EISA) – Ένα ολοκληρωμένο πλαίσιο που ευθυγραμμίζει τις στρατηγικές ασφάλειας με τους επιχειρηματικούς στόχους, βοηθώντας τους οργανισμούς να εφαρμόσουν ισχυρές πρακτικές ασφάλειας πληροφοριών.

Enterprise Mobility Management (EMM) – Ένα σύνολο εργαλείων και τεχνολογιών που χρησιμοποιούνται για τη διαχείριση κινητών συσκευών, εφαρμογών και δεδομένων για τη διασφάλιση της ασφάλειας, ιδίως σε εταιρικά περιβάλλοντα.

Ethical Hacking – Η πρακτική της εσκεμμένης διερεύνησης συστημάτων ή δικτύων για ευπάθειες με άδεια, για τον εντοπισμό αδυναμιών ασφαλείας πριν από την εκμετάλλευσή τους από κακόβουλους χάκερ.

Exfiltration – Η μη εξουσιοδοτημένη μεταφορά ή κλοπή δεδομένων από ένα δίκτυο, που συχνά πραγματοποιείται από χάκερς μετά την παραβίαση ενός συστήματος.

Εκμετάλλευση – Μια συγκεκριμένη μέθοδος/τεχνική που χρησιμοποιείται από τους χάκερ για να εκμεταλλευτούν μια ευπάθεια ή αδυναμία σε ένα σύστημα για να πραγματοποιήσουν κακόβουλες δραστηριότητες.

Exploit Kit – Μια εργαλειοθήκη που χρησιμοποιείται από εγκληματίες του κυβερνοχώρου για τον εντοπισμό και την εκμετάλλευση ευπαθειών σε λογισμικό και την παράδοση κακόβουλου λογισμικού ή άλλου κακόβουλου κώδικα.

Extended Detection and Response (XDR) – Μια τεχνολογία κυβερνοασφάλειας που ενσωματώνει δεδομένα από πολλαπλά επίπεδα ασφαλείας (π.χ., τελικά σημεία, δίκτυα, διακομιστές) για να παρέχει μια πιο ολοκληρωμένη ικανότητα ανίχνευσης και απόκρισης.

External Penetration Testing – Ένας τύπος δοκιμών ασφαλείας που διεξάγεται από ηθικούς χάκερ ή επαγγελματίες της κυβερνοασφάλειας για την αξιολόγηση της ασφάλειας ενός συστήματος ή δικτύου από εξωτερική σκοπιά.

Εξωτερική απειλή – Οποιαδήποτε απειλή για ένα σύστημα ή έναν οργανισμό που προέρχεται εκτός του δικού του δικτύου, όπως χάκερ, απόπειρες phishing ή κακόβουλο λογισμικό που διανέμεται διαδικτυακά.

Extensible Authentication Protocol (EAP) – Ένα πλαίσιο ελέγχου ταυτότητας που χρησιμοποιείται συνήθως σε ασύρματα δίκτυα και συνδέσεις από σημείο σε σημείο, παρέχοντας διάφορες μεθόδους για τον έλεγχο ταυτότητας συσκευών.

Extensible Markup Language (XML) Encryption – Ένα πρότυπο για την κρυπτογράφηση των δεδομένων που περιέχονται σε ένα έγγραφο XML, το οποίο χρησιμοποιείται για την ασφάλεια των πληροφοριών που ανταλλάσσονται μεταξύ συστημάτων, συχνά σε υπηρεσίες ιστού.

Επίθεση μηδενικής ημέρας – Μια κυβερνοεπίθεση που εκμεταλλεύεται μια προηγουμένως άγνωστη ευπάθεια σε λογισμικό ή υλικό, η οποία δεν έχει ακόμη επιδιορθωθεί από τον προμηθευτή, γεγονός που την καθιστά ιδιαίτερα επικίνδυνη.


Z
Z
"Z"

Ψευδής συναγερμός – Ένας συναγερμός που παράγεται από ένα σύστημα ασφαλείας και υποδεικνύει μια πιθανή απειλή που στην πραγματικότητα δεν υφίσταται.

Ψευδώς αρνητικός – Ένα σφάλμα κατά το οποίο μια δοκιμή ή ένα σύστημα ασφαλείας αποτυγχάνει να εντοπίσει μια πραγματική απειλή.

Ψευδώς θετικό – Ένα σφάλμα κατά το οποίο μια δοκιμή ή ένα σύστημα ασφαλείας αναγνωρίζει εσφαλμένα μια καλοήθη κατάσταση ως απειλή.

Federated Identity Management (FIM) – Σύστημα διαχείρισης ταυτοτήτων χρηστών σε πολλούς τομείς ή οργανισμούς με τη χρήση ενός ενιαίου συνόλου διαπιστευτηρίων.

Federated Search – Μια μέθοδος αναζήτησης που ανακτά δεδομένα από πολλαπλές, διαφορετικές πηγές σε ένα ενιαίο αποτέλεσμα αναζήτησης.

Ομοσπονδία – Η χρήση κοινών πρωτοκόλλων και προτύπων που επιτρέπουν τη διαλειτουργικότητα και την ενιαία σύνδεση σε διαφορετικά συστήματα ή οργανισμούς.

Ransomware βασισμένο σε αρχεία – Ransomware που στοχεύει και κρυπτογραφεί συγκεκριμένα αρχεία ή τύπους αρχείων και όχι ολόκληρο το σύστημα.

Κρυπτογράφηση αρχείων – Η διαδικασία μετατροπής αρχείων σε ασφαλή μορφή στην οποία μπορεί να έχει πρόσβαση μόνο με ένα κλειδί αποκρυπτογράφησης.

File Integrity Monitoring (FIM) – Μια διαδικασία εντοπισμού μη εξουσιοδοτημένων αλλαγών σε αρχεία για τη διασφάλιση της ακεραιότητάς τους.

Τείχος προστασίας – Μια συσκευή ασφαλείας δικτύου που παρακολουθεί και ελέγχει την εισερχόμενη και εξερχόμενη κυκλοφορία δικτύου βάσει κανόνων ασφαλείας.

Πολιτική τείχους προστασίας – Ένα σύνολο κανόνων και κατευθυντήριων γραμμών που καθορίζουν τον τρόπο με τον οποίο η δικτυακή κυκλοφορία πρέπει να επιτρέπεται ή να αποκλείεται από ένα τείχος προστασίας.

Κανόνας τείχους προστασίας – Μια συγκεκριμένη συνθήκη ή πολιτική που ορίζεται σε ένα τείχος προστασίας για τον έλεγχο της ροής της κυκλοφορίας και την επιβολή μέτρων ασφαλείας.

Firmware – Λογισμικό που είναι ενσωματωμένο σε συσκευές υλικού για τον έλεγχο και τη διαχείριση λειτουργιών υλικού.

Ιατροδικαστική ανάλυση – Η λεπτομερής εξέταση και διερεύνηση ψηφιακών δεδομένων για την αποκάλυψη αποδεικτικών στοιχείων για εγκλήματα στον κυβερνοχώρο ή άλλα περιστατικά ασφαλείας.

Forensics (Digital Forensics) – Η πρακτική της συλλογής, διατήρησης, ανάλυσης και παρουσίασης ψηφιακών αποδεικτικών στοιχείων για νομικές έρευνες.

Ανίχνευση απάτης (Fraud Detection) – Τεχνικές και συστήματα που χρησιμοποιούνται για τον εντοπισμό και την πρόληψη δόλιων δραστηριοτήτων ή συναλλαγών.

Ανάλυση συχνότητας – Η μελέτη της συχνότητας των γραμμάτων ή ομάδων γραμμάτων σε ένα κρυπτογραφημένο κείμενο για την παραβίαση της κρυπτογράφησης.

Fuzz Testing – Μια τεχνική δοκιμών κατά την οποία τυχαία δεδομένα εισάγονται σε ένα πρόγραμμα για την ανακάλυψη τρωτών σημείων και σφαλμάτων.

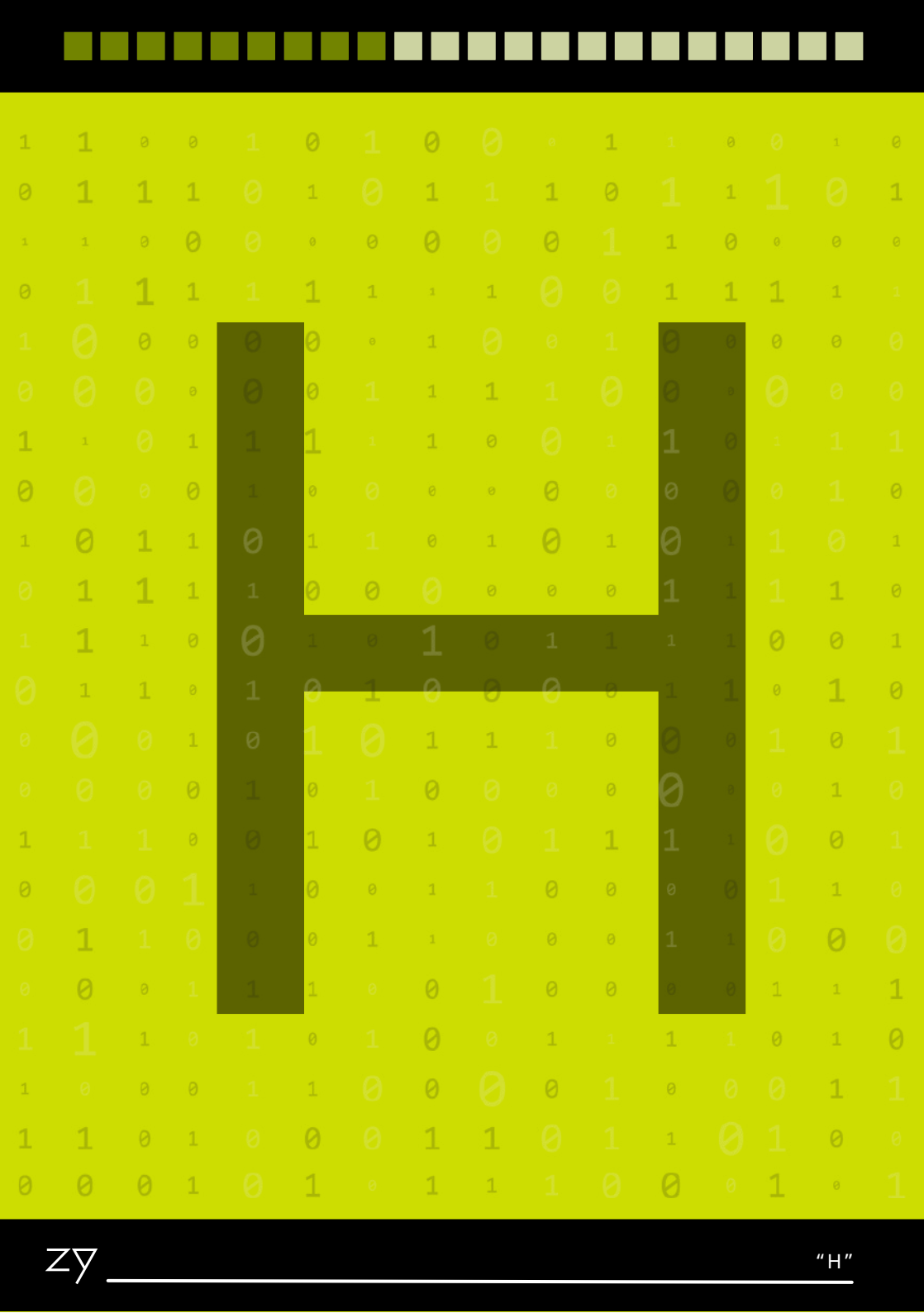
Ασαφής λογική – Μια μορφή λογικής πολλών τιμών που ασχολείται με την προσεγγιστική συλλογιστική, χρήσιμη σε ορισμένους τύπους συστημάτων ασφαλείας και στην ανίχνευση ανωμαλιών.

Λειτουργική ασφάλεια – Μέτρα ασφαλείας σχεδιασμένα για την προστασία της λειτουργικότητας και της απόδοσης ενός συστήματος ή μιας εφαρμογής.

Zero Trust Network Access (ZTNA) – Μια προσέγγιση ασφάλειας που εξασφαλίζει ασφαλή, τμηματοποιημένη πρόσβαση σε δικτυακούς πόρους με βάση την επαλήθευση της ταυτότητας, υποθέτοντας ότι δεν υπάρχει σιωπηρή εμπιστοσύνη για καμία συσκευή ή χρήστη εντός ή εκτός του δικτύου.

Zombie – Ένας υπολογιστής που έχει παραβιαστεί και ελέγχεται εξ αποστάσεως από έναν επιτιθέμενο, ο οποίος συχνά χρησιμοποιείται ως μέρος ενός **botnet** για την εξαπόλυση συντονισμένων επιθέσεων στον κυβερνοχώρο, όπως η κατανεμημένη άρνηση παροχής υπηρεσιών (DDoS).

Zscaler – Εταιρεία ασφάλειας με βάση το **cloud**, η οποία παρέχει λύσεις ασφάλειας διαδικτύου, φιλτραρίσματος ιστού και πρόσβασης στο δίκτυο μηδενικής εμπιστοσύνης (ZTNA) σε επιχειρήσεις για την ασφάλεια των δεδομένων και των χρηστών τους.



Galois/Counter Mode (GCM) – Ένας τρόπος λειτουργίας για κρυπτογραφικούς block ciphers συμμετρικού κλειδιού που παρέχει τόσο κρυπτογράφηση όσο και αυθεντικοποίηση μηνυμάτων και χρησιμοποιείται συνήθως σε πρωτόκολλα ασφαλούς επικοινωνίας.

Garbage Data – Δεδομένα που είναι λανθασμένα, άσχετα ή περιττά, χρησιμοποιούνται συχνά στην κυβερνοασφάλεια ως τακτική παραπλάνησης των επιτιθέμενων ή απόκρυψης πραγματικών δεδομένων.

Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) – Ένας ολοκληρωμένος κανονισμός που επιβάλλεται από την Ευρωπαϊκή Ένωση (ΕΕ) για την προστασία των προσωπικών δεδομένων των ατόμων εντός της ΕΕ και διέπει τις πρακτικές απορρήτου των οργανισμών που χειρίζονται τα δεδομένα αυτά.

Geo-blocking – Η πρακτική του περιορισμού της πρόσβασης σε διαδικτυακό περιεχόμενο με βάση τη γεωγραφική θέση ενός χρήστη, που χρησιμοποιείται συχνά για λόγους ασφάλειας, συμμόρφωσης ή αδειοδότησης.

Geofencing – Μια τεχνολογία ασφαλείας που δημιουργεί εικονικά όρια (γεωπεριοχές) γύρω από μια φυσική τοποθεσία, επιτρέποντας ειδοποιήσεις ή ενέργειες όταν οι συσκευές εισέρχονται ή εξέρχονται από την καθορισμένη περιοχή.

Γεωεντοπισμός – Η διαδικασία προσδιορισμού της φυσικής θέσης μιας συσκευής (π.χ. smartphone, φορητός υπολογιστής) με βάση το GPS, τη διεύθυνση IP ή άλλες μεθόδους εντοπισμού θέσης, που χρησιμοποιείται συχνά στην ασφάλεια στον κυβερνοχώρο για τον εντοπισμό ανώμαλης δραστηριότητας.

Gartner Hype Cycle – Μια γραφική αναπαράσταση που αναπτύχθηκε από την Gartner και παρακολουθεί την ωριμότητα, την υιοθέτηση και την κοινωνική εφαρμογή των αναδυόμενων τεχνολογιών, η οποία χρησιμοποιείται συχνά στην κυβερνοασφάλεια για την αξιολόγηση της ανάπτυξης νέων τεχνολογιών ασφάλειας.

Διακυβέρνηση, κίνδυνοι και συμμόρφωση (GRC) – Στρατηγική για τη διαχείριση της συνολικής διακυβέρνησης ενός οργανισμού (διαδικασίες λήψης αποφάσεων), της διαχείρισης κινδύνων (εντοπισμός και μετριασμός κινδύνων) και της συμμόρφωσης (τήρηση νόμων, κανονισμών και εσωτερικών πολιτικών) σε περιβάλλοντα κυβερνοασφάλειας και απορρήτου δεδομένων.

Gray Hat Hacker – Ένας χάκερ ή εμπειρογνώμονας ασφάλειας που κινείται μεταξύ ηθικής (white hat) και ανήθικης (black hat) συμπεριφοράς, συχνά βρίσκοντας και εκμεταλλευόμενος ευπάθειες χωρίς κακόβουλη πρόθεση αλλά και χωρίς πλήρη άδεια.

Greenfield Network Security – Αναφέρεται σε πρακτικές ασφάλειας δικτύων που εφαρμόζονται σε νέα, πρόσφατα κατασκευασμένα δίκτυα, όπου τα μέτρα ασφάλειας σχεδιάζονται και εφαρμόζονται από την αρχή χωρίς τους περιορισμούς των παλαιών συστημάτων.

Greylist - Ένας μηχανισμός ασφαλείας όπου ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου ή διευθύνσεις IP καθυστερούν προσωρινά ή επισημαίνονται μέχρι να επιβεβαιωθεί η νομιμότητά τους, που χρησιμοποιείται συνήθως στο φιλτράρισμα ηλεκτρονικού ταχυδρομείου για την καταπολέμηση της ανεπιθύμητης αλληλογραφίας.

Guard Bandin - Μια μέθοδος που χρησιμοποιείται στην ασύρματη ασφάλεια η οποία δεσμεύει μέρος του φάσματος συχνοτήτων για την αποφυγή παρεμβολών μεταξύ των καναλιών επικοινωνίας, συμβάλλοντας σε ένα ασφαλέστερο περιβάλλον επικοινωνίας.

Guarded Fabric - Ένας μηχανισμός ασφαλείας που χρησιμοποιείται σε περιβάλλοντα εικονικοποίησης, ιδίως με το Hyper-V, για να διασφαλίσει ότι οι εικονικές μηχανές (VM) προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και παραποίηση.

Guardrails - Πολιτικές ή κατευθυντήριες γραμμές ασφαλείας που εφαρμόζονται σε έναν οργανισμό για την αποτροπή ενεργειών που θα μπορούσαν να οδηγήσουν σε ευπάθειες ή παραβιάσεις της ασφάλειας, εξασφαλίζοντας ένα ασφαλές λειτουργικό περιβάλλον.

Καθοδηγούμενη προσομοίωση κυβερνοασφάλειας - Μια εκπαιδευτική ή μαθησιακή δραστηριότητα όπου οι συμμετέχοντες εμπλέκονται σε προσομοιωμένα σενάρια κυβερνοασφάλειας υπό καθοδήγηση, με σκοπό τη βελτίωση της ευαισθητοποίησης, των δεξιοτήτων και της αντίδρασης σε πραγματικές απειλές κυβερνοασφάλειας.

Καθοδηγούμενη επίθεση κοινωνικής μηχανικής - Μια μορφή επίθεσης κοινωνικής μηχανικής όπου ο επιτιθέμενος παρέχει λεπτές υποδείξεις ή καθοδήγηση για να χειραγωγήσει τον στόχο ώστε να αποκαλύψει εμπιστευτικές πληροφορίες ή να προβεί σε επιβλαβείς ενέργειες.

GUI (Graphical User Interface) Security - Μηχανισμοί ασφαλείας που επικεντρώνονται στη διασφάλιση των διεπαφών χρήστη συστημάτων και εφαρμογών για την αποτροπή μη εξουσιοδοτημένης πρόσβασης ή εκμετάλλευσης τρωτών σημείων στο σχεδιασμό ή την υλοποίηση της διεπαφής.

