DAS DATA GAME A-Z

Glossar

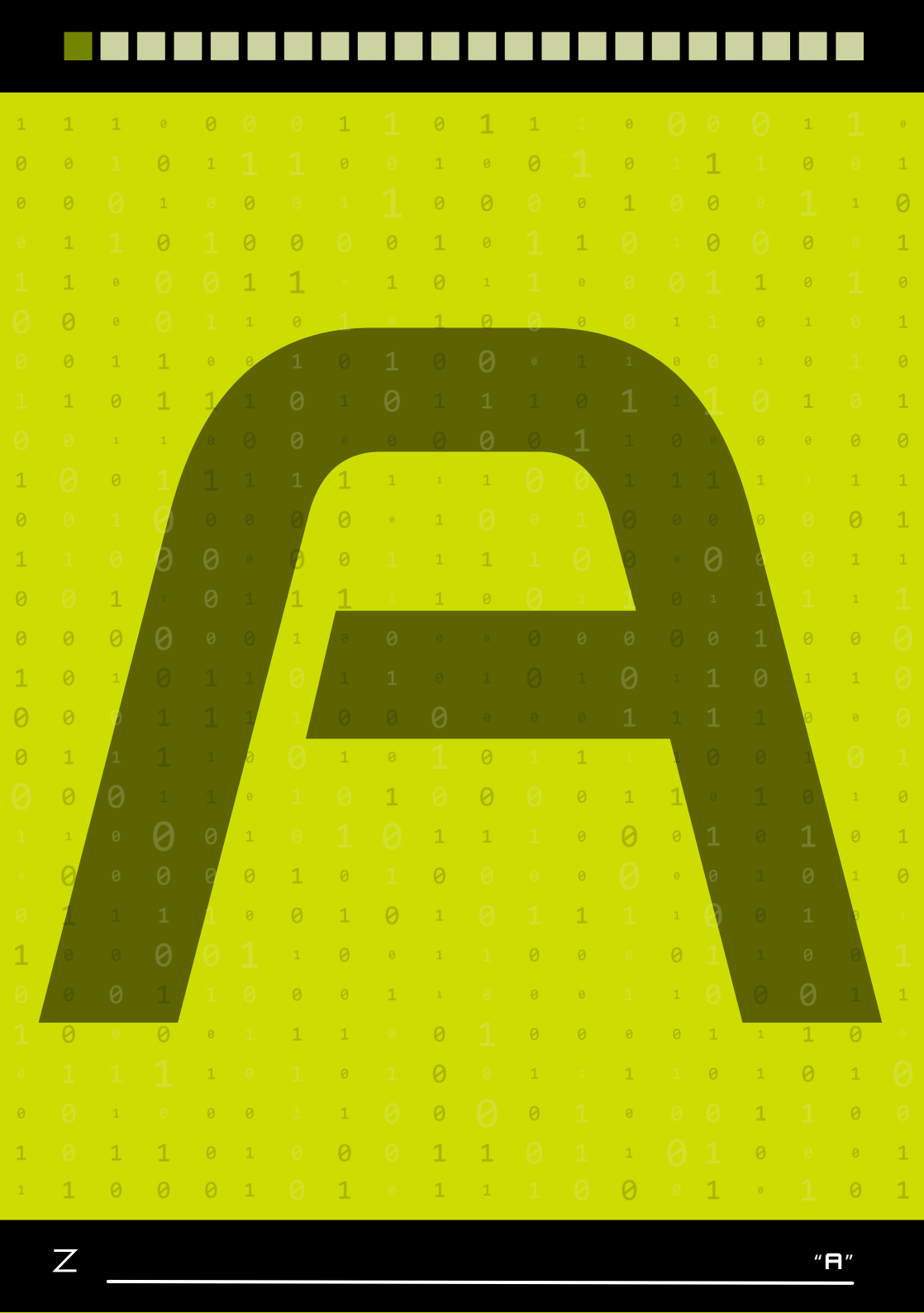
Kofinanziert von der Europäischen Union

Von der Europäischen Union finanziert. Die geäußerten Ansichten und Meinungen entsprechen ausschließlich denen des Autors bzw. der Autoren und spiegeln nicht zwingend die der Europäischen Union oder der OeAD-GmbH wider. Weder die Europäische Union noch die OeAD-GmbH können dafür verantwortlich gemacht werden.
Projektnummer: 2023-1-AT01-KA220-ADU-000157050

In diesem Glossar finden Sie Erklärungen zu allen unbekannten Begriffen, über die Sie im DataGame e-Book gestolpert sind oder über die Sie bei Ihren künftigen Bemühungen rund um das Thema Datenschutz stolpern könnten. Ein Glossar ist sehr nützlich, wenn man sich in diesen Gewässern bewegt.

Und ja, wir nehmen die Sache so ernst, dass wir sogar eine Erklärung des Begriffs „Internet“ für nötig halten.

. . . Was wenn Sie von einem anderen Planeten kommen?


A

Abhören – Das heimliche Mithören privater Kommunikation, in der Regel über ungesicherte Netzwerke, um sensible Informationen zu sammeln.

ACL – siehe Eintrag **Zugriffskontrollliste**

Access-Management bzw. **Zugriffsverwaltung** – Der Prozess der Verwaltung des Benutzerzugriffs auf Ressourcen und Daten innerhalb einer Organisation.

Active Directory – Ein Microsoft-Dienst zur Verwaltung von Berechtigungen und des Zugriffs auf Netzwerkressourcen innerhalb einer Domänenumgebung.

Administratorkonto – Ein Benutzerkonto mit erweiterten Rechten, das die Verwaltung von Systemeinstellungen und Benutzerkonten ermöglicht.

Advanced Encryption Standard (AES) (dt. „fortschrittlicher Verschlüsselungsstandard“) – Ein symmetrischer Verschlüsselungsalgorithmus, der häufig zum Schutz von Daten verwendet wird und als äußerst sicher und effizient gilt.

Advanced Persistent Threat (APT) (dt. „fortgeschrittene andauernde Bedrohung“) – Ein langwieriger und gezielter Cyberangriff, bei dem sich ein:e Angreifer:in unbefugten Zugang zu einem Netzwerk verschafft und über einen längeren Zeitraum unentdeckt bleibt.

Adware – Software, die automatisch (oft unerwünschtes) Werbematerial anzeigt oder herunterlädt, wenn ein:e Benutzer:in online ist.

Angriffserkennungssystem bzw. **Intrusion Detection System (IDS)** – Ein Gerät oder eine Softwareanwendung, die Netzwerk- oder Systemaktivitäten auf schädliche Aktionen oder Richtlinienverstöße überwacht.

Angriffsfläche – Der Gesamtbereich oder die Gesamtheit der Einstiegspunkte in ein System oder Netzwerk, die von Angreifer:innen ausgenutzt werden können.

Angriffsvektor – Die Methode oder der Weg, den ein:e Angreifer:in benutzt, um sich unerlaubten Zugang zu einem System oder Netzwerk zu verschaffen.

Anomalie-Erkennung – Der Prozess der Identifizierung ungewöhnlicher Muster oder Abweichungen vom normalen Verhalten, die auf eine Sicherheitsbedrohung hindeuten können.

Anonymisierung – Der Prozess des Entfernens personenbezogener Daten aus Datensätzen, sodass Einzelpersonen nicht leicht identifiziert werden können.

Anti-Malware – Software zur Erkennung, Abwehr und Entfernung schädlicher Software, darunter Viren, Würmer und Spyware.

Anti-Phishing – Techniken und Tools zur Verhinderung von Phishing-Angriffen, bei denen versucht wird, Personen zur Herausgabe sensibler Informationen zu verleiten.

Anwendungssicherheit – Die Praxis des Schutzes von Anwendungen vor Bedrohungen und Schwachstellen während ihres gesamten Lebenszyklus.

Anwendungsschwachstelle – Eine Sicherheitslücke in einer Anwendung, die von Angreifer:innen ausgenutzt werden kann, um die Sicherheit zu gefährden oder auf sensible Daten zuzugreifen.

API-Sicherheit – Die Praxis der Sicherung von Programmierschnittstellen (Application Programming Interfaces – API), um unbefugten Zugriff und Datenschutzverletzungen zu verhindern.

Application Whitelisting – Eine Sicherheitsmaßnahme, die es nur zugelassenen Anwendungen erlaubt, auf einem System zu laufen, und alle anderen blockiert.

Arbeitnehmerdatenschutz – Der Schutz personenbezogener Daten und der Rechte auf Privatsphäre in der Arbeitsumgebung.

Asymmetrische Verschlüsselung – Eine Art der Verschlüsselung, bei der ein Schlüsselpaar (öffentlich und privat) für die sichere Datenübertragung verwendet wird, wobei ein Schlüssel die Daten verschlüsselt und der andere Schlüssel sie entschlüsselt.

Asset Management – Der Prozess der Verwaltung und Sicherung der physischen und digitalen Vermögenswerte eines Unternehmens, darunter Hardware, Software und Daten.

Audit – Eine systematische Untersuchung eines Systems oder Prozesses, um die Einhaltung von Sicherheitsrichtlinien zu gewährleisten und verbesserungswürdige Bereiche zu identifizieren.

Audit-Log – Eine detaillierte Aufzeichnung von Systemereignissen, darunter Benutzeraktionen und Systemänderungen, die der Sicherheitsüberwachung und Compliance dienen.

Audit-Trail - Eine chronologische Aufzeichnung von Ereignissen, Aktionen oder Änderungen in einem System, die bei der Verfolgung und Überwachung von Benutzeraktivitäten hilft.

Authentifizierung – Der Prozess der Überprüfung der Identität eines:einer Benutzer:in oder Systems, oft durch Passwörter, biometrische Daten oder andere Methoden.

Authentifizierungs-Token – Ein digitales Objekt, das die Identität eines:einer Benutzer:in nachweist und einen sicheren Zugang zu einem System ermöglicht, oft in Form eines Hardware-Geräts oder eines softwarebasierten Codes.

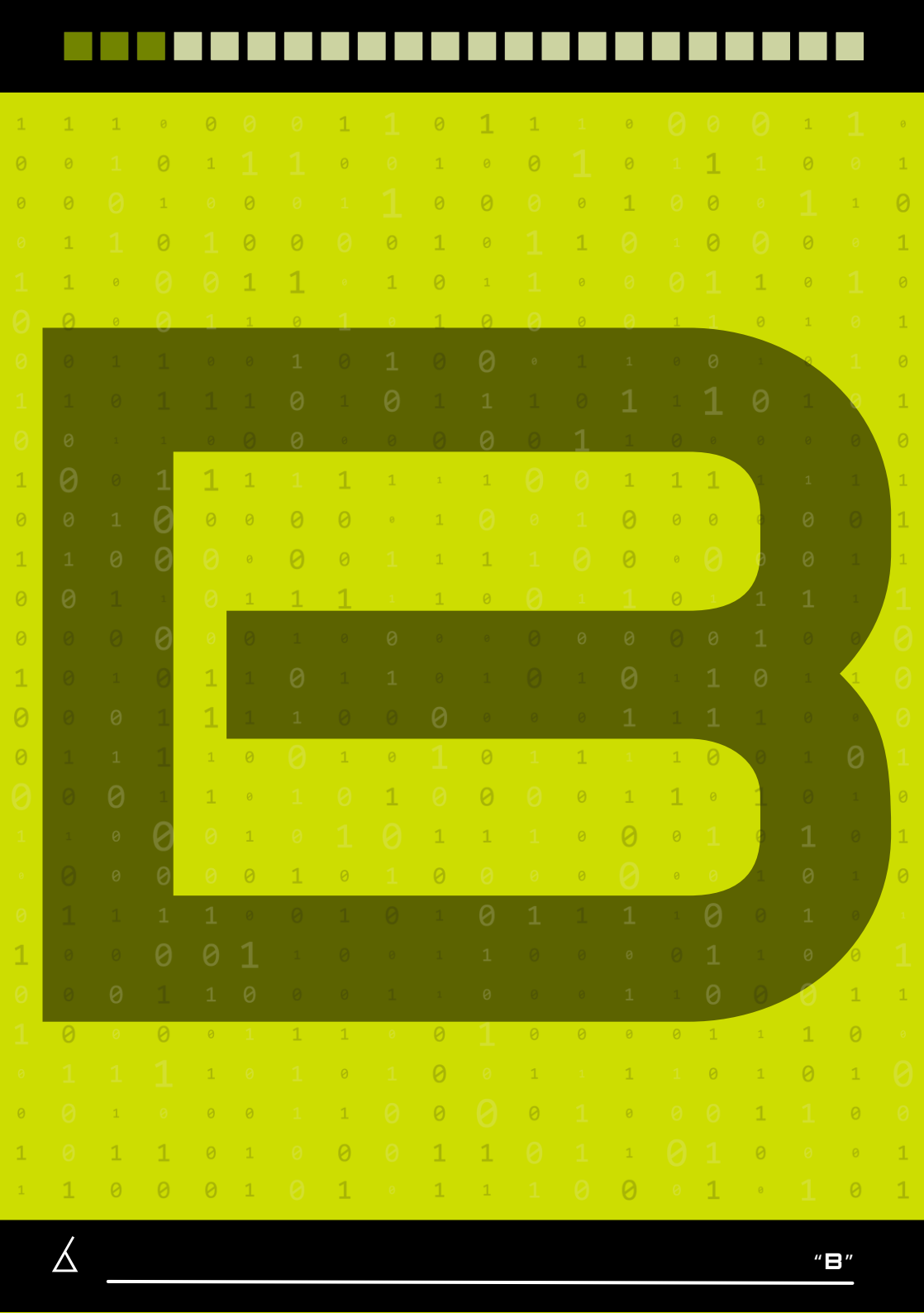
Automatisierte Bedrohungserkennung - Der Einsatz von automatisierten Tools und Technologien, um potenzielle Sicherheitsbedrohungen in Echtzeit zu erkennen und darauf zu reagieren.

Automatisiertes Backup - Ein Backup-Prozess, der automatisch geplant und ausgeführt wird, wodurch der Bedarf an manuellen Eingriffen reduziert wird.

Autorisierung – Der Prozess, bei dem festgestellt wird, ob ein:e Benutzer:in oder ein System das Recht hat, auf eine Ressource zuzugreifen oder bestimmte Aktionen auszuführen.

Autorisierungsprotokoll - Ein Satz von Regeln und Verfahren zur Bestimmung und Durchsetzung von Berechtigungen für den Zugriff auf Ressourcen und die Durchführung von Aktionen.

Availability bzw. **Verfügbarkeit** - Die Gewissheit, dass Daten und Ressourcen bei Bedarf für autorisierte Benutzer:innen zugänglich sind; Teil der CIA-Triade (Confidentiality - Vertraulichkeit, Integrity - Integrität, Availability -Verfügbarkeit) in der Informationssicherheit.


B

Backdoor – Eine versteckte oder nicht autorisierte Methode für den Zugriff auf ein System oder Netzwerk, die oft von Angreifer:innen oder Schadsoftware erstellt wird, um die normalen Sicherheitskontrollen zu umgehen.

Backup – Eine Kopie von Daten oder Systemdateien, die separat gespeichert wird, um einen Verlust im Falle eines Ausfalls oder Datenverlusts zu verhindern.

Backup und Wiederherstellung – Prozesse und Technologien zur Erstellung von Datensicherungen und deren Wiederherstellung im Falle eines Datenverlusts oder einer Datenbeschädigung.

Backup-Verschlüsselung – Die Praxis der Verschlüsselung von Backup-Daten, um deren Vertraulichkeit zu gewährleisten und unbefugten Zugriff zu verhindern.

Backup-Frequenz – Das Intervall, in dem Backups durchgeführt werden, das je nach Wichtigkeit der Daten von stündlich bis jährlich variieren kann.

Backup-Integrität – Die Gewissheit, dass Backup-Daten vollständig, genau und zuverlässig sind und nicht manipuliert oder beschädigt wurden.

Backup-Richtlinien – Ein Satz von Richtlinien und Verfahren für die Erstellung, Verwaltung und Wiederherstellung von Backups zur Gewährleistung der Datenintegrität und -verfügbarkeit.

Backup-Lösung – Ein umfassendes System oder ein Dienst zur Erstellung, Speicherung und Verwaltung von Backups, um den Schutz und die Wiederherstellung von Daten zu gewährleisten.

Backup-Tests – Der Prozess der regelmäßigen Überprüfung der Effektivität und Zuverlässigkeit von Backup-Verfahren, um sicherzustellen, dass die Daten bei Bedarf erfolgreich wiederhergestellt werden können.

Bedrohungsakteur – Eine Einzelperson oder Gruppe, die schädliche Aktivitäten, wie z. B. Cyberangriffe, mit der Absicht durchführt, Systeme zu gefährden, Daten zu stehlen oder den Betrieb zu stören.

Behördliche Vorschriften – Durch Gesetze und Vorschriften auferlegte Verpflichtungen, die Organisationen zur Gewährleistung des Datenschutzes einhalten müssen.

Benutzerfreundlichkeit – Die Einfachheit, mit der ein Tool oder System von den vorgesehenen Benutzer:innen verwendet werden kann.

Betriebliche Kontinuitätsplanung (Business Continuity Planning – BCP) – Der Prozess der Entwicklung von Systemen und Verfahren, die sicherstellen, dass kritische Geschäftsfunktionen während und nach einer Unterbrechung weiterlaufen können.

Betriebliches Risikomanagement – Der Prozess der Identifizierung, Bewertung und Abschwächung von Risiken, die sich auf den Geschäftsbetrieb auswirken könnten, darunter auch Risiken der Cybersicherheit und des Datenschutzes.

Betriebssystem-Härtung – Der Prozess der Sicherung eines Betriebssystems durch Verringerung seiner Angriffsfläche, z. B. durch Deaktivierung unnötiger Dienste, Anwendung von Patches und Konfiguration von Sicherheitseinstellungen.

Betroffene Person bzw. **Data Subject** – Eine Person, deren personenbezogene Daten gemäß der Definition in Datenschutzbestimmungen wie der DSGVO von einer Organisation verarbeitet werden.

Betrugsaufdeckung – Techniken und Systeme zur Erkennung und Verhinderung betrügerischer Aktivitäten oder Transaktionen.

Biometrische Authentifizierung – Eine Methode zur Überprüfung der Identität auf der Grundlage einzigartiger biologischer Merkmale, wie Fingerabdrücke, Gesichtserkennung oder Iris-Scans.

Biometrische Authentifizierungssysteme – Systeme, die biometrische Daten (z. B. Fingerabdrücke, Gesichtserkennung) zur Überprüfung und Authentifizierung von Benutzeridentitäten verwenden.

Biometrische Daten – Informationen über die einzigartigen biologischen Merkmale einer Person, die zu Authentifizierungs- und Identifizierungszwecken verwendet werden.

Biometrische Verifikation – Der Prozess der Bestätigung der Identität einer Person anhand biometrischer Merkmale wie Fingerabdrücke, Stimme oder Irismuster.

Biohacking – Der Einsatz biologischer Techniken und Technologien zur Verbesserung oder Manipulation menschlicher Fähigkeiten, was zu Bedenken hinsichtlich Datenschutz und Sicherheit führen kann.

Blacklist (dt. „Schwarze Liste“) – Eine Liste von Entitäten oder IP-Adressen, denen der Zugang zu einem System oder Netzwerk aufgrund bekannter schädlicher Handlungen oder Sicherheitsrisiken verweigert wird.

Black Hat – Ein Begriff zur Beschreibung von Hacker:innen oder Sicherheitsexpert:innen, die ihre Fähigkeiten für schädliche Zwecke einsetzen, z. B. für den Diebstahl von Daten oder die Störung von Systemen.

Black-Hat-SEO – Schädliche Techniken zur unethischen Manipulation von Suchmaschinen-Rankings, die zur Verbreitung von Malware oder Phishing-Angriffen genutzt werden können.

Blockchain – Eine dezentralisierte digitale Buchführungstechnologie, die Transaktionen über mehrere Computer hinweg aufzeichnet und so die Sicherheit und Transparenz erhöht.

Blockchain-Sicherheit – Die Maßnahmen und Protokolle, die implementiert werden, um die Integrität, Vertraulichkeit und Sicherheit von Blockchain-Transaktionen und -Daten zu gewährleisten.

Blue Team – Das Team, das für die Verteidigung und Sicherung der Systeme und Netzwerke eines Unternehmens gegen Cyberangriffe und andere Sicherheitsbedrohungen zuständig ist.

Bot-Erkennung – Techniken und Tools zur Identifizierung und Blockierung automatisierter Bots, die für schädliche Zwecke eingesetzt werden können, z. B. zum Data-Scraping oder zum Starten von Angriffen.

Bot-Erkennung und -Abwehr – Strategien und Tools zur Identifizierung und Bekämpfung von schädlichen Bots, die die Datensicherheit gefährden oder Dienste stören können.

Botnet(z) – Ein Netzwerk aus kompromittierten Computern oder Geräten, das von einem:einer schädlichen Akteur:in kontrolliert wird und häufig für koordinierte Angriffe oder die Verbreitung von Malware genutzt wird.

Branded Malware – Malware, die so konzipiert ist, dass sie legitime Software oder Dienste imitiert, wobei häufig bekannte Marken oder Namen verwendet werden, um Benutzer:innen zu täuschen.

Breach bzw. **Sicherheitsverletzung** – Ein Vorfall, bei dem es zu einem unbefugten Zugriff oder einer unbefugten Offenlegung von Daten kommt, wodurch der Datenschutz und die Datensicherheit gefährdet werden können.

Breach Detection – Techniken und Tools zur rechtzeitigen Erkennung und Reaktion auf unbefugten Zugriff oder Datenschutzverletzungen.

Breach Notification bzw. **Meldung einer Sicherheitsverletzung** – Der durch Vorschriften und Gesetze vorgeschriebene Prozess der Benachrichtigung betroffener Personen und relevanter Behörden über eine Datenschutzverletzung.

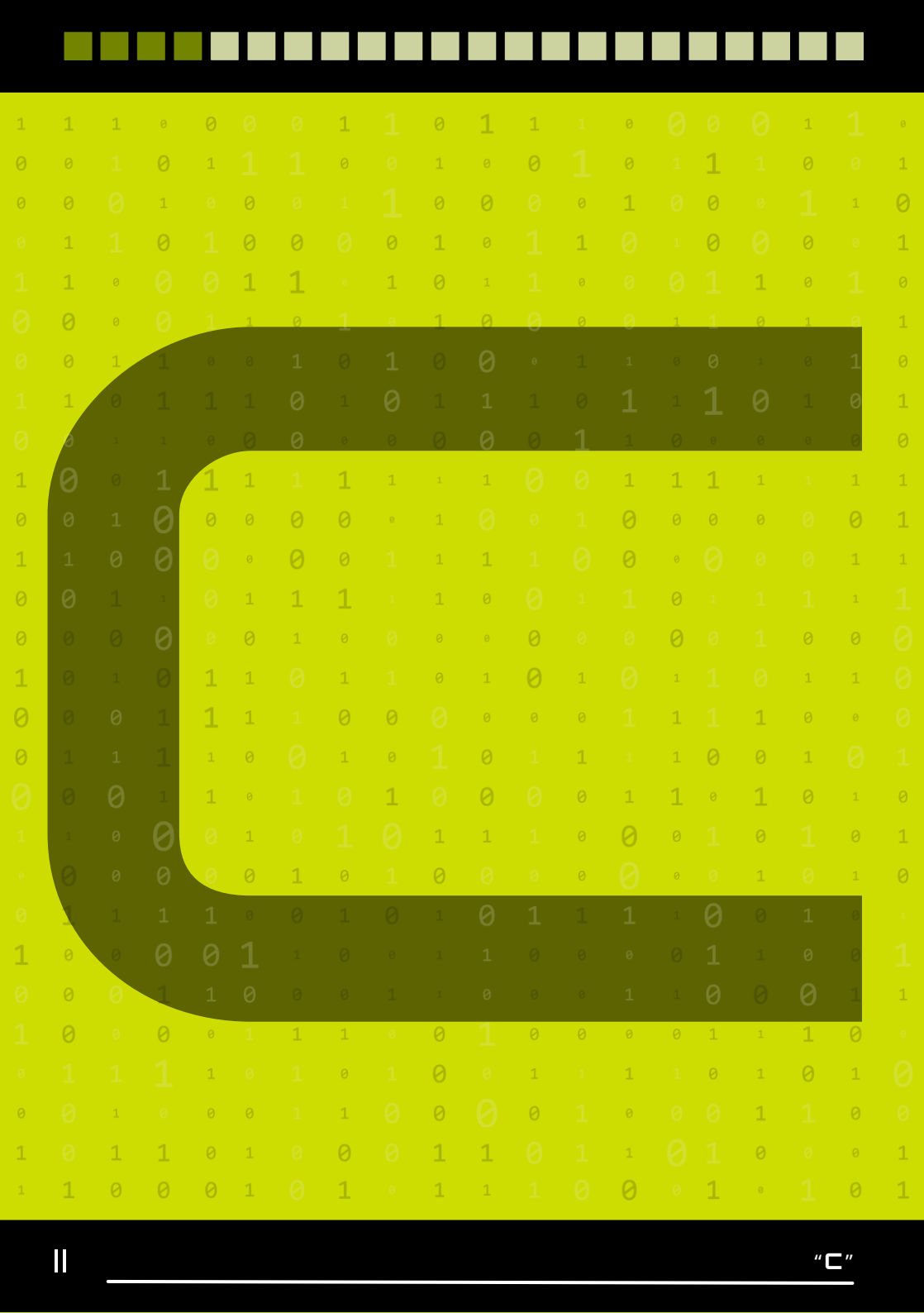
Brute-Force-Angriff – Eine Art von Cyberangriff, bei dem ein:e Angreifer:in systematisch alle möglichen Kombinationen von Passwörtern oder Verschlüsselungsschlüsseln ausprobiert, bis die richtige Kombination gefunden ist.

