IT-Begriffe für alle

Glossar der IT-Begriffe

495 Begriffe aus IT-Sicherheit und API-Programmierung,
auf Deutsch und Englisch erklärt.

Aufbau jedes Eintrags: der Begriff fett, darunter – wo vorhanden – die ausgeschriebene Abkürzung, dann die Erklärung auf Deutsch und in Kursivschrift die englische Fassung.

Die englische Aussprache jedes Begriffs gibt es als Ton auf der Webseite. Dort lässt sich außerdem zwischen Deutsch und Englisch umschalten und die Liste durchsuchen.

Jeder Begriff ist in dieser Datei anklickbar (gepunktet unterstrichen) und öffnet im Browser direkt seinen Eintrag mit Aussprache, Quellen und Anwendungsfall.

it-terms.agcomputing.net

Index

Buchstaben anklicken springt zur jeweiligen Sektion.

A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z				

Stand 03.11.2026 · AGC Computing

A

↑ Index

ABAC
Attribute-Based Access Control

Zugriff wird über Merkmale entschieden (Abteilung, Standort, Uhrzeit) statt nur über die Rolle.

Access decided by attributes such as department, location or time, not only by role.

Accessibility
Barrierefreiheit

Gestaltung, die eine Seite für alle bedienbar macht – Screenreader, Tastatur, ausreichender Kontrast, klare Beschriftungen.

Design that makes a page usable for everyone – screen readers, keyboard, sufficient contrast, clear labels.

Access Token

Zeitlich begrenzter Ausweis, den ein Client bei jeder Anfrage mitschickt. Kurz gültig, damit ein Diebstahl wenig nützt.

Short-lived credential the client sends with every request, kept short so theft does little damage.

Account Takeover

Übernahme eines fremden Kontos, meist durch gestohlene oder erratene Zugangsdaten, Phishing oder eine Lücke – von dort geht es oft weiter zu Geld oder Rufschaden.

Taking over someone else's account, usually with stolen or guessed credentials, phishing or a flaw – from there it often leads to money or reputational damage.

ACL
Access Control List

Liste, die festlegt, wer auf ein Objekt zugreifen darf und was er darf (lesen, schreiben, löschen).

List defining who may access an object and what they may do with it (read, write, delete).

ACME

Das Protokoll, mit dem ein Server ein Zertifikat automatisch beantragt und dabei beweist, dass ihm die Domain gehört.

The protocol a server uses to request a certificate automatically and prove that the domain belongs to it.

ADR
Architecture Decision Record

Kurzes Dokument, das eine technische Entscheidung festhält: Kontext, Optionen, Entscheidung, Folgen.

A short document recording a technical decision: context, options, decision, consequences.

AES
Advanced Encryption Standard

Standard-Symmetrieverfahren für Verschlüsselung; AES-256 gilt als sicher und ist weltweit verbreitet.

Standard symmetric cipher; AES-256 is considered secure and is used worldwide.

Allowlist

Liste ausdrücklich erlaubter Werte, Adressen oder Aktionen. Alles, was nicht darauf steht, ist verboten.

Explicit list of allowed values, addresses or actions. Anything not listed is denied.

Android

Mobiles Betriebssystem von Google, das auf vielen Geräten verschiedener Hersteller läuft – Apps kommen meist aus dem Play Store oder als APK.

Google's mobile operating system, running on devices from many manufacturers – apps usually come from the Play Store or as an APK.

Anmeldung
Login

Der Vorgang, bei dem jemand beweist, wer er ist – meist mit Kennung und Passwort, oft mit einem zweiten Faktor.

The process of proving who you are – usually with an identifier and password, often with a second factor.

Anonymisierung

Daten so verändern, dass ein Personenbezug nicht mehr herstellbar ist – endgültig und irreversibel.

Irreversibly altering data so it can no longer be linked to any person.

Anwendung
App

Ein Programm mit einer bestimmten Aufgabe – vom Warenwirtschaftssystem bis zur Handy-App.

A program with a specific job – from an ERP system to a phone app.

Apache

Der klassische Webserver, der sich pro Verzeichnis über .htaccess konfigurieren lässt; viele WordPress-Seiten laufen darauf.

The classic web server, configurable per directory via .htaccess; many WordPress sites run on it.

API
Application Programming Interface

Schnittstelle, über die zwei Programme miteinander reden – meist HTTP mit JSON.

Interface that lets two programs talk to each other, usually HTTP with JSON.

API-Gateway
Application Programming Interface Gateway

Vorgeschalteter Dienst, der API-Aufrufe annimmt, prüft, begrenzt und an den eigentlichen Dienst weiterleitet.

Front service that receives, authenticates, rate-limits and forwards API calls to the actual service.

API-Key
Application Programming Interface Key

Geheimer Schlüssel, der ein Programm gegenüber einer API ausweist. Gehört nie in Quellcode, Repos oder URLs.

Secret key that identifies a program to an API. Never belongs in source code, repos or URLs.

APK
Android Package

Installationsdatei einer Android-App – technisch ein Paket aus Code, Ressourcen und Manifest.

The install file of an Android app – technically a package of code, resources and manifest.

App-Berechtigung

Erlaubnis, die eine App vom Nutzer braucht, um auf Kamera, Standort, Kontakte oder Mikrofon zuzugreifen.

Permission an app needs from the user to access camera, location, contacts or microphone.

APT
Advanced Persistent Threat

Lange, gezielte und meist staatlich unterstützte Angriffskampagne, die möglichst unentdeckt im Netz bleibt.

Long, targeted, often state-backed campaign that tries to stay undetected inside a network.

Argon2

Modernes Verfahren zum Hashen von Passwörtern, Gewinner des Password Hashing Competition; heute erste Wahl.

Modern password-hashing algorithm and winner of the Password Hashing Competition; the current first choice.

Array
Feld

Geordnete Sammlung mehrerer Werte unter einem Namen, erreichbar über eine Position (Index), die meist bei 0 beginnt.

An ordered collection of several values under one name, accessed by a position (index) that usually starts at 0.

ASCII
American Standard Code for Information Interchange

Zeichentabelle aus 128 Zeichen mit Codes 0–127: Buchstaben, Ziffern, Satzzeichen und Steuerzeichen.

A character table of 128 entries with codes 0–127: letters, digits, punctuation and control characters.

Attack Surface

Summe aller Angriffspunkte: offene Ports, APIs, Formulare, Konten, Abhängigkeiten, Mitarbeiter.

All points an attacker can try: open ports, APIs, forms, accounts, dependencies, people.