Guest Access (Πρόσβαση επισκέπτη) - Μια προσωρινή, περιορισμένη μορφή πρόσβασης στο δίκτυο ή στο σύστημα που παρέχεται σε χρήστες που δεν διαθέτουν κανονικούς λογαριασμούς ή διαπιστευτήρια, η οποία χρησιμοποιείται συνήθως σε εταιρικά ή δημόσια περιβάλλοντα για να εξασφαλιστεί η ασφαλής πρόσβαση των επισκεπτών.

Απομόνωση επισκεπτών - Ένα χαρακτηριστικό ασφαλείας στη δικτύωση όπου οι επισκέπτες χρήστες απομονώνονται από το κύριο εσωτερικό δίκτυο, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση σε ευαίσθητους εσωτερικούς πόρους.

Golden Ticket Attack - Μια εξελιγμένη κυβερνοεπίθεση με στόχο τα συστήματα ελέγχου ταυτότητας Kerberos, όπου οι επιτιθέμενοι πλαστογραφούν εισιτήρια ελέγχου ταυτότητας, δίνοντάς τους ουσιαστικά απεριόριστη πρόσβαση σε πόρους εντός του παραβιασμένου δικτύου.

Λεπτομερής έλεγχος πρόσβασης – Μια λεπτομερής και ακριβής προσέγγιση στον έλεγχο πρόσβασης, που επιτρέπει στους οργανισμούς να καθορίζουν συγκεκριμένα προνόμια, δικαιώματα και ρόλους χρηστών για τον περιορισμό της πρόσβασης σε ευαίσθητα δεδομένα και συστήματα.

Google Authenticator – Μια εφαρμογή για κινητά που δημιουργεί κωδικούς πρόσβασης μίας χρήσης με βάση το χρόνο (TOTP) για έλεγχο ταυτότητας δύο παραγόντων (2FA), ο οποίος χρησιμοποιείται συνήθως για την ενίσχυση της ασφάλειας των λογαριασμών.

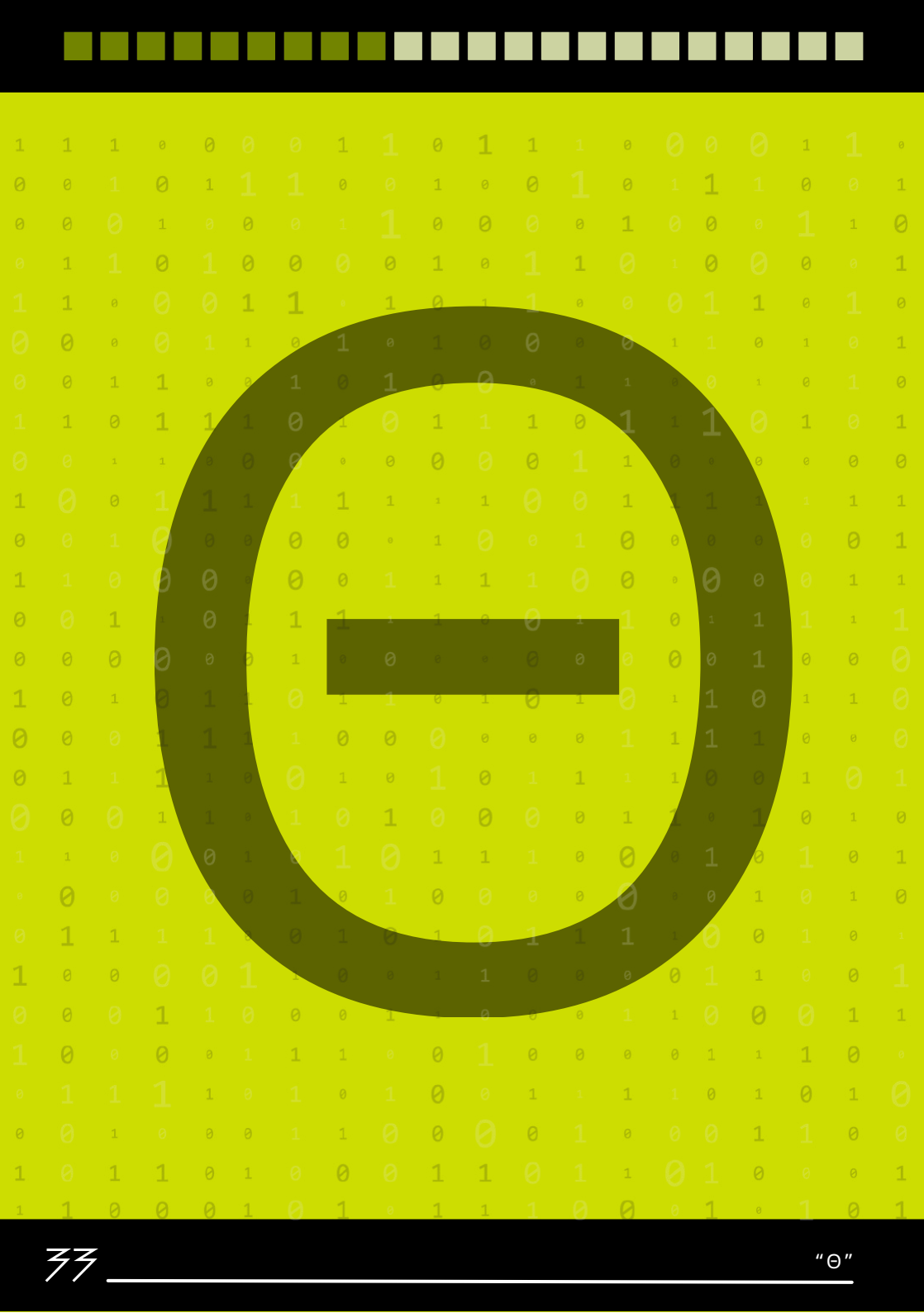
Guideline on the Security Measures for Cloud Services – Ένα σύνολο προτύπων ή συστάσεων που περιγράφουν τα μέτρα ασφαλείας που είναι απαραίτητα για την ασφάλεια των υπηρεσιών υπολογιστικού νέφους, με στόχο την προστασία ευαίσθητων δεδομένων που αποθηκεύονται ή υποβάλλονται σε επεξεργασία σε περιβάλλοντα νέφους.

Group Policy Object (GPO) – Ένα χαρακτηριστικό των Microsoft Windows που επιτρέπει στους διαχειριστές να διαχειρίζονται και να επιβάλλουν ρυθμίσεις ασφαλείας, δικαιώματα χρηστών και πολιτικές σε πολλούς υπολογιστές και χρήστες σε ένα δίκτυο.

GSM Security (Global System for Mobile Communications Security) – Πρωτόκολλα και μηχανισμοί ασφαλείας που έχουν σχεδιαστεί για την προστασία της επικοινωνίας και των δεδομένων που μεταδίδονται μέσω δικτύων GSM, συμπεριλαμβανομένης της κρυπτογράφησης και του ελέγχου ταυτότητας.

Guarded Fabric – Ένας μηχανισμός ασφαλείας που χρησιμοποιείται σε περιβάλλοντα εικονικοποίησης, ιδίως με το Hyper-V, για να διασφαλίσει ότι οι εικονικές μηχανές (VM) προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και παραποίηση.

Guided Penetration Testing (Καθοδηγούμενη δοκιμή διείσδυσης) – Μια ελεγχόμενη δραστηριότητα δοκιμής διείσδυσης όπου στον ελεγκτή παρέχεται κάποιο επίπεδο γνώσης ή βοήθειας από τον υπό δοκιμή οργανισμό, με στόχο τον εντοπισμό ευπαθειών με συνεργατικό τρόπο.


0

IAM (Διαχείριση ταυτότητας και πρόσβασης) - Ένα πλαίσιο πολιτικών και τεχνολογιών που χρησιμοποιούνται για τη διαχείριση και την ασφάλεια της πρόσβασης σε οργανωτικούς πόρους, διασφαλίζοντας ότι τα σωστά άτομα έχουν τα σωστά επίπεδα πρόσβασης.

ICANN (Internet Corporation for Assigned Names and Numbers) - Μη κερδοσκοπικός οργανισμός υπεύθυνος για το συντονισμό της συντήρησης και των διαδικασιών διαφόρων βάσεων δεδομένων που σχετίζονται με τους χώρους ονομάτων του διαδικτύου.

ICS (Industrial Control System) - Συστήματα που χρησιμοποιούνται για τον έλεγχο βιομηχανικών διαδικασιών, όπως η μεταποίηση, η παραγωγή ενέργειας και άλλες υπηρεσίες υποδομής. Η διασφάλιση του ICS αποτελεί σημαντική πτυχή της ασφάλειας στον κυβερνοχώρο.

Ομοσπονδία ταυτοτήτων - Η διαδικασία σύνδεσης της ψηφιακής ταυτότητας ενός χρήστη σε πολλαπλούς τομείς ή οργανισμούς για να επιτραπεί η ενιαία σύνδεση (SSO) και άλλες υπηρεσίες διαχείρισης ταυτότητας.

Απάτη ταυτότητας - Ένας τύπος απάτης όπου ένας επιτιθέμενος χρησιμοποιεί τις προσωπικές πληροφορίες κάποιου άλλου χωρίς την άδειά του, συχνά για να διαπράξει εγκλήματα ή να πραγματοποιήσει μη εξουσιοδοτημένες αγορές.

Διαχείριση περιστατικών - Η διαδικασία εντοπισμού, αντιμετώπισης και μετριασμού των παραβιάσεων δεδομένων και άλλων περιστατικών ασφαλείας.

Μηχανισμός αναφοράς περιστατικών - Η διαδικασία και το σύστημα αναφοράς παραβιάσεων δεδομένων και περιστατικών ασφαλείας σε έναν οργανισμό.

Αντιμετώπιση περιστατικών - Η διαδικασία χειρισμού και διαχείρισης των συνεπειών μιας παραβίασης ασφάλειας ή επίθεσης, με έμφαση στον περιορισμό των ζημιών, την ανάκτηση των επηρεαζόμενων συστημάτων και την πρόληψη μελλοντικών περιστατικών.

Σχέδιο αντιμετώπισης περιστατικών - Ένα σχέδιο που περιγράφει λεπτομερώς τα βήματα που πρέπει να ληφθούν ως απάντηση σε μια παραβίαση δεδομένων ή ένα περιστατικό ασφαλείας.

Ομάδα αντιμετώπισης περιστατικών (IRT) - Μια ομάδα επαγγελματιών που είναι υπεύθυνη για τη διαχείριση και την αντιμετώπιση παραβιάσεων δεδομένων και περιστατικών ασφαλείας.

Indicator of Compromise (IoC) - Ιατροδικαστικά στοιχεία που υποδηλώνουν ότι ένα σύστημα έχει παραβιαστεί, όπως ασυνήθιστα μοτίβα σύνδεσης ή η παρουσία κακόβουλου λογισμικού.

Information Assurance (IA) - Η πρακτική της διασφάλισης της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητα**ς των πληροφοριών, ιδίως σε κυβερνητικά και στρατιωτικά πλαίσια.**

Διαχείριση του κύκλου ζωής των πληροφοριών (ILM) – Στρατηγικές και πρακτικές για τη διαχείριση των πληροφοριών καθ' όλη τη διάρκεια του κύκλου ζωής τους, από τη δημιουργία έως τη διάθεσή τους.

Ασφάλεια πληροφοριών (InfoSec) – Η πρακτική της προστασίας των πληροφοριών μέσω του μετριασμού των κινδύνων και των τρωτών σημείων σε συστήματα, λογισμικό και διαδικασίες.

Σύστημα διαχείρισης ασφάλειας πληροφοριών (ISMS) – Μια συστηματική προσέγγιση για τη διαχείριση ευαίσθητων πληροφοριών ώστε να διατηρούνται ασφαλείς.

Infrared Intrusion Detection System – Συσκευή φυσικής ασφάλειας που χρησιμοποιεί τεχνολογία υπερύθρων για την ανίχνευση μη εξουσιοδοτημένης φυσικής πρόσβασης ή κίνησης σε περιορισμένους χώρους.

Infrastructure as Code (IaC) – Η διαχείριση της υποδομής ΤΠ μέσω κώδικα και αυτοματισμού, εξασφαλίζοντας συνεπείς και ασφαλείς διαμορφώσεις για πόρους cloud και on-premise.

Injection Attack – Ένας τύπος κυβερνοεπίθεσης όπου κακόβουλος κώδικας εισάγεται σε ένα πρόγραμμα ή ερώτημα, όπως SQL injection ή command injection, επιτρέποντας μη εξουσιοδοτημένη πρόσβαση ή χειραγώγηση δεδομένων.

Insider Threat (Απειλή εκ των έσω) – Κίνδυνος ασφάλειας που προέρχεται από άτομα εντός ενός οργανισμού, όπως υπάλληλοι ή εργολάβοι, τα οποία έχουν πρόσβαση σε κρίσιμα συστήματα και δεδομένα.

Ακεραιότητα – Βασική αρχή της ασφάλειας στον κυβερνοχώρο που διασφαλίζει ότι τα δεδομένα παραμένουν ακριβή, πλήρη και αναλλοίωτα, τόσο σε κατάσταση ηρεμίας όσο και κατά τη μεταφορά.

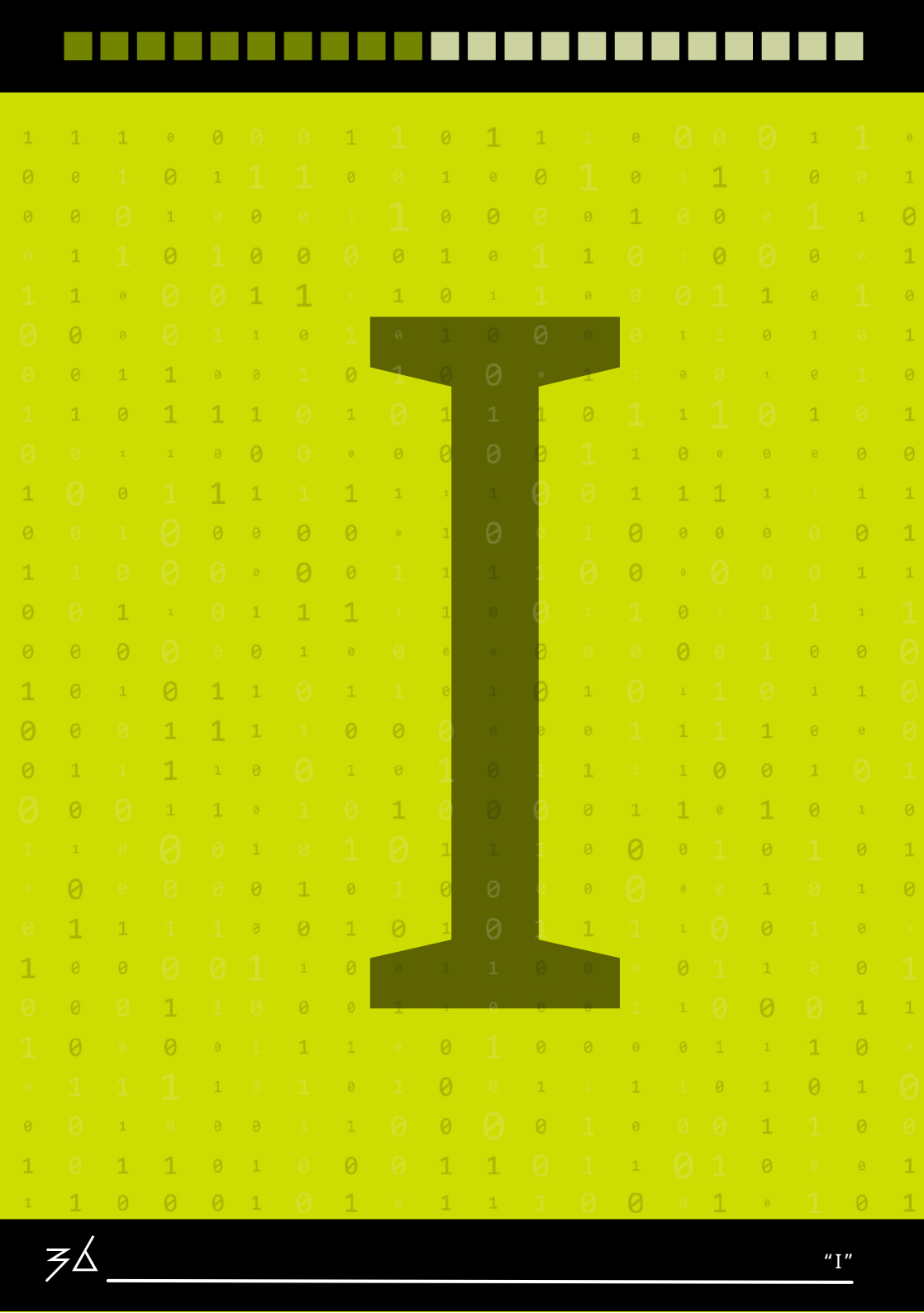
Διαδίκτυο – Αυτός ο περίπλοκος ιστός πληροφοριών και συνδεσιμότητας που σας επιτρέπει να διαβάζετε αυτό το Γλωσσάριο, να παρακολουθείτε βίντεο με γάτες και σκύλους ή να πληρώνετε με κάρτα για τη ζεστή σοκολάτα σας ένα βροχερό κυριακάτικο πρωινό.

Ασφάλεια του Διαδικτύου των Πραγμάτων (IoT) – Η πρακτική της εξασφάλισης της τεράστιας σειράς συσκευών που είναι συνδεδεμένες στο διαδίκτυο και αποτελούν το IoT, διασφαλίζοντας την προστασία τους από πειρατεία, παραβιάσεις της ιδιωτικής ζωής και μη εξουσιοδοτημένη πρόσβαση.

Σύστημα ανίχνευσης εισβολών (IDS) – Μια συσκευή ή εφαρμογή λογισμικού που παρακολουθεί τις δραστηριότητες δικτύου ή συστήματος για κακόβουλες ενέργειες ή παραβιάσεις πολιτικής.

Σύστημα πρόληψης εισβολών (IPS) – Παρόμοιο με το IDS, αλλά με τη δυνατότητα ενεργού αποκλεισμού ή αποτροπής των απειλών που ανιχνεύονται.

Πνευματική ιδιοκτησία – Δημιουργίες του νου για τις οποίες αναγνωρίζονται αποκλειστικά δικαιώματα, συμπεριλαμβανομένων των δεδομένων και του λογισμικού.



Jailbreaking – Η διαδικασία άρσης των περιορισμών λογισμικού που επιβάλλονται από τον κατασκευαστή σε συσκευές όπως τα **smartphones**, εκθέτοντας συχνά τη συσκευή σε κινδύνους ασφαλείας.