Browser-Isolierung – Eine Sicherheitstechnik, bei der die Webbrowsing-Aktivitäten vom restlichen System isoliert werden, um Malware-Infektionen und Datenschutzverletzungen zu verhindern.

Browsersicherheit – Maßnahmen und Praktiken zum Schutz von Webbrowsern vor Sicherheitsbedrohungen wie Malware, Phishing und Datenschutzverletzungen.

Business Process Outsourcing (BPO) – Beauftragung von Drittanbietern mit der Erledigung bestimmter Geschäftsfunktionen, was einen sorgfältigen Umgang mit dem Datenschutz und der Datensicherheit erfordert.

Bypass – Eine Aktion oder Methode zur Umgehung von Sicherheitsmaßnahmen oder -kontrollen, häufig um unbefugten Zugriff zu erhalten oder Schwachstellen auszunutzen.



Certified Information Systems Security Professional (CISSP) – Eine weltweit anerkannte Zertifizierung für Informationssicherheitsexpert:innen, die Fachkenntnisse in verschiedenen Bereichen der Cybersicherheit nachweist.

Cloud Computing (dt. „Datenwolke“) – Die Bereitstellung von Rechendiensten über das Internet, darunter Speicherung, Verarbeitung und Anwendungen, die robuste Sicherheitsmaßnahmen erfordern.

Cloud-Verschlüsselung – Der Prozess der Verschlüsselung von Daten, die in Cloud-Diensten gespeichert oder über diese übertragen werden, um sie vor unberechtigtem Zugriff zu schützen.

Cloud-Sicherheit – Die Gesamtheit der Richtlinien, Technologien und Kontrollen zum Schutz von Daten, Anwendungen und Systemen, die in Cloud-Umgebungen gehostet werden.

Compliance – Einhaltung von Gesetzen, Vorschriften, Standards und Richtlinien in Bezug auf Datenschutz, Privatsphäre und Cybersicherheit.

Compliance-Audit – Eine systematische Überprüfung der Einhaltung von Datenschutzgesetzen, -vorschriften und internen Richtlinien durch ein Unternehmen.

Compliance-Management – Der Prozess, der sicherstellt, dass eine Organisation ihre gesetzlichen und regulatorischen Verpflichtungen in Bezug auf Datenschutz und -sicherheit erfüllt.

Confidentiality bzw. **Vertraulichkeit** – Der Grundsatz, dass Informationen nur jenen zugänglich sind, die dazu berechtigt sind, und dass sie vor unbefugter Offenlegung geschützt sind.

Container-Sicherheit – Die Praxis der Sicherung von containerisierten Anwendungen und deren zugehörigen Daten und Konfigurationen, um unbefugten Zugriff und Schwachstellen zu verhindern.

Cookie – Ein kleiner Datensatz, der von einem Webbrowser auf dem Gerät eines:einer Nutzer:in gespeichert wird und dazu dient, Nutzeraktivitäten und -präferenzen zu erfassen.

Cookies – Kleine Datensätze, die von einer Website auf dem Gerät eines:einer Nutzer:in gespeichert werden und dazu dienen, Nutzeraktivitäten und -präferenzen zu erfassen.

Cross-Site Scripting (XSS) – Eine Sicherheitslücke in Webanwendungen, die es Angreifer:innen ermöglicht, schädliche Skripte in Webseiten einzuschleusen, die von anderen Benutzer:innen aufgerufen werden.

Cryptojacking – Die unbefugte Nutzung der Computerressourcen einer anderen Person zum Schürfen von Kryptowährungen.

Cyberangriff – Ein Versuch von Hacker:innen oder böswilligen Akteur:innen, Computersysteme oder Netzwerke zu stören, zu beschädigen oder sich unbefugten Zugang zu ihnen zu verschaffen.

Cyber-Bedrohung – Ein potenzieller oder tatsächlicher schädlicher Angriff oder eine Aktivität, die sich gegen die Informationssysteme oder Daten einer Organisation richtet.

Cyber-Recht – Die Gesamtheit der Gesetze und Vorschriften, die Aktivitäten im Zusammenhang mit Cybersicherheit, Datenschutz und digitaler Kommunikation regeln.

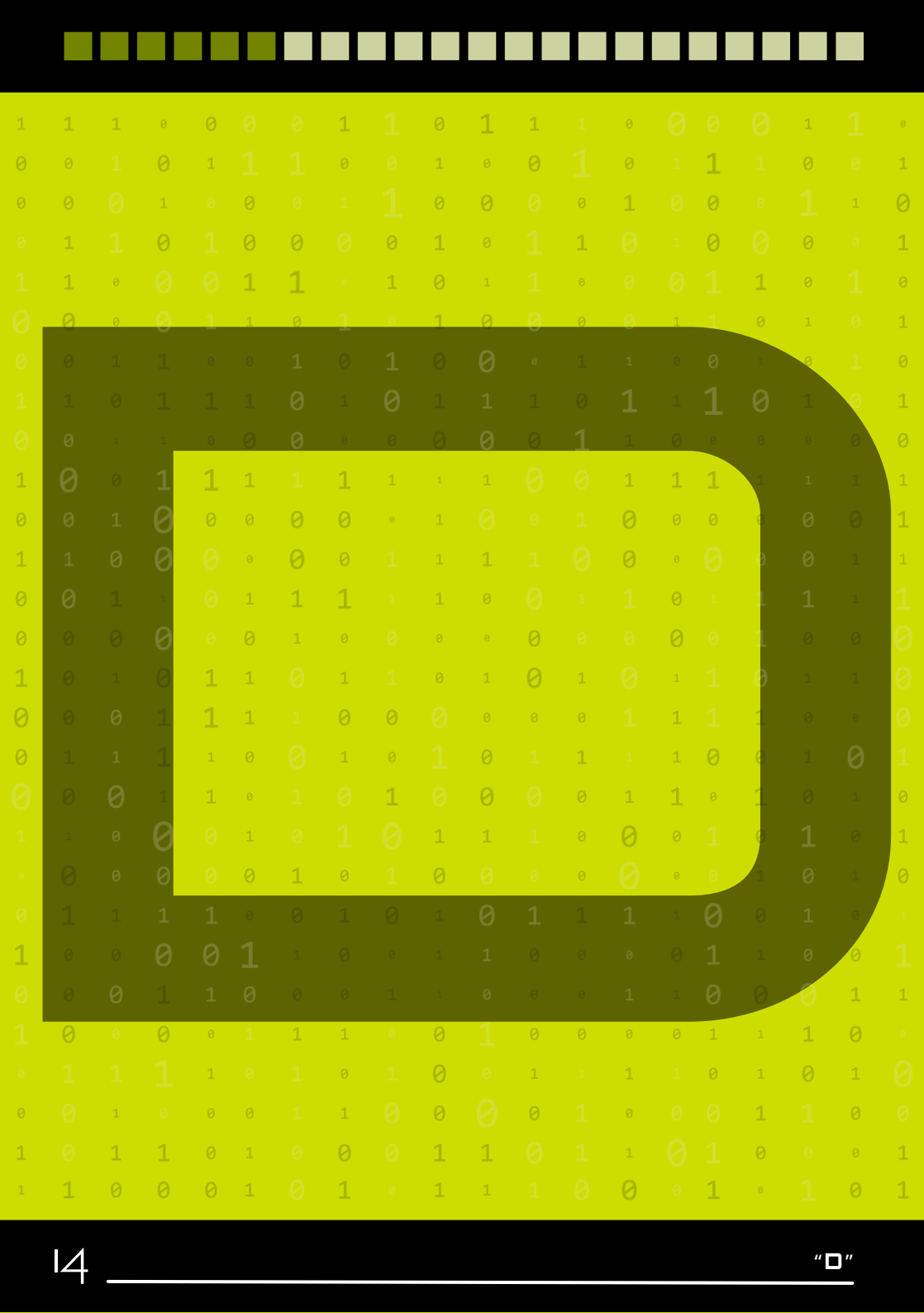
Cyber-Resilienz – Die Fähigkeit einer Organisation, Cyberangriffen und anderen Störungen zu widerstehen und sich von ihnen zu erholen, während die wesentlichen Abläufe aufrechterhalten werden.

Cybersicherheit – Die Praxis des Schutzes von Systemen, Netzwerken und Daten vor digitalen Angriffen, Diebstahl und Schäden.

Cybersicherheitsrichtlinien – Richtlinien und Regeln zum Schutz der digitalen Ressourcen einer Organisation vor Cyberbedrohungen.

Cyberversicherung – Eine Art von Versicherung, die Unternehmen vor den finanziellen Auswirkungen von Cyberangriffen, Datenschutzverletzungen und anderen Cyber-Sicherheitsvorfällen schützen soll.

Cyber-Vorfallreaktion – Der Prozess der Verwaltung und Bearbeitung eines Cyber-Sicherheitsvorfalls, um dessen Auswirkungen zu mindern und weiteren Schaden zu verhindern.



Data Breach Notification bzw. **Meldung einer Datenschutzverletzung –** Die Verpflichtung, die betroffenen Personen und die zuständigen Behörden zu informieren, wenn es zu einer Datenschutzverletzung kommt, die häufig durch Vorschriften wie die DSGVO geregelt wird.

Data Governance – Ein Rahmen für die Verwaltung von Datenverfügbarkeit, -verwendbarkeit, -integrität und -sicherheit innerhalb einer Organisation durch Richtlinien, Verfahren und Kontrollen.

Data-Lifecycle-Management – Der Prozess der Verwaltung von Daten von der Erstellung und Speicherung bis zur Löschung oder Archivierung.

Data Loss Prevention (DLP) – Eine Reihe von Tools und Prozessen, die dazu dienen, die unbefugte Nutzung, Übertragung oder Offenlegung sensibler Daten zu erkennen und zu verhindern.

Data Masking – Der Prozess, bei dem bestimmte Daten innerhalb eines Datensatzes unkenntlich gemacht werden, um sensible Informationen zu schützen und gleichzeitig ihre Verwendbarkeit für autorisierte Zwecke zu bewahren.

Data Subject bzw. **Betroffene Person** – Eine Person, deren personenbezogene Daten gemäß der Definition in Datenschutzbestimmungen wie der DSGVO von einer Organisation verarbeitet werden.

Data Subject Access Request (DSAR) – Antrag einer Einzelperson an eine Organisation auf Zugang zu den personenbezogenen Daten, die diese in Übereinstimmung mit den Datenschutzgesetzen über sie gespeichert hat.

Data Wiping – Der Prozess des sicheren Löschens von Daten auf Speichergeräten, um eine Wiederherstellung zu verhindern, häufig angewandt, wenn Hardware außer Betrieb genommen oder recycelt wird.

Dateibasierte Ransomware – Ransomware, die auf bestimmte Dateien oder Dateitypen abzielt und diese verschlüsselt anstatt das gesamte System.

Dateiverschlüsselung – Der Prozess der Umwandlung von Dateien in ein sicheres Format, auf das nur mit einem Entschlüsselungsschlüssel zugegriffen werden kann.

Datenaggregation – Der Prozess der Kombination von Daten aus mehreren Quellen, um nützliche Informationen zu analysieren und zu extrahieren.

Datenaggregationstools – Technologien, die zur Kombination von Daten aus verschiedenen Quellen für die Analyse und Berichterstattung verwendet werden.

Datenanonymisierung – Der Prozess der Umgestaltung von personenbezogenen Daten, sodass die Person, auf die sich die Daten beziehen, nicht mehr identifiziert werden kann.

Datenbehandlung – Die Verwaltung von Daten während ihres gesamten Lebenszyklus, darunter Erfassung, Speicherung, Übertragung und Löschung, unter Einhaltung von Sicherheits- und Datenschutzstandards.

Daten-Compliance-Audit – Eine Bewertung, die durchgeführt wird, um sicherzustellen, dass die Datenverarbeitungspraktiken den rechtlichen und regulatorischen Standards entsprechen.

Datenerfassung – Der Prozess des Sammelns von Daten aus verschiedenen Quellen zur Analyse oder Verarbeitung.

Datengenauigkeit – Der Grad, in dem Daten das reale Objekt oder Konzept, das sie modellieren sollen, korrekt darstellen.

Datenhoheit – Das Konzept, dass Daten den Gesetzen und Vorschriften des Landes unterliegen, in dem sie gespeichert sind.

Datenintegrität – Die Genauigkeit und Konsistenz von Daten während ihres gesamten Lebenszyklus, sodass sichergestellt ist, dass sie bei der Übertragung oder Speicherung unverändert bleiben.

Datenklassifizierung – Der Prozess der Organisation von Daten in Kategorien auf Grundlage ihrer Sensibilität und Relevanz, um angemessene Sicherheitskontrollen zu gewährleisten.

Datenleck – Die unbefugte Übertragung sensibler Daten innerhalb einer Organisation an eine:n externe:n oder unbefugte:n Empfänger:in.

Datenminimierung – Der Grundsatz, nur so viele personenbezogene Daten zu sammeln und aufzubewahren, wie für einen bestimmten Zweck erforderlich sind, um Risiken für die Privatsphäre zu verringern.

Datenmüll – Falsche, irrelevante oder unnötige Daten, die in der Cybersicherheit oft als Taktik verwendet werden, um Angreifer:innen in die Irre zu führen oder echte Daten zu verschleiern.

Datennutzung – Die Art und Weise, wie gesammelte Daten innerhalb einer Organisation verwendet werden, z. B. für Analysen, Berichte und Entscheidungsfindung.

Datenprüfung – Der Prozess, bei dem sichergestellt wird, dass die Daten richtig, vollständig und gültig sind, bevor sie verarbeitet oder verwendet werden.

Datenqualität – Das Maß für die Genauigkeit, Vollständigkeit und Zuverlässigkeit von Daten.

Datenresidenz – Der physische Ort, an dem Daten gespeichert werden, was je nach Gerichtsbarkeit Auswirkungen auf die Einhaltung von Datenschutzgesetzen haben kann.

Datensanitisierung – Der Prozess des sicheren Löschens oder Vernichtens von Daten aus einem System, um zu verhindern, dass sie wiederhergestellt werden können.

Datenschutz – Die rechtlichen und technischen Maßnahmen zum Schutz personenbezogener und sensibler Daten vor unbefugtem Zugriff, unbefugter Nutzung oder Offenlegung.

Datenschutzbeauftragte:r – Eine Person, die ernannt wird, um die Einhaltung von Datenschutzgesetzen und -praktiken zu überwachen und zu gewährleisten und den ordnungsgemäßen Umgang mit personenbezogenen Daten sicherzustellen.

Datenschutzbehörde – Eine Aufsichtsbehörde, die für die Überwachung der Durchsetzung von Datenschutzgesetzen, wie der DSGVO, zuständig ist.

Datenschutzbestimmungen – Gesetze und Normen zum Schutz personenbezogener Daten vor Missbrauch und unbefugtem Zugriff.

Datenschutz-Folgenabschätzung (DSFA) – Ein Risikobewertungsprozess, den Organisationen verwenden, um die potenziellen Datenschutzrisiken im Zusammenhang mit der Verarbeitung personenbezogener Daten zu bewerten.

Datenschutzgrundverordnung (DSGVO) – Eine von der Europäischen Union (EU) durchgesetzte umfassende Verordnung zum Schutz der personenbezogenen Daten von Individuen innerhalb der EU und zur Regelung der Datenschutzpraktiken von Organisationen, die mit solchen Daten umgehen.

Datenschutzhinweise – Dokumente, die Einzelpersonen zur Verfügung gestellt werden und in denen erläutert wird, wie ihre Daten erfasst, verwendet und geschützt werden.

Datenschutzrichtlinien – Dokumente, in denen dargelegt wird, wie eine Organisation personenbezogene Daten sammelt, verwendet und schützt.

Datenschutzverletzung (Data Breach) – Ein Vorfall, bei dem sensible, vertrauliche oder geschützte Informationen von unbefugten Personen eingesehen, offengelegt oder gestohlen werden.

Datenschwärzung – Der Prozess der Bearbeitung oder Schwärzung sensibler Informationen in einem Dokument, bevor es weitergegeben wird, um die Privatsphäre oder Vertraulichkeit zu schützen.

Datensicherheit – Die Schutzmaßnahmen, die ergriffen werden, um Daten vor unbefugtem Zugriff, Beschädigung oder Diebstahl zu schützen und ihre Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten.

Datenspeicherlösungen – Technologien und Methoden zur sicheren Speicherung von Daten, darunter physische und cloudbasierte Optionen.

Daten-Tokenisierung – Der Prozess des Ersetzens sensibler Daten durch eindeutige Identifikationssymbole oder „Token“, die wesentliche Informationen beibehalten, ohne die ursprünglichen Daten preiszugeben.

Datentransfer – Verschieben von Daten von einem System oder Ort zu einem anderen, was unter Umständen die Beachtung von Datenschutzgesetzen erfordert.

Datentransferabkommen (Data Transfer Agreement – DTA) – Ein rechtliches Dokument, das die Bedingungen für die Übertragung von Daten zwischen Organisationen festlegt und die Einhaltung von Datenschutz- und Sicherheitsvorschriften gewährleistet.

Datenübertragbarkeit – Die Möglichkeit, personenbezogene Daten von einer Organisation zu einer anderen zu übertragen.

Datenverantwortliche:r – Eine Instanz, die den Zweck und die Mittel der Verarbeitung personenbezogener Daten entsprechend der Definition in Datenschutzgesetzen wie der DSGVO festlegt.

Datenverarbeitung – Die Operationen, die mit Daten durchgeführt werden, darunter Erhebung, Speicherung, Änderung und Löschung.

Datenverlust – Die versehentliche oder böswillige Zerstörung oder Löschung von Daten, die aufgrund von Hardwarefehlern, Cyberangriffen oder menschlichem Versagen erfolgen kann.

Datenvernichtung – Der Prozess des dauerhaften Löschens oder Vernichtens von Daten, um sicherzustellen, dass sie nicht wiederhergestellt oder rekonstruiert werden können.

Datenverschlüsselung – Der Prozess der Umwandlung lesbarer Daten in ein verschlüsseltes Format, das nur von autorisierten Benutzer:innen mit dem richtigen Entschlüsselungscode gelesen werden kann.

Datenverschlüsselungsstandards – Protokolle und Richtlinien für die Verschlüsselung von Daten, um deren Sicherheit zu gewährleisten.

Datenzugriffsprotokolle – Aufzeichnungen darüber, wer wann auf Daten zugegriffen hat und welche Aktionen durchgeführt wurden.

Deep Packet Inspection (DPI) – Eine Netzwerküberwachungsmethode, die den Inhalt von Datenpaketen beim Durchlaufen eines Kontrollpunkts untersucht und häufig zur Identifizierung und Eindämmung von Bedrohungen eingesetzt wird.

Denial-of-Service-(DoS-)Angriff – Ein Cyberangriff, bei dem der:die Angreifer:in ein Netzwerk oder einen Dienst mit übermäßigen Anfragen überflutet, so dass dieser für legitime Benutzer:innen nicht mehr verfügbar ist.

Digitale Forensik – Der Prozess des Sammelns, Analysierens und Bewahrens digitaler Beweise von Computern, Netzwerken und Geräten bei der Untersuchung von Cyberkriminalität oder -vorfällen.

Digitale Identität – Eine Reihe von Attributen und Berechtigungsnachweisen, die die Identität von Benutzer:innen bei digitalen Interaktionen definieren und häufig durch Authentifizierungsmethoden wie Passwörter oder biometrische Daten überprüft werden.

Digitale Signatur – Eine elektronische, kryptografische Signatur, die zur Überprüfung der Authentizität und Integrität einer Nachricht, eines Dokuments oder einer Transaktion verwendet wird.

Digitaler Fußabdruck – Die Datenspur, die eine Person bei der Nutzung digitaler Plattformen hinterlässt.

Digitales Zertifikat – Ein elektronisches Dokument zum Nachweis der Identität einer Website oder von Nutzer:innen, das häufig in Verbindung mit Verschlüsselung zur Sicherung der Online-Kommunikation verwendet wird.

Disaster Recovery (DR) – Ein Plan und Prozess zur Wiederherstellung von IT-Systemen und Daten nach einer größeren Störung oder Katastrophe, der die Geschäftskontinuität gewährleistet.

Distributed-Denial-of-Service-(DDoS-)Angriff – Eine Art von Cyberangriff, bei dem mehrere Systeme ein Ziel mit einer Flut von Datenverkehr überschwemmen, was zu Serviceausfällen führt.

DNS-Spoofing – Eine Art von Cyberangriff, bei dem ein:e Hacker:in DNS-Anfragen abfängt und abändert, um Benutzer:innen ohne ihr Wissen auf schädliche Websites umzuleiten.