Attack Vector

Der konkrete Weg eines Angriffs im Internet, zum Beispiel eine Phishing-Mail oder eine ungeschützte API.

The concrete path an attack takes, for example a phishing mail or an unprotected API.

Audit-Log

Unveränderbares Protokoll: wer hat wann was getan. Grundlage für Forensik und Nachweise.

Tamper-proof record of who did what and when. Basis for forensics and audits.

Authentication

Wer bist du? Nachweis der Identität, etwa per Passwort, Token oder Zertifikat.

Who are you? Proving identity, for example with a password, token or certificate.

Authorization

Was darfst du? Prüfung der Rechte – erst nach erfolgreicher Anmeldung sinnvoll.

What may you do? Checking permissions, meaningful only after a successful login.

Availability

Verfügbarkeit: Systeme müssen erreichbar bleiben. Eines der drei Schutzziele der CIA-Triade.

Availability: systems must stay reachable. One of the three CIA-triad protection goals.

B

↑ Index

Backdoor

Heimlicher Zugang zu einem System – absichtlich eingebaut oder von Malware hinterlassen.

Hidden access path into a system, built in on purpose or left behind by malware.

Backend

Der Serverteil einer Anwendung: Geschäftslogik, Datenbank, Schnittstellen.

The server side of an application: business logic, database, interfaces.

Backlog

Geordnete Liste aller offenen Aufgaben – priorisiert, aber nicht terminiert.

The ordered list of all open work – prioritised but not scheduled.

Backup

Eine Sicherungskopie von Daten und Konfiguration, aus der man im Schadensfall wiederherstellen kann.

A copy of data and configuration from which you can restore after damage.

Bandbreite

Wie viel Daten in einer bestimmten Zeit übertragen werden können – die Breite der Leitung, nicht die Geschwindigkeit eines einzelnen Pakets.

How much data can be transferred in a given time – the width of the line, not the speed of a single packet.

Base64

Base 64

Kodierung, die Binärdaten als Text darstellt. Wichtig: Base64 ist Verschlüsselung nicht – jeder kann es zurückrechnen.

Encoding that turns binary data into text. Important: Base64 is not encryption – anyone can reverse it.

bcrypt

Bewährtes Passwort-Hash-Verfahren mit einstellbarer Rechenzeit, das Hashes absichtlich langsam macht.

Long-standing password-hashing function with adjustable cost that deliberately keeps hashing slow.

Bearer Token

Inhaber-Token: Wer ihn vorzeigen kann, gilt als berechtigt. Darum nie in URLs, Logs oder Screenshots preisgeben.

Holder token: whoever can present it counts as authorised. Never leak it in URLs, logs or screenshots.

Bedingung

Anweisung, die nur ausgeführt wird, wenn ein Ausdruck wahr ist – das if/else des Programms.

A statement executed only when an expression is true – the if/else of a program.

Benutzer

Benutzerkonto

Eine Identität im System, unter der jemand arbeitet – mit eigenem Namen, eigenem Passwort und eigenen Rechten.

An identity in the system that someone works under – own name, own password, own rights.

Berechtigung

Recht

Erlaubnis, eine bestimmte Sache zu tun – lesen, schreiben, löschen. Sie hängt an Rolle, Gruppe oder Person.

Permission to do a specific thing – read, write, delete. It attaches to a role, group or person.

Betriebssystem

Die Grundsoftware eines Rechners, die Programme startet und Hardware wie Speicher, Festplatte und Netzwerk verwaltet.

A machine's base software that starts programs and manages hardware such as memory, disk and network.

BFLA

Broken Function Level Authorization

Schwachstelle, bei der normale Nutzer Funktionen für Administratoren aufrufen dürfen (OWASP API #5).

Flaw that lets ordinary users call administrator-level functions (OWASP API #5).

Bikeshedding

Ausgiebiges Streiten über Nebensächlichkeiten, während die großen Fragen offen bleiben – benannt nach dem Beispiel Fahrradschuppen.

Arguing at length about trivia while big questions stay open – named after the bicycle shed example.

Binärsystem

Zahlensystem mit nur zwei Ziffern (0 und 1). Rechner rechnen damit, weil sich zwei Zustände – Strom an, Strom aus – technisch sauber unterscheiden lassen.

A number system with only two digits (0 and 1). Computers calculate with it because two states – current on, current off – can be distinguished reliably.

Bit

Binary Digit

Kleinste Informationseinheit eines Rechners: entweder 0 oder 1 – wie ein Lichtschalter, der an oder aus ist.

The smallest unit of information in a computer: either 0 or 1 – like a light switch that is on or off.

Bitmaske

Muster aus Bits, mit dem man einzelne Bits einer Zahl gezielt prüft oder setzt – typisch für Rechte, Flags und Hardware-Register.

A bit pattern used to test or set individual bits of a number – typical for permissions, flags and hardware registers.

Bit-Shifting

Verschieben der Bits einer Zahl nach links oder rechts – im Kern eine Multiplikation oder Division mit Zweierpotenzen, sehr schnell für den Prozessor.

Shifting the bits of a number left or right – essentially multiplying or dividing by powers of two, very fast for the processor.

Blameless Postmortem

Auswertung ohne Schuldzuweisung – Ziel ist der Systemfehler, nicht die Person, die ihn ausgelöst hat.

A review without blame – the goal is the system flaw, not the person who triggered it.

Blocker

Problem, das jede weitere Arbeit an einer Aufgabe verhindert – muss zuerst gelöst werden.

A problem that prevents any further work on a task – it must be solved first.

Blue Team

Die Verteidiger im Sicherheitsteam: überwachen, erkennen und reagieren auf Angriffe.

The defensive side of a security team: monitor, detect and respond to attacks.

Boilerplate

Immer wiederkehrender Standardcode, der nichts Fachliches tut – Konfiguration, Rahmen, Wiederholungen.

Repeated standard code that does nothing domain-specific – configuration, scaffolding, repetition.

BOLA

Broken Object Level Authorization

Häufigste API-Schwachstelle: die API prüft nur die Objekt-ID, nicht den Besitzer – fremde Datensätze werden sichtbar (OWASP API #1).

Most common API flaw: the API checks the object ID but not the owner, exposing other users' records (OWASP API #1).

Boolean

Wahrheitswert

Datentyp mit genau zwei Werten: wahr oder falsch. Grundlage jeder Bedingung im Programm.

A data type with exactly two values: true or false. The foundation of every condition in a program.