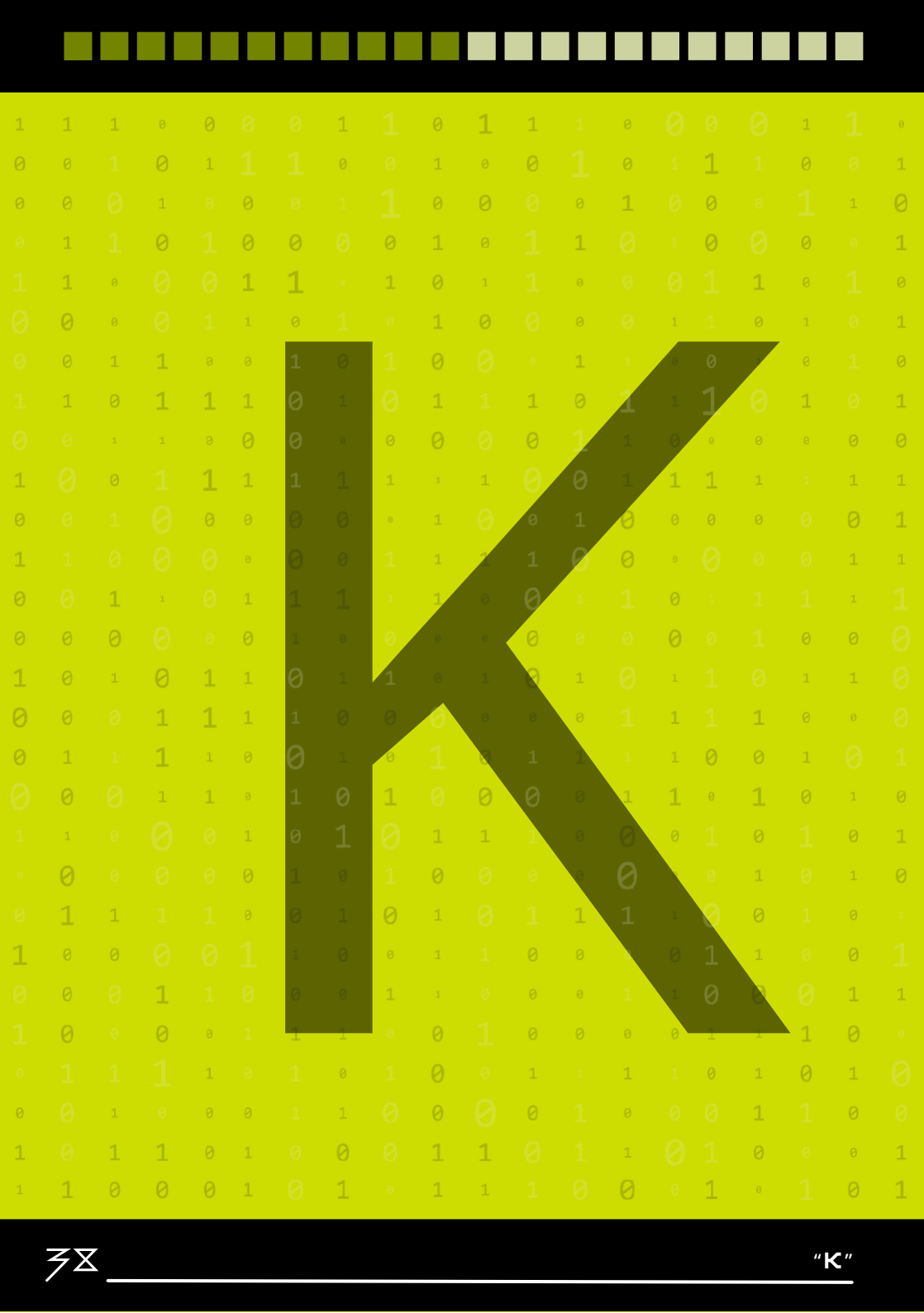
JavaScript Injection – Ένας τύπος επίθεσης έγχυσης όπου κακόβουλος κώδικας **JavaScript** εισάγεται σε έναν ιστότοπο, που χρησιμοποιείται συχνά σε επιθέσεις **cross-site scripting (XSS)**.

Joint Authorization Board (JAB) – Μια ομάδα εντός της κυβέρνησης των ΗΠΑ που είναι υπεύθυνη για την εξέταση και την έγκριση παρόχων υπηρεσιών **cloud** για ομοσπονδιακή χρήση στο πλαίσιο του προγράμματος **FedRAMP**.

Jitter – Ένα ζήτημα απόδοσης δικτύου όπου τα πακέτα δεδομένων παρουσιάζουν ποικίλες καθυστερήσεις, επηρεάζοντας δυνητικά την ποιότητα των υπηρεσιών **VoIP** ή τηλεδιάσκεψης.

Just-in-Time (JIT) Access – Μια έννοια ασφάλειας που επιτρέπει στους χρήστες προσωρινή και περιορισμένη πρόσβαση σε κρίσιμα συστήματα ή δεδομένα, εξασφαλίζοντας ότι έχουν αρκετό χρόνο για να ολοκληρώσουν μια εργασία πριν ανακληθεί η πρόσβαση.

Δικαιοδοσία – Η γεωγραφική περιοχή εντός της οποίας ισχύουν οι νόμοι και οι κανονισμοί για την προστασία των δεδομένων.


K

Key Derivation Function (KDF) - Μια κρυπτογραφική συνάρτηση που χρησιμοποιείται για την εξαγωγή κλειδιών από μια βασική τιμή, η οποία χρησιμοποιείται συχνά στον κατακερματισμό και την κρυπτογράφηση κωδικών πρόσβασης.

Key Escrow - Ένα σύστημα όπου τα κρυπτογραφικά κλειδιά φυλάσσονται με εγγύηση, συχνά από τρίτο μέρος, για να επιτρέπεται η πρόσβαση σε περιπτώσεις έκτακτης ανάγκης ή κανονιστικών απαιτήσεων.

Key Management Interoperability Protocol (KMIP) - Τυποποιημένο πρωτόκολλο που χρησιμοποιείται για τη διαχείριση κλειδιών κρυπτογράφησης σε διαφορετικά συστήματα και περιβάλλοντα, βελτιώνοντας την ασφάλεια και τη συμμόρφωση.

Πολιτική εναλλαγής κλειδιών - Μια πολιτική ασφαλείας που ορίζει πόσο συχνά πρέπει να εναλλάσσονται ή να αλλάζουν τα κρυπτογραφικά κλειδιά ώστε να ελαχιστοποιείται ο κίνδυνος παραβίασης των κλειδιών.

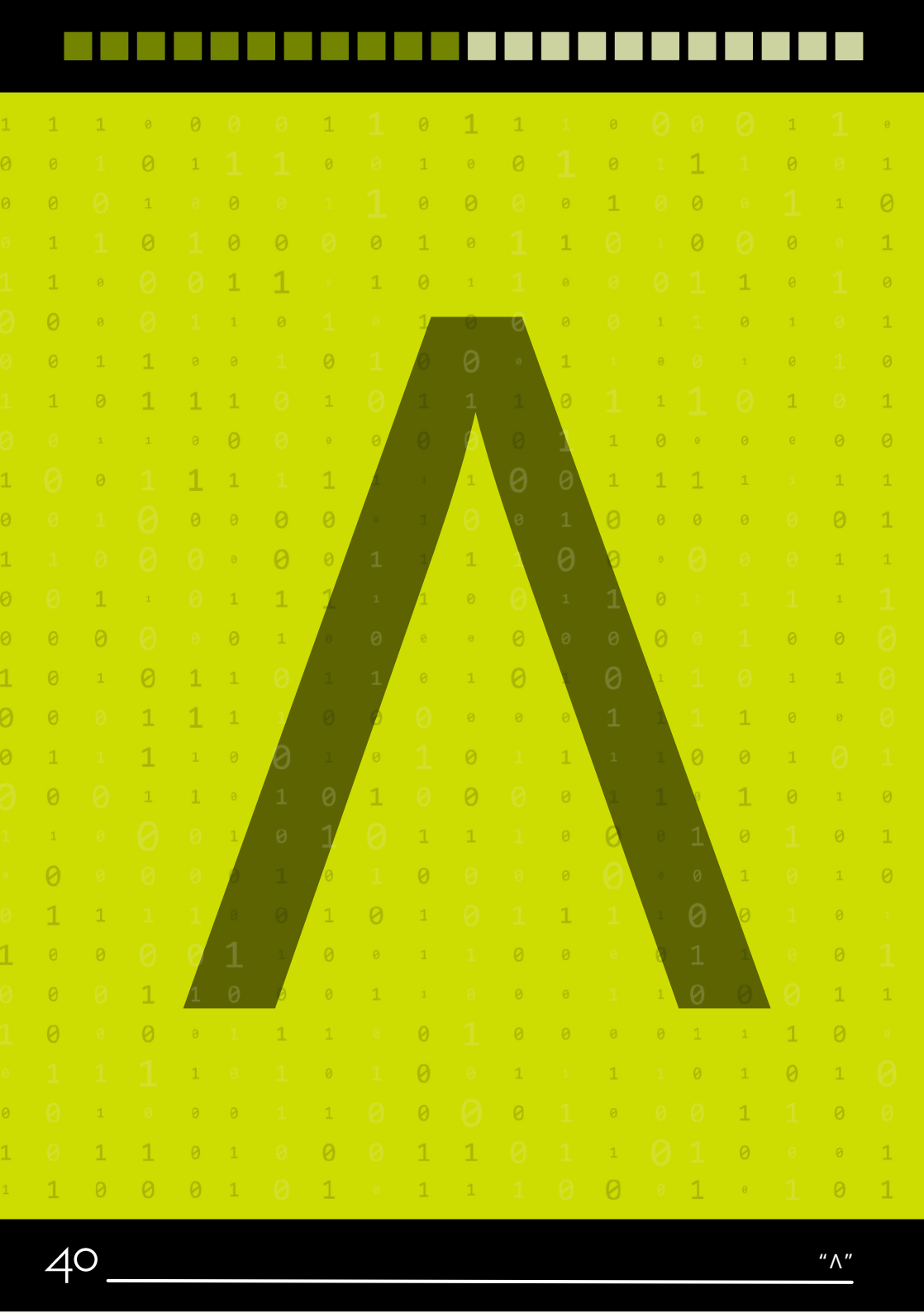
Κρυπτογράφηση πληκτρολόγησης - Μια μέθοδος κρυπτογράφησης των πληκτρολογήσεων μεταξύ του πληκτρολογίου και της εφαρμογής για την αποτροπή επιθέσεων keylogging.

Kill Process Attack - Μια επίθεση κατά την οποία κακόβουλος κώδικας αναγκάζει κρίσιμες διεργασίες ή εφαρμογές να τερματιστούν, οδηγώντας συχνά σε κατάρρευση του συστήματος ή σε ευπάθειες.

Ανακάλυψη γνώσης σε βάσεις δεδομένων (KDD) - Η διαδικασία ανακάλυψης χρήσιμων πληροφοριών και μοτίβων από μεγάλα σύνολα δεδομένων, που χρησιμοποιείται συχνά στην ανάλυση ασφάλειας για τον εντοπισμό πιθανών απειλών.

Known Plaintext Attack (KPA) - Μια τεχνική κρυπτανάλυσης όπου ο επιτιθέμενος έχει πρόσβαση τόσο στο απλό κείμενο όσο και στο αντίστοιχο κρυπτογραφημένο κείμενο, χρησιμοποιώντας αυτές τις πληροφορίες για να αποκαλύψει τη μέθοδο κρυπτογράφησης.

Επίθεση Krack - Μια ευπάθεια στο πρωτόκολλο κρυπτογράφησης WPA2 Wi-Fi που επιτρέπει στους επιτιθέμενους να υποκλέπτουν και να χειρίζονται την κυκλοφορία μεταξύ συσκευών και ασύρματων δικτύων.



LAN (Local Area Network) – Ένα δίκτυο που συνδέει υπολογιστές σε μια περιορισμένη περιοχή, όπως το σπίτι, το σχολείο ή το γραφείο, συχνά ασφαλές μέσω τειχών προστασίας και κρυπτογράφησης.

LDAP (Lightweight Directory Access Protocol) – Ένα πρωτόκολλο που χρησιμοποιείται για την πρόσβαση και τη διαχείριση υπηρεσιών πληροφοριών καταλόγου μέσω ενός δικτύου IP, το οποίο χρησιμοποιείται συχνά σε κεντρικά συστήματα ελέγχου ταυτότητας και εξουσιοδότησης.

Νόμιμη βάση επεξεργασίας – Οι νομικοί λόγοι βάσει των οποίων ένας οργανισμός μπορεί να επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, όπως ορίζονται από τους νόμους περί προστασίας δεδομένων.

Νομική βάση για την επεξεργασία δεδομένων – Η αιτιολόγηση που απαιτείται σύμφωνα με τους νόμους περί προστασίας δεδομένων για την επεξεργασία δεδομένων προσωπικού χαρακτήρα, όπως η συγκατάθεση ή η συμβατική αναγκαιότητα.

Νομική συμμόρφωση – Η διαδικασία διασφάλισης ότι ένας οργανισμός τηρεί τους σχετικούς νόμους, κανονισμούς και κατευθυντήριες γραμμές που σχετίζονται με το απόρρητο των δεδομένων, την ασφάλεια στον κυβερνοχώρο και την προστασία των δεδομένων (π.χ. GDPR, HIPAA).

Νομοθετικό πλαίσιο – Το σύνολο των νόμων και κανονισμών που διέπουν το απόρρητο και την προστασία των δεδομένων.

Letterbomb – Ένας τύπος επίθεσης μέσω ηλεκτρονικού ταχυδρομείου ή μηνύματος που περιέχει κακόβουλο κώδικα σχεδιασμένο να εκμεταλλεύεται τρωτά σημεία όταν το ανοίγει ο παραλήπτης.

Library Injection – Μέθοδος εισαγωγής κακόβουλου κώδικα στη βιβλιοθήκη λογισμικού ενός προγράμματος για την αλλαγή της κανονικής συμπεριφοράς του ή την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε πόρους του συστήματος.

Linux Security Modules (LSM) – Ένα πλαίσιο στο λειτουργικό σύστημα Linux που επιτρέπει την επιβολή υποχρεωτικών ελέγχων πρόσβασης, επιτρέποντας στους διαχειριστές να ορίζουν και να εφαρμόζουν πολιτικές ασφαλείας.

Συγκέντρωση αρχείων καταγραφής – Η διαδικασία συλλογής και συγκέντρωσης δεδομένων καταγραφής από διάφορα συστήματα και εφαρμογές σε μια ενιαία τοποθεσία για ανάλυση και παρακολούθηση της ασφάλειας.

Διαχείριση αρχείων καταγραφής – Η πρακτική της καταγραφής, αποθήκευσης και ανάλυσης των αρχείων καταγραφής που παράγονται από το λογισμικό, το υλικό και τις συσκευές δικτύου για σκοπούς αντιμετώπισης προβλημάτων και ασφάλειας.

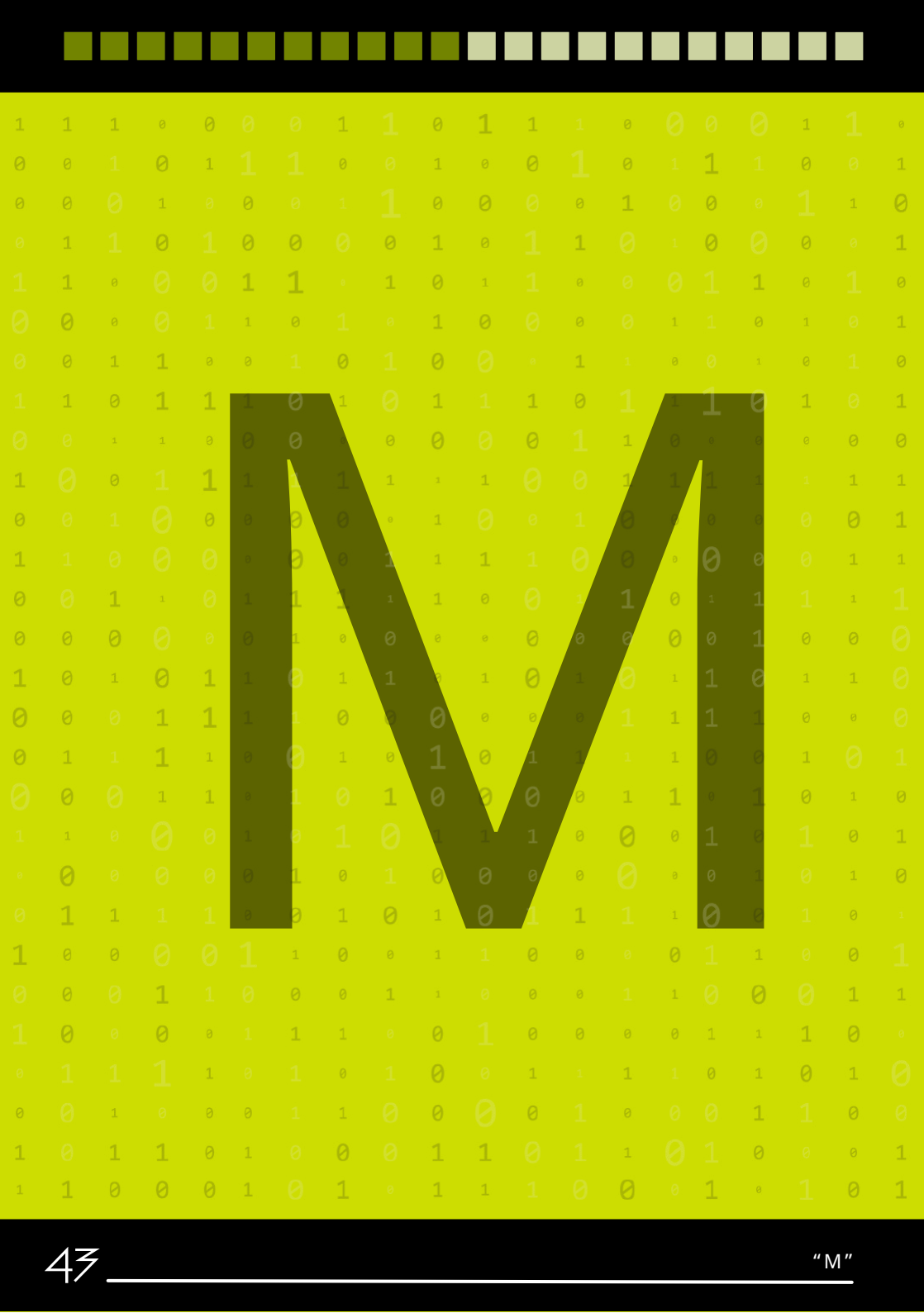
Πολιτική διατήρησης αρχείων καταγραφής – Ένα σύνολο κατευθυντήριων γραμμών που καθορίζουν πόσο καιρό θα πρέπει να διατηρούνται τα δεδομένα καταγραφής πριν αρχειοθετηθούν ή διαγραφούν, συχνά απαιτείται για τη συμμόρφωση με τους κανονισμούς απορρήτου δεδομένων.

Λογικός έλεγχος πρόσβασης - Μηχανισμοί ασφαλείας που περιορίζουν την πρόσβαση σε δεδομένα ή πόρους με βάση προκαθορισμένους κανόνες, οι οποίοι συνήθως διαχειρίζονται μέσω συστημάτων ελέγχου ταυτότητας και εξουσιοδότησης.

Λογική βόμβα - Κακόβουλο πρόγραμμα ή κώδικας που παραμένει αδρανής σε ένα σύστημα έως ότου ενεργοποιηθεί από συγκεκριμένες συνθήκες, οπότε και ενεργοποιείται και προκαλεί βλάβη.

Long-Term Persistence Attack - Ένας τύπος κυβερνοεπίθεσης όπου ένας επιτιθέμενος διατηρεί απαρατήρητη πρόσβαση σε ένα σύστημα για παρατεταμένο χρονικό διάστημα, επιτρέποντάς του να συλλέξει πληροφορίες ή να πραγματοποιήσει περαιτέρω επιθέσεις.