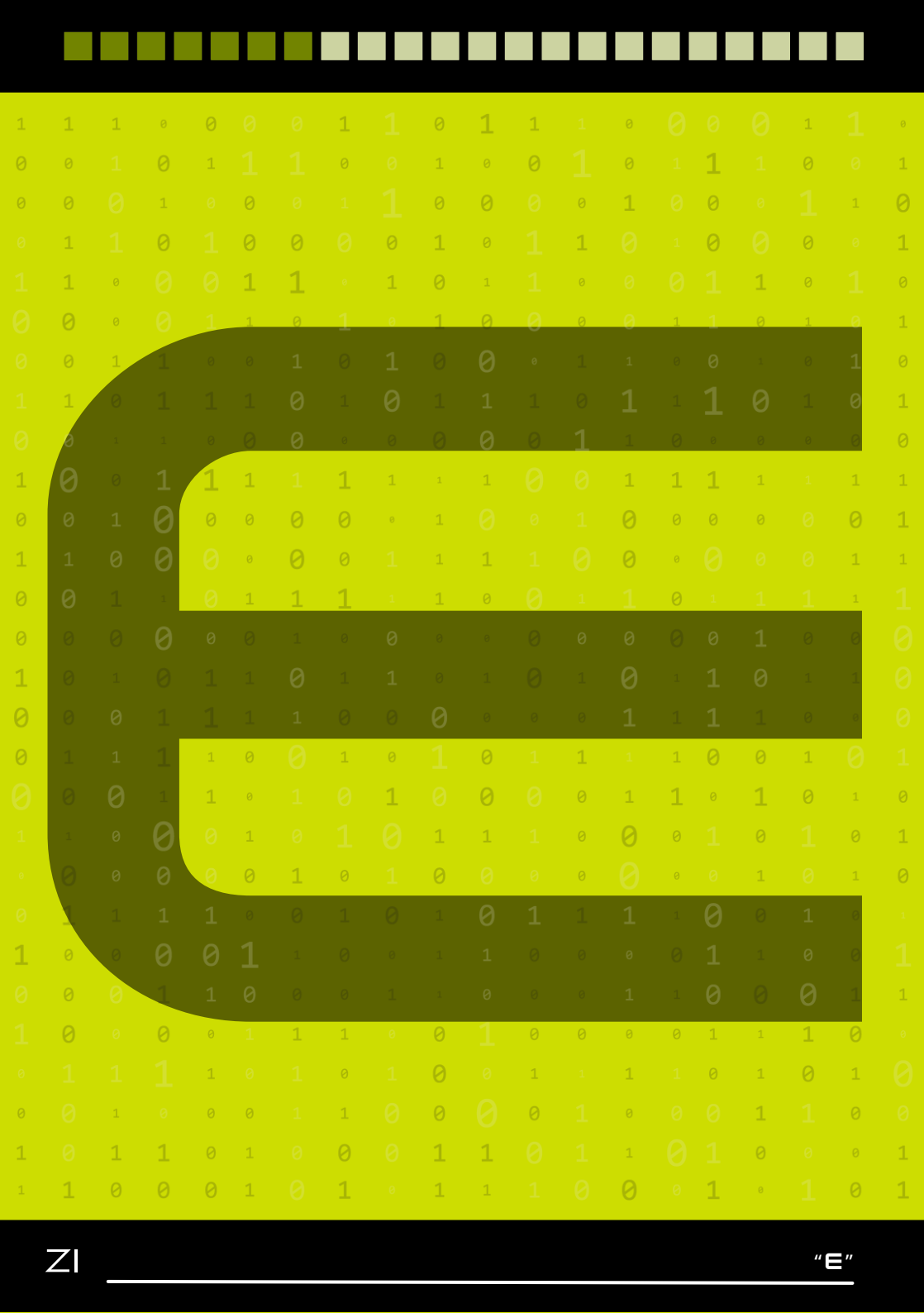
Domain Name System (DNS) – Das hierarchische System, das verwendet wird, um Domain-Namen (z. B. www.example.com) in IP-Adressen zu übersetzen und so die Navigation im Internet zu ermöglichen.

Domain-based Message Authentication, Reporting & Conformance (DMARC) – Ein E-Mail-Authentifizierungsprotokoll, das zum Schutz vor Spoofing und Phishing verwendet wird, indem es die Domäne des:der Absender:in verifiziert.

Drittanbieter – Externe Organisationen oder Einzelpersonen, die einem Unternehmen Dienstleistungen oder Produkte zur Verfügung stellen, was auch den Umgang mit Daten beinhalten kann.

Drive-by-Download – Eine Art von Cyberangriff, bei dem schädliche Software automatisch und ohne Zustimmung auf das Gerät eines:einer Benutzer:in heruntergeladen wird, normalerweise durch den Besuch einer kompromittierten Website.

Dumpster Diving (dt. „Mülltauchen“) – Eine physische Sicherheitsbedrohung, bei der Angreifer:innen weggeworfene Materialien, wie z. B. Papierdokumente oder alte Hardware, durchsuchen, um sensible Informationen zu finden.


E

E-Discovery (Electronic Discovery) – Der Prozess der Identifizierung, Sammlung und Vorlage elektronisch gespeicherter Informationen (ESI) für Gerichtsverfahren oder Untersuchungen.

Einverständnis – Die freiwillige Zustimmung einer Person zur Verarbeitung ihrer personenbezogenen Daten für bestimmte Zwecke.

E-Mail-Authentifizierung – Techniken zur Überprüfung der Authentizität von E-Mail-Nachrichten, um sicherzustellen, dass sie aus legitimen Quellen stammen und nicht schädlich sind.

E-Mail-Verschlüsselung – Der Prozess der Verschlüsselung von E-Mail-Nachrichten, um deren Inhalt während der Übertragung oder im Speicher vor unbefugtem Zugriff zu schützen.

E-Mail-Filterung – Software- oder hardwarebasierte Tools, die unerwünschte oder verdächtige E-Mails, wie Spam oder Phishing-Versuche, blockieren oder kennzeichnen.

E-Mail-Spoofing – Eine Cyberangriffstechnik, bei der der:die Absender:in einer E-Mail die Absenderadresse fälscht, um den Anschein zu erwecken, sie stamme von einer seriösen Quelle.

Embedded System Security – Die Praxis der Absicherung der Hardware- und Softwarekomponenten eingebetteter Systeme, bei denen es sich um spezielle Computersysteme innerhalb größerer Systeme handelt (z. B. medizinische Geräte, Autos).

Endgerät (engl. *Endpoint*) – Any device connected to a network, such as computers, smartphones, or IoT devices, which can be vulnerable to security risks and attacks.

Endgerätesicherheit – Die Praxis des Schutzes von Endgeräten vor Cyber-Bedrohungen mithilfe von Tools wie Antiviren-Software, Firewalls und Intrusion-Prevention-Systemen.

Endgeräteverschlüsselung – Die Verwendung von Verschlüsselungstechniken auf Endgeräten (z. B. Laptops, Mobiltelefone) zum Schutz sensibler Daten, die auf diesen Geräten gespeichert oder übertragen werden.

Endpoint Detection and Response (EDR) – Eine Cybersicherheitslösung, die kontinuierlich Daten von Endgeräten (z. B. Computer, mobile Geräte) überwacht und sammelt, um potenzielle Sicherheitsbedrohungen zu erkennen und darauf zu reagieren.

Enhanced Security Administrative Environment (ESAE) (dt. „Erweiterte Sicherheitsadministratorumgebung“) - Eine spezielle, isolierte Verwaltungsumgebung, die zum Schutz vor Angriffen auf privilegierte Konten in sensiblen oder risikoreichen Netzwerken entwickelt wurde.

Enterprise Information Security Architecture (EISA) - Ein umfassender Rahmen, der die Sicherheitsstrategien mit den Unternehmenszielen in Einklang bringt und Unternehmen bei der Implementierung zuverlässiger Informationssicherheitsverfahren unterstützt.

Enterprise Mobility Management (EMM) - Eine Reihe von Tools und Technologien zur Verwaltung mobiler Geräte, Anwendungen und Daten, um die Sicherheit zu gewährleisten, insbesondere in Unternehmensumgebungen.

Ethisches Hacking - Die Praxis des absichtlichen Sondierens von Systemen oder Netzwerken auf Schwachstellen mit Genehmigung, um Sicherheitslücken zu identifizieren, bevor böswillige Hacker:innen sie ausnutzen.

EU-US Privacy Shield/-Datenschutzschild - Ein Rahmen zum Schutz personenbezogener Daten, die zwischen der Europäischen Union und den Vereinigten Staaten übermittelt werden (Anmerkung: nach Nichtigerklärung durch andere Abkommen ersetzt).

Exfiltration - Die unbefugte Übertragung oder der Diebstahl von Daten aus einem Netzwerk, häufig von Hacker:innen durchgeführt, nachdem sie in ein System eingedrungen sind.

Exploit - Eine spezifische Methode/Technik, die von Hacker:innen verwendet wird, um eine Schwachstelle oder einen Schwachpunkt in einem System auszunutzen, um schädliche Aktivitäten auszuführen.

Exploit-Kit - Ein Toolkit, das von Cyberkriminellen verwendet wird, um Schwachstellen in Software zu identifizieren und auszunutzen und Malware oder anderen schädlichen Code einzuschleusen.

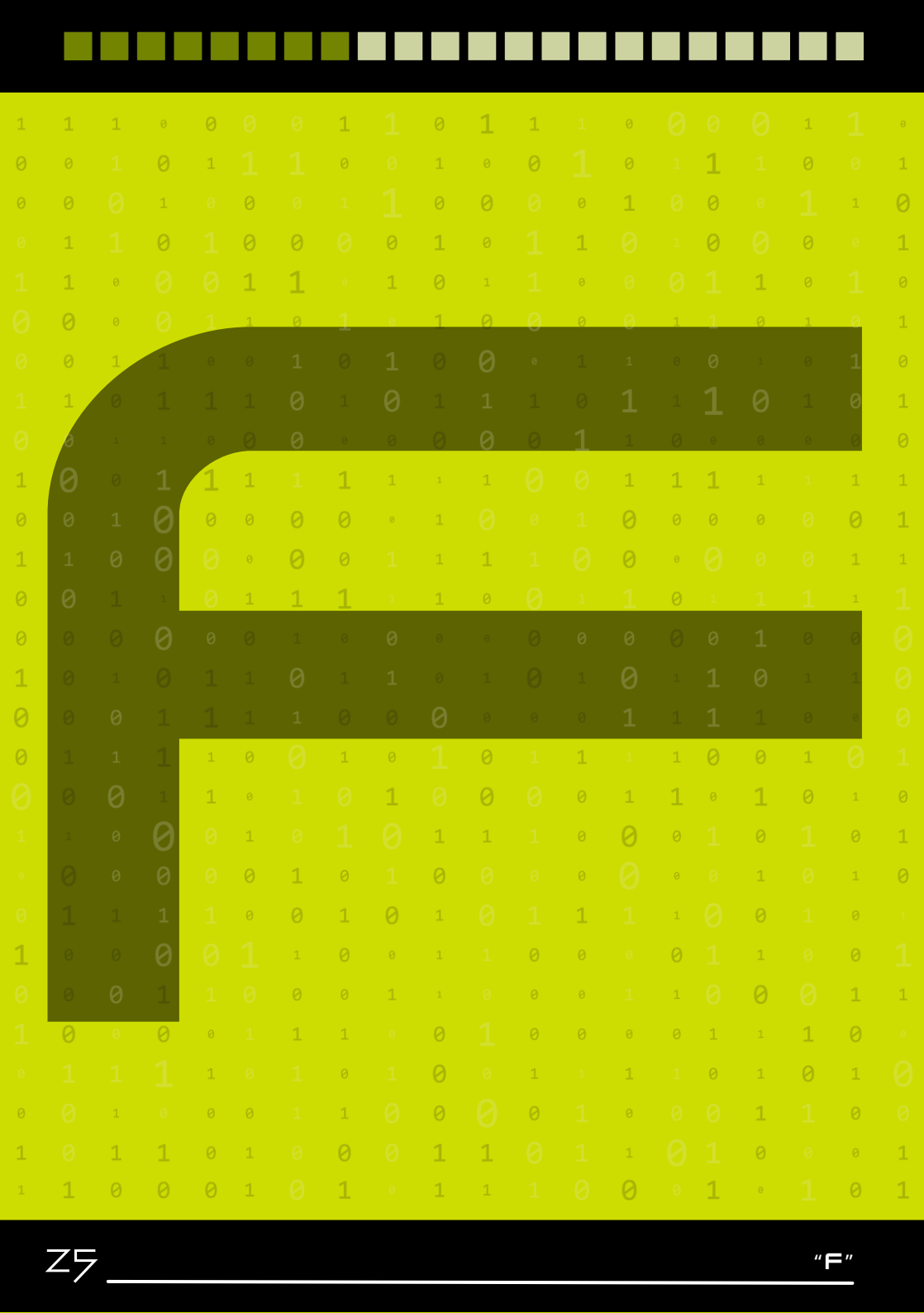
Extended Detection and Response (XDR) - Eine Cybersicherheitstechnologie, die Daten aus mehreren Sicherheitsebenen (z. B. Endgeräte, Netzwerke, Server) integriert, um eine umfassendere Erkennungs- und Reaktionsfähigkeit zu gewährleisten.

Externe Bedrohung - Jede Bedrohung für ein System oder eine Organisation, die von außerhalb des eigenen Netzwerks ausgeht, z. B. Hacker:innen, Phishing-Versuche oder online verbreitete Malware.

Externer Penetrationstest - Eine Art von Sicherheitstests, die von ethischen Hacker:innen oder Cybersicherheitsexpert:innen durchgeführt werden, um die Sicherheit eines Systems oder Netzwerks aus einer externen Perspektive zu bewerten.

Extensible Authentication Protocol (EAP) - Ein Authentifizierungsrahmen, der häufig in drahtlosen Netzwerken und Punkt-zu-Punkt-Verbindungen verwendet wird und verschiedene Methoden zur Authentifizierung von Geräten bietet.

Extensible-Markup-Language-(XML-)Verschlüsselung - Ein Standard zur Verschlüsselung der in einem XML-Dokument enthaltenen Daten, der zum Schutz der zwischen Systemen ausgetauschten Informationen, häufig in Webdiensten, verwendet wird.



Fallstudien – Detaillierte Untersuchungen bestimmter Fälle oder Szenarien im Zusammenhang mit Datenschutzproblemen und -lösungen.

Falscher Alarm – Ein von einem Sicherheitssystem erzeugter Alarm, der eine potenzielle Bedrohung anzeigt, die in Wirklichkeit nicht existiert.

Falsch-negativer Fehler – Ein Fehler, bei dem ein Test oder ein Sicherheitssystem eine tatsächliche Bedrohung nicht erkennt.

Falsch-positiver Fehler – Ein Fehler, bei dem ein Test- oder Sicherheitssystem eine harmlose Situation fälschlicherweise als Bedrohung identifiziert.

File Integrity Monitoring (FIM) bzw. **Überwachung der Dateiintegrität** – Ein Verfahren zur Erkennung nicht autorisierter Änderungen an Dateien, um deren Integrität sicherzustellen.

Firewall – Ein Netzwerksicherheitsgerät, das den ein- und ausgehenden Netzwerkverkehr anhand von Sicherheitsregeln überwacht und kontrolliert.

Firewall-Regel – Eine spezifische Bedingung oder Richtlinie, die innerhalb einer Firewall festgelegt wird, um den Verkehrsfluss zu kontrollieren und Sicherheitsmaßnahmen durchzusetzen.

Firewall-Regelwerk – Ein Satz von Regeln und Richtlinien, die festlegen, wie der Netzwerkverkehr durch eine Firewall zugelassen oder blockiert werden soll.

Firmware – Software, die in Hardwaregeräte eingebettet ist, um Hardwarefunktionen zu steuern und zu verwalten.

Föderation – Die Verwendung gemeinsamer Protokolle und Standards, um Interoperabilität und Einmalanmeldung über verschiedene Systeme oder Organisationen hinweg zu ermöglichen.

Föderierte Identität – Der Prozess der Verknüpfung der digitalen Identität eines:einer Benutzer:in über mehrere Domänen oder Organisationen hinweg, um eine Einmalanmeldung und andere Identitätsverwaltungsdienste zu ermöglichen.

Föderierte Suche – Eine Suchmethode, die Daten aus mehreren, unterschiedlichen Quellen in einem einheitlichen Suchergebnis abruft.

Föderiertes Identitätsmanagement (FIM) – Ein System zur Verwaltung von Benutzeridentitäten über mehrere Domänen oder Organisationen hinweg mit einem einzigen Satz von Anmeldeinformationen.

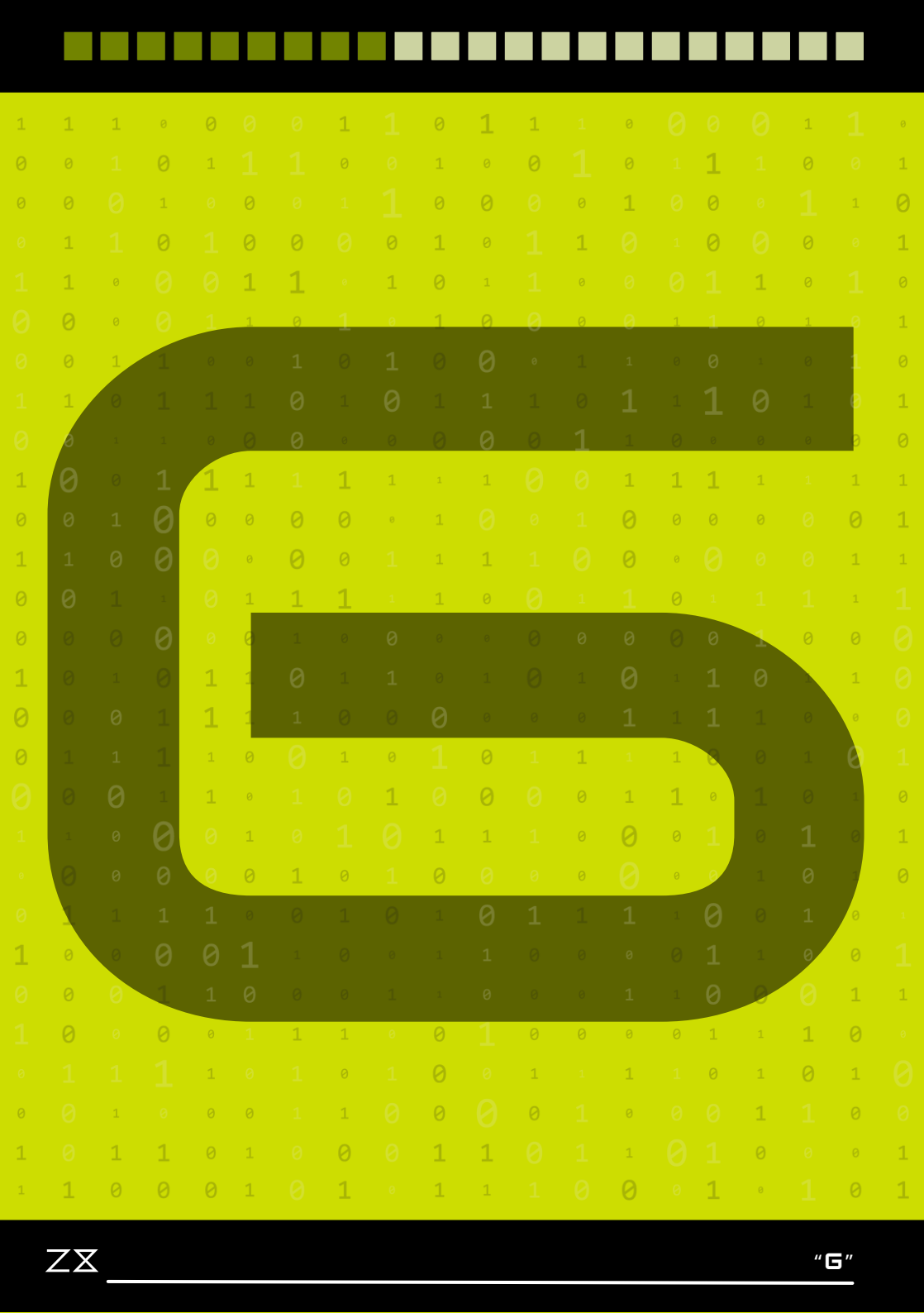
Forensik (Digitale Forensik) – Die Praxis des Sammelns, Bewahrens, Analysierens und Präsentierens digitaler Beweise für rechtliche Untersuchungen.

Forensische Analyse – Die detaillierte Prüfung und Untersuchung digitaler Daten, um Beweise für Cyberkriminalität oder andere Sicherheitsvorfälle zu finden.

Fuzz Testing – Eine Testtechnik, bei der zufällige Daten in ein Programm eingespeist werden, um Schwachstellen und Bugs zu entdecken.

Fuzzy Logic – Eine Form der mehrwertigen Logik, die sich mit annähernden Schlussfolgerungen befasst und bei bestimmten Arten von Sicherheitssystemen und der Erkennung von Anomalien nützlich ist.

Funktionale Sicherheit – Sicherheitsmaßnahmen, die die Funktionalität und Leistung eines Systems oder einer Anwendung schützen sollen.


ZX
"G"

Galois/Counter Mode (GCM) – Ein Betriebsmodus für kryptografische Blockchiffren mit symmetrischem Schlüssel, der sowohl Verschlüsselung als auch Nachrichtenauthentifizierung bietet und häufig in sicheren Kommunikationsprotokollen verwendet wird.

Gastisolation – Ein Sicherheitsmerkmal in Netzwerken, bei dem Gastbenutzer:innen vom internen Hauptnetzwerk isoliert werden, um unbefugten Zugriff auf sensible interne Ressourcen zu verhindern.

Gastzugang – Eine zeitlich begrenzte, eingeschränkte Form des Netzwerk- oder Systemzugriffs, die Benutzer:innen ohne reguläre Konten oder Anmeldedaten gewährt wird und häufig in Unternehmen oder öffentlichen Umgebungen verwendet wird, um einen sicheren Zugang für Besucher:innen zu gewährleisten.

Geführte Cybersicherheitssimulation – Eine Trainings- oder Lernaktivität, bei der die Teilnehmer:innen unter Anleitung simulierte Cybersicherheitsszenarien durchführen, um das Bewusstsein, die Fähigkeiten und die Reaktion auf reale Cybersicherheitsbedrohungen zu verbessern.

Geführter Penetrationstest – Eine kontrollierte Penetrationstest-Aktivität, bei der die Tester:innen ein gewisses Maß an Wissen oder Unterstützung von der getesteten Organisation erhalten, um gemeinsam Schwachstellen zu identifizieren.

Geführter Social-Engineering-Angriff – Eine Form des Social-Engineering-Angriffs, bei dem der:die Angreifer:in subtile Hinweise oder Anleitungen gibt, um das Ziel zu manipulieren, damit es vertrauliche Informationen preisgibt oder schädliche Handlungen vornimmt.

Gegenseitige Authentifizierung – Ein Sicherheitsverfahren, bei dem sich sowohl der:die Benutzer:in als auch das System gegenseitig authentifizieren, um sicherzustellen, dass beide Parteien legitimiert sind; wird häufig in der sicheren Kommunikation verwendet.

Geistiges Eigentum – Geistige Schöpfungen, für die Exklusivrechte gelten, darunter Daten und Software.

Geoblocking – Die Praxis, den Zugang zu Internetinhalten auf der Grundlage des geografischen Standorts von Nutzer:innen einzuschränken, was häufig zu Sicherheits-, Compliance- oder Lizenzierungszwecken erfolgt.

Geofencing - Eine Sicherheitstechnologie, die virtuelle Grenzen (Geofences) um einen physischen Standort schafft und Warnungen oder Aktionen ermöglicht, wenn Geräte den definierten Bereich betreten oder verlassen.

Geolokalisierung - Der Prozess der Bestimmung des physischen Standorts eines Geräts (z. B. eines Smartphones oder Laptops) auf der Grundlage von GPS, IP-Adresse oder anderen Methoden zur Standorterkennung, der häufig im Bereich der Cybersicherheit zur Erkennung anomaler Aktivitäten eingesetzt wird.

Golden-Ticket-Angriff - Ein ausgeklügelter Cyberangriff auf Kerberos-Authentifizierungssysteme, bei dem Angreifer:innen Authentifizierungstickets fälschen und damit praktisch uneingeschränkten Zugang zu Ressourcen innerhalb des angegriffenen Netzwerks erhalten.

Google Authenticator - Eine mobile App, die zeitbasierte Einmalpasswörter (time-based one-time passwords - TOTP) für die Zwei-Faktor-Authentifizierung (2FA) generiert, die üblicherweise zur Verbesserung der Kontosicherheit verwendet wird.

Governance, Risk, and Compliance (GRC) - Eine Strategie für die Verwaltung der gesamten Governance (Entscheidungsprozesse), des Risikomanagements (Identifizierung und Abschwächung von Risiken) und der Compliance (Einhaltung von Gesetzen, Vorschriften und internen Richtlinien) einer Organisation in Kontexten der Cybersicherheit und des Datenschutzes.

Granulare Zugriffskontrolle - Ein detaillierter und präziser Ansatz für die Zugriffskontrolle, der es Unternehmen ermöglicht, spezifische Benutzerprivilegien, Berechtigungen und Rollen zu definieren, um den Zugriff auf sensible Daten und Systeme zu beschränken.

Greenfield-Netzwerksicherheit - Bezieht sich auf Netzwerksicherheitspraktiken, die auf neue, frisch gebaute Netzwerke angewandt werden, bei denen Sicherheitsmaßnahmen von Grund auf ohne die Einschränkungen von Altsystemen entworfen und implementiert werden.

Grenzüberschreitender Datentransfer - Die Bewegung von Daten über internationale Grenzen hinweg, die die Einhaltung bestimmter Vorschriften erfordern kann.