BOPLA

Broken Object Property Level Authorization

Schwachstelle, bei der einzelne Felder eines Datensatzes ungeschützt sind: Die Anwendung liefert zu viele Felder aus oder akzeptiert Felder, die der Nutzer nicht ändern darf.

A flaw where individual fields of a record are unprotected: the application returns too many fields or accepts fields the user must not change.

Botnet

robot network

Viele gekaperte Rechner, die gemeinsam angreifen, Spam versenden oder Kryptowährung schürfen.

Many hijacked machines that attack, send spam or mine crypto together.

Branch

Zweig

Abzweigung in der Versionskontrolle, in der man ungestört arbeiten kann, ohne den Hauptstand zu verändern.

A fork in version control where you can work undisturbed without touching the main line.

Breakpoint

Halterpunkt

Festgelegte Breite, ab der ein Layout umschaltet – etwa 720 Pixel: darunter Handy-Ansicht, darüber Desktop.

A defined width where a layout switches – 720 pixels, for example: below it the phone view, above it desktop.

Broken Access Control

Sammelbegriff für fehlerhafte Rechteprüfung: Ein Nutzer kommt an Daten oder Funktionen, die ihm nicht zustehen – Platz 1 der OWASP Top 10.

A collective term for faulty permission checks: a user reaches data or functions they are not entitled to – number one in the OWASP Top 10.

Browser

Das Programm, mit dem man Webseiten öffnet – es holt die Inhalte, baut die Seite auf und führt Skripte aus.

The program used to open websites – it fetches content, builds the page and runs scripts.

Brute Force

Systematisches Durchprobieren von Passwörtern oder Schlüsseln, bis eines passt.

Systematically trying passwords or keys until one works.

BSI

Bundesamt für Sicherheit in der Informationstechnik

Deutsche Behörde für IT-Sicherheit. Veröffentlicht Warnungen, IT-Grundschutz-Kataloge und Handlungsempfehlungen.

German federal cyber-security authority publishing warnings, IT baseline protection catalogues and guidance.

Bug Bounty

Programm, das Finder von Sicherheitslücken belohnt – statt sie zu verklagen.

Programme that pays researchers for reporting vulnerabilities instead of suing them.

Bundler

Werkzeug, das viele Dateien und Bibliotheken zu wenigen Paketen zusammenfasst, damit der Browser weniger laden muss.

A tool that packs many files and libraries into a few bundles so the browser has less to load.

Business Logic Flaw

Schwachstelle nicht im Code, sondern im Geschäftsablauf: Die Anwendung tut genau, was programmiert ist – erlaubt aber eine Reihenfolge oder Menge, die nie vorgesehen war.

A flaw not in the code but in the business process: the application does exactly what it was programmed to do but allows an order or quantity never intended.

Byte

Gruppe von acht Bits – die übliche Einheit, in der Daten gemessen werden: ein Zeichen im Text, ein Farbwert, ein Messwert.

A group of eight bits – the usual unit for measuring data: one character of text, one colour value, one reading.

C

↑ Index

CA

Certificate Authority

Stelle, die TLS-Zertifikate signiert und damit bestätigt, dass ein Schlüssel zu einer Domain gehört.

Entity that signs TLS certificates, vouching that a key belongs to a domain.

Cache Poisoning

Angriff, bei dem ein Zwischenspeicher mit einer manipulierten Antwort gefüttert wird, die anschließend allen Besuchern ausgeliefert wird – ein Treffer, viele Opfer.

An attack that feeds a cache a tampered response which is then served to all visitors – one hit, many victims.

Callback

Vereinbarte Rücksprung-Adresse: der Server ruft später den Client oder eine andere URL auf.

Agreed return address: the server calls the client or another URL back later.

CAPTCHA

Completely Automated Public Turing test to tell Computers and Humans Apart

Test, der Mensch und Bot unterscheiden soll, etwa durch Bilderrätsel.

Test meant to separate humans from bots, for example with image puzzles.

Certbot

Das Programm, das Sicherheitszertifikate bei Let's Encrypt beantragt, einrichtet und automatisch erneuert.

The program that requests, installs and automatically renews certificates from Let's Encrypt.

Certificate Pinning

Die App akzeptiert nur ein ganz bestimmtes Zertifikat. Das schützt auch dann, wenn eine Zertifizierungsstelle kompromittiert ist.

The app accepts only one specific certificate, which protects even if a certificate authority is compromised.

Checksum

Kurzer Prüfwert, der erkennt, ob Daten unbemerkt verändert wurden – etwa bei Downloads.

Short value revealing whether data changed unnoticed, for example after a download.

chmod

Legt fest, wer eine Datei lesen, schreiben oder ausführen darf – unterschieden nach Eigentümer, Gruppe und allen anderen.

Defines who may read, write or execute a file – separately for owner, group and everyone else.

CI/CD

Eine automatisierte Kette: Code-Änderungen werden geprüft, getestet, gebaut und ausgeliefert, ohne Handarbeit.

An automated pipeline: code changes are checked, tested, built and shipped without manual work.

CIDR

Classless Inter-Domain Routing

Schreibweise für IP-Bereiche: 10.0.0.0/24 bedeutet 256 Adressen von 10.0.0.0 bis 10.0.0.255.

Notation for IP ranges: 10.0.0.0/24 means 256 addresses from 10.0.0.0 to 10.0.0.255.

Cipher

Ein Verschlüsselungsverfahren beziehungsweise der zugehörige Algorithmus.

A cryptographic algorithm used for encryption.

CIS Benchmark

Center for Internet Security Benchmark

Abgestimmte Härtungsempfehlungen für Betriebssysteme und Software: welche Dienste abzuschalten, welche Einstellungen zu setzen sind.

Consensus hardening recommendations for operating systems and software: which services to disable, which settings to apply.

CISO

Chief Information Security Officer

Die für Informationssicherheit verantwortliche Führungsperson im Unternehmen.

The executive responsible for an organisation's information security.

CLI

Command Line Interface

Arbeit über die Kommandozeile mit getippten Befehlen statt per Maus und Fenster.

Working through typed commands on a command line instead of with mouse and windows.

Clickjacking

Eine unsichtbare Schicht über einer Webseite lässt Nutzer unbemerkt klicken. Abwehr: Header X-Frame-Options.

An invisible layer over a page makes users click without realising. Defence: the X-Frame-Options header.

Client

Das Programm oder Gerät, das etwas anfragt – der Gegenpart zum Server. Dein Browser ist ein Client, deine Handy-App auch.

The program or device asking for something – the counterpart to the server. Your browser is a client, so is your phone app.