Lua-based Security - Μέτρα και έλεγχοι ασφαλείας που υλοποιούνται με τη χρήση της γλώσσας σεναρίων Lua, η οποία χρησιμοποιείται συχνά σε ενσωματωμένα συστήματα και παιχνίδια για χαρακτηριστικά ασφαλείας όπως ο έλεγχος ταυτότητας σεναρίων.


M

MAC (Mandatory Access Control) – Ένας τύπος ελέγχου πρόσβασης όπου η πρόσβαση σε πόρους χορηγείται με βάση πολιτικές που καθορίζονται από μια κεντρική αρχή, συνήθως σε ιδιαίτερα ασφαλή περιβάλλοντα.

Διεύθυνση MAC (Media Access Control Address) – Μοναδικό αναγνωριστικό που εκχωρείται σε διεπαφές δικτύου για επικοινωνία στο επίπεδο ζεύξης δεδομένων ενός δικτύου, το οποίο χρησιμοποιείται συχνά για την ταυτοποίηση συσκευών και την ασφάλεια του δικτύου.

Μηχανική μάθηση – Ένας τύπος τεχνητής νοημοσύνης που επιτρέπει στα συστήματα να μαθαίνουν και να λαμβάνουν αποφάσεις από δεδομένα χωρίς να προγραμματίζονται ρητά.

Machine Learning Security – Η εφαρμογή αλγορίθμων μηχανικής μάθησης για τον εντοπισμό ανωμαλιών, την πρόβλεψη απειλών και τη βελτίωση της άμυνας στον κυβερνοχώρο με βάση μεγάλα σύνολα δεδομένων.

Κακόβουλος κώδικας – Κάθε κώδικας ή λογισμικό που έχει σχεδιαστεί για να βλάψει, να εκμεταλλευτεί ή να θέσει με άλλο τρόπο σε κίνδυνο ένα σύστημα, συμπεριλαμβανομένων ιών, σκουληκιών, δούρειων ίππων, ransomware και spyware.

Κακόβουλο λογισμικό (Malware) – Ένας όρος που αναφέρεται σε λογισμικό ειδικά σχεδιασμένο για να διαταράξει, να βλάψει ή να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε ένα σύστημα ή δίκτυο.

Man-in-the-Middle Attack (MITM) – Επίθεση κατά την οποία ένας κακόβουλος φορέας υποκλέπτει και ενδεχομένως τροποποιεί την επικοινωνία μεταξύ δύο μερών εν αγνοία τους, η οποία συχνά χρησιμοποιείται για την κλοπή ευαίσθητων δεδομένων.

Υποχρεωτική κρυπτογράφηση – Μια πολιτική που απαιτεί την κρυπτογράφηση όλων των ευαίσθητων δεδομένων τόσο κατά την ηρεμία όσο και κατά τη μεταφορά, ώστε να διασφαλίζεται η εμπιστευτικότητα και η ακεραιότητά τους.

Χειροκίνητη δοκιμή διείσδυσης – Η διαδικασία χειροκίνητης δοκιμής ενός συστήματος ή δικτύου για ευπάθειες μέσω προσομοίωσης πραγματικών σεναρίων επίθεσης, σε αντίθεση με τη χρήση αυτοματοποιημένων εργαλείων.

Ιός κύριας εγγραφής εκκίνησης (MBR) – Ένας τύπος ιού που μολύνει την κύρια εγγραφή εκκίνησης ενός σκληρού δίσκου, επιτρέποντάς του να φορτώνει πριν από την εκκίνηση του λειτουργικού συστήματος και καθιστώντας δύσκολη την ανίχνευσή του.

MD5 (Message Digest Algorithm 5) – Μια ευρέως χρησιμοποιούμενη κρυπτογραφική συνάρτηση κατακερματισμού που παράγει μια τιμή κατακερματισμού 128 bit, η οποία χρησιμοποιείται συνήθως για την επαλήθευση της ακεραιότητας των δεδομένων, αλλά δεν θεωρείται πλέον ασφαλής λόγω ευπάθειας σε επιθέσεις σύγκρουσης.

Διαφθορά μνήμης - Μια ευπάθεια λογισμικού κατά την οποία τα περιεχόμενα της μνήμης ενός υπολογιστή τροποποιούνται ακούσια, επιτρέποντας δυνητικά σε έναν εισβολέα να εκμεταλλευτεί το σύστημα.

Memory Dump - Ένα αρχείο που καταγράφει τα περιεχόμενα της μνήμης σε μια δεδομένη χρονική στιγμή, το οποίο χρησιμοποιείται συχνά για εγκληματολογική ανάλυση κατά την αντιμετώπιση περιστατικών για τη διερεύνηση επιθέσεων.

Ακεραιότητα μηνύματος - Μια έννοια ασφάλειας που διασφαλίζει ότι ένα μήνυμα ή δεδομένα δεν έχουν αλλοιωθεί κατά τη μεταφορά, η οποία συνήθως επιτυγχάνεται μέσω κατακερματισμού ή ψηφιακών υπογραφών.

Μεταδεδομένα - Δεδομένα που παρέχουν πληροφορίες σχετικά με άλλα δεδομένα, όπως το μέγεθος του αρχείου ή η ημερομηνία δημιουργίας.

Ασφάλεια μεταδεδομένων - Η προστασία των μεταδεδομένων (δεδομένα σχετικά με τα δεδομένα), τα οποία θα μπορούσαν να αποκαλύψουν ευαίσθητες πληροφορίες σχετικά με συστήματα, αρχεία ή επικοινωνίες, ακόμη και αν τα υποκείμενα δεδομένα είναι κρυπτογραφημένα.

Μετριασμός - Η διαδικασία μείωσης της σοβαρότητας, του αντίκτυπου ή της πιθανότητας μιας απειλής ή ευπάθειας στον κυβερνοχώρο μέσω διαφόρων μέτρων ασφαλείας.

Mobile Device Management (MDM) - Μια λύση λογισμικού που χρησιμοποιείται από οργανισμούς για τη διαχείριση, την παρακολούθηση και την ασφάλεια κινητών συσκευών, όπως **smartphones** και **tablets**, διασφαλίζοντας τη συμμόρφωση με τις πολιτικές ασφαλείας.

Multi-Factor Authentication (MFA) - Μια διαδικασία ασφαλείας που απαιτεί από τους χρήστες να παρέχουν δύο ή περισσότερους παράγοντες επαλήθευσης για να αποκτήσουν πρόσβαση σε ένα σύστημα, προσθέτοντας ένα επιπλέον επίπεδο ασφάλειας πέρα από τους απλούς κωδικούς πρόσβασης.

Αμοιβαίος έλεγχος ταυτότητας - Μια διαδικασία ασφάλειας όπου τόσο ο χρήστης όσο και το σύστημα πιστοποιούν ο ένας τον άλλον για να διασφαλιστεί ότι και τα δύο μέρη είναι νόμιμα, χρησιμοποιείται συχνά σε ασφαλείς επικοινωνίες.


N

NAC (Network Access Control) – Μια λύση ασφαλείας που περιορίζει την πρόσβαση μη εξουσιοδοτημένων συσκευών σε ένα δίκτυο, επιβάλλοντας πολιτικές ασφαλείας και ελέγχους συμμόρφωσης.

Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) – Ομοσπονδιακός οργανισμός των ΗΠΑ που αναπτύσσει και προωθεί πρότυπα, συμπεριλαμβανομένων πλαισίων κυβερνοασφάλειας, για τη διασφάλιση της ασφάλειας των δεδομένων και την προστασία των υποδομών ζωτικής σημασίας.

Network Address Translation (NAT) – Μια τεχνική που χρησιμοποιείται στη δικτύωση για τη μετάφραση ιδιωτικών διευθύνσεων IP εντός ενός τοπικού δικτύου σε μια δημόσια διεύθυνση IP, επιτρέποντας σε πολλές συσκευές να μοιράζονται μια ενιαία διεύθυνση IP.

Network Forensics – Η διαδικασία σύλληψης, καταγραφής και ανάλυσης της κίνησης δικτύου για τη διερεύνηση και κατανόηση περιστατικών ή εγκλημάτων ασφαλείας που βασίζονται στο δίκτυο.

Network Intrusion Detection System (NIDS) – Ένα σύστημα που παρακολουθεί την κυκλοφορία του δικτύου για ύποπτη δραστηριότητα και πιθανές απειλές, το οποίο συνήθως αναπτύσσεται σε στρατηγικά σημεία ενός δικτύου.

Network Intrusion Prevention System (NIPS) – Ένα σύστημα που έχει σχεδιαστεί για να ανιχνεύει και να αποτρέπει πιθανές απειλές, παρακολουθώντας την κυκλοφορία του δικτύου και εμποδίζοντας τις κακόβουλες δραστηριότητες πριν προλάβουν να βλάψουν το σύστημα.

Χαρτογράφηση δικτύου – Η διαδικασία ανακάλυψης και απεικόνισης της διάταξης ενός δικτύου, συμπεριλαμβανομένων των συσκευών, των συνδέσεων και των διαμορφώσεων, που χρησιμοποιείται συχνά για αξιολογήσεις και διαχείριση της ασφάλειας.

Πολιτική δικτύου – Κανόνες και κατευθυντήριες γραμμές που διέπουν τη διαχείριση, τη διαμόρφωση και την ασφάλεια των πόρων του δικτύου, συμπεριλαμβανομένων των ελέγχων πρόσβασης και των πολιτικών χρήσης.

Ασφάλεια δικτύου – Τα μέτρα και οι πρακτικές που χρησιμοποιούνται για την προστασία ενός δικτύου από μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και κακή χρήση, συμπεριλαμβανομένης της χρήσης τειχών προστασίας, συστημάτων ανίχνευσης εισβολών και κρυπτογράφησης.

Τμηματοποίηση δικτύου – Η πρακτική της διαίρεσης ενός δικτύου υπολογιστών σε μικρότερα, απομονωμένα υποδίκτυα για τη μείωση της επιφάνειας επίθεσης και την αποτροπή της πλευρικής μετακίνησης των επιτιθέμενων εντός του δικτύου.

Ανάλυση κίνησης δικτύου – Η διαδικασία εξέτασης των δεδομένων που διακινούνται μέσω ενός δικτύου για την παρακολούθηση της απόδοσης, την ανίχνευση ανωμαλιών και τον εντοπισμό πιθανών απειλών ασφαλείας.

Ανιχνευτής τρωτών σημείων δικτύου – Ένα εργαλείο που χρησιμοποιείται για τη σάρωση δικτύων για γνωστά τρωτά σημεία και αδυναμίες ασφαλείας, συμβάλλοντας στον εντοπισμό και την αντιμετώπιση πιθανών κινδύνων πριν από την εκμετάλλευσή τους.

Μη συμμόρφωση – Μη τήρηση των νόμων και των κανονισμών προστασίας δεδομένων.

Non-Repudiation – Μια έννοια ασφάλειας που εξασφαλίζει τη γνησιότητα και την ακεραιότητα των επικοινωνιών, καθιστώντας αδύνατο για τον αποστολέα να αρνηθεί την αποστολή ενός μηνύματος ή μιας συναλλαγής.

Nonce – Μια τυχαία ή μοναδική τιμή που χρησιμοποιείται στην κρυπτογραφική επικοινωνία για να εξασφαλιστεί ότι οι παλιές επικοινωνίες δεν μπορούν να επαναχρησιμοποιηθούν σε επιθέσεις αναπαραγωγής.

Null Cipher – Μια μέθοδος απόκρυψης μηνυμάτων μέσα σε ένα μπλοκ μη απόρρητων πληροφοριών, όπου το μήνυμα εξάγεται χρησιμοποιώντας ένα προκαθορισμένο μοτίβο ή κλειδί.

Μηδενική κρυπτογράφηση – Ένας όρος που αναφέρεται σε κρυπτογράφηση που είναι ουσιαστικά ανύπαρκτη, συχνά λόγω αδύναμων ή σπασμένων αλγορίθμων κρυπτογράφησης που δεν παρέχουν επαρκή προστασία.

Null Session – Ένας τύπος μη εξουσιοδοτημένης σύνδεσης σε ένα σύστημα των Windows που μπορεί να επιτρέψει στους επιτιθέμενους να απαριθμήσουν τις κοινότητες, τους χρήστες και άλλες ευαίσθητες πληροφορίες.

Nullification (Μηδενισμός) – Η διαδικασία αδρανοποίησης δεδομένων ή ενός χαρακτηριστικού ασφαλείας, που χρησιμοποιείται συχνά στο πλαίσιο επιθέσεων παράκαμψης ασφαλείας ή ανάκλησης πρόσβασης.

Ασφάλεια NVRAM (Non-Volatile Random Access Memory) – Μηχανισμοί ασφαλείας που εφαρμόζονται στην αποθήκευση NVRAM για την προστασία κρίσιμων δεδομένων διαμόρφωσης από αλλοίωση ή μη εξουσιοδοτημένη πρόσβαση.

Κανονικοποίηση – Η διαδικασία τυποποίησης δεδομένων σε κοινή μορφή για τη βελτίωση της συνέπειας, της χρηστικότητας και της ανάλυσης, που χρησιμοποιείται συχνά στη διαχείριση βάσεων δεδομένων και στην επεξεργασία δεδομένων.

Βάση δεδομένων NoSQL – Ένας τύπος βάσης δεδομένων που παρέχει έναν μηχανισμό αποθήκευσης και ανάκτησης δεδομένων μοντελοποιημένων με τρόπους διαφορετικούς από τις σχέσεις σε μορφή πίνακα που χρησιμοποιούνται στις βάσεις δεδομένων SQL, ο οποίος χρησιμοποιείται συχνά για τη διαχείριση μεγάλου όγκου μη δομημένων δεδομένων.

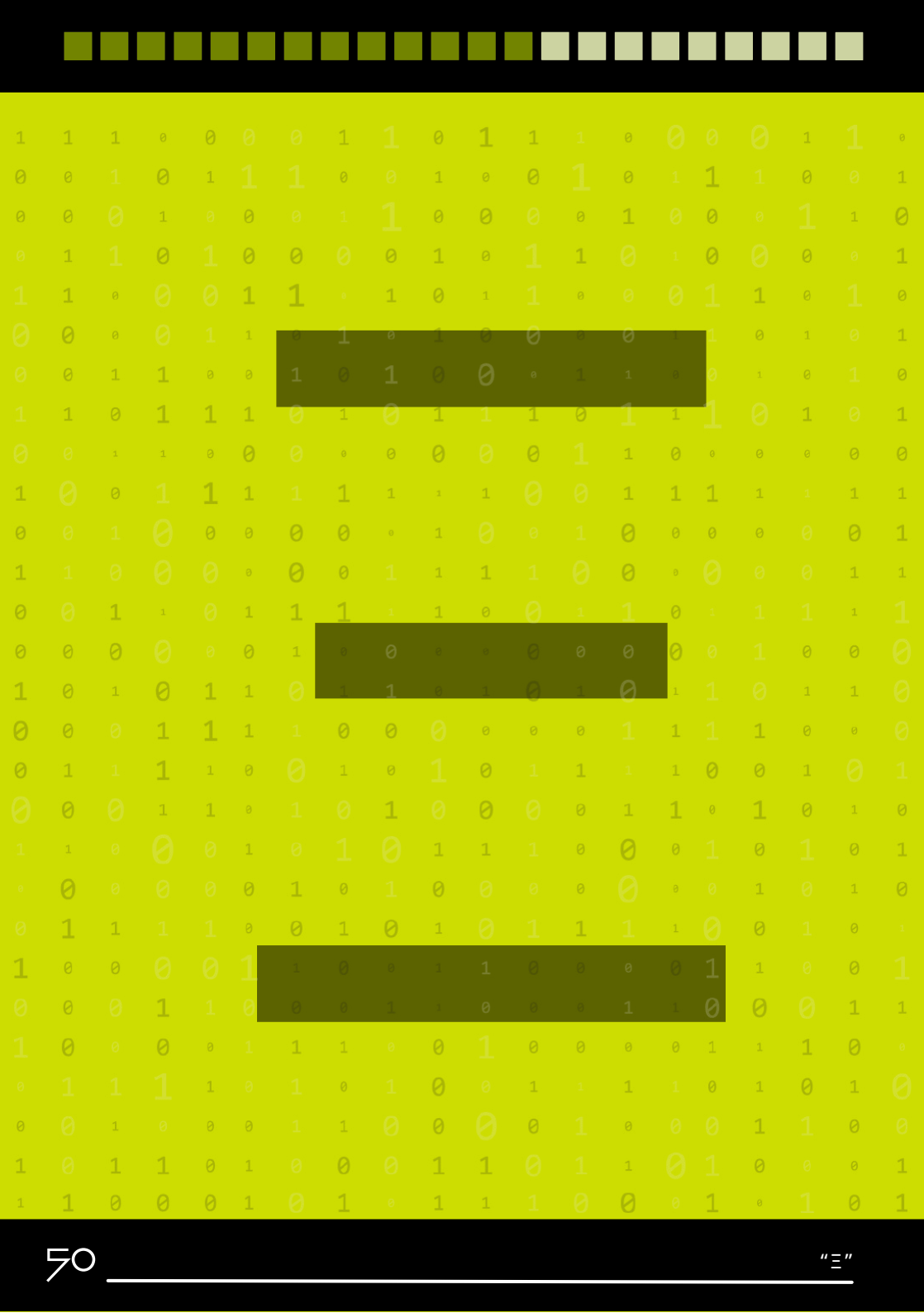
Κόμβος – Μια συσκευή δικτύου ή ένα σημείο όπου γίνεται επεξεργασία ή μετάδοση δεδομένων, όπως ένας υπολογιστής, ένας δρομολογητής ή ένας μεταγωγέας, στο πλαίσιο μιας υποδομής δικτύου.

Αυθεντικοποίηση κόμβου – Η διαδικασία επαλήθευσης της ταυτότητας ενός κόμβου (π.χ. μιας συσκευής ή ενός συστήματος) μέσα σε ένα δίκτυο για να διασφαλιστεί ότι είναι εξουσιοδοτημένος να έχει πρόσβαση ή να επικοινωνεί με άλλους κόμβους.

Ασφάλεια νευρωνικών δικτύων – Η εφαρμογή τεχνικών βασισμένων σε νευρωνικά δίκτυα για την ενίσχυση της ασφάλειας στον κυβερνοχώρο, όπως η χρήση τεχνητών νευρωνικών δικτύων για την ανίχνευση ανωμαλιών και την πρόβλεψη απειλών.

Μη ασφαλές πρωτόκολλο – Ένα πρωτόκολλο επικοινωνίας που δεν παρέχει κρυπτογράφηση ή άλλα μέτρα ασφαλείας για την προστασία των δεδομένων κατά τη μετάδοση, όπως το HTTP (σε αντίθεση με το HTTPS).

Non-Disclosure Agreement (NDA) – Μια νομική σύμβαση μεταξύ των μερών για την προστασία ευαίσθητων πληροφοριών από την αποκάλυψη σε μη εξουσιοδοτημένα άτομα ή οντότητες.



OAuth (Open Authorization) – Ένα ανοιχτό πρότυπο για έλεγχο ταυτότητας και εξουσιοδότηση στο διαδίκτυο με βάση token, το οποίο χρησιμοποιείται συχνά για να επιτρέπει σε εφαρμογές τρίτων να έχουν πρόσβαση σε πληροφορίες χρηστών χωρίς να εκθέτουν κωδικούς πρόσβασης.

Υποχρεώσεις των υπευθύνων επεξεργασίας δεδομένων – Υποχρεώσεις που έχουν οι οργανισμοί που καθορίζουν τους σκοπούς και τα μέσα επεξεργασίας δεδομένων.