Grey-Hat-Hacker:in - Ein:e Hacker:in oder Sicherheitsexpert:in, der:die sich zwischen ethischem (White Hat) und unethischem (Black Hat) Verhalten bewegt und oft Schwachstellen ohne böswillige Absicht, aber auch ohne volle Erlaubnis findet und ausnutzt.

Greylist (dt. „graue Liste“) – Ein Sicherheitsmechanismus, bei dem verdächtige E-Mail-Nachrichten oder IP-Adressen vorübergehend verzögert oder markiert werden, bis ihre Legitimität bestätigt werden kann; wird häufig bei der E-Mail-Filterung zur Bekämpfung von Spam eingesetzt.

Grundsätze der Datenverarbeitung – Grundprinzipien, die regeln, wie personenbezogene Daten verarbeitet werden sollten, darunter Rechtmäßigkeit, Fairness und Transparenz.

Grundschutz – Das Mindestmaß an Sicherheitsmaßnahmen und -praktiken, das erforderlich ist, um die Vermögenswerte und Daten eines Unternehmens vor bekannten Bedrohungen und Schwachstellen zu schützen.

Gruppenrichtlinienobjekt (Group Policy Object – GPO) – Eine Funktion in Microsoft Windows, mit der Administrator:innen Sicherheitseinstellungen, Benutzerrechte und Richtlinien für mehrere Computer und Benutzer:innen in einem Netzwerk verwalten und durchsetzen können.

GSM-Sicherheit (Global System for Mobile Communications Security) – Sicherheitsprotokolle und -mechanismen zum Schutz der über GSM-Netze übertragenen Kommunikation und Daten, darunter Verschlüsselung und Authentifizierung.

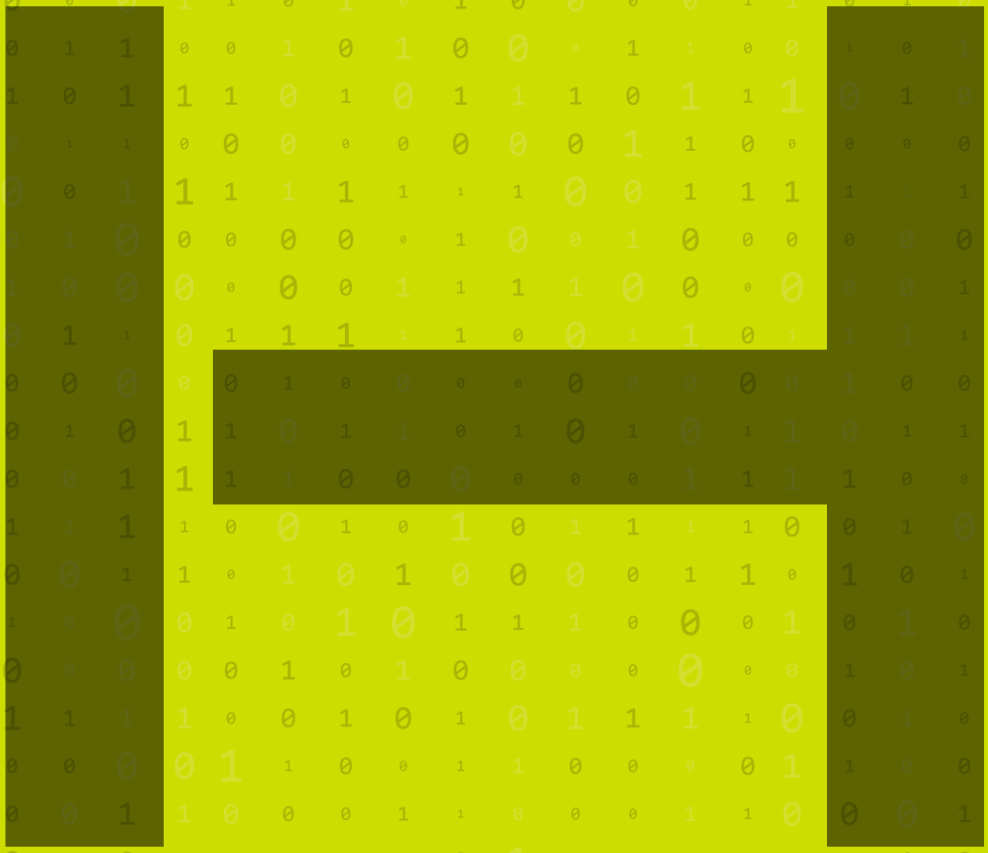
Guard Banding – Eine in der drahtlosen Sicherheit verwendete Methode, die einen Teil des Frequenzspektrums reserviert, um Interferenzen zwischen Kommunikationskanälen zu verhindern und so zu einer sichereren Kommunikationsumgebung beizutragen.

Guarded Fabric – Ein Sicherheitsmechanismus, der in Virtualisierungsumgebungen, insbesondere mit Hyper-V, eingesetzt wird, um sicherzustellen, dass virtuelle Maschinen (VMs) vor unbefugtem Zugriff und Manipulationen geschützt sind.

Guardrails – Sicherheitsrichtlinien, die in einer Organisation implementiert werden, um Handlungen zu verhindern, die zu Schwachstellen oder Sicherheitsverletzungen führen könnten, und so eine sichere Betriebsumgebung zu gewährleisten.

GUI-Sicherheit (Graphical User Interface) – Sicherheitsmechanismen, die sich auf die Absicherung der Benutzeroberflächen von Systemen und Anwendungen konzentrieren, um unbefugten Zugriff oder die Ausnutzung von Schwachstellen im Design oder in der Implementierung der Oberfläche zu verhindern.

Guideline on the Security Measures for Cloud Services (dt. „Leitfaden zu den Sicherheitsmaßnahmen für Cloud-Dienste“)- Eine Sammlung von Standards oder Empfehlungen, die die notwendigen Sicherheitsmaßnahmen für die Absicherung von Cloud-Computing-Diensten umreißen und darauf abzielen, sensible Daten zu schützen, die in Cloud-Umgebungen gespeichert oder verarbeitet werden.



Häufigkeitsanalyse – Die Untersuchung der Häufigkeit von Buchstaben oder Buchstabengruppen in einem Chiffretext, um die Verschlüsselung zu brechen.

Hype-Zyklus – Eine von Gartner entwickelte grafische Darstellung, die den Entwicklungsstand, die Akzeptanz und die gesellschaftliche Anwendung neuer Technologien verfolgt und im Bereich der Cybersicherheit häufig zur Bewertung der Entwicklung neuer Sicherheitstechnologien verwendet wird.

IAM (Identity and Access Management bzw. Identitäts- und Zugriffsmanagement) – Ein Rahmen von Richtlinien und Technologien zur Verwaltung und Sicherung des Zugriffs auf Unternehmensressourcen, um sicherzustellen, dass die richtigen Personen über die richtigen Zugriffsrechte verfügen.

ICANN (Internet Corporation for Assigned Names and Numbers) – Eine gemeinnützige Organisation, die für die Koordination der Wartung und der Verfahren verschiedener Datenbanken im Zusammenhang mit den Namensräumen des Internets zuständig ist.

ICS (Industrial Control System bzw. Industrielles Kontrollsystem) – Systeme, die zur Steuerung industrieller Prozesse wie Fertigung, Stromerzeugung und anderer Infrastrukturdienste verwendet werden. Die Sicherung von ICS ist ein wichtiger Aspekt der Cybersicherheit.

Identitätsdiebstahl – Eine Art von Betrug, bei dem ein:e Angreifer:in die persönlichen Daten einer anderen Person ohne deren Erlaubnis verwendet, oft um Straftaten zu begehen oder unberechtigte Einkäufe zu tätigen.

Indicator of Compromise (IoC) – Forensische Beweise, die darauf hindeuten, dass ein System kompromittiert wurde, z. B. ungewöhnliche Anmeldemuster oder das Vorhandensein von Malware.

Information Assurance (IA) – Die Praxis der Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, insbesondere im staatlichen und militärischen Kontext.

Inhaltsfilterung – Die Praxis des Blockierens oder Erlaubens des Zugriffs auf bestimmte Arten von Inhalten in einem Netzwerk oder System, um Benutzer:innen vor schädlichem oder unangemessenem Material zu schützen.

Informationslebenszyklusmanagement (ILM) – Strategien und Verfahren zur Verwaltung von Informationen während ihres gesamten Lebenszyklus, von der Erstellung bis zur Entsorgung.

Informationssicherheit (InfoSec) – Die Praxis des Schutzes von Informationen durch Abschwächung von Risiken und Schwachstellen in Systemen, Software und Prozessen.

Informationssicherheitsmanagementsystem (ISMS) – Ein systematischer Ansatz zur Verwaltung sensibler Informationen, um deren Sicherheit zu gewährleisten.

Infrarot-Angriffserkennungssystem – Ein physisches Sicherheitsgerät, das Infrarottechnologie verwendet, um unbefugten physischen Zugriff oder Bewegung in gesperrten Bereichen zu erkennen.

Infrastructure as Code (IaC) – Die Verwaltung der IT-Infrastruktur durch Code und Automatisierung, die konsistente und sichere Konfigurationen für Cloud- und Vor-Ort-Ressourcen gewährleistet.

Injektionsangriff – Eine Art von Cyberangriff, bei dem schädlicher Code in ein Programm oder eine Abfrage eingefügt wird, z. B. SQL-Injektion oder Command Injection, wodurch unbefugter Zugriff oder Manipulation von Daten ermöglicht wird.

Insider-Bedrohung – Ein Sicherheitsrisiko, das von Einzelpersonen innerhalb einer Organisation ausgeht, z. B. von Mitarbeiter:innen oder Auftragnehmer:innen, die Zugang zu wichtigen Systemen und Daten haben.

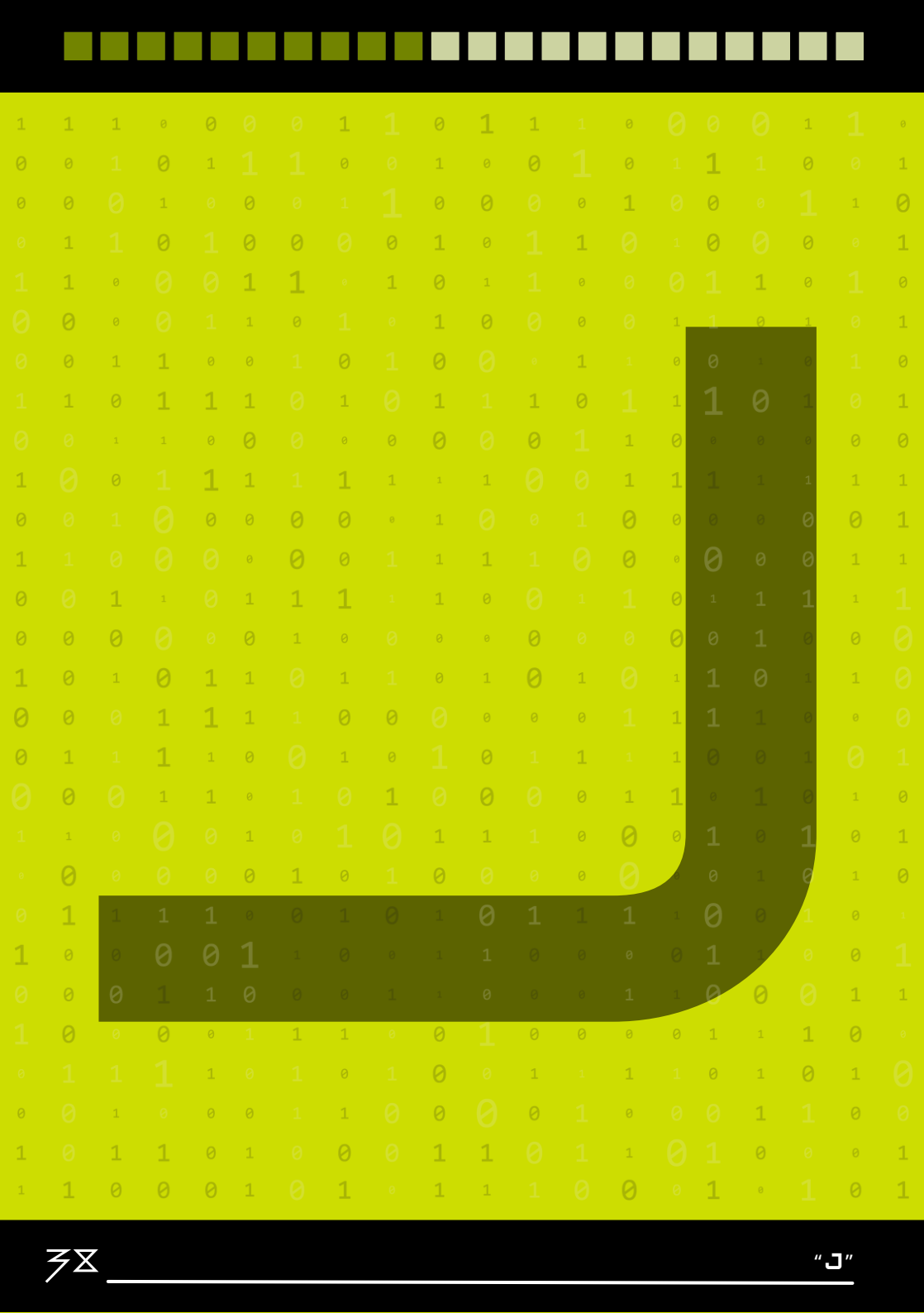
Integrität – Ein Schlüsselprinzip der Cybersicherheit, das gewährleistet, dass Daten sowohl in gespeichertem Zustand als auch bei der Übertragung korrekt, vollständig und unverändert bleiben.

Internet – Das komplexe Netz von Informationen und Konnektivität, das es Ihnen ermöglicht, dieses Glossar zu lesen, Katzen- und Hundevideos anzuschauen oder an einem verregneten Sonntagmorgen Ihre heiße Schokolade mit Karte zu bezahlen.

IoT-Sicherheit (Internet of Things – Internet der Dinge) – Die Praxis der Sicherung der riesigen Anzahl von mit dem Internet verbundenen Geräten, die das IoT bilden, um sicherzustellen, dass sie vor Hackerangriffen, Datenschutzverletzungen und unbefugtem Zugriff geschützt sind.

Intrusion Detection System (IDS) bzw. **Angriffserkennungssystem** – Ein Gerät oder eine Softwareanwendung, die Netzwerk- oder Systemaktivitäten auf schädliche Aktionen oder Richtlinienverstöße überwacht.

Intrusion Prevention System (IPS) – Ähnlich wie IDS, jedoch mit der Fähigkeit, erkannte Bedrohungen aktiv zu blockieren oder zu verhindern.

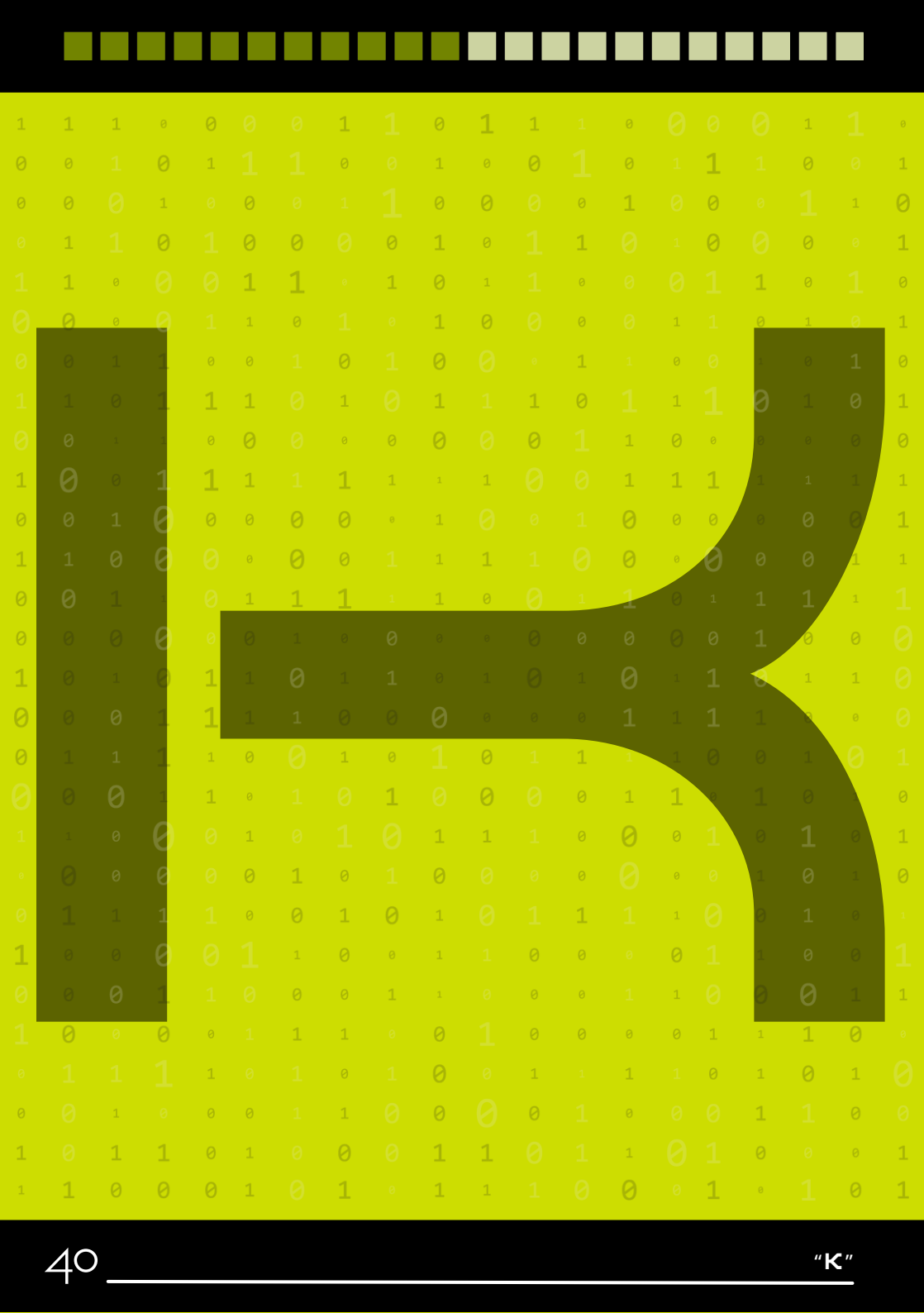


Jailbreak - Der Prozess des Entfernens von Softwarebeschränkungen, die vom Hersteller auf Geräten wie Smartphones auferlegt wurden, was das Gerät oft Sicherheitsrisiken aussetzt.

JavaScript-Injektion - Eine Art von Injektionsangriff, bei dem schädlicher JavaScript-Code auf einer Website eingeschleust wird, der häufig bei Cross-Site-Scripting-Angriffen (XSS) verwendet wird.

Jitter - Ein Netzwerkleistungsproblem, bei dem Datenpakete unterschiedliche Verzögerungen erfahren, was die Qualität von VoIP- oder Videokonferenzdiensten beeinträchtigen kann.

Just-In-Time-(JIT-)Zugriff - Ein Sicherheitskonzept, das Benutzer:innen einen zeitlich begrenzten und eingeschränkten Zugriff auf kritische Systeme oder Daten ermöglicht und sicherstellt, dass sie genau genug Zeit haben, eine Aufgabe zu erledigen, bevor der Zugriff widerrufen wird.



Key Derivation Function (KDF) bzw. **Schlüsselableitung** – Eine kryptografische Funktion, die zur Ableitung von Schlüsseln aus einem Basiswert verwendet wird und häufig beim Passwort-Hashing und der Verschlüsselung zum Einsatz kommt.

Key-Escrow – Ein System, bei dem kryptografische Schlüssel treuhänderisch verwahrt werden, häufig von einer dritten Partei, um den Zugriff in Notfällen oder aufgrund gesetzlicher Bestimmungen zu ermöglichen.

Key Management Interoperability Protocol (KMIP) – Ein standardisiertes Protokoll, das zur Verwaltung von Verschlüsselungsschlüsseln in verschiedenen Systemen und Umgebungen verwendet wird, um die Sicherheit und Compliance zu verbessern.

Keystroke Encryption – Eine Methode zur Verschlüsselung von Tastenanschlägen zwischen der Tastatur und der Anwendung, um Keylogging-Angriffe zu verhindern.

Kill Process Attack – Ein Angriff, bei dem bösartiger Code kritische Prozesse oder Anwendungen zum Beenden zwingt, was häufig zu Systemabstürzen oder Sicherheitslücken führt.

Klartext – Daten, die lesbar und nicht verschlüsselt sind, wodurch sie bei unsicherer Übertragung anfällig für ein Abfangen oder unbefugten Zugriff sind.

Knowledge Discovery in Databases (KDD) bzw. **Wissensentdeckung in Datenbanken** – Der Prozess der Entdeckung nützlicher Informationen und Muster aus großen Datenbeständen, der häufig bei Sicherheitsanalysen zur Identifizierung potenzieller Bedrohungen eingesetzt wird.

Known-Plaintext-Angriff (KPA) – Eine Kryptoanalysetechnik, bei der der:die Angreifer:in sowohl auf den Klartext als auch auf den dazugehörigen Chiffretext zugreifen kann und diese Informationen nutzt, um die Verschlüsselungsmethode aufzudecken.

Konfigurationsverwaltung – Der Prozess der Verwaltung und Instandhaltung von Systemeinstellungen und -konfigurationen, um Sicherheit und Compliance zu gewährleisten.

Kontinuierliche Überwachung – Der laufende Prozess der Bewertung und Analyse von Sicherheitsereignissen und Schwachstellen, um Bedrohungen in Echtzeit zu erkennen und darauf zu reagieren.

Kontrollierter Zugang – Die Praxis, den Zugriff auf Systeme, Daten oder Ressourcen auf autorisierte Personen oder Einheiten zu beschränken.

Krack-Angriff – Eine Schwachstelle im WPA2-Wi-Fi-Verschlüsselungsprotokoll, die es Angreifer:innen ermöglicht, den Datenverkehr zwischen Geräten und drahtlosen Netzwerken abzufangen und zu manipulieren.

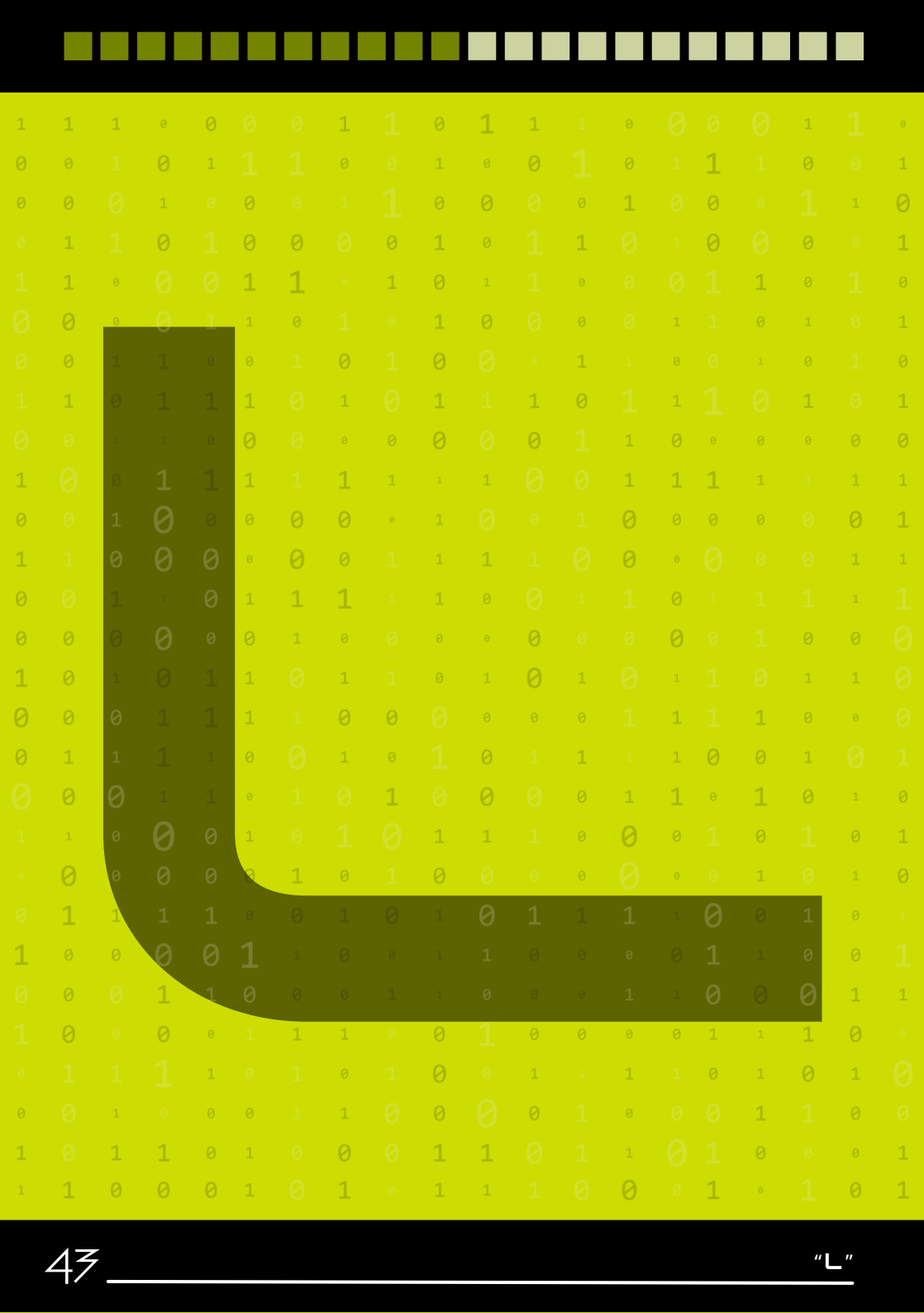
Kritische Daten – Informationen, die für den Betrieb einer Organisation wichtig sind und aufgrund ihrer Sensibilität einen erhöhten Schutz erfordern.