Client Credentials

OAuth-Ablauf für Maschinen: Die Anwendung weist sich mit ihrer Kennung und ihrem Geheimnis aus und erhält dafür ein Token.

The OAuth flow for machines: the application identifies itself with its ID and secret and receives a token in return.

Cloud

Gemietete Rechenleistung bei einem Anbieter statt eigener Server im Haus – bezahlt nach Nutzung.

Rented computing power from a provider instead of servers in your own building – paid by usage.

Code Review

Vier-Augen-Prinzip im Code: Eine zweite Person liest die Änderung, bevor sie zusammengeführt wird.

The four-eyes principle in code: a second person reads the change before it is merged.

Code Signing

Kryptografische Signatur von Software, damit das Gerät prüfen kann, ob sie vom Hersteller stammt und unverändert ist.

The cryptographic signing of software so a device can verify it comes from the vendor and is unaltered.

Command Injection

Ein Angreifer schleust Betriebssystem-Befehle über ein Eingabefeld ein und führt sie auf dem Server aus.

An attacker smuggles operating-system commands through an input field and runs them on the server.

Commit

Gespeicherter Zwischenstand in der Versionskontrolle mit einer Nachricht, was geändert wurde – der kleinste dokumentierte Schritt.

A saved snapshot in version control with a message saying what changed – the smallest documented step.

Compiler

Programm, das Quellcode vollständig in Maschinensprache übersetzt, bevor das Programm läuft – Fehler fallen früh auf.

A program that translates source code fully into machine language before it runs – errors surface early.

Compliance

Erfüllung von Vorgaben: Gesetze, Normen und Anforderungen aus Audits.

Meeting required rules: laws, standards and audit requirements.

Container

Abgeschottete, portable Laufzeitumgebung für eine Anwendung, etwa mit Docker.

Isolated, portable runtime for an application, for example with Docker.

Cookie

Kleines Datenpaket im Browser, das oft die Sitzung trägt. Sicher nur mit HttpOnly, Secure und SameSite.

Small data item in the browser that often carries the session. Secure only with HttpOnly, Secure and SameSite.

CORS
Cross-Origin Resource Sharing

Browser-Regeln, die festlegen, welche fremde Webseite eine API aufrufen darf.

Browser rules defining which foreign website may call an API.

Credential Stuffing

Gestohlene Passwortlisten werden automatisiert bei vielen anderen Diensten durchprobiert.

Stolen password lists are replayed automatically against many other services.

Cron

Zeitplaner unter Linux, der Befehle und Skripte regelmäßig ausführt.

Scheduler on Linux that runs commands and scripts on a timetable.

CSP
Content Security Policy

Sicherheits-Header, der dem Browser sagt, welche Skripte, Bilder und Quellen erlaubt sind.

Security header telling the browser which scripts, images and sources are allowed.

CSRF
Cross-Site Request Forgery

Eine fremde Seite lässt den eingeloggten Nutzer unbemerkt Aktionen ausführen. Abwehr: CSRF-Token und SameSite-Cookies.

A foreign page makes the logged-in user perform actions unnoticed. Defence: CSRF tokens and SameSite cookies.

CSS
Cascading Style Sheets

Regelwerk für das Aussehen einer Seite – Farben, Abstände, Schrift, Layout – getrennt von der Struktur in HTML.

The rule set for a page's appearance – colours, spacing, type, layout – kept separate from the HTML structure.

CVE
Common Vulnerabilities and Exposures

Eindeutige Nummer für eine bekannte Sicherheitslücke, zum Beispiel CVE-2024-12345.

Unique identifier for a known vulnerability, for example CVE-2024-12345.

CVSS
Common Vulnerability Scoring System

Punkteskala von 0 bis 10 für die Schwere einer Lücke: ab 7 hoch, ab 9 kritisch.

0 to 10 severity score for a vulnerability: 7 and above is high, 9 and above critical.

CWE
Common Weakness Enumeration

Systematische Nummerierung von Schwachstellenarten, nicht einzelner Vorfälle: CWE-79 steht zum Beispiel für Cross-Site Scripting.

A systematic numbering of weakness types, not individual incidents: CWE-79, for instance, stands for cross-site scripting.

D

↑ Index

Daemon

Ein Hintergrundprogramm, das dauerhaft läuft und auf Aufgaben wartet – ohne Fenster und ohne dass jemand es startet.

A background program that keeps running and waits for work – no window, nobody starting it by hand.

Daily / Standup

Kurzes tägliches Treffen im Stehen: Was ist geschafft, was kommt, was blockiert – maximal 15 Minuten.

A short daily standing meeting: what is done, what is next, what is blocked – fifteen minutes at most.

DAST

Dynamic Application Security Testing

Automatischer Sicherheitstest der laufenden Anwendung von außen, ohne Kenntnis des Quellcodes.

Automated black-box security test of the running application without source-code access.

Data Breach

Vorfall, bei dem geschützte Daten abfließen. Meist meldepflichtig, oft mit Fristen von 72 Stunden.

Incident in which protected data leaks. Often must be reported, frequently within 72 hours.

Datei

Gespeicherte Daten unter einem Namen – ein Text, ein Bild, eine Konfiguration. Sie liegt in einem Verzeichnis und hat Rechte.

Stored data under a name – text, image, configuration. It lives in a directory and carries permissions.

Datenbank

Programm, das Daten dauerhaft und geordnet speichert und auf Anfragen hin wieder heraussucht – das Gedächtnis einer Anwendung.

A program that stores data permanently and in order and looks it up on request – an application's memory.

Datensatz

Alle Felder, die zusammengehören – eine Zeile in einer Tabelle, zum Beispiel ein kompletter Kunde.

All fields that belong together – one row in a table, a complete customer for instance.

Datentyp

Festlegung, welche Art von Wert in ein Feld darf – Zahl, Text, Datum, Ja/Nein. Verhindert, dass Unsinn hineingerät.

A definition of which kind of value a field accepts – number, text, date, yes/no. It stops nonsense getting in.

DDoS

Distributed Denial of Service

Viele Systeme überfluten gleichzeitig einen Dienst mit Anfragen, bis er nicht mehr antwortet.

Many systems flood a service with requests at once until it stops responding.

Debugging

Systematisches Aufspüren von Fehlern: Haltepunkte setzen, Werte beobachten, den Ablauf nachvollziehen – nicht raten.

Systematically tracking down bugs: setting breakpoints, watching values, following the flow – not guessing.

Deeplink

Direkter Link in eine App oder auf eine bestimmte Stelle darin – statt nur auf die Startseite.

A direct link into an app or a specific place inside it – not just to the start screen.