Υποχρεώσεις των υπευθύνων επεξεργασίας δεδομένων – Υποχρεώσεις των οργανισμών που επεξεργάζονται δεδομένα για λογαριασμό των υπευθύνων επεξεργασίας δεδομένων.

Ασφάλεια σε επίπεδο αντικειμένου – Μέτρα ασφαλείας που εφαρμόζονται σε μεμονωμένα αντικείμενα, όπως αρχεία ή εγγραφές βάσεων δεδομένων, ώστε να διασφαλίζεται ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση σε αυτά ή να τα τροποποιούν.

Επιθετική ασφάλεια – Κλάδος της ασφάλειας στον κυβερνοχώρο που επικεντρώνεται στην προσομοίωση επιθέσεων για τον εντοπισμό τρωτών σημείων και τη βελτίωση της αμυντικής στάσης ενός συστήματος ή δικτύου.

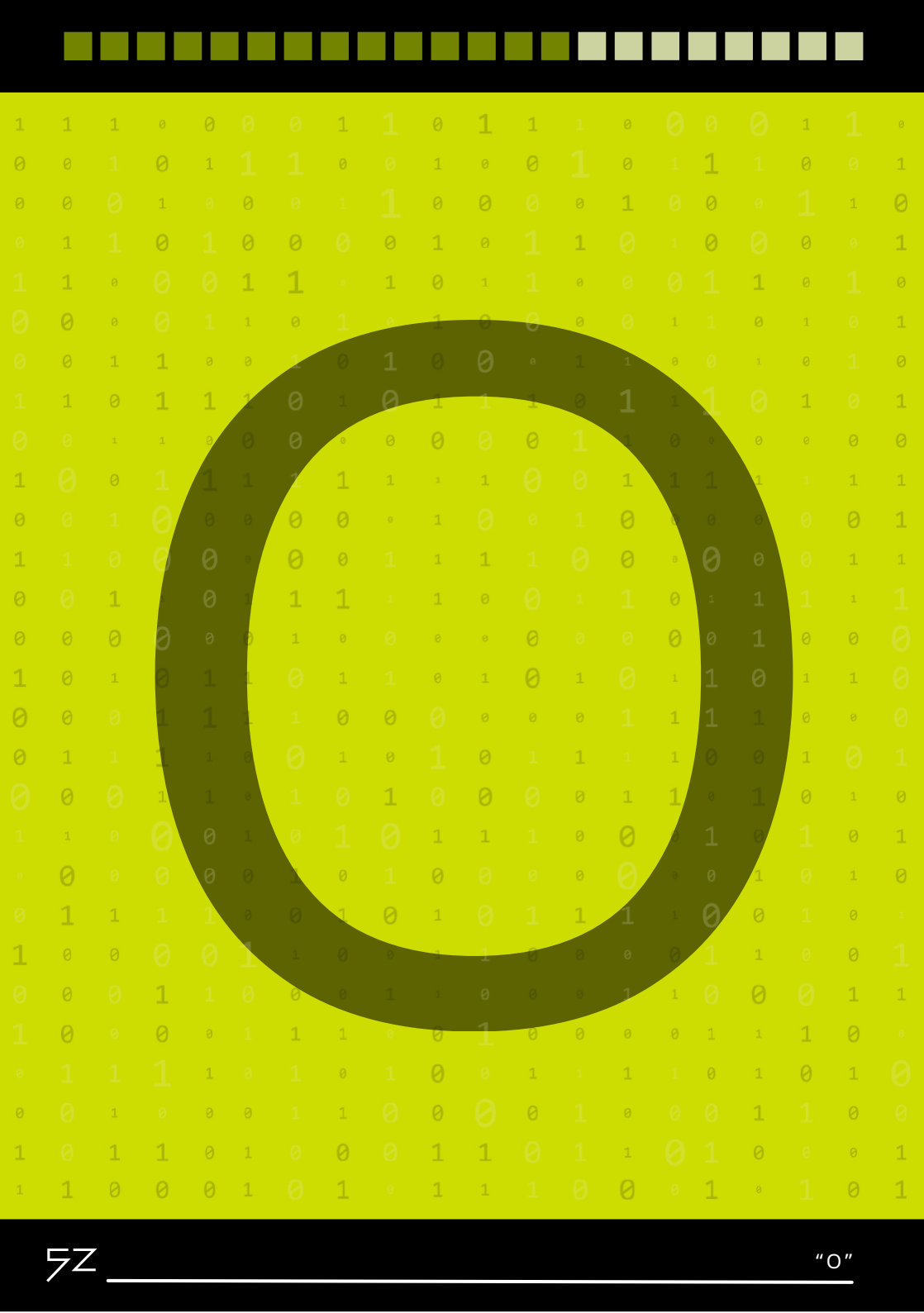
One-Time Pad (OTP) – Μια θεωρητικά άθραυστη μέθοδος κρυπτογράφησης όπου ένα τυχαίο κλειδί, που χρησιμοποιείται μόνο μία φορά, συνδυάζεται με το απλό κείμενο για την παραγωγή του κρυπτοκειμένου.

Open Source Intelligence (OSINT) – Η πρακτική της συλλογής και ανάλυσης δημοσίως διαθέσιμων δεδομένων από ανοικτές πηγές (όπως μέσα κοινωνικής δικτύωσης, δημόσια αρχεία και ιστότοποι) για σκοπούς κυβερνοασφάλειας και πληροφοριών σχετικά με απειλές.

Σκλήρυνση λειτουργικού συστήματος – Η διαδικασία διασφάλισης ενός λειτουργικού συστήματος με τη μείωση της επιφάνειας επίθεσής του, όπως η απενεργοποίηση περιττών υπηρεσιών, η εφαρμογή επιδιορθώσεων και η διαμόρφωση ρυθμίσεων ασφαλείας.

Over-The-Air (OTA) Update Security – Μέτρα ασφαλείας που προστατεύουν τις ενημερώσεις λογισμικού που παραδίδονται ασύρματα σε συσκευές όπως τα smartphones και οι συσκευές IoT, διασφαλίζοντας ότι οι ενημερώσεις είναι αυθεντικές και δεν έχουν αλλοιωθεί.

Obfuscation – Η διαδικασία που καθιστά σκόπιμα τον κώδικα ή τα δεδομένα δυσκολότερα κατανοητά ή αναστρέψιμα, η οποία χρησιμοποιείται συχνά για την προστασία ευαίσθητων πληροφοριών ή την αποτροπή της ανάλυσης κακόβουλου λογισμικού.


0

Φιλτράρισμα πακέτων – Μια τεχνική τείχους προστασίας που εξετάζει τις επικεφαλίδες των πακέτων δεδομένων και τα επιτρέπει ή τα αποκλείει με βάση προκαθορισμένους κανόνες, όπως οι διευθύνσεις IP πηγής και προορισμού.

Σπάσιμο κωδικού πρόσβασης – Η διαδικασία ανάκτησης κωδικών πρόσβασης από δεδομένα που είναι αποθηκευμένα ή μεταδίδονται από ένα σύστημα υπολογιστή, συνήθως μέσω μεθόδων όπως οι επιθέσεις ωμής βίας ή λεξικού.

Πολιτική κωδικού πρόσβασης – Ένα σύνολο κανόνων που επιβάλλεται από έναν οργανισμό για την ενίσχυση της ασφάλειας με τον καθορισμό απαιτήσεων για τη δημιουργία και τη διατήρηση ασφαλών κωδικών πρόσβασης.

Διαχείριση επιδιορθώσεων – Η διαδικασία διαχείρισης ενημερώσεων και επιδιορθώσεων λογισμικού, η οποία διασφαλίζει τη διόρθωση των ευπαθειών για τη διατήρηση της ασφάλειας του συστήματος.

Penetration Testing (Pentest) – Μια μέθοδος δοκιμών ασφαλείας κατά την οποία ηθικοί χάκερ προσομοιώνουν επιθέσεις σε ένα σύστημα για τον εντοπισμό και την εκμετάλλευση ευπαθειών, παρέχοντας πληροφορίες για την αποκατάσταση.

Personally Identifiable Information (PII) – Κάθε πληροφορία που μπορεί να χρησιμοποιηθεί για την ταυτοποίηση ενός ατόμου, όπως ονόματα, αριθμοί κοινωνικής ασφάλισης και διευθύνσεις, οι οποίες πρέπει να προστατεύονται σύμφωνα με τους κανονισμούς προστασίας προσωπικών δεδομένων.

Pharming – Μια τεχνική κυβερνοεπίθεσης κατά την οποία η κυκλοφορία ανακατευθύνεται από έναν νόμιμο ιστότοπο σε έναν δόλιο ιστότοπο για την κλοπή ευαίσθητων πληροφοριών, συχνά μέσω δηλητηρίασης DNS.

Phishing – Μια επίθεση κοινωνικής μηχανικής κατά την οποία οι επιτιθέμενοι εμφανίζονται ως αξιόπιστες οντότητες για να εξαπατήσουν άτομα ώστε να αποκαλύψουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή οικονομικά στοιχεία.

PII (Personally Identifiable Information) – Οποιαδήποτε δεδομένα που θα μπορούσαν να ταυτοποιήσουν ένα συγκεκριμένο άτομο, όπως ονόματα, αριθμοί κοινωνικής ασφάλισης ή διευθύνσεις ηλεκτρονικού ταχυδρομείου, που συχνά αποτελούν στόχο παραβιάσεων δεδομένων.

Pirate Box – Συσκευή που χρησιμοποιείται για την κοινή χρήση αρχείων και δεδομένων μέσω τοπικού δικτύου χωρίς σύνδεση στο διαδίκτυο, συχνά σχεδιασμένη να είναι ανώνυμη.

Απλό κείμενο – Δεδομένα που είναι αναγνώσιμα και όχι κρυπτογραφημένα, καθιστώντας τα ευάλωτα σε υποκλοπή και μη εξουσιοδοτημένη πρόσβαση εάν μεταδίδονται με μη ασφαλή τρόπο.

Πλατφόρμα ως υπηρεσία (PaaS) – Ένα μοντέλο υπολογιστικού νέφους όπου ένας τρίτος πάροχος παρέχει εργαλεία υλικού και λογισμικού μέσω του διαδικτύου, επιτρέποντας στους χρήστες να αναπτύσσουν, να εκτελούν και να διαχειρίζονται εφαρμογές χωρίς την πολυπλοκότητα της κατασκευής και της συντήρησης της υποκείμενης υποδομής.

Σάρωση θυρών – Μια μέθοδος που χρησιμοποιείται από επιτιθέμενους για την ανακάλυψη ανοικτών θυρών σε ένα σύστημα, οι οποίες μπορεί να υποδεικνύουν πιθανά σημεία εισόδου για επιθέσεις.

Κλιμάκωση προνομίων (Privilege Escalation) – Ένας τύπος επίθεσης όπου ένας χρήστης αποκτά υψηλότερα προνόμια πρόσβασης από τα αρχικά χορηγηθέντα, επιτρέποντάς του να εκτελεί μη εξουσιοδοτημένες ενέργειες σε ένα σύστημα.

Υποδομή δημόσιου κλειδιού (PKI) – Ένα πλαίσιο διαχείρισης ψηφιακών πιστοποιητικών και κρυπτογράφησης δημόσιου κλειδιού για την ασφάλεια των επικοινωνιών και την αυθεντικοποίηση των χρηστών.

PUP (Potentially Unwanted Program) – Λογισμικό που μπορεί να μην είναι κακόβουλο, αλλά είναι συχνά ανεπιθύμητο από τον χρήστη, όπως γραμμές εργαλείων ή διαφημιστικά προγράμματα, τα οποία μπορούν να θέσουν κινδύνους για την ασφάλεια αν αφεθούν ανεξέλεγκτα.

Pwn – όρος αργκό που προέρχεται από το "own" και χρησιμοποιείται συχνά στην κουλτούρα του hacking για να περιγράψει την ανάληψη του ελέγχου ή την ήττα ενός συστήματος ή ενός στόχου.

Προσωπικά δεδομένα – Πληροφορίες που αφορούν ένα ταυτοποιημένο ή αναγνωρίσιμο άτομο.

Κανονισμοί προστασίας προσωπικών δεδομένων – Νόμοι και πρότυπα που αποσκοπούν στην προστασία των προσωπικών δεδομένων από κακή χρήση και μη εξουσιοδοτημένη πρόσβαση.

Privacy by Design – Η αρχή της ενσωμάτωσης μέτρων προστασίας δεδομένων στο σχεδιασμό συστημάτων και διαδικασιών.

Αξιολόγηση αντικτύπου στην ιδιωτική ζωή (PIA) – Αξιολόγηση για την αξιολόγηση του αντικτύπου ενός έργου ή συστήματος στην ιδιωτική ζωή και την προστασία των δεδομένων.

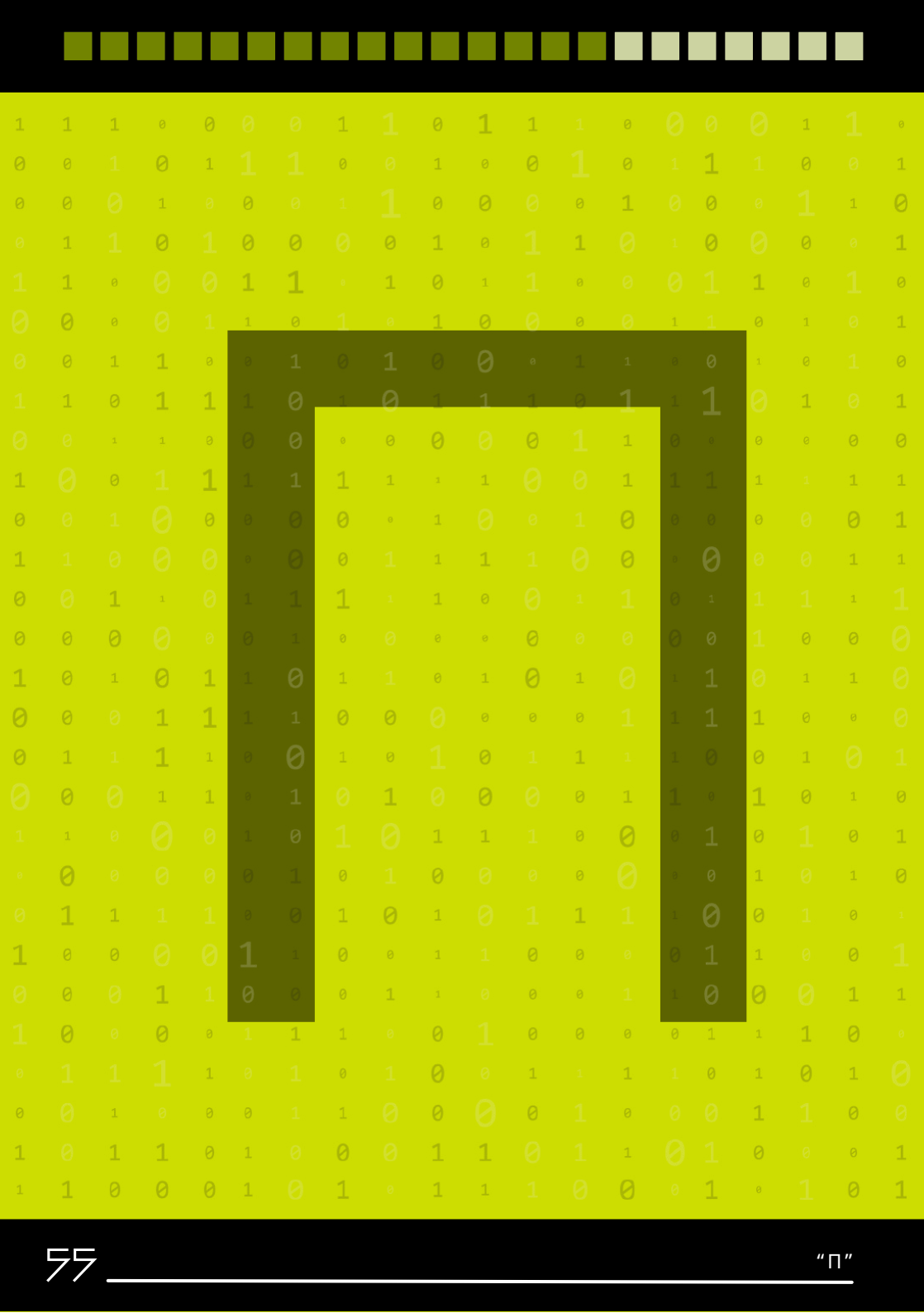
Ειδοποιήσεις απορρήτου – Έγγραφα που παρέχονται σε ιδιώτες και εξηγούν πώς θα συλλέγονται, θα χρησιμοποιούνται και θα προστατεύονται τα δεδομένα τους.

Πολιτικές απορρήτου – Έγγραφα που περιγράφουν τον τρόπο με τον οποίο ένας οργανισμός συλλέγει, χρησιμοποιεί και προστατεύει τα προσωπικά δεδομένα.

Privacy Shield Framework – Πλαίσιο σχεδιασμένο για την προστασία των προσωπικών δεδομένων που μεταφέρονται μεταξύ της Ευρωπαϊκής Ένωσης και των Ηνωμένων Πολιτειών (Σημείωση: αντικαταστάθηκε από άλλες συμφωνίες μετά την ακύρωση).

Δημιουργία προφίλ – Η αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα για την αξιολόγηση ορισμένων πτυχών της συμπεριφοράς ή των χαρακτηριστικών ενός ατόμου.

Ψευδωνυμοποίηση – Η διαδικασία αντικατάστασης αναγνωρίσιμων πληροφοριών με ψευδώνυμα για την προστασία της ατομικής ταυτότητας.