Kritische Infrastrukturen – Die wesentlichen Systeme und Anlagen, die für den Betrieb einer Organisation unerlässlich sind und deren Unterbrechung erhebliche Folgen haben könnte.

Kryptographischer Schlüssel – Eine Informationseinheit, die in kryptographischen Algorithmen zur Verschlüsselung oder Entschlüsselung von Daten verwendet wird.

Kryptographie – Die Verwendung mathematischer Algorithmen zum Ver- und Entschlüsseln von Daten, um deren Vertraulichkeit und Integrität zu gewährleisten.

Künstliche Intelligenz (KI oder AI) im Bereich Sicherheit – Der Einsatz von KI-Technologien zur Verbesserung von Sicherheitsmaßnahmen, z. B. zur Erkennung von Bedrohungen, Risikobewertung und Vorfallsreaktion.



LAN (Local Area Network) – Ein Netzwerk, das Computer innerhalb eines begrenzten Bereichs, z. B. zu Hause, in der Schule oder im Büro, miteinander verbindet und häufig durch Firewalls und Verschlüsselung gesichert ist.

LDAP (Lightweight Directory Access Protocol) – Ein Protokoll, das für den Zugriff und die Verwaltung von Verzeichnisinformationsdiensten über ein IP-Netzwerk verwendet wird und häufig in zentralisierten Authentifizierungs- und Autorisierungssystemen zum Einsatz kommt.

Letterbomb – Eine Art von E-Mail oder nachrichtenbasiertem Angriff, der schädlichen Code enthält, der Schwachstellen ausnutzen soll, wenn er von Empfänger:innen geöffnet wird.

Library Injection – Eine Methode, bei der schädlicher Code in die Softwarebibliothek eines Programms eingefügt wird, um dessen normales Verhalten zu verändern oder unbefugten Zugriff auf Systemressourcen zu erhalten.

Linux Security Modules (LSM) – Ein Framework im Linux-Betriebssystem, das die Durchsetzung von obligatorischen Zugriffskontrollen ermöglicht und es Administrator:innen erlaubt, Sicherheitsrichtlinien zu definieren und umzusetzen.

Log Aggregation – Der Prozess des Sammelns und Zentralisierens von Logdaten aus verschiedenen Systemen und Anwendungen an einem einzigen Ort zur Sicherheitsanalyse und -überwachung.

Log Management – Die Aufzeichnung, Speicherung und Analyse von Protokollen, die von Software-, Hardware- und Netzwerkgeräten zur Fehlerbehebung und zu Sicherheitszwecken erstellt werden.

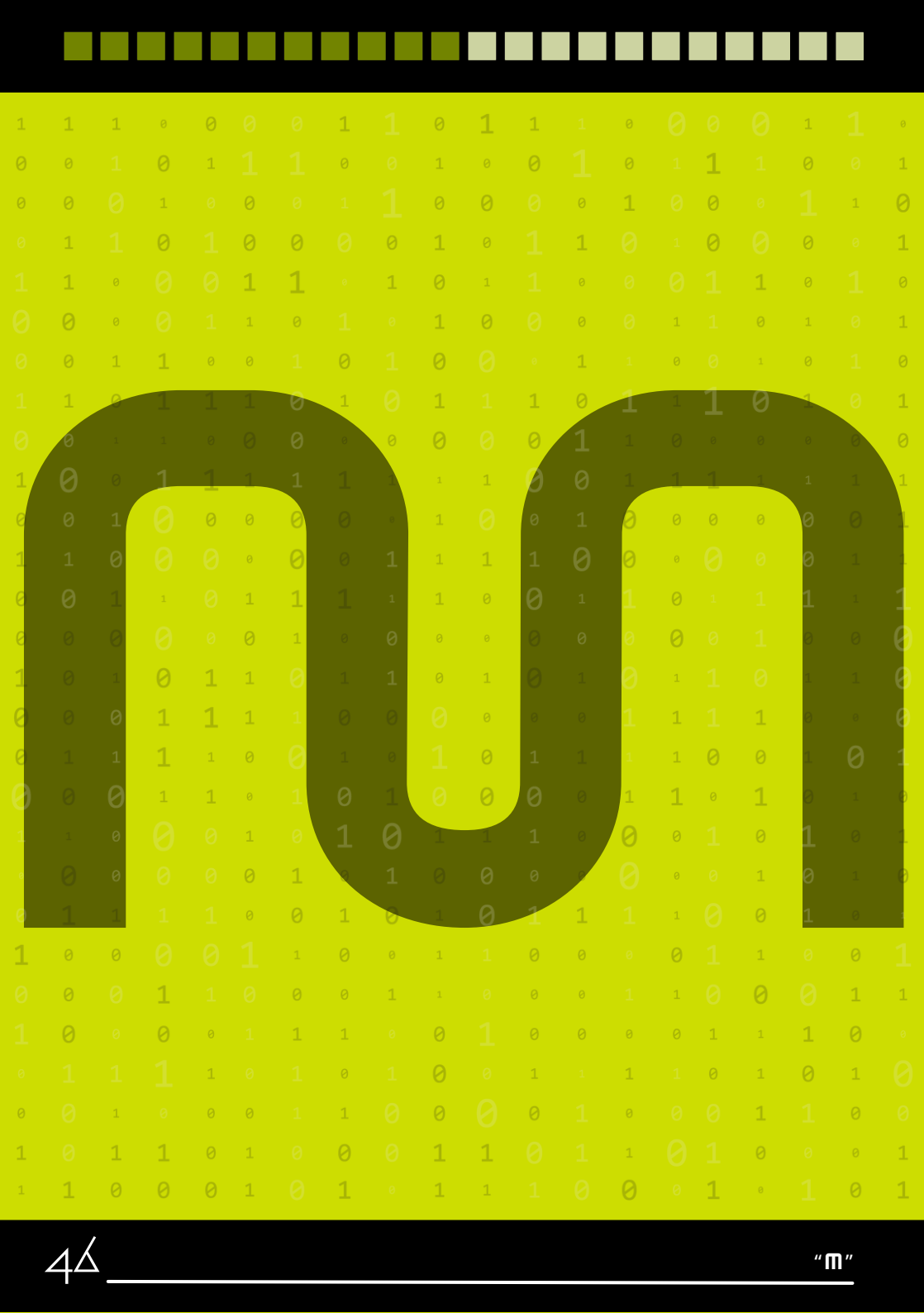
Log Retention Policy – Eine Reihe von Richtlinien, die festlegen, wie lange Protokolldaten aufbewahrt werden sollen, bevor sie archiviert oder gelöscht werden.

Logische Zugriffskontrolle – Sicherheitsmechanismen, die den Zugriff auf Daten oder Ressourcen auf der Grundlage vordefinierter Regeln einschränken und typischerweise durch Authentifizierungs- und Autorisierungssysteme verwaltet werden.

Logikbombe – Ein schädliches Programm oder ein schädlicher Code, der in einem System schlummert, bis er unter spezifischen Bedingungen aktiviert wird und Schaden anrichtet.

Long-Term Persistence Attack – Eine Art von Cyberangriff, bei dem ein:e Angreifer:in über einen längeren Zeitraum hinweg unbemerkt Zugang zu einem System erhält und so Informationen sammeln oder weitere Angriffe durchführen kann.

Lua-basierte Sicherheit – Sicherheitsmaßnahmen und -kontrollen, die unter Verwendung der Skriptsprache Lua implementiert werden und häufig in eingebetteten Systemen und Spielen für Sicherheitsfunktionen wie die Skriptauthentifizierung verwendet werden.



MAC (Mandatory Access Control) – Eine Art der Zugangskontrolle, bei der der Zugang zu Ressourcen auf der Grundlage von Richtlinien gewährt wird, die von einer zentralen Behörde festgelegt werden, in der Regel in hochsicheren Umgebungen.

MAC Adresse (Media-Access-Control-Adresse) – Eine eindeutige Kennung, die Netzwerkschnittstellen für die Kommunikation auf der Datenübertragungsschicht eines Netzwerks zugewiesen wird und häufig zur Geräteidentifizierung und Netzwerksicherheit verwendet wird.

Malicious Code (dt. „schädlicher Code“) – Jeglicher Code oder jegliche Software, die darauf abzielt, ein System zu schädigen, auszunutzen oder anderweitig zu kompromittieren, darunter Viren, Würmer, Trojaner, Ransomware und Spyware.

Malware (Malicious Software) – Ein Begriff, der sich auf Software bezieht, die speziell entwickelt wurde, um ein System oder Netzwerk zu stören, zu beschädigen oder sich unbefugten Zugang zu verschaffen.

Man-in-the-Middle-Angriff (MITM) – Ein Angriff, bei dem ein:e böswillige:r Akteur:in die Kommunikation zwischen zwei Parteien ohne deren Wissen abfängt und potenziell verändert, oft mit dem Ziel des Diebstahls sensibler Daten.

Manipulationserkennung – Eine Sicherheitsfunktion, die unbefugte Änderungen oder Manipulationsversuche an Systemen oder Daten identifiziert und oft einen Alarm auslöst, wenn eine Manipulation festgestellt wird.

Manuelle Penetrationstests – Der Prozess des manuellen Testens eines Systems oder Netzwerks auf Schwachstellen, indem reale Angriffsszenarien simuliert werden, im Gegensatz zur Verwendung automatisierter Tools.

Maschinelles Lernen – ine Art der künstlichen Intelligenz, die es Systemen ermöglicht, aus Daten zu lernen und Entscheidungen zu treffen, ohne explizit programmiert zu werden.

Master-Boot-Record-(MBR-)Virus – Ein Virustyp, der den Master Boot Record einer Festplatte infiziert, sodass er vor dem Start des Betriebssystems geladen wird und schwer aufzuspüren ist.

MD5 (Message Digest Algorithm 5) – Eine weit verbreitete kryptografische Hash-Funktion, die einen 128-Bit-Hashwert erzeugt. Sie wird häufig zur Überprüfung der Datenintegrität verwendet, gilt aber wegen der Anfälligkeit für Kollisionsangriffe nicht mehr als sicher.

Meldung einer Datenschutzverletzung bzw. **Data Breach Notification** – Die Verpflichtung, die betroffenen Personen und die zuständigen Behörden zu informieren, wenn es zu einer Datenschutzverletzung kommt, die häufig durch Vorschriften wie die DSGVO geregelt wird.

Meldung einer Sicherheitsverletzung bzw. **Breach Notification –** Der durch Vorschriften und Gesetze vorgeschriebene Prozess der Benachrichtigung betroffener Personen und relevanter Behörden über eine Datenschutzverletzung.

Message Integrity – Ein Sicherheitskonzept, das sicherstellt, dass eine Nachricht oder Daten während der Übertragung nicht verändert wurden, normalerweise erreicht durch Hashing oder digitale Signaturen.

Metadaten – Daten, die Informationen über andere Daten liefern, wie z. B. die Dateigröße oder das Erstellungsdatum.

Metadatensicherheit – Der Schutz von Metadaten (Daten über Daten), die sensible Informationen über Systeme, Dateien oder Kommunikation preisgeben könnten, selbst wenn die zugrunde liegenden Daten verschlüsselt sind.

Mitigation – Der Prozess der Verringerung des Schweregrads, der Auswirkungen oder der Wahrscheinlichkeit einer Bedrohung oder Schwachstelle der Cybersicherheit durch verschiedene Sicherheitsmaßnahmen.

Mobile-Device-Management (MDM) – Eine Softwarelösung, die von Unternehmen verwendet wird, um mobile Geräte wie Smartphones und Tablets zu verwalten, zu überwachen und zu sichern und die Einhaltung von Sicherheitsrichtlinien zu gewährleisten.

Multi-Faktor-Authentifizierung (MFA) – Ein Sicherheitsprozess, bei dem Benutzer:innen zwei oder mehr Verifizierungsfaktoren angeben müssen, um Zugang zu einem System zu erhalten, was eine zusätzliche Sicherheitsebene über Passwörter hinaus darstellt.

NAC (Network Access Control – Netzwerkzugangskontrolle) – Eine Sicherheitslösung, die den Zugriff nicht autorisierter Geräte auf ein Netzwerk durch die Durchsetzung von Sicherheitsrichtlinien und Konformitätsprüfungen einschränkt.

Nachkonstruktion bzw. **Reverse Engineering** – Der Prozess der Analyse von Software oder Hardware, um ihr Design, ihre Architektur oder ihren Quellcode zu entdecken, oft im Rahmen der Schwachstellenforschung oder der Malware-Analyse eingesetzt.

Nachweisbarkeit – Ein Sicherheitskonzept, das die Authentizität und Integrität der Kommunikation sicherstellt und es dem:der Absender:in unmöglich macht, zu leugnen, dass er eine Nachricht oder Transaktion gesendet hat.

National Institute of Standards and Technology (NIST) – Eine US-Bundesbehörde, die Standards entwickelt und fördert, darunter auch Rahmenwerke für die Cybersicherheit, um die Datensicherheit zu gewährleisten und kritische Infrastrukturen zu schützen.

Network Intrusion Detection System (NIDS) – Ein System, das den Netzwerkverkehr auf verdächtige Aktivitäten und potenzielle Bedrohungen überwacht und in der Regel an strategischen Punkten innerhalb eines Netzwerks eingesetzt wird.

Network Intrusion Prevention System (NIPS) – Ein System, das potenzielle Bedrohungen erkennt und verhindert, indem es den Netzwerkverkehr überwacht und schädliche Aktivitäten blockiert, bevor sie dem System schaden können.

Netzhautscan – Eine biometrische Sicherheitsmaßnahme, die einzigartige Muster in der Netzhaut einer Person zur Identifizierung und Authentifizierung verwendet.

Netzknoten – Ein Netzwerkgerät oder -punkt, an dem Daten verarbeitet oder übertragen werden, wie z. B. ein Computer, Router oder Switch innerhalb einer Netzwerkinfrastruktur.

Netzwerkadressübersetzung (Network Address Translation – NAT) – Eine Technik, die in Netzwerken verwendet wird, um private IP-Adressen innerhalb eines lokalen Netzwerks in eine öffentliche IP-Adresse zu übersetzen, damit mehrere Geräte eine einzige IP-Adresse gemeinsam nutzen können.

Netzwerk-Forensik – Der Prozess der Erfassung, Aufzeichnung und Analyse des Netzwerkverkehrs, um netzwerkbasierte Sicherheitsvorfälle oder Straftaten zu untersuchen und zu verstehen.

Netzwerk-Mapping – Der Prozess der Erkennung und Visualisierung des Layouts eines Netzwerks, darunter Geräte, Verbindungen und Konfigurationen, der häufig für Sicherheitsbewertungen und -management verwendet wird.

Netzwerkrichtlinie – Regeln und Richtlinien, die die Verwaltung, Konfiguration und Sicherheit von Netzwerkressourcen regeln, darunter Zugriffskontrollen und Nutzungsrichtlinien.

Netzwerk-Schwachstellen-Scanner – Ein Tool, mit dem Netzwerke auf bekannte Schwachstellen und Sicherheitslücken gescannt werden, um potenzielle Risiken zu erkennen und zu beseitigen, bevor sie ausgenutzt werden können.

Netzwerksegmentierung – Die Praxis der Aufteilung eines Computernetzwerks in kleinere, isolierte Teilnetzwerke, um die Angriffsfläche zu verringern und Angreifer:innen daran zu hindern, sich seitlich im Netzwerk zu bewegen.

Netzwerksicherheit – Die Maßnahmen und Praktiken zum Schutz eines Netzwerks vor unbefugtem Zugriff, Angriffen und Missbrauch, darunter die Verwendung von Firewalls, Angriffserkennungssystemen und Verschlüsselung.

Netzwerkverkehrsanalyse – Der Prozess der Untersuchung von Daten, die sich durch ein Netzwerk bewegen, um die Leistung zu überwachen, Anomalien zu erkennen und potenzielle Sicherheitsbedrohungen zu identifizieren.

Nicht vertrauenswürdiges Netzwerk – Ein Netzwerk, das nicht von der Organisation kontrolliert wird und als unsicher gilt, wie z. B. öffentliches WLAN, bei dem die Kommunikation durch Abhören oder Angriffe gefährdet sein kann.

Nonce – Ein zufälliger oder eindeutiger Wert, der in der kryptografischen Kommunikation verwendet wird, um sicherzustellen, dass alte Mitteilungen nicht für Replay-Angriffe wiederverwendet werden können.

Non-Compliance bzw. **Nichtkonformität** – Versagen bei der Einhaltung von Datenschutzgesetzen und -vorschriften.

Node Authentication - Der Prozess der Überprüfung der Identität eines Netzknotens (z. B. eines Geräts oder Systems) innerhalb eines Netzes, um sicherzustellen, dass er zum Zugriff auf oder zur Kommunikation mit anderen Knoten berechtigt ist.

Normalisierung - Der Prozess der Standardisierung von Daten auf ein gemeinsames Format zur Verbesserung der Konsistenz, Nutzbarkeit und Analyse, der häufig in der Datenbankverwaltung und Datenverarbeitung verwendet wird.

NoSQL-Datenbank - Eine Art von Datenbank, die einen Mechanismus für die Speicherung und den Abruf von Daten bietet, die auf andere Weise modelliert sind als die in SQL-Datenbanken verwendeten tabellarischen Beziehungen, und die häufig für die Verarbeitung großer Mengen unstrukturierter Daten verwendet wird.

Null-Chiffre - Eine Methode zum Verbergen von Nachrichten innerhalb eines Blocks nicht geheimer Informationen, bei der die Nachricht mithilfe eines vorgegebenen Musters oder Schlüssels extrahiert wird.

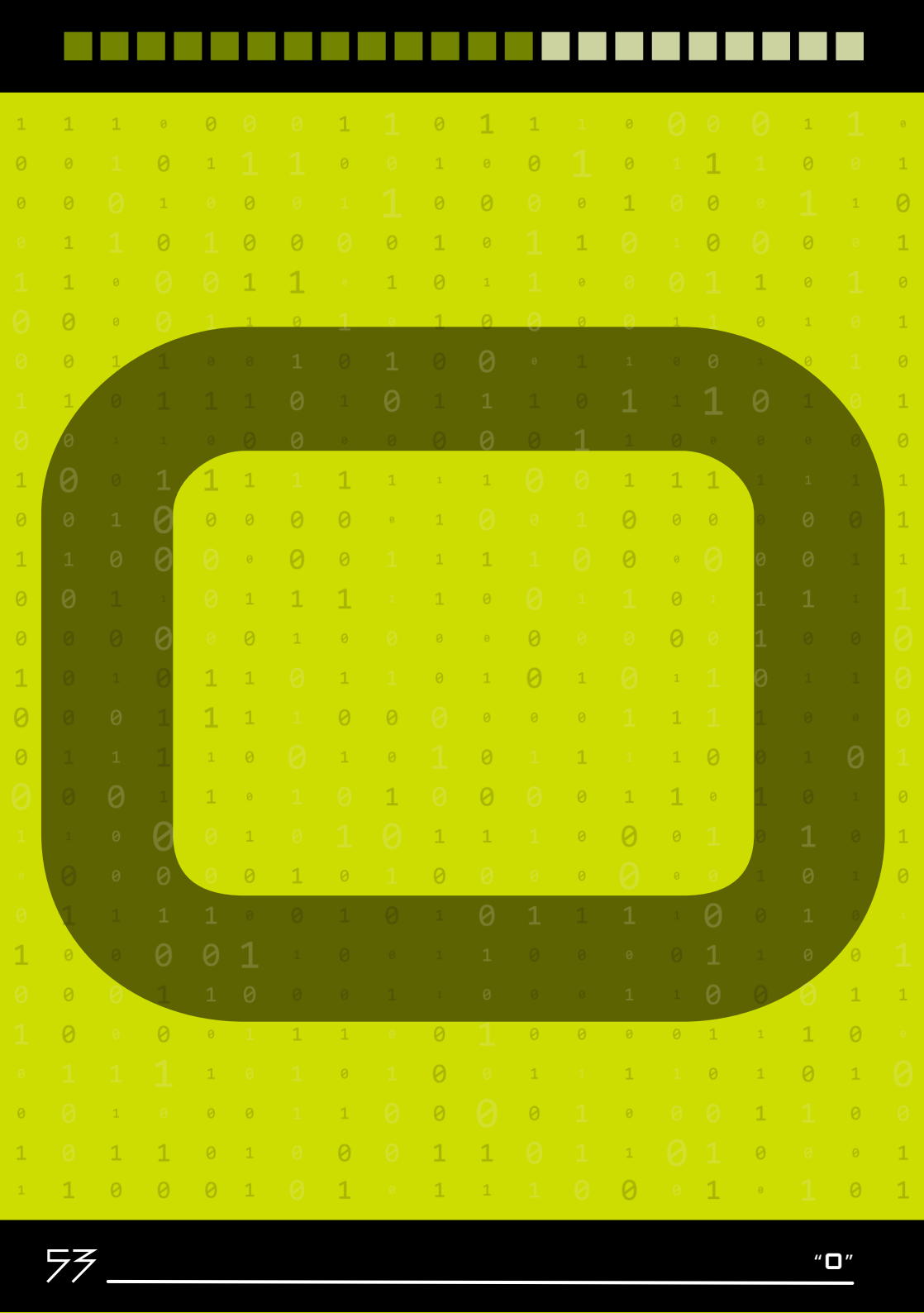
Null-Verschlüsselung - Ein Begriff, der sich auf eine Verschlüsselung bezieht, die effektiv nicht existiert, oft aufgrund von schwachen oder defekten Verschlüsselungsalgorithmen, die keinen angemessenen Schutz bieten.

Null Session - Eine nicht autorisierte Verbindung zu einem Windows-System, die es Angreifer:innen ermöglichen kann, Freigaben, Benutzer:innen und andere vertrauliche Informationen zu erfassen.

Nullification - Der Prozess, bei dem Daten oder eine Sicherheitsfunktion unwirksam gemacht werden, häufig im Zusammenhang mit Sicherheitsumgehungsangriffen oder dem Entzug des Zugriffs verwendet.

Nutzungsbedingungen - Rechtliche Vereinbarungen, in denen die Regeln und Bedingungen für die Nutzung eines Dienstes oder Produkts festgelegt sind.