Defense in Depth

Mehrere Sicherheitsschichten hintereinander, damit eine einzelne Lücke nicht sofort alles öffnet.

Several security layers in a row so a single flaw does not open everything.

Dependency

Fremdes Software-Paket, das der eigene Code benötigt – Angriffsfläche und Pflegeaufwand zugleich.

A third-party package the code depends on – both attack surface and maintenance burden.

Dependency Confusion

Angriff auf die Paketversorgung: Ein intern verwendeter Paketname wird in einem öffentlichen Repository registriert, weil das Build-System öffentliche Quellen bevorzugt – und der fremde Code landet im Produkt.

An attack on package supply: a package name used internally is registered in a public repository, the build system prefers public sources, and foreign code ends up in the product.

Deserialization

Rückverwandlung von Daten in Objekte. Ohne Prüfung ein beliebter Weg, fremden Code auszuführen.

Turning data back into objects. Without validation a popular route for executing foreign code.

DevSecOps

Development, Security and Operations

Sicherheit ist fest in Entwicklung und Betrieb eingebaut statt nachträglich geprüft.

Security is built into development and operations instead of being checked afterwards.

DHCP
Dynamic Host Configuration Protocol

Verteilt IP-Adressen und Netzwerkeinstellungen automatisch an Geräte im Netz.

Hands out IP addresses and network settings to devices automatically.

Dienst
Service

Ein Programm im Hintergrund, das eine Aufgabe für andere erledigt – Mailversand, Suche, Sicherung.

A background program that does a job for others – sending mail, searching, backing up.

Digital Signature

Kryptografische Unterschrift: beweist Herkunft und Unverändertheit eines Dokuments oder Tokens.

Cryptographic signature proving origin and integrity of a document or token.

Django

Ein vollständiges Python-Framework mit Datenbankanbindung, Verwaltungsoberfläche und Nutzerverwaltung.

A full-featured Python framework with database layer, admin interface and user management.

DMZ
Demilitarized Zone

Abgetrennter Netzbereich für öffentlich erreichbare Server, getrennt vom internen Netz.

Segregated network zone for publicly reachable servers, separated from the internal network.

DNS
Domain Name System

Übersetzt Namen wie example.com in IP-Adressen – das Telefonbuch des Internets.

Translates names such as example.com into IP addresses – the internet's phone book.

Docker

Verbreitete Container-Plattform, um Anwendungen samt Umgebung zu bauen und auszuführen.

Widely used container platform for building and running applications with their environment.

Dogfooding

Das eigene Produkt selbst benutzen, um Schwächen zu finden, bevor es Kunden tun.

Using your own product to find weaknesses before customers do.

DOM
Document Object Model

Objektmodell, in das der Browser eine Seite zerlegt – jedes Element wird zu einem Knoten, den Skripte lesen und verändern können.

The object model a browser builds from a page – every element becomes a node that scripts can read and change.

DPO
Data Protection Officer

Datenschutzbeauftragter: überwacht die Einhaltung der DSGVO im Unternehmen.

Data protection officer who oversees GDPR compliance in an organisation.

DRY
Don't Repeat Yourself

Prinzip: Eine Regel soll nur an einer Stelle stehen, sonst muss man sie überall gleichzeitig ändern.

A principle: a rule should live in exactly one place, or you must change it everywhere at once.

DSFA
Datenschutz-Folgenabschätzung

Pflichtprüfung bei riskanter Datenverarbeitung nach Artikel 35 DSGVO, englisch DPIA.

Mandatory assessment for high-risk data processing under Article 35 GDPR, also called DPIA.

DSGVO / GDPR
Datenschutz-Grundverordnung / General Data Protection Regulation

EU-Datenschutzrecht: regelt, was mit personenbezogenen Daten erlaubt ist und welche Rechte Betroffene haben.

EU privacy law governing what may be done with personal data and which rights individuals have.

E

↑ Index

E2E-Verschlüsselung
End to End

Nur Sender und Empfänger können mitlesen; der Transportweg sieht nur verschlüsselte Daten.

Only sender and receiver can read the content; the transport path sees encrypted data only.

EDR
Endpoint Detection and Response

Schutzsoftware auf Endgeräten, die Verhalten beobachtet, Angriffe erkennt und darauf reagiert.

Protective software on devices that watches behaviour, detects attacks and responds to them.

Egress Filtering
Ausgangskontrolle: legt fest, wohin ein Server überhaupt Verbindungen aufbauen darf.

Outbound control: defines where a server is even allowed to connect to.

Emulator

Programm, das ein anderes Gerät vollständig nachbildet – inklusive Prozessorarchitektur – damit Software dafür läuft.

Software that fully imitates another device, including its processor architecture, so software for it can run.

Encoding

Umwandlung von Daten in eine andere Darstellung, etwa URL-Encoding für Sonderzeichen. Keine Verschlüsselung.

Converting data into another representation, such as URL encoding for special characters. Not encryption.

Encryption

Verschlüsselung: Daten werden mit einem Schlüssel unlesbar gemacht und sind ohne Schlüssel wertlos.

Encryption: data is made unreadable with a key and is worthless without that key.

Endpoint

Eine ansprechbare Adresse einer API – im weiteren Sinn auch ein Endgerät wie Laptop oder Handy.

A callable address of an API – and more broadly any device such as a laptop or phone.

Entropy

Maß für Zufälligkeit. Passwörter und Schlüssel brauchen hohe Entropie, damit sie nicht erratbar sind.

A measure of randomness. Passwords and keys need high entropy so they cannot be guessed.

Enumeration

Systematisches Durchzählen möglicher Werte, etwa Benutzernamen oder IDs, um Gültiges zu finden.

Systematically walking through possible values such as usernames or IDs to find valid ones.

Environment Variable

Ein Wert, den man einem Programm von außen mitgibt – etwa Zugangsdaten oder Betriebsmodus – statt ihn im Quellcode zu hinterlegen.

A value passed to a program from outside – credentials or mode settings – instead of hard-coding it in the source.

EOL

End of Life

Produkt wird nicht mehr gepflegt und bekommt keine Sicherheitsupdates mehr – ein Risiko.

A product no longer maintained and no longer receiving security updates – a risk.

Epic

Grosse Aufgabe, die in mehrere kleinere Tickets zerlegt wird – der Rahmen für Wochen Arbeit.

A large piece of work broken into smaller tickets – the frame for weeks of work.

EPSS
Exploit Prediction Scoring System

Schätzwert zwischen 0 und 1, wie wahrscheinlich eine Lücke innerhalb der nächsten 30 Tage ausgenutzt wird – ergänzt die Schwere um die Wahrscheinlichkeit.