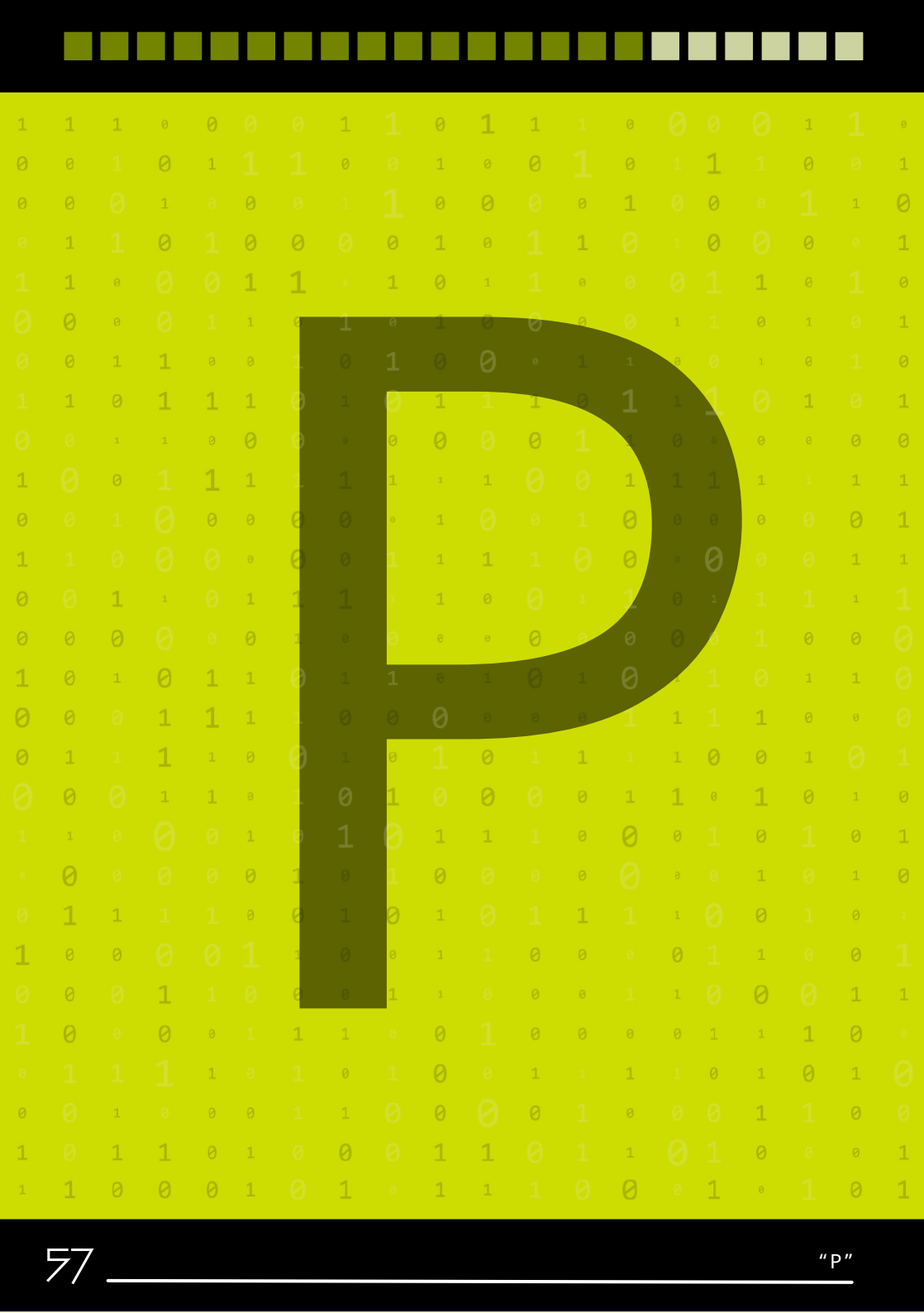
Κβαντική κρυπτογραφία - Μια μέθοδος κρυπτογράφησης που χρησιμοποιεί τις αρχές της κβαντικής μηχανικής για την ασφάλεια των δεδομένων, καθιστώντας τα δυνητικά απαραβίαστα με τις κλασικές μεθόδους υπολογισμού.

Καραντίνα - Η απομόνωση δυνητικά επιβλαβών αρχείων ή συστημάτων ώστε να μην μπορούν να προκαλέσουν ζημιά, συνήθως χρησιμοποιείται σε λογισμικό προστασίας από ιούς για τον χειρισμό εντοπισμένου κακόβουλου λογισμικού.

Query Flood Attack - Ένας τύπος επίθεσης άρνησης παροχής υπηρεσιών που κατακλύζει ένα σύστημα-στόχο με την αποστολή μεγάλου όγκου ερωτημάτων ή αιτημάτων, καθιστώντας το μη ανταποκρινόμενο.

Quick Response (QR) Code Security - Μέτρα ασφαλείας για την προστασία από κακόβουλους κώδικες QR που μπορούν να ανακατευθύνουν τους χρήστες σε επιβλαβείς ιστότοπους ή να δρομολογήσουν ανεπιθύμητες ενέργειες.

Έλεγχος πρόσβασης βάσει απαρτίας (Quorum-based Access Control) - Ένας μηχανισμός ασφαλείας που απαιτεί από πολλά μέρη να εγκρίνουν ή να εξουσιοδοτούν την πρόσβαση σε ευαίσθητους πόρους ή λειτουργίες, ενισχύοντας την προστασία από κακή χρήση.


P

Ransomware – Ένας τύπος κακόβουλου λογισμικού που κρυπτογραφεί τα δεδομένα του θύματος ή κλειδώνει το σύστημά του, απαιτώντας πληρωμή (συνήθως σε κρυπτονόμισμα) για το κλειδί αποκρυπτογράφησης ή την αποκατάσταση της πρόσβασης.

Red Teaming – Μια άσκηση κυβερνοασφάλειας κατά την οποία μια ανεξάρτητη ομάδα (η Red Team) προσομοιώνει πραγματικές επιθέσεις για να ελέγξει την αποτελεσματικότητα της άμυνας ασφαλείας ενός οργανισμού.

Reflected XSS (Cross-Site Scripting) – Ένας τύπος ευπάθειας εφαρμογών ιστού όπου κακόβουλα σενάρια αντανακλώνται από έναν διακομιστή ιστού και εκτελούνται στο πρόγραμμα περιήγησης ενός χρήστη, που συχνά χρησιμοποιείται για την κλοπή ευαίσθητων πληροφοριών.

Remote Access Trojan (RAT) – Ένας τύπος κακόβουλου λογισμικού που επιτρέπει στους επιτιθέμενους να ελέγχουν εξ αποστάσεως ένα μολυσμένο σύστημα, το οποίο χρησιμοποιείται συχνά για κατασκοπεία, κλοπή δεδομένων ή χειραγώγηση του συστήματος.

Remote Code Execution (RCE) – Μια ευπάθεια ασφαλείας που επιτρέπει σε έναν εισβολέα να εκτελέσει αυθαίρετο κώδικα σε ένα απομακρυσμένο μηχάνημα, οδηγώντας συχνά σε πλήρη παραβίαση του συστήματος.

Επίθεση επανάληψης – Ένας τύπος επίθεσης δικτύου όπου η έγκυρη μετάδοση δεδομένων επαναλαμβάνεται ή καθυστερεί με κακόβουλο ή δόλιο τρόπο, επιτρέποντας στους επιτιθέμενους να υποδυθούν ή να διακόψουν την επικοινωνία.

Resident Virus – Ένας τύπος ιού υπολογιστή που εγκαθίσταται στη μνήμη ενός συστήματος, επιτρέποντάς του να μολύνει αρχεία και προγράμματα κάθε φορά που γίνεται πρόσβαση σε αυτά.

Σάρωση αμφιβληστροειδούς – Ένα βιομετρικό μέτρο ασφαλείας που χρησιμοποιεί μοναδικά μοτίβα στον αμφιβληστροειδή χιτώνα ενός ατόμου για σκοπούς ταυτοποίησης και ελέγχου ταυτότητας.

Reverse Engineering – Η διαδικασία ανάλυσης λογισμικού ή υλικού για την ανακάλυψη του σχεδιασμού, της αρχιτεκτονικής ή του πηγαίου κώδικα, που χρησιμοποιείται συχνά στην έρευνα ευπαθειών ή στην ανάλυση κακόβουλου λογισμικού.

Αξιολόγηση κινδύνου – Η διαδικασία εντοπισμού, ανάλυσης και αξιολόγησης των κινδύνων για τα πληροφοριακά συστήματα και τα δεδομένα ενός οργανισμού, η οποία συχνά ακολουθείται από μέτρα για τον μετριασμό ή την εξάλειψη αυτών των κινδύνων.

Έλεγχος πρόσβασης βάσει ρόλων (RBAC) – Ένα μοντέλο ασφάλειας που εκχωρεί δικαιώματα πρόσβασης με βάση τους ρόλους που έχουν ανατεθεί στους χρήστες σε έναν οργανισμό, διασφαλίζοντας ότι έχουν πρόσβαση μόνο στα δεδομένα που είναι απαραίτητα για το ρόλο τους.

Rootkit – Μια συλλογή εργαλείων κακόβουλου λογισμικού που επιτρέπουν σε έναν εισβολέα να αποκτήσει και να διατηρήσει τον έλεγχο ενός συστήματος απαρατήρητο, συχνά αποκρύπτοντας την παρουσία του.

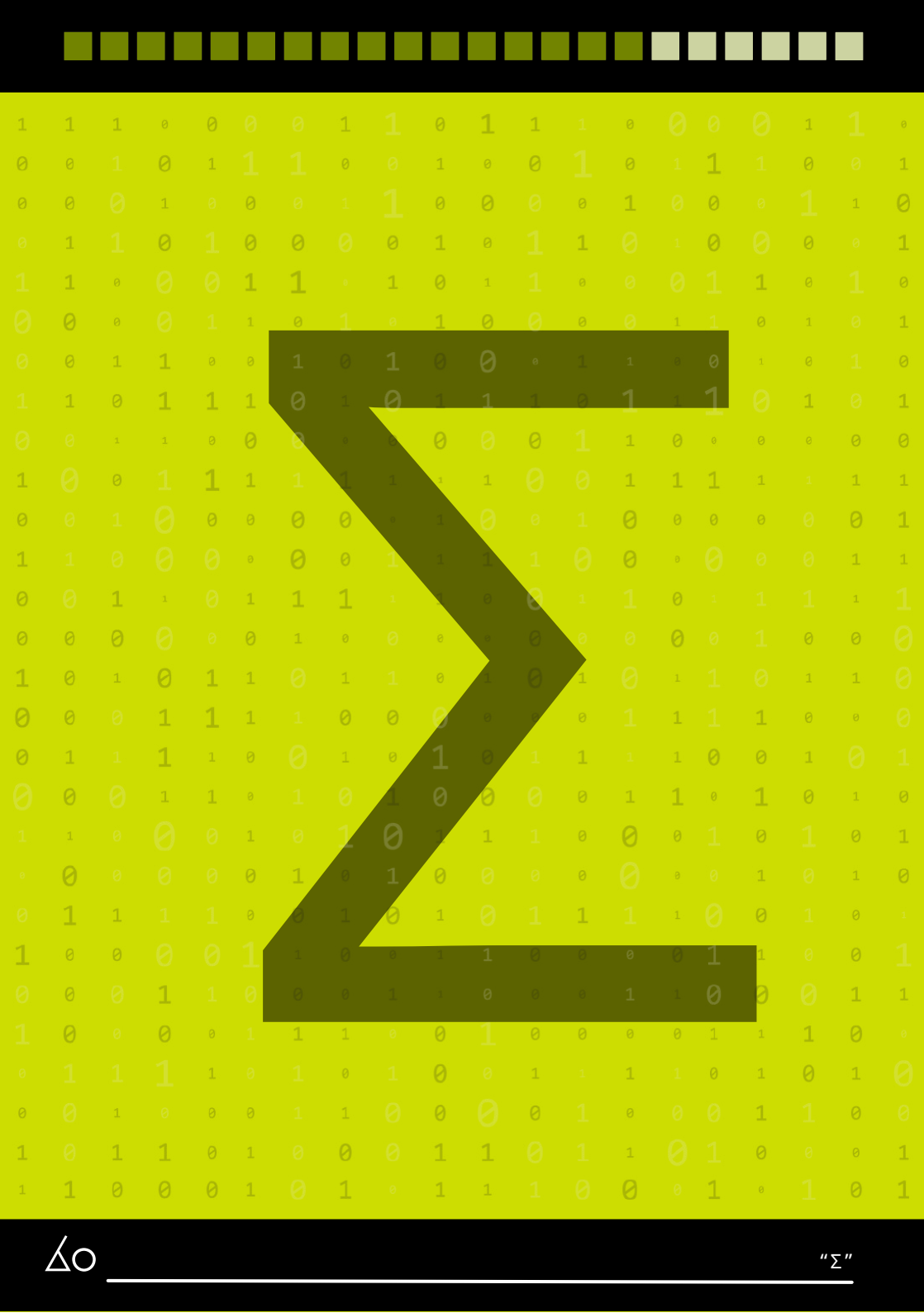
RSA (Rivest-Shamir-Adleman) - Ένα ευρέως χρησιμοποιούμενο κρυπτοσύστημα δημόσιου κλειδιού για την ασφαλή μετάδοση δεδομένων, το οποίο πήρε το όνομά του από τους εφευρέτες του και είναι γνωστό για το ρόλο του στην κρυπτογράφηση και την ασφάλεια ευαίσθητων πληροφοριών.

Κανονιστική συμμόρφωση - Τήρηση των νόμων και των κανονισμών που διέπουν την προστασία των δεδομένων και της ιδιωτικής ζωής.

Ρυθμιστικές απαιτήσεις - Υποχρεώσεις που επιβάλλονται από νόμους και κανονισμούς τις οποίες πρέπει να ακολουθούν οι οργανισμοί για να διασφαλίζουν την προστασία των δεδομένων.

Πλαίσιο διαχείρισης κινδύνων - Μια δομημένη προσέγγιση για τον εντοπισμό, την αξιολόγηση και τη διαχείριση των κινδύνων που σχετίζονται με την προστασία των δεδομένων.

Ανοχή κινδύνου - Το επίπεδο κινδύνου που είναι διατεθειμένος να αποδεχθεί ένας οργανισμός κατά τη διαχείριση της προστασίας και της ασφάλειας των δεδομένων.


Σ

Επίθεση σαλάμι – Ένας τύπος κυβερνοεπίθεσης που περιλαμβάνει την κλοπή μικρών χρηματικών ποσών ή δεδομένων με την πάροδο του χρόνου, συχνά πολύ μικρών για να γίνουν αντιληπτά σε μεμονωμένες συναλλαγές, αλλά που αθροίζονται σε σημαντικές απώλειες.

Sandboxing – Ένας μηχανισμός ασφαλείας που χρησιμοποιείται για την απομόνωση δυνητικά επιβλαβών προγραμμάτων ή κώδικα από κρίσιμα συστήματα, επιτρέποντάς τους να εκτελούνται σε ένα περιορισμένο περιβάλλον χωρίς να κινδυνεύουν να προκαλέσουν ζημιά στο ευρύτερο δίκτυο.

Scareware – Κακόβουλο λογισμικό που έχει σχεδιαστεί για να εξαπατά τους χρήστες ώστε να πιστεύουν ότι ο υπολογιστής τους έχει μολυνθεί από κακόβουλο λογισμικό, οδηγώντας συχνά στην αγορά ψεύτικου λογισμικού ασφαλείας ή στην αποκάλυψη προσωπικών πληροφοριών.

Script Kiddie – Υποτιμητικός όρος για έναν άπειρο χάκερ που χρησιμοποιεί προκατασκευασμένα σενάρια ή εργαλεία για να πραγματοποιήσει κυβερνοεπιθέσεις χωρίς να κατανοεί πλήρως τον τρόπο λειτουργίας τους.

Secure Boot (Ασφαλής εκκίνηση) – Ένα πρότυπο ασφαλείας για τη διασφάλιση ότι μια συσκευή εκκινείται μόνο με τη χρήση αξιόπιστου λογισμικού, αποτρέποντας τη φόρτωση μη εξουσιοδοτημένων ή κακόβουλων λειτουργικών συστημάτων.

Secure Socket Layer (SSL) – Ένα πρωτόκολλο ασφαλείας που χρησιμοποιείται για την κρυπτογράφηση δεδομένων που μεταδίδονται μέσω του διαδικτύου, το οποίο χρησιμοποιείται συνήθως στο HTTPS για την προστασία ευαίσθητων πληροφοριών, όπως τα στοιχεία σύνδεσης και οι αριθμοί πιστωτικών καρτών.

Εκπαίδευση ευαισθητοποίησης σε θέματα ασφάλειας – Προγράμματα που αποσκοπούν στην εκπαίδευση των εργαζομένων ή των χρηστών σχετικά με τις βέλτιστες πρακτικές κυβερνοασφάλειας, τις απειλές κοινωνικής μηχανικής και τον τρόπο αναγνώρισης και αποτροπής κυβερνοεπιθέσεων.

Γνωστοποίηση παραβίασης ασφάλειας – Η απαίτηση ενημέρωσης των επηρεαζόμενων ατόμων και των ρυθμιστικών αρχών σχετικά με μια παραβίαση δεδομένων.

Πιστοποιήσεις ασφαλείας – Επίσημη αναγνώριση ότι οι πρακτικές προστασίας δεδομένων ενός οργανισμού πληρούν συγκεκριμένα πρότυπα.

Διαχείριση περιστατικών ασφαλείας – Οι διεργασίες και οι διαδικασίες για το χειρισμό και τον μετριασμό περιστατικών ασφαλείας.

Security Information and Event Management (SIEM) – Ένα σύστημα που συλλέγει, αναλύει και συσχετίζει συμβάντα ασφαλείας από διάφορες πηγές σε πραγματικό χρόνο, βοηθώντας τους οργανισμούς να εντοπίζουν και να ανταποκρίνονται αποτελεσματικότερα στις απειλές.

Session Hijacking – Ένας τύπος επίθεσης όπου ένας επιτιθέμενος αναλαμβάνει τη σύνοδο ενός χρήστη σε έναν ιστότοπο ή μια εφαρμογή, συχνά κλέβοντας το session token ή το cookie.

Shoulder Surfing – Μια φυσική απειλή για την ασφάλεια κατά την οποία ένας εισβολέας παρατηρεί έναν χρήστη να εισάγει ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή PIN, κοιτάζοντας πάνω από τον ώμο του ή χρησιμοποιώντας εξοπλισμό παρακολούθησης.

Επίθεση πλευρικού καναλιού – Ένας τύπος επίθεσης που εκμεταλλεύεται φυσικά ή ειδικά για την υλοποίηση χαρακτηριστικά ενός συστήματος (όπως η κατανάλωση ενέργειας ή οι πληροφορίες χρονισμού) για να αποκτήσει πρόσβαση σε ευαίσθητα δεδομένα.

Ανίχνευση βάσει υπογραφής – Μια μέθοδος που χρησιμοποιείται σε συστήματα προστασίας από ιούς και συστήματα ανίχνευσης εισβολών, η οποία εντοπίζει απειλές βάσει προκαθορισμένων μοτίβων ή "υπογραφών" γνωστού κακόβουλου λογισμικού.

Single Sign-On (SSO) – Μια διαδικασία ελέγχου ταυτότητας χρήστη που επιτρέπει σε έναν χρήστη να συνδεθεί μία φορά και να αποκτήσει πρόσβαση σε πολλαπλές εφαρμογές ή συστήματα χωρίς να χρειάζεται να συνδεθεί ξανά για κάθε μία από αυτές.

Smishing – Μια επίθεση phishing που πραγματοποιείται μέσω μηνυμάτων SMS (κειμένου), όπου ο επιτιθέμενος προσπαθεί να εξαπατήσει το θύμα ώστε να αποκαλύψει προσωπικές πληροφορίες ή να κάνει κλικ σε έναν κακόβουλο σύνδεσμο.

Sniffing – Η πράξη υποκλοπής και ανάλυσης της κίνησης δικτύου, που χρησιμοποιείται συχνά από επιτιθέμενους για τη σύλληψη ευαίσθητων δεδομένων, όπως διαπιστευτήρια σύνδεσης ή αριθμούς πιστωτικών καρτών.

Social Engineering – Μια τεχνική χειραγώγησης που χρησιμοποιείται από επιτιθέμενους για να εξαπατήσουν άτομα ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες ή να εκτελέσουν ενέργειες που θέτουν σε κίνδυνο την ασφάλεια, όπως να κάνουν κλικ σε κακόβουλους συνδέσμους.

Spear Phishing – Μια στοχευμένη επίθεση phishing που απευθύνεται σε συγκεκριμένο άτομο ή οργανισμό, χρησιμοποιώντας συχνά εξατομικευμένα μηνύματα και λεπτομέρειες για να αυξηθεί η πιθανότητα επιτυχίας.

Spoofing – Η πράξη πλαστοπροσωπίας άλλου χρήστη, συσκευής ή συστήματος για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε ένα σύστημα ή τη χειραγώγηση της επικοινωνίας.

Spyware – Κακόβουλο λογισμικό που παρακολουθεί και συλλέγει κρυφά πληροφορίες από το σύστημα ενός χρήστη, όπως συνήθειες περιήγησης ή προσωπικά δεδομένα, συχνά εν αγνοία του χρήστη.