NVRAM (Non-Volatile Random Access Memory)-Sicherheit - Sicherheitsmechanismen, die auf NVRAM-Speicher angewendet werden, um kritische Konfigurationsdaten vor Manipulationen oder unbefugtem Zugriff zu schützen.



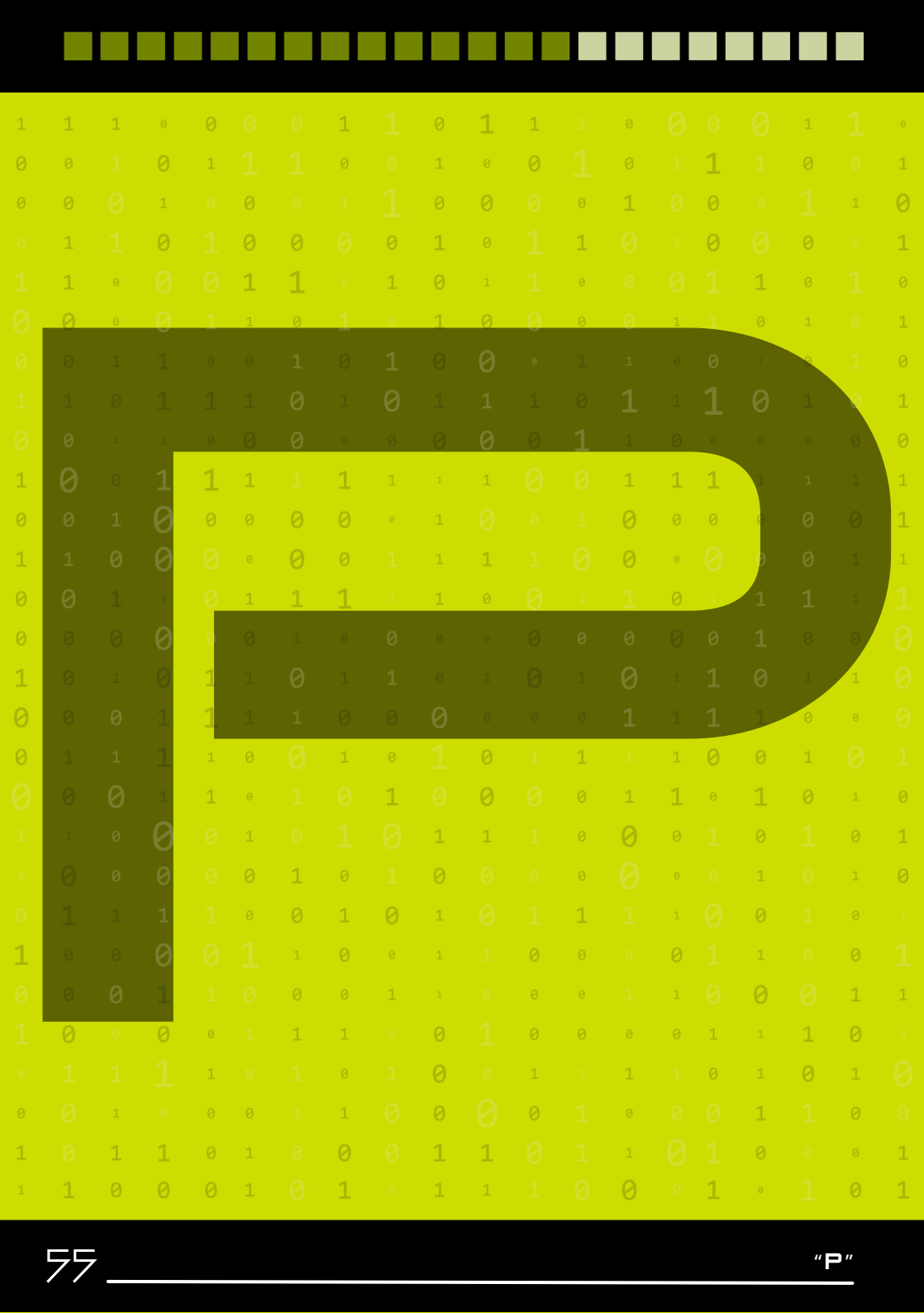
OAuth (Open Authorization) – Ein offener Standard für die tokenbasierte Authentifizierung und Autorisierung im Internet, der häufig verwendet wird, um Anwendungen von Drittanbietern den Zugriff auf Benutzerinformationen zu ermöglichen, ohne Passwörter preiszugeben.

Offensive Sicherheit – Ein Zweig der Cybersicherheit, der sich auf die Simulation von Angriffen konzentriert, um Schwachstellen zu identifizieren und die Verteidigungsposition eines Systems oder Netzwerks zu verbessern.

One-Time-Pad (OTP) – Eine theoretisch unknackbare Verschlüsselungsmethode, bei der ein zufälliger Schlüssel, der nur einmal verwendet wird, mit dem Klartext kombiniert wird, um den Chiffretext zu erzeugen.

Open Source Intelligence (OSINT) – Das Sammeln und Analysieren öffentlich zugänglicher Daten aus offenen Quellen (z. B. soziale Medien, Behördendaten und Websites) zu Zwecken der Cybersicherheit und Bedrohungsanalyse.

Over-The-Air (OTA)-Update-Sicherheit – Sicherheitsmaßnahmen zum Schutz von Software-Updates, die drahtlos an Geräte wie Smartphones und IoT-Geräte übertragen werden, um sicherzustellen, dass die Updates authentisch sind und nicht manipuliert wurden.



Paketfilter – Eine Firewall-Technik, die die Kopfzeilen von Datenpaketen untersucht und sie auf der Grundlage vordefinierter Regeln, wie Quell- und Ziel-IP-Adressen, zulässt oder blockiert.

Passwortknacken – Der Prozess des Herausfindens von Passwörtern aus Daten, die in einem Computersystem gespeichert sind oder von diesem übertragen werden, in der Regel durch Methoden wie Brute-Force- oder Wörterbuchangriffe.

Passwortrichtlinie – Eine Reihe von Regeln, die von einer Organisation festgelegt werden, um die Sicherheit zu erhöhen, indem Anforderungen für die Erstellung und Verwaltung sicherer Passwörter definiert werden.

Patch-Management – Der Prozess der Verwaltung von Software-Updates und Patches, der sicherstellt, dass Schwachstellen behoben werden, um die Systemsicherheit zu gewährleisten.

Penetrationstests (Pentest) – Eine Sicherheitstestmethode, bei der ethische Hacker:innen Angriffe auf ein System simulieren, um Schwachstellen zu identifizieren und auszunutzen und so Erkenntnisse für Abhilfemaßnahmen zu gewinnen.

Personenbezogene Daten – Jegliche Informationen, die zur Identifizierung einer Person verwendet werden können, wie z. B. Namen, Sozialversicherungsnummern und (Mail-)Adressen, die häufig Ziel von Datenschutzverletzungen sind und gemäß den Datenschutzrichtlinien geschützt werden müssen.

Pflichten der Datenverantwortlichen – Verantwortlichkeiten von Organisationen, die die Zwecke und Mittel der Datenverarbeitung festlegen.

Pflichten von Datenverarbeiter:innen – Verantwortlichkeiten von Organisationen, die Daten im Auftrag der Datenverantwortlichen verarbeiten.

Pharming – Eine Cyberangriffstechnik, bei der der Datenverkehr von einer legitimen Website auf eine betrügerische umgeleitet wird, um sensible Informationen zu stehlen, häufig durch DNS-Poisoning.

Phishing – Ein Social-Engineering-Angriff, bei dem sich Angreifer:innen als vertrauenswürdige Personen ausgeben, um Personen zur Preisgabe vertraulicher Informationen wie Passwörter oder Finanzdaten zu verleiten.

Pirate Box – Ein Gerät, das für den Austausch von Dateien und Daten über ein lokales Netzwerk ohne Internetverbindung verwendet wird und oft anonym konzipiert ist.

Platform as a Service (PaaS) – Ein Cloud-Computing-Modell, bei dem ein Drittanbieter Hardware- und Software-Tools über das Internet bereitstellt, sodass Benutzer:innen Anwendungen entwickeln, ausführen und verwalten können, ohne die zugrunde liegende Infrastruktur aufbauen und warten zu müssen.

Port-Scanning – Eine Methode, die von Angreifer:innen verwendet wird, um offene Ports in einem System zu entdecken, die potenzielle Einstiegspunkte für Angriffe darstellen können.

Profiling – Die automatisierte Verarbeitung personenbezogener Daten, um bestimmte Aspekte des Verhaltens oder der Eigenschaften einer Person zu bewerten.

Pseudonymisierung – Der Prozess, bei dem identifizierbare Informationen durch Pseudonyme ersetzt werden, um individuelle Identitäten zu schützen.

Public-Key-Infrastruktur (PKI) – Ein Rahmen für die Verwaltung digitaler Zertifikate und Public-Key-Verschlüsselung zur Sicherung der Kommunikation und Authentifizierung von Benutzer:innen.

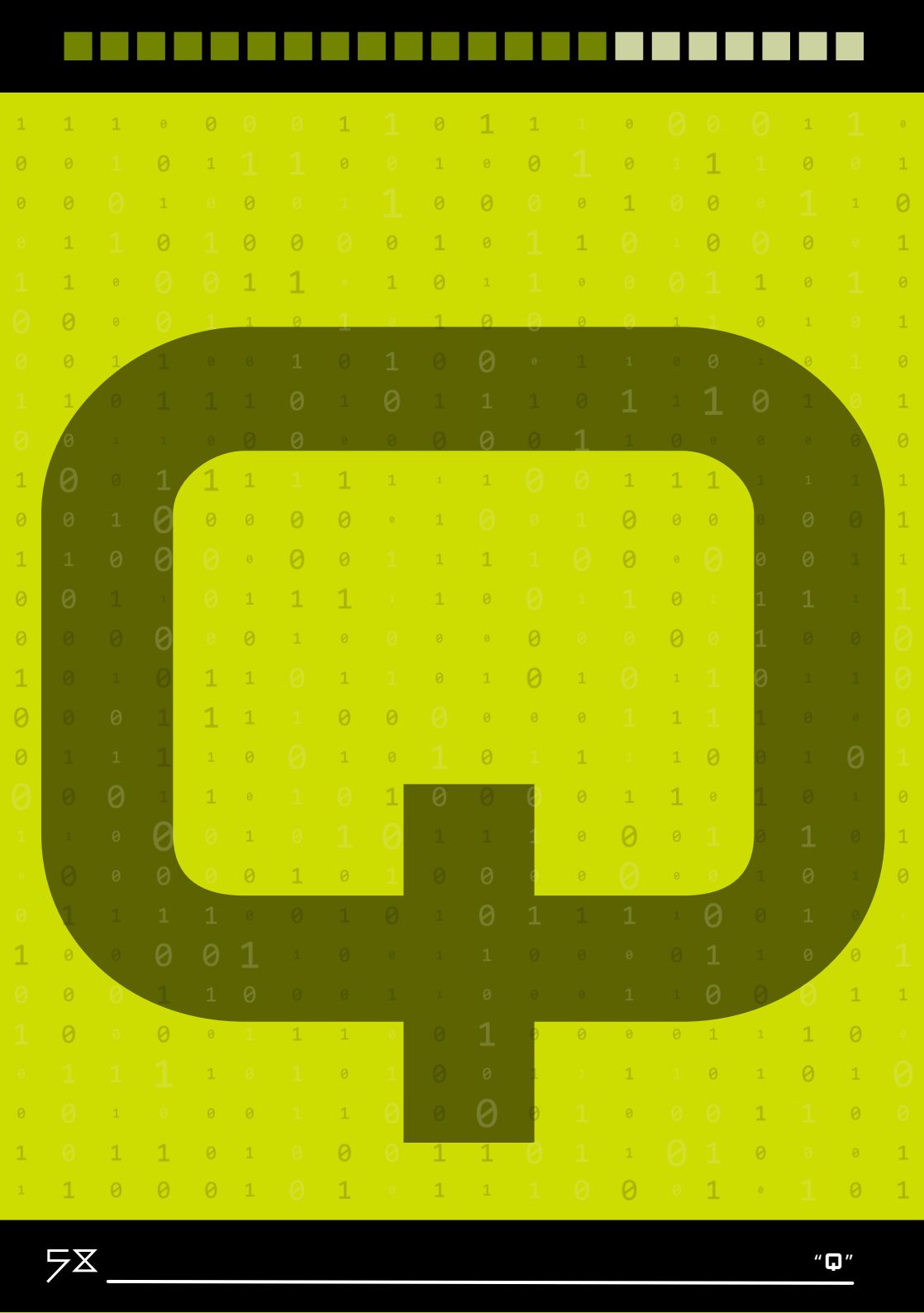
Pufferüberlauf – Eine Schwachstelle, die auftritt, wenn ein Programm mehr Daten in einen Zwischenspeicher schreibt, als dieser fassen kann, wodurch ein:e Angreifer:in potenziell die Möglichkeit hat, beliebige Codes auszuführen.

Pufferzone – Eine Sicherheitsmaßnahme, die einen geschützten Bereich um ein kritisches System oder Netzwerk schafft, um unbefugten Zugriff oder Angriffe zu verhindern.

PUP (Potentiell unerwünschtes Programm) – Software, die zwar nicht schädlich, aber häufig von den Benutzer:innen unerwünscht ist, z. B. Symbolleisten oder Adware, die ein Sicherheitsrisiko darstellen können, wenn sie nicht kontrolliert werden.

Pwn – Ein Slangbegriff, der sich von „own“ (dt. „besitzen“, aber in der Computerspielszene auch „haushoch besiegen“/„vernichtend schlagen“) ableitet, und in der Hackerkultur häufig verwendet wird, um zu beschreiben, dass ein System oder ein Ziel unter Kontrolle gebracht oder besiegt wurde.

Privacy by Design – Das Prinzip der Integration von Datenschutzmaßnahmen in das Design von Systemen und Prozessen.



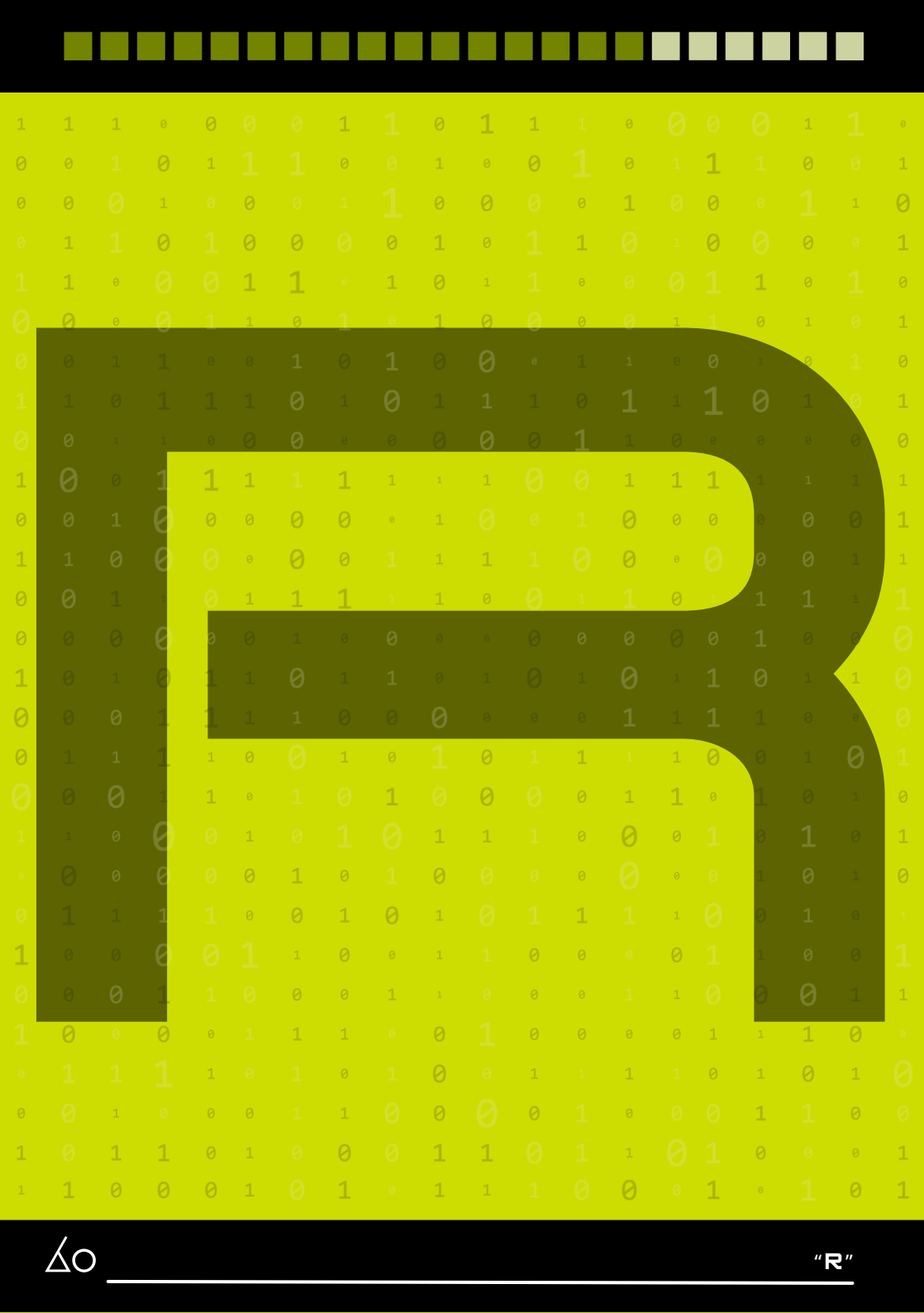
Quantenkryptografie – Eine Verschlüsselungsmethode, die die Prinzipien der Quantenmechanik nutzt, um Daten zu sichern, sdass sie mit klassischen Computermethoden potenziell nicht geknackt werden können.

Quarantäne – Die Isolierung potenziell schädlicher Dateien oder Systeme, um zu verhindern, dass sie Schaden anrichten; wird in der Regel in Antivirensoftware verwendet, um erkannte Malware zu behandeln.

Query Flood Attack – Eine Art von Denial-of-Service-Angriff, bei dem ein Zielsystem durch das Senden einer großen Anzahl von Anfragen überlastet wird, sodass es nicht mehr reagiert.

QR (Quick Response)-Code-Sicherheit – Sicherheitsmaßnahmen zum Schutz vor schädlichen QR-Codes, die Benutzer:innen auf schädliche Websites umleiten oder unbeabsichtigte Aktionen auslösen können.

Quorum-basierte Zugriffskontrolle – Ein Sicherheitsmechanismus, bei dem mehrere Parteien den Zugriff auf sensible Ressourcen oder Vorgänge genehmigen oder autorisieren müssen, um den Schutz vor Missbrauch zu erhöhen.


R

Rahmen für Cybersicherheit – Eine Reihe von Richtlinien und bewährten Verfahren, die Unternehmen bei der Verwaltung und Verringerung von Cybersicherheitsrisiken helfen sollen.

Ransomware – Eine Art von Schadsoftware, die die Daten eines Opfers verschlüsselt oder sein System sperrt und eine Zahlung (in der Regel in Kryptowährung) für den Entschlüsselungsschlüssel oder die Wiederherstellung des Zugangs verlangt.

Rechenschaftspflicht – Der Grundsatz, dass eine Organisation oder eine Person für ihre Handlungen und Entscheidungen verantwortlich ist, insbesondere in Bezug auf Datenschutz und Sicherheit.

Recht auf Datenübertragbarkeit – Das Recht von Einzelpersonen, ihre personenbezogenen Daten über verschiedene Dienste hinweg zu erhalten und wiederzuverwenden.

Rechteausweitung – Eine Art von Angriff, bei dem ein:e Benutzer:in höhere Zugriffsrechte als ursprünglich festgelegt erlangt, was es ihm:ihr ermöglicht, nicht autorisierte Aktionen auf einem System durchzuführen.

Rechtmäßigkeit der Verarbeitung – Die rechtliche Grundlage, auf der eine Organisation gemäß den Datenschutzgesetzen personenbezogene Daten verarbeiten darf.

Rechtsgrundlagen der Datenverarbeitung – Die nach den Datenschutzgesetzen erforderliche Begründung für die Verarbeitung personenbezogener Daten, z. B. die Zustimmung oder die vertragliche Notwendigkeit.

Rechtsrahmen – Die Gesamtheit der Gesetze und Vorschriften, die den Datenschutz und die Datensicherheit regeln.

Rechtsraum – Das geografische Gebiet, in dem die Datenschutzgesetze und -vorschriften gelten.

Rechtssicherheit – Der Prozess, mit dem sichergestellt wird, dass ein Unternehmen die relevanten Gesetze, Vorschriften und Richtlinien in Bezug auf Datenschutz, Cybersicherheit und Datensicherheit einhält (z. B. DSGVO, HIPAA).

Red Teaming – Eine Cybersicherheitsübung, bei der eine unabhängige Gruppe (das Red Team) reale Angriffe simuliert, um die Wirksamkeit der Sicherheitsvorkehrungen eines Unternehmens zu testen.

Reflektiertes XSS (Cross-Site Scripting) – Eine Art von Schwachstelle in Webanwendungen, bei der schädliche Skripte von einem Webserver reflektiert und im Browser eines:einer Benutzer:in ausgeführt werden, was häufig zum Diebstahl sensibler Daten genutzt wird.

Remote-Access-Trojaner (RAT) – Eine Art von Malware, die es Angreifer:innen ermöglicht, ein infiziertes System aus der Ferne zu steuern, was häufig für Spionage, Datendiebstahl oder Systemmanipulation genutzt wird.

Remote Code Execution (RCE) – Eine Sicherheitslücke, die es einem:einer Angreifer:in ermöglicht, beliebigen Code auf einem entfernten Rechner auszuführen, was oft zu einer vollständigen Kompromittierung des Systems führt.

Replay-Angriff – Eine Art von Netzwerkangriff, bei dem eine gültige Datenübertragung in schädlicher oder betrügerischer Absicht wiederholt oder verzögert wird, sodass sich Angreifer:innen als andere Personen ausgeben oder die Kommunikation unterbrechen können.

Residenter Virus – Eine Art von Computervirus, der sich im Speicher eines Systems installiert und so Dateien und Programme infizieren kann, sobald auf sie zugegriffen wird.

Reverse Engineering bzw. **Nachkonstruktion** – Der Prozess der Analyse von Software oder Hardware, um ihr Design, ihre Architektur oder ihren Quellcode zu entdecken, oft im Rahmen der Schwachstellenforschung oder der Malware-Analyse eingesetzt.

Richtlinie zur Vorratsdatenspeicherung – Eine formelle Richtlinie, die den Zeitraum festlegt, für den ein Unternehmen Daten aufbewahrt, sowie den Prozess zur sicheren Löschung der Daten, sobald sie nicht mehr benötigt werden.

Risikobeurteilung – Der Prozess der Identifizierung, Analyse und Bewertung von Risiken für die Informationssysteme und Daten einer Organisation, oft gefolgt von Maßnahmen zur Abschwächung oder Beseitigung dieser Risiken.