An estimate between 0 and 1 of how likely a flaw is to be exploited within the next 30 days – it adds likelihood to severity.

Escaping

Sonderzeichen in Eingaben werden unschädlich gemacht, damit sie nicht als Code oder SQL wirken.

Making special characters in input harmless so they cannot act as code or SQL.

ETA
Estimated Time of Arrival

Voraussichtlicher Zeitpunkt der Fertigstellung – im Projektalltag die Antwort auf „wann ist es fertig?“.

The expected completion time – in day-to-day project work the answer to “when will it be done?”.

Exception
Ausnahme

Ein Fehlerzustand, den ein Programm gezielt behandeln kann, statt abzustürzen – etwa „Datei nicht gefunden“.

An error state a program can handle deliberately instead of crashing – “file not found”, for instance.

Exploit

Ein ausnutzbarer Fehler – oder das konkrete Werkzeug, mit dem ein Angreifer ihn ausnutzt.

An exploitable flaw – or the concrete tool an attacker uses to exploit it.

F

↑ Index

fail2ban

Ein Dienst, der Protokolle beobachtet und IP-Adressen nach zu vielen Fehlversuchen sperrt – typisch für Anmelde- und SSH-Versuche.

A service that watches logs and blocks IP addresses after too many failed attempts – typical for logins and SSH.

False Positive

Fehlalarm: das System meldet einen Angriff, der keiner ist. Zu viele davon machen Warnungen wertlos.

False alarm: the system reports an attack that is not one. Too many make alerts worthless.

Feature Flag

Schalter im Code, mit dem sich eine Funktion ohne neue Auslieferung ein- oder ausschalten lässt – auch für einzelne Nutzergruppen.

A switch in the code that enables or disables a feature without a new release – also for specific user groups.

Federated Identity

Ein Konto gilt über mehrere Systeme hinweg, etwa Anmeldung bei vielen Diensten über einen Anbieter.

One identity works across several systems, e.g. logging into many services through one provider.

Feld

Ein benannter Platz für einen Wert in einer Datenstruktur – die Spalte eines Datensatzes.

A named slot for a value in a data structure – the column of a record.

FIDO2

Fast Identity Online 2

Standard für passwortlose Anmeldung mit Hardware-Schlüssel oder Fingerabdruck.

Standard for passwordless login using a hardware key or fingerprint.

Fingerprinting

Erkennen von Systemen oder Nutzern anhand von Merkmalen wie Browserkennung oder Verhalten.

Recognising systems or users by traits such as browser signature or behaviour.

Firewall

Türsteher für Netzwerkverkehr: erlaubt oder blockt Verbindungen nach festen Regeln.

Gatekeeper for network traffic: allows or blocks connections by fixed rules.

Firmware

Feste Software in Hardware, etwa im Router oder in der Kamera. Wird selten aktualisiert und ist darum beliebt bei Angreifern.

Software baked into hardware, e.g. in a router or camera. Rarely updated and therefore popular with attackers.

Flaky Test

Test, der ohne Codeänderung manchmal besteht und manchmal scheitert – meist wegen Zeitabhängigkeit oder Reihenfolge.

A test that sometimes passes and sometimes fails without any code change – usually timing or ordering.

Flask

Ein schlankes Python-Framework für kleine Webanwendungen und Programmierschnittstellen.

A lightweight Python framework for small web applications and APIs.

Float

Gleitkommazahl

Datentyp für Zahlen mit Nachkommastellen. Intern binär gespeichert, wodurch kleine Rundungsfehler entstehen können.

A data type for numbers with decimals. Stored in binary internally, which can produce small rounding errors.

Flutter

Framework von Google, mit dem man aus einer Codebasis Apps für Android und iOS baut – eigene Oberflächen, nicht die des Systems.

Google's framework for building Android and iOS apps from one codebase – its own interface elements, not the system's.

Foo / Bar

Platzhalter-Namen in Beispielen, wenn der eigentliche Name egal ist – „Foo“ und „Bar“ sind reine Konvention.

Placeholder names in examples where the real name does not matter – “foo” and “bar” are pure convention.

Forensics

Digitale Forensik: nach einem Vorfall rekonstruieren, was passiert ist und wer es getan hat.

Digital forensics: reconstructing after an incident what happened and who did it.

Forward Proxy

Vermittler, der im Auftrag der Clients nach außen geht, etwa für Filterung oder Anonymisierung.

Intermediary that goes outward on behalf of clients, e.g. for filtering or anonymity.

Four-Eyes Principle

Vier-Augen-Prinzip: Kritische Aktionen brauchen die Bestätigung einer zweiten berechtigten Person.

The four-eyes principle: critical actions require confirmation by a second authorised person.

Framework

Vorgefertigtes Gerüst, das den Aufbau einer Anwendung vorgibt und viele Aufgaben abnimmt – man füllt Lücken, statt alles selbst zu bauen.

A prepared scaffold that prescribes an application's structure and does much of the work – you fill gaps instead of building everything.

Funktion

Benannter Block von Anweisungen, der eine Aufgabe erledigt, Eingaben verarbeitet und ein Ergebnis zurückgibt – einmal geschrieben, beliebig oft genutzt.

A named block of statements that performs a task, processes input and returns a result – written once, used often.

Fuzzing

Automatisches Testen mit zufälligen oder bewusst kaputten Daten, um Abstürze und Fehler zu finden.

Automated testing with random or deliberately broken data to find crashes and bugs.

FYI

For Your Information

Zur Kenntnis, keine Aktion nötig – kennzeichnet Mitteilungen ohne Handlungsbedarf.

For your information, no action needed – marks messages that require nothing from you.

G

↑ Index

Gated

Feature Gate

Zustand, in dem eine Funktion nur nach einer Prüfung erreichbar ist – hinter einer Freigabe, einem Schalter, einem Login oder einer Zahlung.

A state where a feature is reachable only after a check – behind an approval, a switch, a login or a payment.

Gateway

Übergang zwischen zwei Netzen oder Systemen, der Daten umsetzt und weiterleitet.

A boundary between two networks or systems that translates and forwards data.

GET-Request

GET

HTTP-Methode zum Lesen von Daten. Darf nichts verändern und sollte keine Geheimnisse in der URL tragen.

HTTP method for reading data. Must not change anything and should not carry secrets in the URL.

GraphQL

Graph Query Language

Abfragesprache für APIs, bei der der Client selbst bestimmt, welche Felder er bekommt.