SQL Injection – Ένας τύπος επίθεσης όπου ένας επιτιθέμενος εκμεταλλεύεται ευπάθειες στη διεπαφή ερωτημάτων βάσης δεδομένων μιας εφαρμογής εισάγοντας κακόβουλο κώδικα SQL για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα ή να τα χειριστεί.

Κρατικά χρηματοδοτούμενη επίθεση – Μια κυβερνοεπίθεση που πραγματοποιείται ή υποστηρίζεται από μια κυβέρνηση, συνήθως με στόχο άλλα έθνη, οργανισμούς ή άτομα για κατασκοπεία, σαμποτάζ ή άλλους στρατηγικούς σκοπούς.

Στεγανογραφία – Η πρακτική της απόκρυψης πληροφοριών μέσα σε άλλα δεδομένα, όπως η ενσωμάτωση ενός μηνύματος μέσα σε μια εικόνα ή ένα αρχείο ήχου, που χρησιμοποιείται συχνά για κρυφή επικοινωνία.

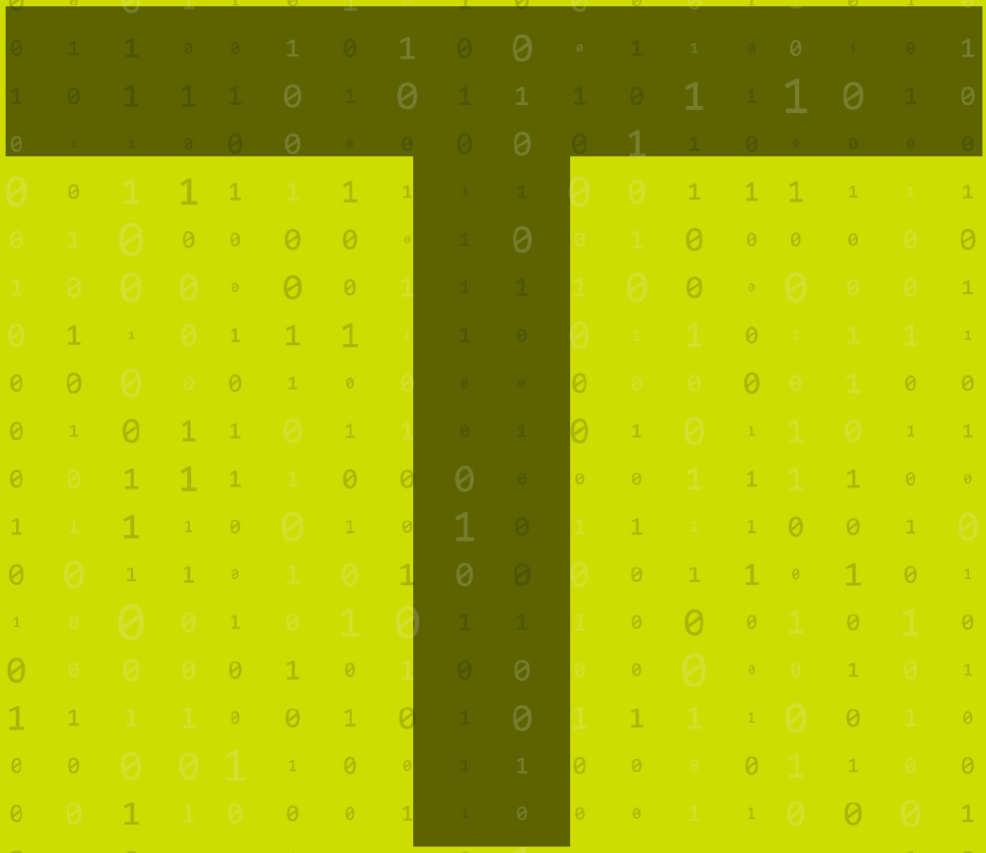
Επίθεση στην εφοδιαστική αλυσίδα – Ένας τύπος επίθεσης όπου ένας επιτιθέμενος στοχεύει σε λιγότερο ασφαλή στοιχεία της εφοδιαστικής αλυσίδας, όπως τρίτους προμηθευτές ή παρόχους υπηρεσιών, για να θέσει σε κίνδυνο την ασφάλεια ενός μεγαλύτερου οργανισμού.

Συμμετρική κρυπτογράφηση – Ένας τύπος κρυπτογράφησης όπου το ίδιο κλειδί χρησιμοποιείται τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση των δεδομένων, που χρησιμοποιείται συχνά σε πρωτόκολλα ασφαλούς επικοινωνίας.

Ευαίσθητα δεδομένα – Προσωπικά δεδομένα που απαιτούν πρόσθετη προστασία λόγω της φύσης τους, όπως πληροφορίες υγείας ή οικονομικά στοιχεία.

Κοινωνική μηχανική – Τεχνικές που χρησιμοποιούνται για τη χειραγώγηση ατόμων ώστε να αποκαλύψουν εμπιστευτικές πληροφορίες.

Τυποποιημένες συμβατικές ρήτρες (ΤΣΡ) – Νομικές συμφωνίες που χρησιμοποιούνται για την εξασφάλιση επαρκούς προστασίας δεδομένων κατά τη διαβίβαση δεδομένων εκτός του Ευρωπαϊκού Οικονομικού Χώρου (ΕΟΧ).



Tails (The Amnesic Incognito Live System) – Ένα λειτουργικό σύστημα Linux με επίκεντρο την ασφάλεια, σχεδιασμένο για ανώνυμη χρήση του διαδικτύου και προστασία της ιδιωτικής ζωής. Τρέχει από ένα στικάκι USB ή DVD και δεν αφήνει κανένα ίχνος στο μηχάνημα.

Ανίχνευση παραβίασης – Ένα χαρακτηριστικό ασφαλείας που εντοπίζει μη εξουσιοδοτημένες τροποποιήσεις ή απόπειρες χειραγώγησης συστημάτων ή δεδομένων, ενεργοποιώντας συχνά ειδοποιήσεις όταν εντοπίζεται παραβίαση.

Τεχνικά και οργανωτικά μέτρα (TOM) – Μέτρα που λαμβάνονται για τη διασφάλιση της ασφάλειας των προσωπικών δεδομένων, συμπεριλαμβανομένων τεχνικών λύσεων και οργανωτικών πρακτικών.

Τεχνικά τρωτά σημεία – Αδυναμίες σε ένα σύστημα που θα μπορούσαν να αξιοποιηθούν για την απόκτηση μη εξουσιοδοτημένης πρόσβασης σε δεδομένα.

Όροι χρήσης – Νομικές συμφωνίες που περιγράφουν τους κανόνες και τους όρους χρήσης μιας υπηρεσίας ή ενός προϊόντος.

Διαχείριση κινδύνων από τρίτους – Η διαδικασία αξιολόγησης και διαχείρισης των κινδύνων που σχετίζονται με τρίτους προμηθευτές που χειρίζονται δεδομένα.

Προμηθευτές τρίτων – Εξωτερικοί οργανισμοί ή άτομα που παρέχουν υπηρεσίες ή προϊόντα σε μια εταιρεία, τα οποία μπορεί να περιλαμβάνουν χειρισμό δεδομένων.

Φορέας απειλής – Ένα άτομο ή μια ομάδα που εμπλέκεται σε κακόβουλες δραστηριότητες, όπως επιθέσεις στον κυβερνοχώρο, με σκοπό να θέσει σε κίνδυνο τα συστήματα, να κλέψει δεδομένα ή να διαταράξει τις λειτουργίες.

Threat Hunting – Μια προληπτική πρακτική κυβερνοασφάλειας κατά την οποία οι επαγγελματίες ασφαλείας αναζητούν ενεργά απειλές ή δείκτες συμβιβασμού (IoCs) σε ένα δίκτυο πριν οδηγήσουν σε παραβίαση.

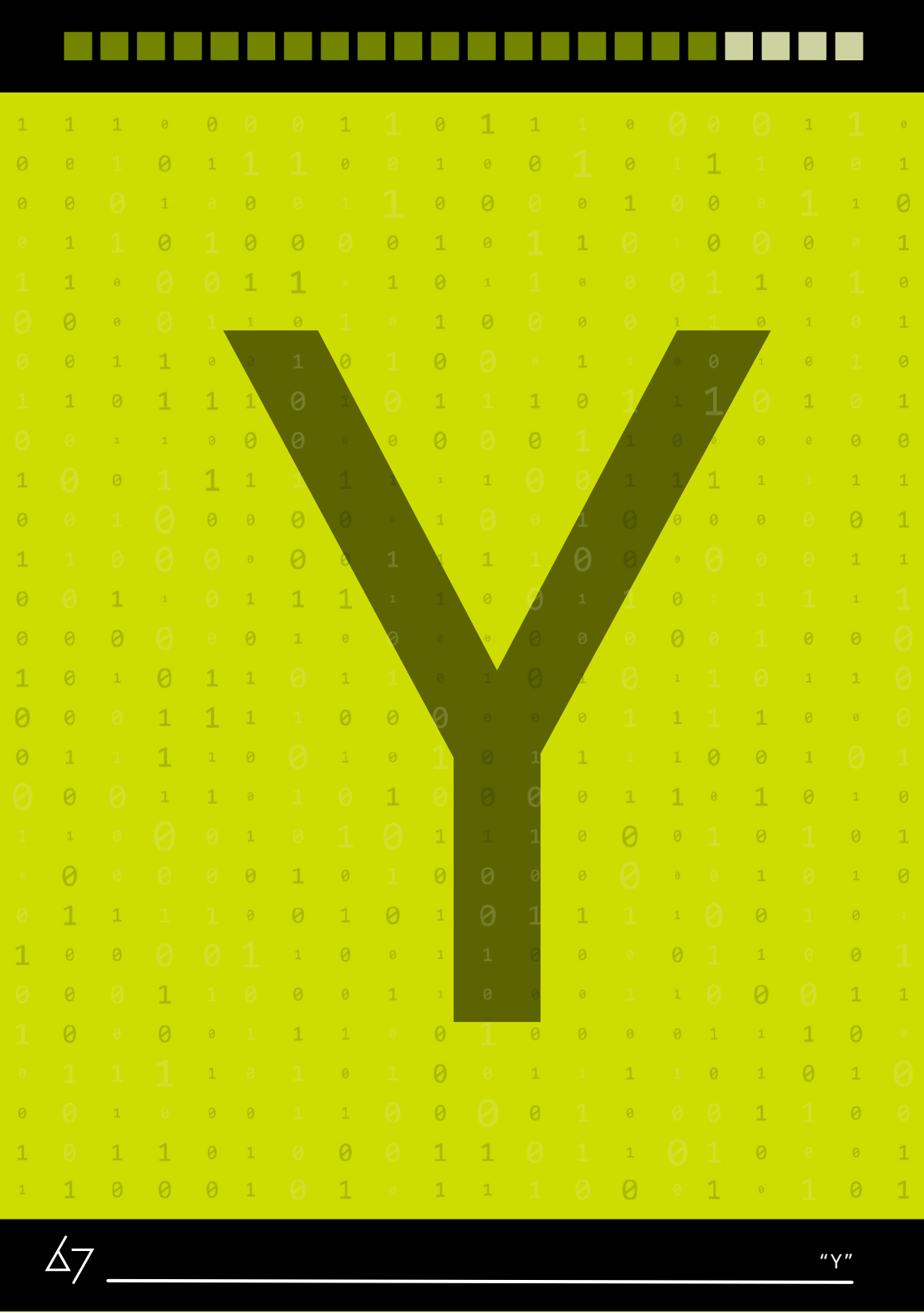
Threat Intelligence – Πληροφορίες σχετικά με τρέχουσες ή δυνητικές απειλές στον κυβερνοχώρο που συλλέγονται από διάφορες πηγές για να βοηθήσουν τους οργανισμούς να εντοπίσουν, να αποτρέψουν και να ανταποκριθούν σε επιθέσεις.

Tokenisation – Μια διαδικασία που αντικαθιστά τα ευαίσθητα δεδομένα με ένα μοναδικό αναγνωριστικό ή token, μειώνοντας τον κίνδυνο έκθεσης των πραγματικών δεδομένων κατά την αποθήκευση ή τη μετάδοση.

Διαφάνεια – Η αρχή της ανοικτής και σαφούς πληροφόρησης σχετικά με τις πρακτικές συλλογής δεδομένων και τον τρόπο χρήσης των δεδομένων.

Αυθεντικοποίηση δύο παραγόντων (2FA) - Μια διαδικασία ασφαλείας που απαιτεί δύο ξεχωριστές μεθόδους επαλήθευσης (όπως ένας κωδικός πρόσβασης και ένας κωδικός μιας χρήσης που αποστέλλεται σε μια κινητή συσκευή) για την αυθεντικοποίηση ενός χρήστη, ενισχύοντας την ασφάλεια του λογαριασμού.

Typo Squatting - Μια επίθεση κοινωνικής μηχανικής κατά την οποία οι εγκληματίες του κυβερνοχώρου δημιουργούν ψεύτικους ιστότοπους με ονόματα τομέα παρόμοια με δημοφιλή, ελπίζοντας ότι οι χρήστες θα πληκτρολογήσουν λάθος τη διεύθυνση URL και θα καταλήξουν στον κακόβουλο ιστότοπο.


Y

UDP (User Datagram Protocol) - Πρωτόκολλο επικοινωνίας που χρησιμοποιείται στο διαδίκτυο για γρήγορη μετάδοση δεδομένων χωρίς σύνδεση. Χρησιμοποιείται συχνά σε εφαρμογές όπως streaming και VoIP, αλλά είναι λιγότερο ασφαλές από το TCP.

UEBA (User and Entity Behavior Analytics) - Μια τεχνολογία κυβερνοασφάλειας που χρησιμοποιεί μηχανική μάθηση και ανάλυση για τον εντοπισμό ανωμαλιών στη συμπεριφορά χρηστών και οντοτήτων, εντοπίζοντας πιθανές απειλές ή κακόβουλους εσωτερικούς χρήστες.

Underground Economy - όρος που αναφέρεται στη μαύρη αγορά όπου οι εγκληματίες του κυβερνοχώρου αγοράζουν, πωλούν και ανταλλάσσουν παράνομα αγαθά και υπηρεσίες, όπως κλεμμένα δεδομένα, κακόβουλο λογισμικό ή εργαλεία hacking.

Uniform Resource Locator (URL) - Μια αναφορά (διεύθυνση) που χρησιμοποιείται για την πρόσβαση σε πόρους στο διαδίκτυο. Οι κακόβουλες διευθύνσεις URL χρησιμοποιούνται συχνά σε επιθέσεις phishing για να ανακατευθύνουν τους χρήστες σε επιβλαβείς ιστότοπους.

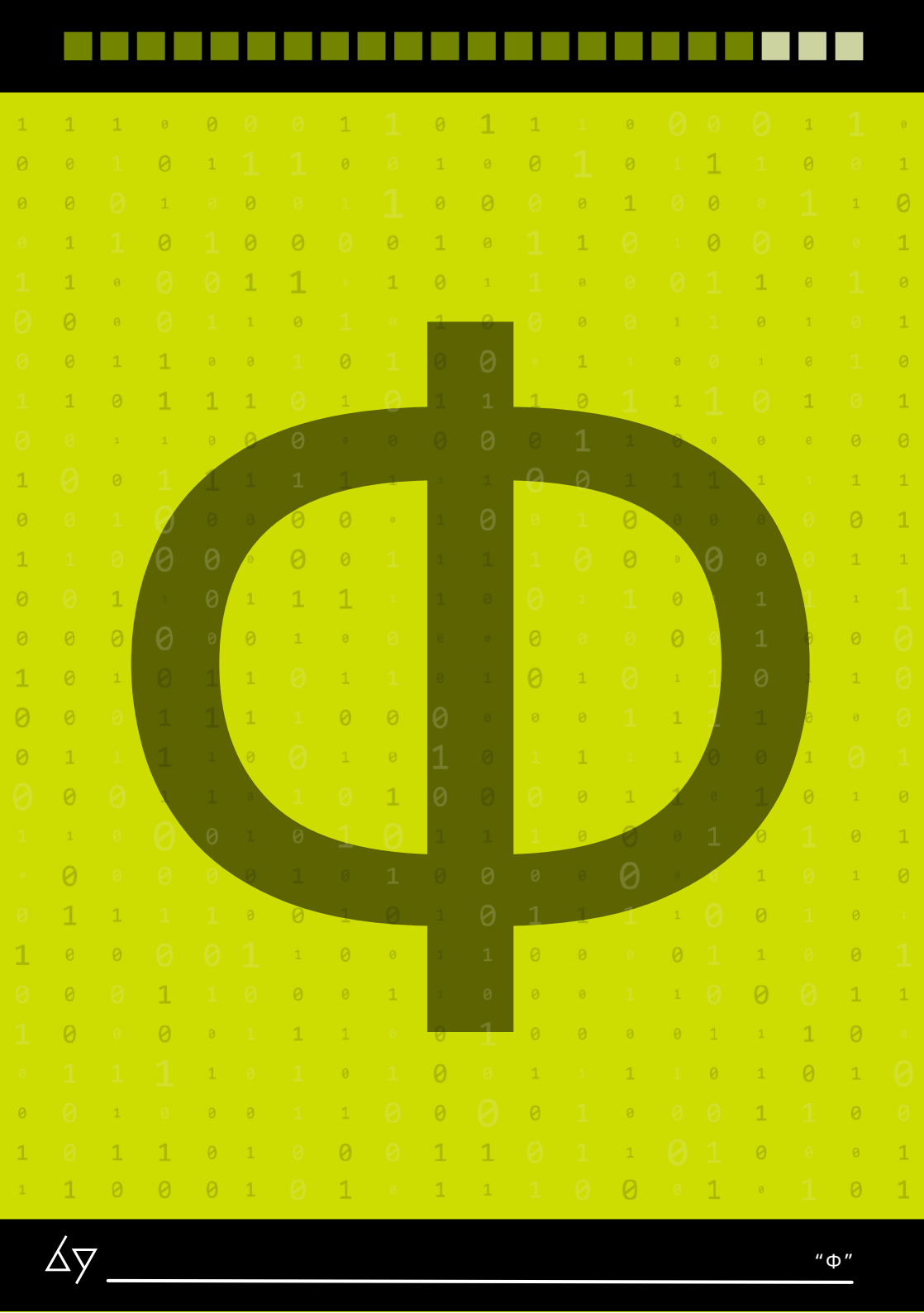
Μη αξιόπιστο δίκτυο - Ένα δίκτυο που δεν ελέγχεται από τον οργανισμό και θεωρείται μη ασφαλές, όπως το δημόσιο Wi-Fi, όπου οι επικοινωνίες μπορεί να είναι ευάλωτες σε υποκλοπές ή επιθέσεις.

Φιλτράρισμα URL - Ένα μέτρο ασφαλείας που εμποδίζει ή επιτρέπει την πρόσβαση σε συγκεκριμένους ιστότοπους με βάση τις διευθύνσεις URL, το οποίο χρησιμοποιείται συχνά για να αποτρέψει την πρόσβαση των χρηστών σε κακόβουλο ή ακατάλληλο περιεχόμενο.

Ασφάλεια USB - Οι πολιτικές και τα μέτρα για την προστασία των συστημάτων από τους κινδύνους ασφαλείας που σχετίζονται με τις μονάδες USB, οι οποίες μπορούν να εισάγουν κακόβουλο λογισμικό ή να διευκολύνουν τη διαρροή δεδομένων.