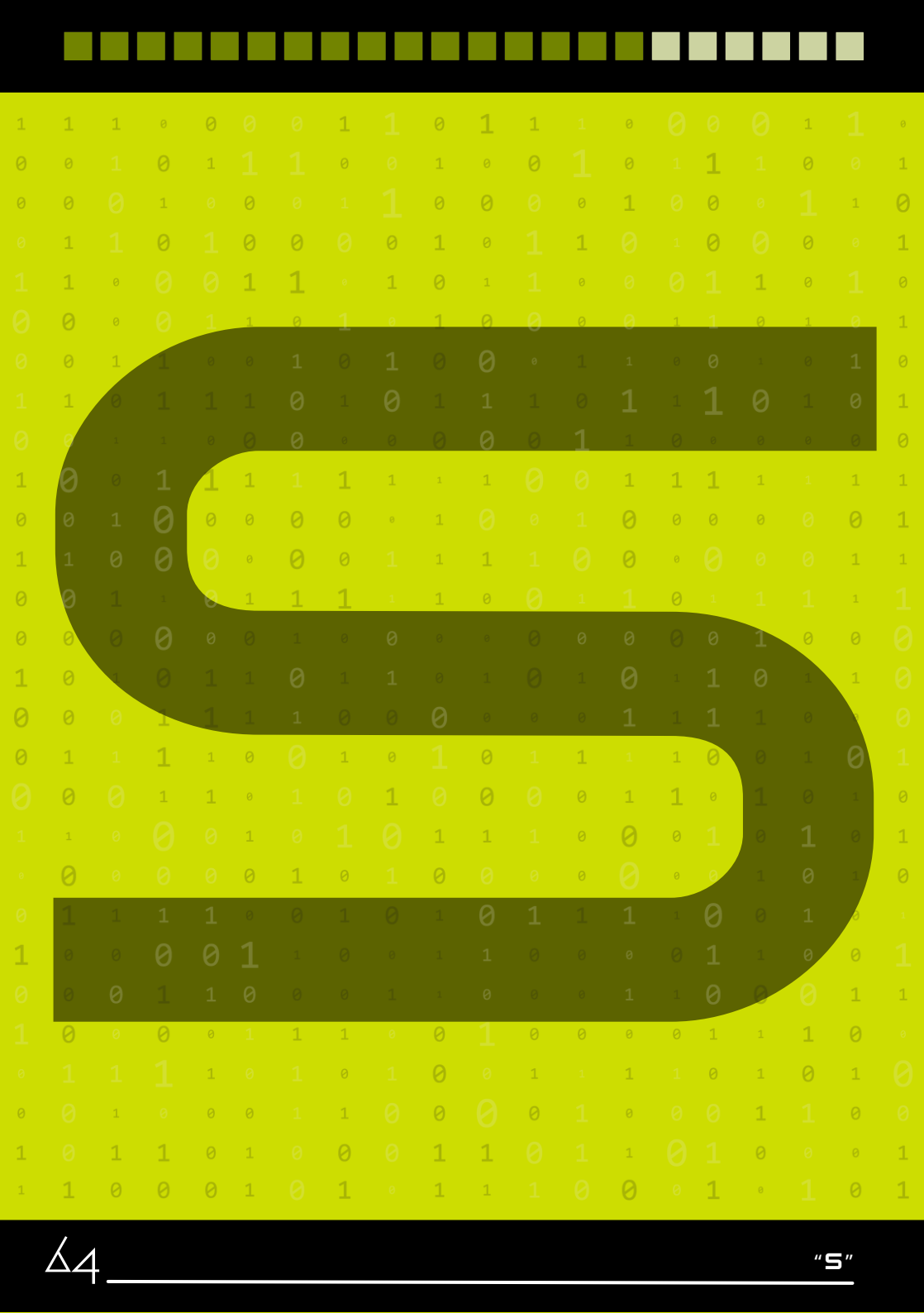
Risikomanagement-Rahmen – Ein strukturierter Ansatz zur Identifizierung, Bewertung und Verwaltung von Risiken im Zusammenhang mit dem Datenschutz.

Risikotoleranz – Der Risikograd, den eine Organisation bei der Verwaltung von Datenschutz und -sicherheit zu akzeptieren bereit ist.

Role-Based Access Control (RBAC; dt. „Rollenbasierte Zugriffskontrolle“**)** – Ein Sicherheitsmodell, das Benutzer:innen innerhalb einer Organisation Zugriffsrechte auf der Grundlage der ihnen zugewiesenen Rollen zuweist und so sicherstellt, dass sie nur auf die für ihre Rolle erforderlichen Daten zugreifen können.

Rootkit – Eine Sammlung von Malware-Tools, die es einem:einer Angreifer:in ermöglichen, unbemerkt die Kontrolle über ein System zu erlangen und aufrechtzuerhalten, oft indem sie seine:ihre Anwesenheit verbergen.

RSA (Rivest-Shamir-Adleman) – Ein weit verbreitetes Public-Key-Kryptosystem für die sichere Datenübertragung, benannt nach seinen Erfindern und bekannt für seine Rolle bei der Verschlüsselung und Sicherung sensibler Daten.



Salami-Angriff – Eine Art von Cyberangriff, bei dem im Laufe der Zeit kleine Geld- oder Datenbeträge gestohlen werden, die oft zu klein sind, um in einzelnen Transaktionen bemerkt zu werden, sich aber zu erheblichen Verlusten summieren.

Sandboxing – Ein Sicherheitsmechanismus, der dazu dient, potenziell schädliche Programme oder Code von kritischen Systemen zu isolieren, sodass sie in einer eingeschränkten Umgebung ausgeführt werden können, ohne das größere Netzwerk zu gefährden.

Scareware – Schadsoftware, die Benutzer:innen vorgaukelt, dass ihr Computer mit Malware infiziert ist, was oft zum Kauf von falscher Sicherheitssoftware oder zur Preisgabe persönlicher Daten führt.

Schattenwirtschaft – Ein Begriff, der sich auf den Schwarzmarkt bezieht, auf dem Cyberkriminelle illegale Waren und Dienstleistungen wie gestohlene Daten, Malware oder Hacking-Tools kaufen, verkaufen und handeln.

Schlüsselableitung bzw. **Key Derivation Function (KDF)** – Eine kryptografische Funktion, die zur Ableitung von Schlüsseln aus einem Basiswert verwendet wird und häufig beim Passwort-Hashing und der Verschlüsselung zum Einsatz kommt.

Schlüsselrotationsrichtlinie – Eine Sicherheitsrichtlinie, die festlegt, wie oft kryptografische Schlüssel rotiert oder geändert werden sollten, um das Risiko einer Schlüsselkompromittierung zu minimieren.

Schwachstelle – Eine Schwäche oder ein Fehler in Software, Hardware oder Verfahren, der von einem:einer Angreifer:in ausgenutzt werden kann, um sich unerlaubten Zugang zu verschaffen oder Schaden anzurichten.

Schwachstellenanalyse – Ein systematischer Prozess zur Identifizierung, Quantifizierung und Priorisierung der Schwachstellen in einem System, um die Risiken zu verstehen und sie zu beseitigen, bevor sie ausgenutzt werden.

Schwachstellenmanagement – Der kontinuierliche Prozess der Identifizierung, Bewertung, Behandlung und Meldung von Schwachstellen in Systemen, um das Zeitfenster für Angriffe zu verringern.

Scriptkiddie – Eine abfällige Bezeichnung für eine:n unerfahrene:n Hacker:in, der:die vorgefertigte Skripte oder Tools verwendet, um Cyberangriffe durchzuführen, ohne deren Funktionsweise vollständig zu verstehen.

Secure Boot – Ein Sicherheitsstandard, der sicherstellt, dass ein Gerät nur mit vertrauenswürdiger Software gebootet wird, um das Laden von nicht autorisierten oder schädlichen Betriebssystemen zu verhindern.

Secure Socket Layer (SSL) – Ein Sicherheitsprotokoll zur Verschlüsselung von Daten, die über das Internet übertragen werden. Es wird häufig in HTTPS verwendet, um sensible Informationen wie Anmeldedaten und Kreditkartennummern zu schützen.

Security-Awareness-Training (dt. „Training für Sicherheitsbewusstsein") – Programme, die Arbeitnehmer:innen oder Nutzer:innen über bewährte Praktiken der Cybersicherheit, Social-Engineering-Bedrohungen und das Erkennen und Verhindern von Cyberangriffen aufklären.

Security Incident Management – Die Prozesse und Verfahren zur Behandlung und Eindämmung von Sicherheitsvorfällen.

Security Information and Event Management (SIEM) – Ein System, das Sicherheitsereignisse aus verschiedenen Quellen in Echtzeit sammelt, analysiert und korreliert und Unternehmen dabei hilft, Bedrohungen effektiver zu erkennen und darauf zu reagieren.

Seitenkanalattacke – Eine Angriffsart, bei der physische oder implementierungsspezifische Merkmale eines Systems (z. B. Stromverbrauch oder Zeitinformationen) ausgenutzt werden, um Zugriff auf sensible Daten zu erhalten.

Sensible Daten – Personenbezogene Daten, die aufgrund ihrer Beschaffenheit einen zusätzlichen Schutz erfordern, z. B. Gesundheitsinformationen oder finanzielle Details.

Session-Hijacking – Eine Angriffsart, bei der ein:e Angreifer:in die Sitzung eines Benutzers auf einer Website oder in einer Anwendung übernimmt, häufig durch Diebstahl des Sitzungs-Tokens oder Cookies.

Shoulder Surfing – Eine physische Sicherheitsbedrohung, bei der Angreifer:innen Benutzer:innen bei der Eingabe sensibler Daten wie Passwörter oder PINs beobachten, indem sie ihnen über die Schulter schauen oder Überwachungsgeräte einsetzen.

Sicherheit auf Objektebene – Sicherheitsmaßnahmen, die auf einzelne Objekte wie Dateien oder Datenbankeinträge angewendet werden, um sicherzustellen, dass nur autorisierte Benutzer:innen darauf zugreifen oder sie ändern können.

Sicherheit durch maschinelles Lernen – Die Anwendung von Algorithmen des maschinellen Lernens zur Erkennung von Anomalien, zur Vorhersage von Bedrohungen und zur Verbesserung der Cybersicherheitsabwehr auf der Grundlage großer Datensätze.

Sicherheit durch neuronale Netze – Die Anwendung von auf neuronalen Netzen basierenden Techniken zur Verbesserung der Cybersicherheit, z. B. die Verwendung künstlicher neuronaler Netze zur Erkennung von Anomalien und zur Vorhersage von Bedrohungen.

Sicherheitsverletzung bzw. **Breach** – Ein Vorfall, bei dem es zu einem unbefugten Zugriff oder einer unbefugten Offenlegung von Daten kommt, wodurch der Datenschutz und die Datensicherheit gefährdet werden können.

Sicherheitszertifizierungen – Offizielle Anerkennung, dass die Datenschutzpraktiken einer Organisation bestimmten Standards entsprechen.

Signaturbasierte Erkennung – Eine in Antiviren- und Angriffserkennungssystemen verwendete Methode, die Bedrohungen auf der Grundlage vordefinierter Muster oder „Signaturen" bekannter Malware identifiziert.

Single Sign-On (SSO; dt. „Einmalanmeldung"**)** – Ein Verfahren zur Benutzerauthentifizierung, das es einem:einer Benutzer:in ermöglicht, sich einmalig anzumelden und Zugang zu mehreren Anwendungen oder Systemen zu erhalten, ohne sich für jede Anwendung erneut anmelden zu müssen.

Smishing – Ein Phishing-Angriff, der über SMS-Nachrichten ausgeführt wird und bei dem der:die Angreifer:in versucht, das Opfer dazu zu bringen, persönliche Informationen preiszugeben oder auf einen schädlichen Link zu klicken.

Sniffing – Das Abfangen und Analysieren des Netzwerkverkehrs, das häufig von Angreifer:innen genutzt wird, um sensible Daten wie Anmeldedaten oder Kreditkartennummern abzufangen.

Social Engineering – Eine Manipulationstechnik, die von Angreifer:innen eingesetzt wird, um Personen dazu zu bringen, vertrauliche Informationen preiszugeben oder sicherheitsgefährdende Aktionen auszuführen, z. B. auf schädliche Links zu klicken.

Spear-Phishing - Ein gezielter Phishing-Angriff, der sich an eine bestimmte Person oder Organisation richtet und oft personalisierte Nachrichten und Details verwendet, um die Erfolgswahrscheinlichkeit zu erhöhen.

Speicherauszug - Eine Datei, die den Inhalt des Speichers zu einem bestimmten Zeitpunkt aufzeichnet und häufig für forensische Analysen bei der Reaktion auf einen Vorfall zur Untersuchung von Angriffen verwendet wird.

Speicherkorruption - Eine Software-Schwachstelle, bei der der Inhalt des Computerspeichers unbeabsichtigt verändert wird, was einem:einer Angreifer:in die Möglichkeit gibt, das System zu missbrauchen.

Spoofing - Der Akt, sich als ein:e andere:r Benutzer:in, ein anderes Gerät oder ein anderes System auszugeben, um unbefugten Zugriff auf ein System zu erhalten oder die Kommunikation zu manipulieren.

Spyware - Schadsoftware, die das System eines:einer Benutzer:in heimlich überwacht und Informationen sammelt, wie z. B. Surfgewohnheiten oder persönliche Daten, oft ohne das Wissen des:der Benutzer:in.

SQL-Injection - Eine Angriffsart, bei der ein:e Angreifer:in Schwachstellen in der Datenbankabfrage-Schnittstelle einer Anwendung ausnutzt, indem er:sie bösartigen SQL-Code einfügt, um unbefugten Zugriff auf Daten zu erhalten oder diese zu manipulieren.

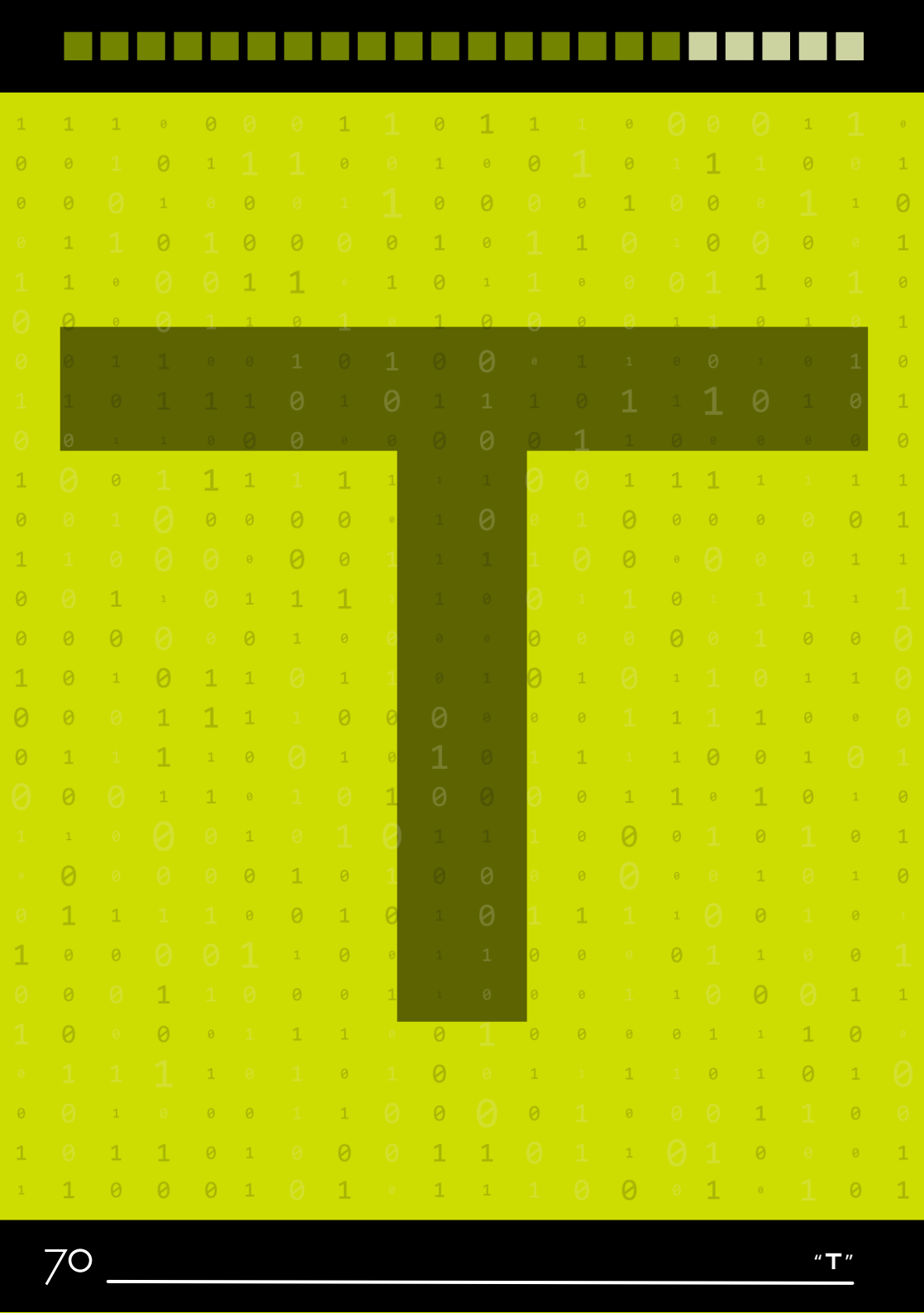
Staatlich geförderter Angriff - Ein von einer Regierung durchgeführter oder unterstützter Cyberangriff, der in der Regel auf andere Nationen, Organisationen oder Einzelpersonen zu Spionage-, Sabotage- oder anderen strategischen Zwecken abzielt.

Standardvertragsklauseln - Rechtliche Vereinbarungen zur Gewährleistung eines angemessenen Datenschutzes bei der Übermittlung von Daten außerhalb des Europäischen Wirtschaftsraums (EWR).

Steganographie - Die Praxis des Versteckens von Informationen in anderen Daten, z. B. das Einbetten einer Nachricht in eine Bild- oder Audiodatei, die häufig zur verdeckten Kommunikation verwendet wird.

Supply-Chain-Attacke - Eine Art von Angriff, bei dem ein:e Angreifer:in auf weniger sichere Elemente in der Versorgungskette abzielt, z. B. Drittanbieter oder Dienstleister, um die Sicherheit einer größeren Organisation zu gefährden.

Symmetrische Verschlüsselung – Eine Art der Verschlüsselung, bei der derselbe Schlüssel sowohl für die Verschlüsselung als auch für die Entschlüsselung der Daten verwendet wird; wird häufig in sicheren Kommunikationsprotokollen eingesetzt.



Tails (The Amnesic Incognito Live System) – Ein sicherheitsorientiertes Linux-basiertes Betriebssystem, das für die anonyme Internetnutzung und den Schutz der Privatsphäre entwickelt wurde. Es läuft von einem USB-Stick oder einer DVD und hinterlässt keine Spuren auf dem Rechner.

Technische und organisatorische Maßnahmen (TOMs) – Maßnahmen, die ergriffen werden, um die Sicherheit von personenbezogenen Daten zu gewährleisten, darunter technische Lösungen und organisatorische Praktiken.

Technische Schwachstellen – Schwachstellen in einem System, die ausgenutzt werden können, um unbefugten Zugang zu Daten zu erhalten.

Third-Party-Risikomanagement – Der Prozess der Bewertung und Verwaltung von Risiken im Zusammenhang mit Drittanbietern, die Daten verarbeiten.

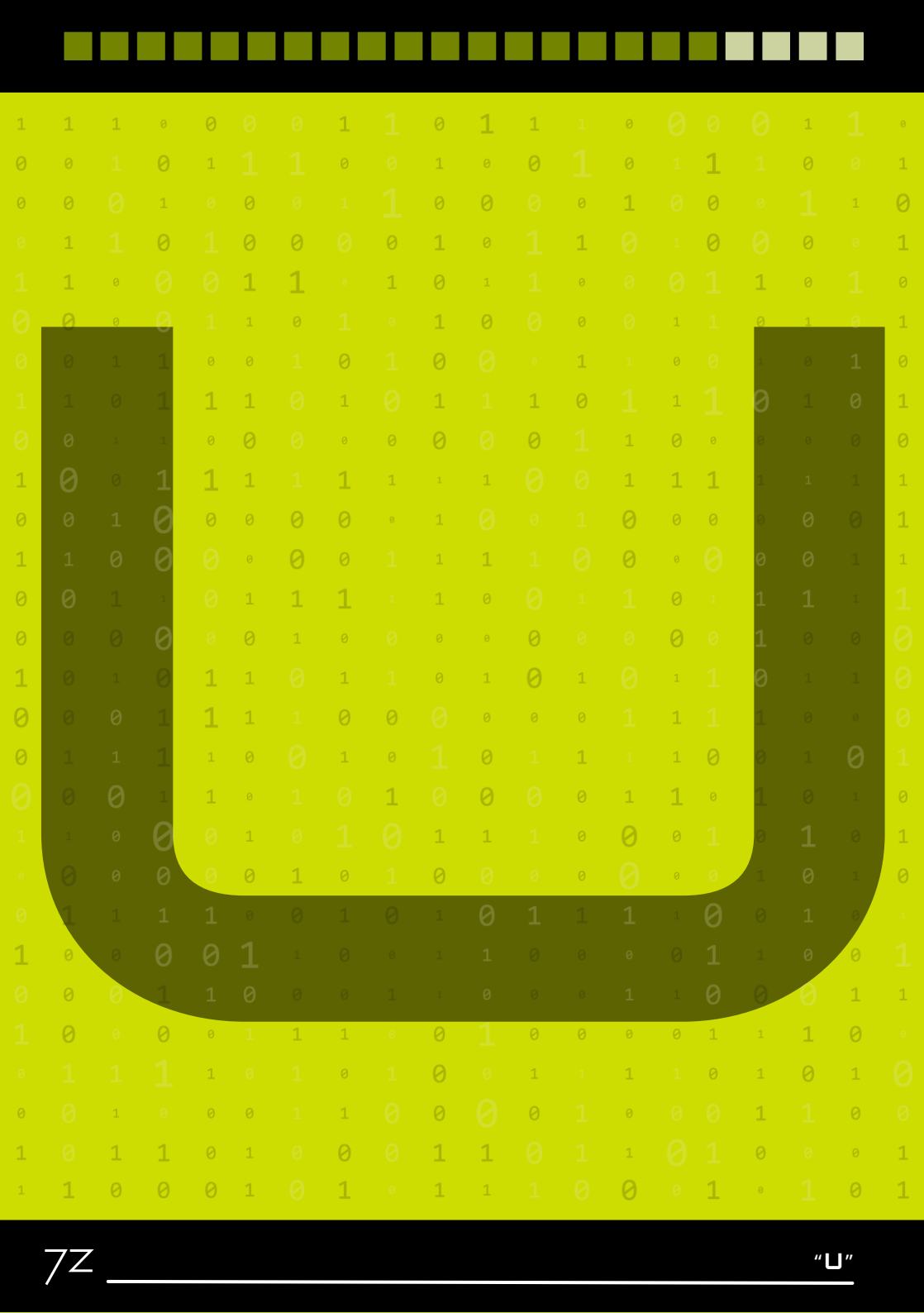
Threat Hunting – Eine proaktive Cybersicherheitspraxis, bei der Sicherheitsexpert:innen aktiv nach Bedrohungen oder Indicators of Compromise (IoCs) innerhalb eines Netzwerks suchen, bevor sie zu einer Sicherheitsverletzung führen.

Threat Intelligence – Informationen über aktuelle oder potenzielle Cyber-Bedrohungen, die aus verschiedenen Quellen zusammengetragen werden, um Unternehmen dabei zu helfen, Angriffe zu erkennen, zu verhindern und darauf zu reagieren.

Tokenisierung – Ein Prozess, bei dem sensible Daten durch eine eindeutige Kennung oder ein Token ersetzt werden, wodurch das Risiko der Offenlegung der eigentlichen Daten während der Speicherung oder Übertragung verringert wird.

Transparenz – Der Grundsatz der Offenheit und Klarheit in Bezug auf die Datenerfassungspraktiken und die Verwendung der Daten.

Typosquatting – Ein Social-Engineering-Angriff, bei dem Cyberkriminelle gefälschte Websites mit Domänennamen erstellen, die bekannten Websites ähneln, in der Hoffnung, dass Benutzer:innen die URL falsch eingeben und auf der schädlichen Website landen.



Überwachung der Dateiintegrität bzw. **File Integrity Monitoring (FIM)** – Ein Verfahren zur Erkennung nicht autorisierter Änderungen an Dateien, um deren Integrität sicherzustellen.

UDP (User Datagram Protocol) – Ein Kommunikationsprotokoll, das im Internet für die schnelle, verbindungslose Datenübertragung verwendet wird. Es wird häufig in Anwendungen wie Streaming und VoIP verwendet, ist aber weniger sicher als TCP (Transmission Control Protocol).

UEBA (User and Entity Behavior Analytics) – Eine Cybersicherheitstechnologie, die maschinelles Lernen und Analysen einsetzt, um Anomalien im Verhalten von Benutzer:innen und Entitäten zu erkennen, um potenzielle Bedrohungen oder schädliche Insider zu identifizieren.