API query language where the client decides which fields it receives.

gRPC

gRPC Remote Procedure Call

Schnelles Binärprotokoll für API-Aufrufe, auf HTTP/2 und Protobuf basierend.

Fast binary protocol for API calls, built on HTTP/2 and Protobuf.

Gunicorn

Ein Anwendungsserver, der Python-Webanwendungen im Betrieb ausführt – mit mehreren Arbeitsprozessen parallel.

An application server that runs Python web applications in production – with several worker processes in parallel.

H

↑ Index

Hardening

Härtung: ein System absichtlich robuster machen – unnötige Dienste abschalten, Rechte beschränken, absichern.

Hardening: deliberately making a system more robust by disabling unneeded services and limiting rights.

Hardware

Die greifbaren Teile eines Systems: Rechner, Festplatten, Kabel, Prozessor, Netzwerktechnik.

The tangible parts of a system: machines, disks, cables, processor, network equipment.

Hash

Fingerabdruck aus Daten, der nicht zurückgerechnet werden kann. Gleiche Eingabe ergibt immer denselben Hash.

A fingerprint derived from data that cannot be reversed. The same input always gives the same hash.

Header

Kopfzeile einer HTTP-Nachricht mit Metadaten wie Content-Type, Authorization oder User-Agent.

Header line of an HTTP message carrying metadata such as Content-Type, Authorization or User-Agent.

Health Check

Eine kleine Abfrage, die prüft, ob ein Dienst wirklich arbeitet – nicht nur, ob der Prozess läuft.

A small query that checks whether a service really works – not merely whether the process exists.

Heap

Frei verwalteter Speicherbereich für Objekte, deren Größe erst zur Laufzeit feststeht – langsamer als der Stack.

A freely managed memory area for objects whose size is only known at runtime – slower than the stack.

Hello World

Erstes Minimalprogramm, das nur eine Begrüßung ausgibt – Test, ob Werkzeuge und Umgebung überhaupt funktionieren.

The first minimal program that prints a greeting – a test that tools and environment work at all.

Hexadezimal

Schreibweise für Zahlen zur Basis 16 (Ziffern 0–9 und A–F). Weil 16 eine Zweierpotenz ist, lässt sich jede Binärzahl kurz und verlustfrei darstellen.

A base-16 notation (digits 0–9 and A–F). Because 16 is a power of two, any binary number can be written shortly and without loss.

HMAC

Hash-based Message Authentication Code

Signatur aus Nachricht und geheimem Schlüssel: beweist, dass die Nachricht echt und unverändert ist.

Signature built from message and secret key, proving the message is genuine and unchanged.

Honeypot

Absichtliche Köder-Systeme, die niemand legal nutzen würde – sie verraten Angreifer und ihre Methoden.

Deliberate decoy systems that no legitimate user would touch, revealing attackers and their methods.

Host Header Injection

Schwachstelle, bei der eine Anwendung den Host-Kopf der Anfrage ungeprüft übernimmt – etwa für Links in Mails. Angreifer können so Passwort-Links auf ihre Seite umleiten.

A flaw where an application takes the request's host header unchecked – for links in emails, say – letting attackers redirect password links to their own site.

Hostname

Der Name eines Rechners im Netz, zum Beispiel shop.example – der Mensch liest ihn, das System übersetzt ihn in eine Adresse.

A machine's name on the network, shop.example for instance – humans read it, the system translates it into an address.

Hotfix

Schnelle Korrektur ausserhalb des normalen Ablaufs, wenn ein Fehler den Betrieb blockiert.

A quick fix outside the normal process when a bug blocks operations.

HSM

Hardware Security Module

Spezielles Gerät, das kryptografische Schlüssel schützt und Rechenoperationen ausführt, ohne sie herauszugeben.

Dedicated device that protects cryptographic keys and performs operations without releasing them.

HSTS

HTTP Strict Transport Security

Header, der den Browser zwingt, eine Seite künftig nur noch über HTTPS zu laden.

Header forcing the browser to load a site over HTTPS only from then on.

↑ Index

.htaccess

Eine versteckte Konfigurationsdatei im Web-Verzeichnis, die Apache pro Ordner liest – für Weiterleitungen, Zugriffsschutz und Umschreibe-Regeln.

A hidden configuration file in the web directory that Apache reads per folder – for redirects, access control and rewrite rules.

H

↑ Index

HTML
Hypertext Markup Language

Auszeichnungssprache, die festlegt, was auf einer Seite steht: Überschrift, Absatz, Bild, Formular – die Struktur, nicht das Aussehen.

The markup language describing what is on a page: heading, paragraph, image, form – structure, not appearance.

HTTP-Methoden
HTTP Methods

GET liest, POST legt an, PUT ersetzt, PATCH ändert teilweise, DELETE löscht.

GET reads, POST creates, PUT replaces, PATCH partially updates, DELETE removes.

HTTP Request Smuggling

Angriff zwischen zwei Servern, die sich über die Länge einer Anfrage uneinig sind: Ein Teil der Anfrage wird als nächste Anfrage eines anderen Nutzers ausgeführt.

An attack between two servers that disagree about a request's length: part of one request is executed as the next request from another user.

HTTPS
Hypertext Transfer Protocol Secure

HTTP über eine TLS-verschlüsselte Verbindung – heute Pflicht für jede Website.

HTTP over a TLS-encrypted connection – mandatory for any website today.

HTTP-Statuscode
HTTP Status Code

Dreistellige Antwort: 200 ok, 201 angelegt, 400 fehlerhafte Anfrage, 401 nicht eingeloggt, 403 verboten, 404 nicht gefunden, 429 zu viele Anfragen, 500 Serverfehler.

Three-digit answer: 200 ok, 201 created, 400 bad request, 401 not logged in, 403 forbidden, 404 not found, 429 too many requests, 500 server error.

I

↑ Index

IAM
Identity and Access Management

Gesamtsystem für Benutzerkonten, Rollen und Rechte, inklusive Anmelde- und Löschprozessen.

The overall system for accounts, roles and permissions, including joiner-mover-leaver processes.

Idempotenz

Gleicher Aufruf mehrfach ausgeführt führt zum selben Ergebnis – wichtig für sichere Wiederholungen.

Calling the same request repeatedly yields the same result – essential for safe retries.

Identity Provider

Stelle, die Anmeldungen prüft und bestätigt, etwa Keycloak, Entra ID oder Google.

The party that verifies logins and vouches for them, e.g. Keycloak, Entra ID or Google.