Διαχείριση συγκατάθεσης χρηστών - Διαδικασίες και εργαλεία για την απόκτηση και διαχείριση της συγκατάθεσης των ατόμων για δραστηριότητες επεξεργασίας δεδομένων.

Φιλικότητα προς τον χρήστη - Η ευκολία με την οποία ένα εργαλείο ή σύστημα μπορεί να χρησιμοποιηθεί από τους προβλεπόμενους χρήστες.


Ф

Ιός - Ένας τύπος κακόβουλου λογισμικού που, όταν εκτελείται, αναπαράγεται τροποποιώντας άλλα προγράμματα υπολογιστή και εισάγοντας τον δικό του κώδικα, προκαλώντας ενδεχομένως ζημιά σε συστήματα και δεδομένα.

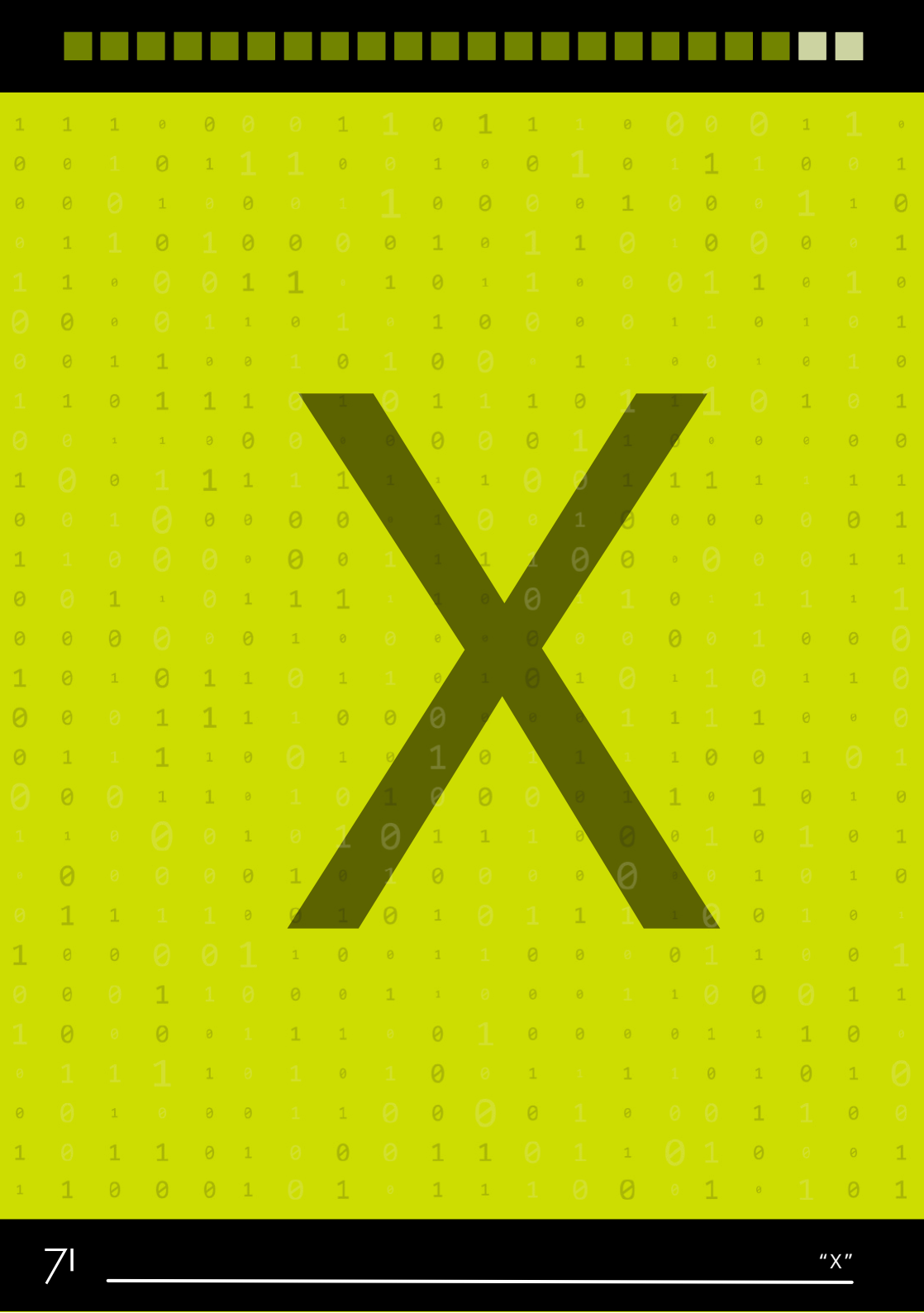
Εικονικό ιδιωτικό δίκτυο (VPN) - Μια υπηρεσία που κρυπτογραφεί την κυκλοφορία στο διαδίκτυο και αποκρύπτει τη διεύθυνση IP του χρήστη, παρέχοντας μια ασφαλή σύνδεση μεταξύ του χρήστη και ενός απομακρυσμένου δικτύου. Χρησιμοποιείται συχνά για λόγους προστασίας της ιδιωτικής ζωής και ασφάλειας.

Vishing - Ένας τύπος επίθεσης phishing που πραγματοποιείται μέσω τηλεφώνου, όπου οι επιτιθέμενοι υποδύονται νόμιμες οντότητες για να υποκλέψουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή στοιχεία πιστωτικών καρτών.

Ευπάθεια - Μια αδυναμία ή ένα ελάττωμα σε λογισμικό, υλικό ή διαδικασίες που μπορεί να αξιοποιηθεί από έναν επιτιθέμενο για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση ή να προκαλέσει βλάβη.

Αξιολόγηση τρωτότητας - Μια συστηματική διαδικασία εντοπισμού, ποσοτικοποίησης και ιεράρχησης των τρωτών σημείων ενός συστήματος για την κατανόηση των κινδύνων και την αντιμετώπισή τους πριν από την εκμετάλλευσή τους.

Διαχείριση τρωτών σημείων - Η συνεχής διαδικασία εντοπισμού, αξιολόγησης, αντιμετώπισης και υποβολής εκθέσεων σχετικά με τα τρωτά σημεία των συστημάτων, ώστε να μειωθεί το παράθυρο ευκαιρίας για επιθέσεις.


X

Watering Hole Attack – Μια στοχευμένη επίθεση κατά την οποία οι εγκληματίες του κυβερνοχώρου παραβιάζουν έναν ιστότοπο που επισκέπτονται συχνά τα υποψήφια θύματά τους, εισάγοντας κακόβουλο λογισμικό στον ιστότοπο για να μολύνουν τις συσκευές των επισκεπτών.

Web Scraping – Η αυτοματοποιημένη εξαγωγή δεδομένων από ιστότοπους, που συχνά απαιτεί συμμόρφωση με τους νόμους περί προστασίας δεδομένων.

WEP (Wired Equivalent Privacy) – Ένα ξεπερασμένο πρωτόκολλο ασφαλείας που χρησιμοποιείται για την προστασία ασύρματων δικτύων. Έχει αντικατασταθεί από πιο ασφαλή πρωτόκολλα όπως το WPA λόγω των τρωτών σημείων του.

Whaling – Μια μορφή επίθεσης phishing που στοχεύει ειδικά σε υψηλόβαθμα στελέχη ή σημαντικά άτομα σε έναν οργανισμό, συχνά με στόχο την κλοπή ευαίσθητων πληροφοριών ή κεφαλαίων.

White Hat Hacker – Ένας ηθικός χάκερ που χρησιμοποιεί τις δεξιότητές του για τον εντοπισμό και τη διόρθωση ευπαθειών ασφαλείας σε συστήματα με την άδεια του ιδιοκτήτη, συχνά απασχολείται από οργανισμούς για τη βελτίωση της ασφάλειας.

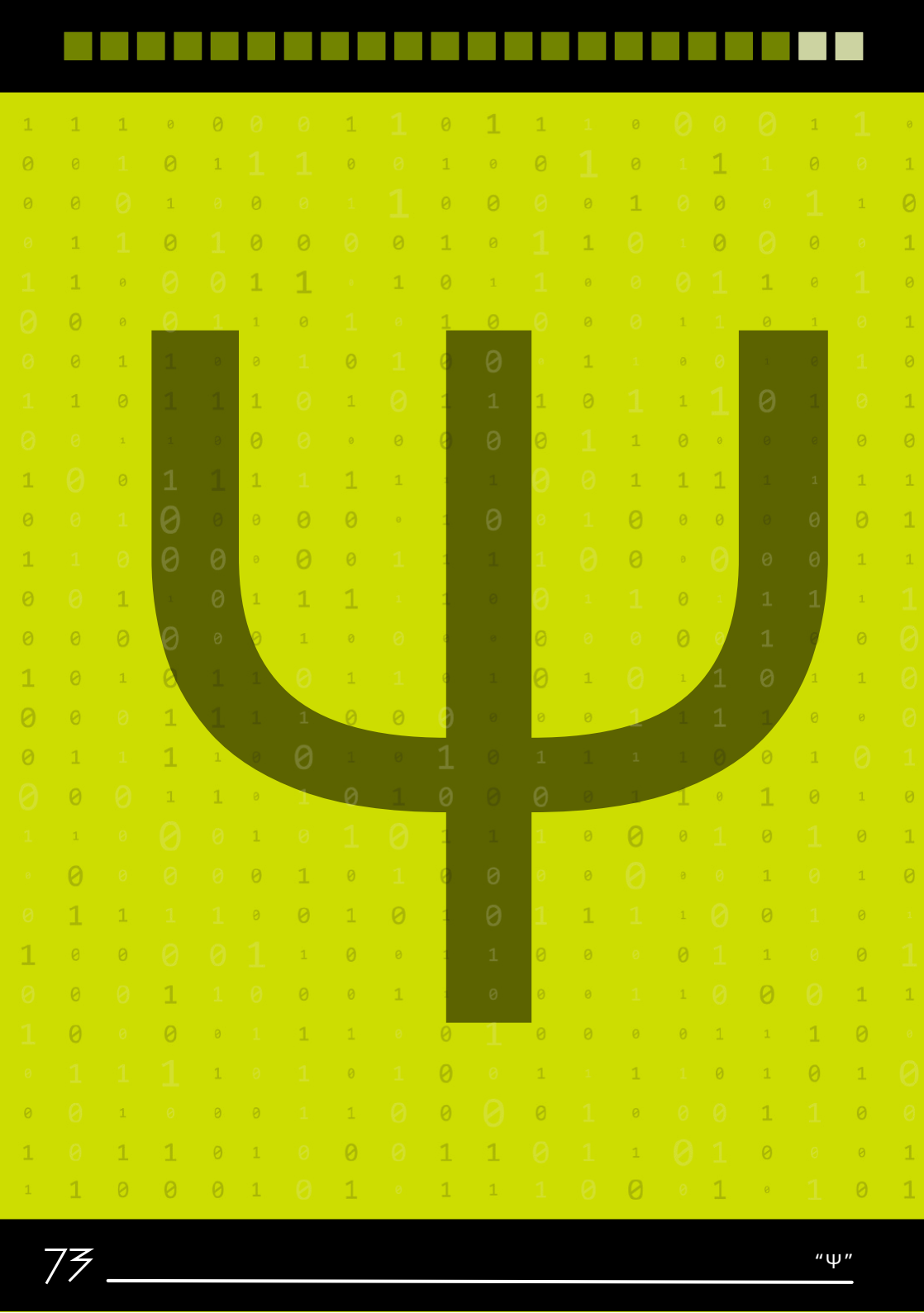
Whistleblowing – Αναφορά ανήθικων ή παράνομων πρακτικών, συμπεριλαμβανομένων των παραβιάσεων δεδομένων ή της μη συμμόρφωσης με τους νόμους περί προστασίας δεδομένων.

Wi-Fi Protected Access (WPA/WPA2) – Πρωτόκολλο ασφαλείας που χρησιμοποιείται για την ασφάλεια ασύρματων δικτύων και παρέχει ισχυρότερη κρυπτογράφηση από τον προκάτοχό του WEP. Το WPA2 είναι σήμερα το πρότυπο για την ασφαλή επικοινωνία μέσω Wi-Fi.

Σκουλήκι – Ένας τύπος αυτοαναπαραγόμενου κακόβουλου λογισμικού που εξαπλώνεται σε δίκτυα εκμεταλλευόμενο ευπάθειες, χωρίς την ανάγκη ανθρώπινης αλληλεπίδρασης ή προσκόλλησης σε αρχεία.

Απόρρητο στο χώρο εργασίας – Η προστασία των προσωπικών δεδομένων και των δικαιωμάτων ιδιωτικότητας στο εργασιακό περιβάλλον.

WPA3 (Wi-Fi Protected Access 3) – Το πιο πρόσφατο πρωτόκολλο ασφαλείας για ασύρματα δίκτυα, σχεδιασμένο να παρέχει ισχυρότερη προστασία δεδομένων και ασφαλή κρυπτογράφηση τόσο σε προσωπικά όσο και σε εταιρικά περιβάλλοντα.



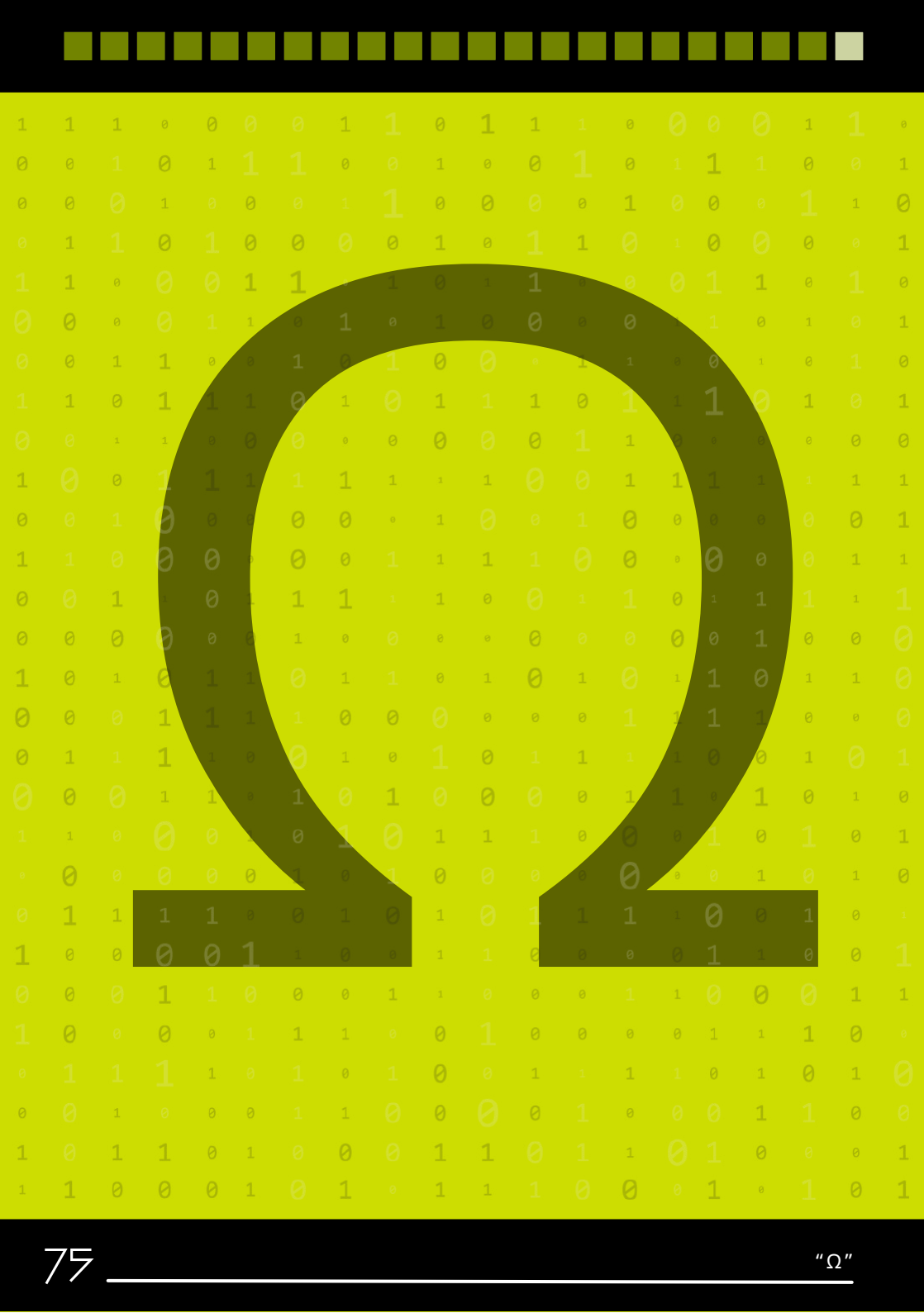
ΠιστοποιητικόX.509 – Ένα ψηφιακό πιστοποιητικό που χρησιμοποιεί το πρότυπο υποδομής δημόσιου κλειδιού (PKI) X.509 για την επαλήθευση της ταυτότητας ατόμων, συσκευών και διακομιστών μέσω του διαδικτύου, εξασφαλίζοντας ασφαλή επικοινωνία.

XACML (eXtensible Access Control Markup Language) – Ένα πλαίσιο βασισμένο σε XML για τον ορισμό και την επιβολή πολιτικών ελέγχου πρόσβασης. Χρησιμοποιείται συνήθως για τη διαχείριση της εξουσιοδότησης σε συστήματα και δίκτυα.

XDR (Extended Detection and Response) – Μια λύση ασφαλείας που ενσωματώνει και συσχετίζει δεδομένα από πολλαπλά προϊόντα ασφαλείας για την παροχή ολοκληρωμένης ανίχνευσης, διερεύνησης και αντιμετώπισης απειλών σε όλο το δίκτυο ενός οργανισμού.

Κρυπτογράφηση XML – Ένα πρότυπο για την κρυπτογράφηση του περιεχομένου των εγγράφων XML, το οποίο διασφαλίζει ότι τα ευαίσθητα δεδομένα που μεταδίδονται σε μορφή XML προστατεύονται από μη εξουσιοδοτημένη πρόσβαση.

XML Firewall – Ένα σύστημα ασφαλείας που έχει σχεδιαστεί για την προστασία των διαδικτυακών υπηρεσιών που βασίζονται σε XML, φιλτράροντας την κυκλοφορία XML, αποτρέποντας επιθέσεις όπως η έγχυση XML ή η άρνηση παροχής υπηρεσιών.



YARA – Ένα εργαλείο που χρησιμοποιείται για τον εντοπισμό και την ταξινόμηση κακόβουλου λογισμικού με τη δημιουργία περιγραφών (κανόνων) κακόβουλων μοτίβων αρχείων. Χρησιμοποιείται ευρέως στο κυνήγι απειλών και στην έρευνα κακόβουλου λογισμικού.

YubiKey – Μια συσκευή ελέγχου ταυτότητας υλικού που υποστηρίζει έλεγχο ταυτότητας δύο παραγόντων (2FA), παρέχοντας ισχυρή ασφάλεια με τη δημιουργία κωδικών πρόσβασης μιας χρήσης ή κρυπτογραφικών κλειδιών για σκοπούς σύνδεσης.

Κίτρινη ομάδα – Στο πλαίσιο της ασφάλειας στον κυβερνοχώρο, μια ομάδα που επικεντρώνεται στη συνεργασία μεταξύ των επιθετικών (κόκκινη ομάδα) και αμυντικών (μπλε ομάδα) προσπαθειών ασφάλειας, συμβάλλοντας συχνά στη βελτίωση του συντονισμού και της ανταλλαγής γνώσεων μεταξύ των δύο ομάδων.