Uniform Resource Locator (URL) – Eine Referenz (Adresse), die für den Zugriff auf Ressourcen im Internet verwendet wird. Bösartige URLs werden häufig bei Phishing-Angriffen verwendet, um Benutzer:innen auf schädliche Websites umzuleiten.

Unsicheres Protokoll – Ein Kommunikationsprotokoll, das keine Verschlüsselung oder andere Sicherheitsmaßnahmen zum Schutz von Daten während der Übertragung bietet, wie z. B. HTTP (im Gegensatz zu HTTPS).

URL-Filterung – Eine Sicherheitsmaßnahme, die den Zugriff auf bestimmte Websites auf der Grundlage von URL-Adressen sperrt oder zulässt und häufig verwendet wird, um zu verhindern, dass Benutzer:innen auf schädliche oder unangemessene Inhalte zugreifen.

USB-Sicherheit – Richtlinien und Maßnahmen zum Schutz von Systemen vor Sicherheitsrisiken im Zusammenhang mit USB-Laufwerken, die Malware einschleusen oder die Datenexfiltration erleichtern können.

User Consent Management – Verfahren und Tools zur Einholung und Verwaltung der Zustimmung von Personen zu Datenverarbeitungsaktivitäten.


U

Verfahren zur Meldung von Vorfällen – Der Prozess und das System zur Meldung von Datenschutzverletzungen und Sicherheitsvorfällen innerhalb einer Organisation.

Verfügbarkeit bzw. **Availability** – Die Gewissheit, dass Daten und Ressourcen bei Bedarf für autorisierte Benutzer:innen zugänglich sind; Teil der CIA-Triade (Confidentiality – Vertraulichkeit, Integrity – Integrität, Availability –Verfügbarkeit) in der Informationssicherheit.

Verhaltensanalytik – Die Analyse von Benutzer- und Systemverhaltensmustern zur Erkennung von Anomalien und potenziellen Sicherheitsbedrohungen.

Verhaltensbasierte Erkennung – Ein Sicherheitsansatz, der Bedrohungen durch die Analyse von Verhaltensmustern identifiziert, anstatt sich ausschließlich auf bekannte Signaturen oder Muster zu verlassen.

Verletzung der Datensicherheit – Ein Vorfall, bei dem ein unbefugter Zugriff, eine unbefugte Offenlegung, eine unbefugte Änderung oder eine unbefugte Zerstörung von Daten erfolgt, wodurch deren Vertraulichkeit, Integrität oder Verfügbarkeit beeinträchtigt wird.

Verschleierung – Der Prozess, bei dem Code oder Daten absichtlich schwerer verständlich gemacht oder rückentwickelt werden, oft zum Schutz vertraulicher Informationen oder zur Verhinderung der Analyse von Malware.

Verschlüsselung – Der Prozess, bei dem lesbare Daten (Klartext) in ein unlesbares Format (Chiffretext) umgewandelt werden, um sie vor unbefugtem Zugriff zu schützen; in der Regel nur mit einem Entschlüsselungsschlüssel umkehrbar.

Verschlüsselungspflicht – Eine Richtlinie, die vorschreibt, dass alle sensiblen Daten sowohl in gespeichertem Zustand als auch bei der Übertragung verschlüsselt werden müssen, um ihre Vertraulichkeit und Integrität zu gewährleisten.

Vertraulichkeit bzw. **Confidentiality** – Der Grundsatz, dass Informationen nur jenen zugänglich sind, die dazu berechtigt sind, und dass sie vor unbefugter Offenlegung geschützt sind.

Vertraulichkeitsvereinbarung – Ein rechtlicher Vertrag, in dem sich die Parteien verpflichten, bestimmte vertrauliche Informationen geheim zu halten und sie nicht an Unbefugte weiterzugeben.

Virus – Eine Art von Schadsoftware, die sich selbst repliziert, wenn sie ausgeführt wird, indem sie andere Computerprogramme verändert und ihren eigenen Code einfügt, was zu Schäden an Systemen und Daten führen kann.

Virtual Private Network (VPN) – Ein Dienst, der den Internetverkehr verschlüsselt und die IP-Adresse des:der Benutzer:in verbirgt, um eine sichere Verbindung zwischen dem:der Benutzer:in und einem entfernten Netzwerk herzustellen. Er wird häufig zum Schutz der Privatsphäre und der Sicherheit eingesetzt.

Vishing – Eine Art von Phishing-Angriff über das Telefon, bei dem sich Angreifer:innen als legitime Personen ausgeben, um sensible Informationen wie Passwörter oder Kreditkartendaten zu stehlen.

Vorfallmanagement – Der Prozess der Identifizierung, Reaktion und Entschärfung von Datenverletzungen und anderen Sicherheitsvorfällen.

Vorfallsreaktion – Der Prozess der Bearbeitung und Verwaltung der Folgen einer Sicherheitsverletzung oder eines Angriffs, wobei der Schwerpunkt auf der Begrenzung des Schadens, der Wiederherstellung der betroffenen Systeme und der Vermeidung künftiger Vorfälle liegt.

Vorfallsreaktionsplan – Ein Plan, der detailliert die Schritte beschreibt, die als Reaktion auf eine Datenschutzverletzung oder einen Sicherheitsvorfall zu unternehmen sind.

Vorfallsreaktionsteam (Incident Response Team – IRT) – Eine Gruppe von Fachleuten, die für die Verwaltung und Reaktion auf Datenschutzverletzungen und Sicherheitsvorfälle zuständig ist.

Vorratsdatenspeicherung – Die Richtlinien und Praktiken zur Speicherung von Daten für einen bestimmten Zeitraum, bevor sie gelöscht oder archiviert werden.

Vorschriften zur Meldung von Datenschutzverletzungen – Gesetze, die Unternehmen dazu verpflichten, betroffene Personen und Aufsichtsbehörden im Falle einer Datenschutzverletzung zu benachrichtigen.

Watering-Hole-Angriff – Ein gezielter Angriff, bei dem Cyberkriminelle eine von ihren Opfern häufig besuchte Website kompromittieren und Malware in die Website einschleusen, um die Geräte der Besucher:innen zu infizieren.

Web Scraping – Die automatisierte Extraktion von Daten aus Websites, wobei oft das Datenschutzrecht eingehalten werden muss.

WEP (Wired Equivalent Privacy) – Ein veraltetes Sicherheitsprotokoll, das zum Schutz drahtloser Netzwerke verwendet wird. Es wurde aufgrund seiner Schwachstellen durch sicherere Protokolle wie WPA ersetzt.

Whaling – Eine Form des Phishing-Angriffs, die speziell auf hochrangige Führungskräfte oder wichtige Personen innerhalb eines Unternehmens ausgerichtet ist, oft mit dem Ziel, sensible Informationen oder Finanzmittel zu stehlen.

White-Hat-Hacker:in – Ein:e ethische:r Hacker:in, der:die die eigenen Fähigkeiten einsetzt, um Sicherheitsschwachstellen in Systemen mit der Erlaubnis des Eigentümers zu identifizieren und zu beheben, und der:die oft von Organisationen zur Verbesserung der Sicherheit eingesetzt wird.

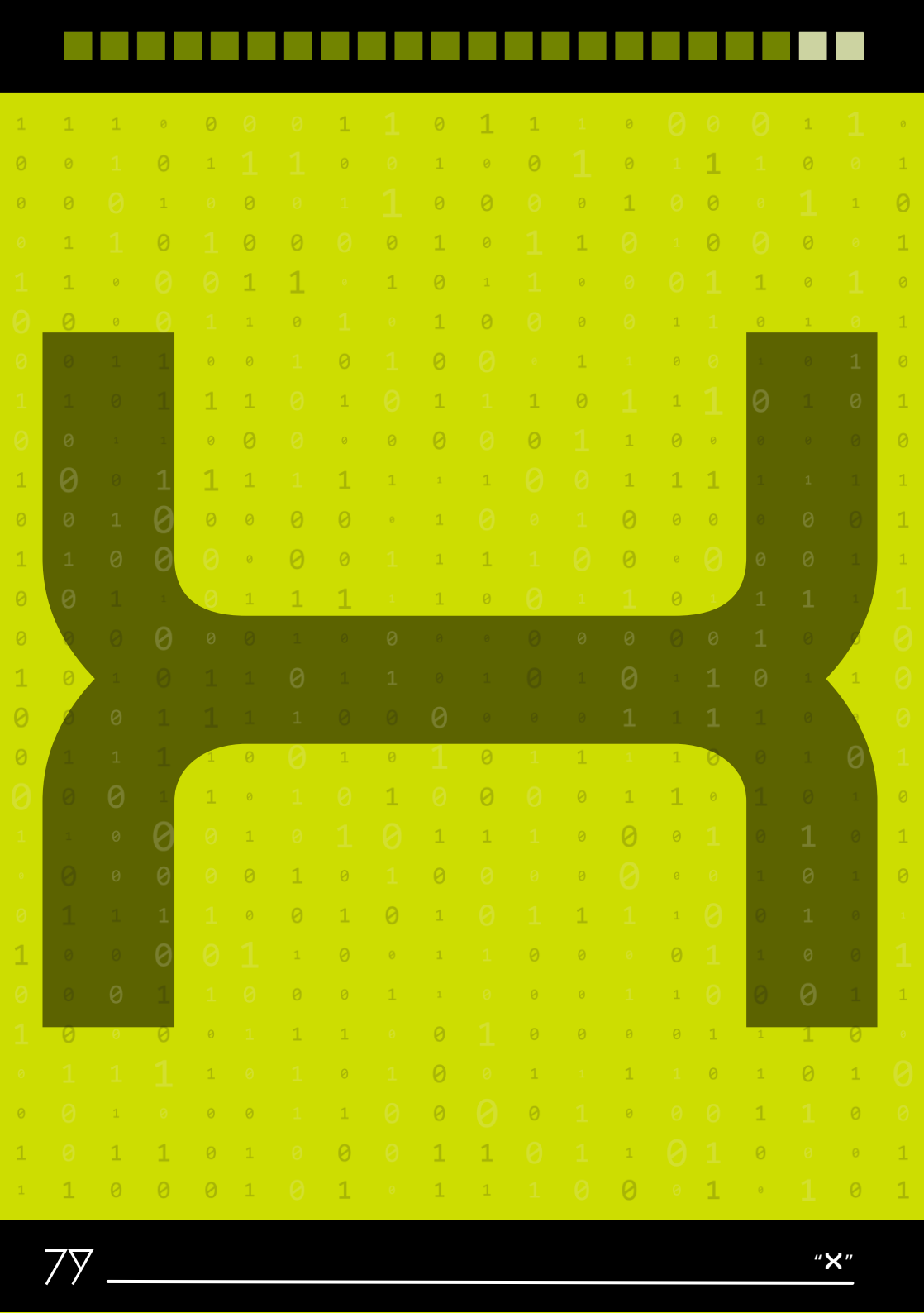
Whistleblowing – Meldung unethischer oder illegaler Praktiken, darunter Datenschutzverletzungen oder die Nichteinhaltung von Datenschutzgesetzen.

Wi-Fi Protected Access (WPA/WPA2) – Ein Sicherheitsprotokoll zur Sicherung drahtloser Netzwerke, das eine stärkere Verschlüsselung als sein Vorgänger WEP bietet. WPA2 ist derzeit der Standard für sichere WLAN-Kommunikation.

Wissensentdeckung in Datenbanken bzw. **Knowledge Discovery in Databases (KDD)** – Der Prozess der Entdeckung nützlicher Informationen und Muster aus großen Datenbeständen, der häufig bei Sicherheitsanalysen zur Identifizierung potenzieller Bedrohungen eingesetzt wird.

Wurm – Eine Art selbstreplizierende Malware, die sich über Netzwerke verbreitet, indem sie Schwachstellen ausnutzt, ohne dass ein Mensch eingreifen muss, oder sich an Dateien anhängt.

WPA3 (Wi-Fi Protected Access 3) – Das neueste Sicherheitsprotokoll für drahtlose Netzwerke, das einen stärkeren Datenschutz und eine sichere Verschlüsselung sowohl in privaten als auch in Unternehmensumgebungen bieten soll.



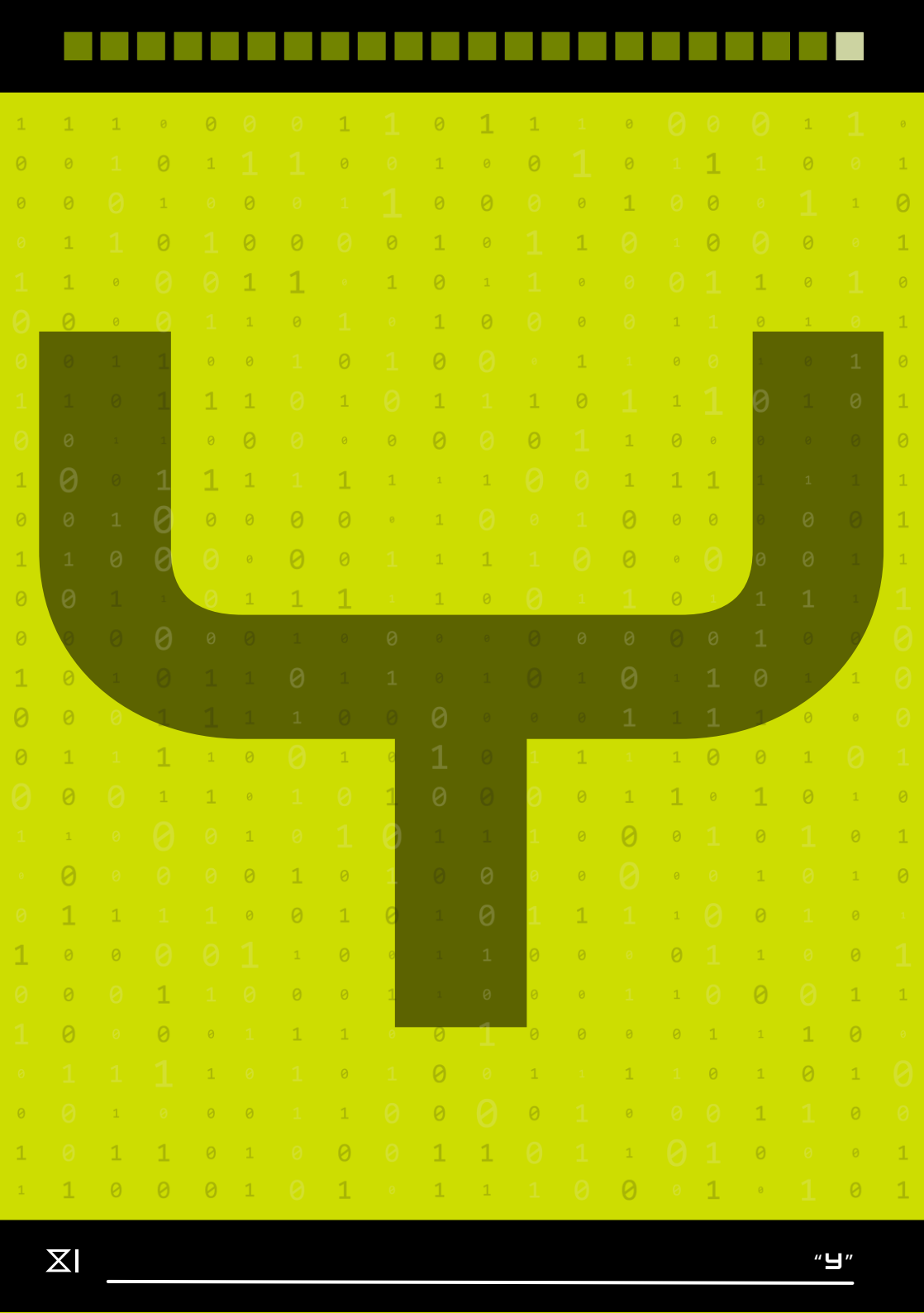
X.509-Zertifikat - Ein digitales Zertifikat, das den X.509 Public-Key-Infrastruktur (PKI)-Standard verwendet, um die Identität von Personen, Geräten und Servern über das Internet zu überprüfen und so eine sichere Kommunikation zu gewährleisten.

XACML (eXtensible Access Control Markup Language) - Ein XML-basierter Rahmen zur Definition und Durchsetzung von Zugriffskontrollrichtlinien. Es wird häufig für die Verwaltung von Berechtigungen in Systemen und Netzwerken verwendet.

XDR (Extended Detection and Response) - Eine Sicherheitslösung, die Daten aus mehreren Sicherheitsprodukten integriert und korreliert, um eine umfassende Erkennung, Untersuchung und Reaktion auf Bedrohungen im gesamten Netzwerk eines Unternehmens zu ermöglichen.

XML Encryption - Ein Standard zur Verschlüsselung des Inhalts von XML-Dokumenten, der sicherstellt, dass sensible Daten, die im XML-Format übertragen werden, vor unbefugtem Zugriff geschützt sind.

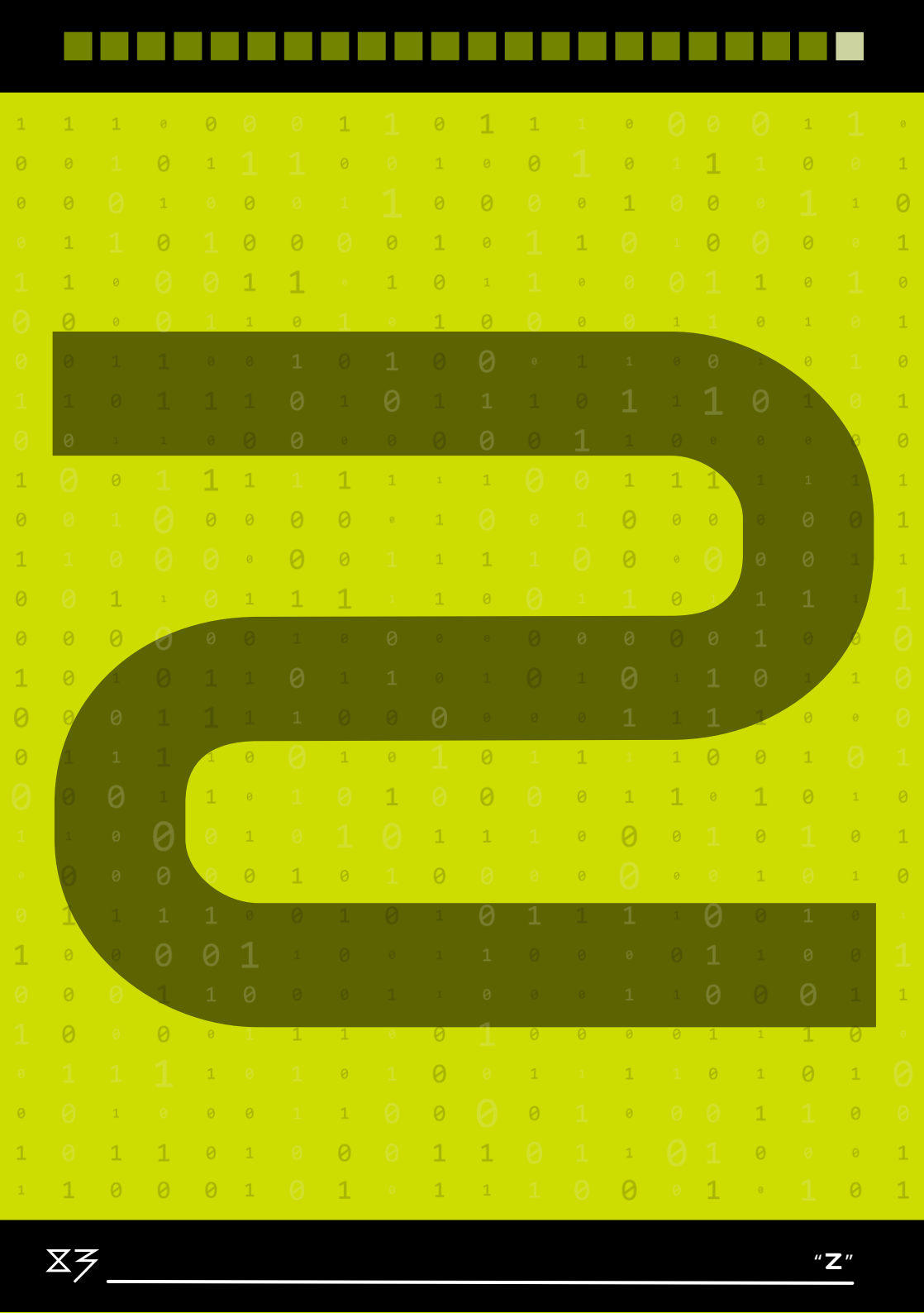
XML-Firewall - Ein Sicherheitssystem, das XML-basierte Webdienste schützt, indem es den XML-Datenverkehr filtert und Angriffe wie XML-Injection oder Denial-of-Service verhindert.



YARA – Ein Tool zur Identifizierung und Klassifizierung von Malware durch die Erstellung von Beschreibungen (Regeln) von schädlichen Dateimustern. Es wird häufig beim Threat Hunting und in der Malware-Forschung eingesetzt.

YubiKey – Ein Hardware-Authentifizierungsgerät, das die Zwei-Faktor-Authentifizierung (2FA) unterstützt und durch die Generierung von Einmal-Passwörtern oder kryptografischen Schlüsseln für Anmeldezwecke eine hohe Sicherheit bietet.

Yellow Team – Im Kontext der Cybersicherheit eine Gruppe, die sich auf die Zusammenarbeit zwischen offensiven („Red Team“) und defensiven („Blue Team“) Sicherheitsbemühungen konzentriert und oft dazu beiträgt, die Koordination und den Wissensaustausch zwischen den beiden zu verbessern.



Zero-Day-Angriff – Ein Cyberangriff, bei dem eine bisher unbekannte Schwachstelle in Software oder Hardware ausgenutzt wird, die vom Hersteller noch nicht gepatcht wurde, was den Angriff sehr gefährlich macht.

Zero-Trust-Architektur – Ein Sicherheitsmodell, bei dem davon ausgegangen wird, dass weder Netzwerke noch Geräte oder Benutzer:innen standardmäßig vertrauenswürdig sind und der Zugriff nur nach einer kontinuierlichen Überprüfung der Identität und des Sicherheitsstatus gewährt wird.

Zero Trust Network Access (ZTNA) – Ein Sicherheitsansatz, der einen sicheren, segmentierten Zugriff auf Netzwerkressourcen auf der Grundlage einer Identitätsüberprüfung gewährleistet, wobei kein implizites Vertrauen für ein Gerät oder eine:n Benutzer:in innerhalb oder außerhalb des Netzwerks vorausgesetzt wird.

Zertifizierungsstelle (Certificate Authority – **CA**) – An entity that issues digital certificates used to verify the authenticity of websites, software, and communications.

Zombie – Ein Computer, der kompromittiert wurde und von einem:einer Angreifer:in ferngesteuert wird. Er wird oft als Teil eines Botnetzes verwendet, um koordinierte Cyberangriffe wie Distributed Denial of Service (DDoS) zu starten.

Zscaler – Ein Cloud-basiertes Sicherheitsunternehmen, das Lösungen für Internetsicherheit, Webfilterung und Zero Trust Network Access (ZTNA) für Unternehmen anbietet, um ihre Daten und Nutzer:innen zu schützen.

Zugriffskontrolle – Mechanismen und Richtlinien, die regeln, wer Ressourcen in einer Computerumgebung einsehen oder nutzen darf.

Zugriffskontrollliste (Access Control List – ACL) – Eine Liste von Berechtigungen, die einem Objekt zugeordnet ist und festlegt, welche Benutzer:innen oder Systeme darauf zugreifen und welche Aktionen sie durchführen dürfen.

Zugriffsverwaltung bzw. **Access-Management** – Der Prozess der Verwaltung des Benutzerzugriffs auf Ressourcen und Daten innerhalb einer Organisation.

Zwei-Faktor-Authentifizierung (2FA) – Ein Sicherheitsprozess, der zwei separate Verifizierungsmethoden erfordert (z. B. ein Passwort und einen Fingerabdruck oder einen Einmalcode, der an ein mobiles Gerät gesendet wird), um die Identität eines:einer Benutzer:in zu überprüfen und zu authentifizieren, um die Kontosicherheit zu erhöhen.