IDOR

Insecure Direct Object Reference

Schwachstelle, bei der die Anwendung ein Objekt nur über eine ID anspricht und nicht prüft, ob es dem Anfragenden gehört – Kunde A sieht die Rechnung von Kunde B, weil er die Nummer ändert.

A flaw where the application addresses an object only by its ID without checking that it belongs to the caller – customer A sees customer B's invoice by changing the number.

IDS

Intrusion Detection System

Erkennt Angriffe im Netzwerkverkehr und meldet sie – blockt aber nicht.

Detects attacks in network traffic and reports them, without blocking.

IMO

In My Opinion

„Meiner Meinung nach“ – kennzeichnet eine Einschätzung, nicht eine Tatsache.

“In my opinion” – marks an assessment rather than a fact.

Incident Response

Festgelegter Ablauf bei einem Sicherheitsvorfall: erkennen, eindämmen, beseitigen, lernen.

Defined procedure for a security incident: detect, contain, eradicate, learn.

Injection

Fremder Code oder fremde Befehle werden über eine Eingabe in eine Abfrage eingeschleust.

Foreign code or commands are smuggled into a query through an input.

Input Validation

Eingaben werden geprüft und nur erlaubte Formate zugelassen – erste Verteidigungslinie gegen Injection.

Input is checked and only allowed formats pass – the first line of defence against injection.

Insecure Design

Sicherheitslücke schon im Entwurf: sauber programmiert, aber das Konzept selbst erlaubt Missbrauch – nachträgliches Flicken hilft wenig.

A flaw present in the design: cleanly programmed, but the concept itself allows abuse – patching afterwards helps little.

Integer

Ganzzahl

Datentyp für ganze Zahlen ohne Nachkommastellen – üblich in 32 oder 64 Bit, mit festem Wertebereich.

A data type for whole numbers without decimals – usually 32 or 64 bit, with a fixed range.

Integrity

Unversehrtheit: Daten sind vollständig und wurden nicht unbemerkt verändert.

Integrity: data is complete and has not been changed unnoticed.

Interpreter

Programm, das Quellcode Anweisung für Anweisung ausführt, ohne vorher eine Datei zu erzeugen – langsamer, dafür flexibler.

A program that executes source code statement by statement without producing a file first – slower but more flexible.

IOC

Indicator of Compromise

Hinweis auf einen Angriff, etwa eine verdächtige IP, ein Datei-Hash oder eine Domain.

A sign of compromise, such as a suspicious IP, file hash or domain.

iOS

Mobiles Betriebssystem von Apple, das nur auf Apple-Geräten läuft – Apps kommen ausschließlich aus dem App Store oder per Test-Verteilung.

Apple's mobile operating system, running only on Apple devices – apps come solely from the App Store or via test distribution.

IPA

iOS App Store Package

Installationsdatei einer iOS-App – ohne signiertes Profil lässt sie sich auf keinem Gerät starten.

The install file of an iOS app – without a signed profile it will start on no device.

IP-Adresse

Numerische Adresse eines Geräts im Netz, etwa 192.0.2.10 oder als IPv6.

Numeric address of a device on a network, for example 192.0.2.10 or an IPv6 address.

IPS

Intrusion Prevention System

Erkennt Angriffe nicht nur, sondern blockt sie aktiv im laufenden Verkehr.

Not only detects attacks but actively blocks them in live traffic.

IPSec

Internet Protocol Security

Protokollfamilie, die IP-Verbindungen verschlüsselt – Grundlage vieler VPNs.

Protocol family that encrypts IP connections – the basis of many VPNs.

iptables

Die Regel-Engine der Linux-Firewall, auf der auch ufw aufsetzt: Sie filtert Pakete nach Adresse, Port und Protokoll.

The rule engine of the Linux firewall that ufw builds on: it filters packets by address, port and protocol.

ISO 27001
ISO/IEC 27001

Internationale Norm für ein Managementsystem für Informationssicherheit, oft als Zertifizierung gefordert.

International standard for an information security management system, often required as a certification.

Issue
Ticket

Eintrag in einem Aufgabenwerkzeug für einen Fehler, eine Aufgabe oder eine Idee – mit Zuständigkeit und Status.

An entry in a task tool for a bug, a task or an idea – with owner and status.

J

↑ Index

Jailbreak

Ausbruch aus einer Absicherung – bei Handys aus der Herstellersperre, bei KI-Modellen aus den Sicherheitsregeln.

Breaking out of a safeguard – of a phone's vendor lock, or of an AI model's safety rules.

JavaScript

Programmiersprache, die im Browser läuft und Seiten lebendig macht – Reaktionen auf Klicks, Nachladen von Daten, Animationen.

The programming language running in the browser that brings pages to life – reactions to clicks, loading data, animations.

J/C
Jira / Confluence

Kürzel für die beiden Atlassian-Werkzeuge: Jira für Tickets und Aufgaben, Confluence für Dokumentation und Wikis.

Shorthand for the two Atlassian tools: Jira for tickets and tasks, Confluence for documentation and wikis.

JIT Access
Just-in-Time Access

Berechtigungen werden nur für die Dauer einer Aufgabe vergeben und danach automatisch entzogen.

Permissions are granted only for the duration of a task and removed automatically afterwards.

journalctl

Das Werkzeug, um die Protokolle von systemd zu lesen: was gestartet wurde, was abgestürzt ist und mit welcher Fehlermeldung.

The tool for reading systemd's logs: what started, what crashed and with which error message.

JSON
JavaScript Object Notation

Textformat für strukturierte Daten mit Schlüsseln und Werten; Standard in modernen APIs.

Text format for structured data with keys and values; the standard in modern APIs.

JSON Schema
JavaScript Object Notation Schema

Regelwerk, das beschreibt, wie ein JSON-Dokument aufgebaut sein muss – für Prüfung und Dokumentation.

Rule set describing how a JSON document must be structured – for validation and documentation.

JWT
JSON Web Token

Signierter Ausweis im JSON-Format, oft als Access Token. Prüfen muss man Signatur, Ablaufzeit und Aussteller.

Signed credential in JSON format, often used as an access token. Validate signature, expiry and issuer.

K

↑ Index

Kanban
Arbeitsweise mit einem Brett aus Spalten (offen, in Arbeit, fertig), in dem Aufgaben sichtbar durchlaufen – ohne feste Sprints.

A working method with a board of columns (to do, doing, done) that tasks visibly flow through – without fixed sprints.

Kerberos
Klassisches Anmeldeverfahren in Firmennetzen, das Tickets statt Passwörter durchs Netz schickt.

Classic authentication protocol in corporate networks that sends tickets instead of passwords.

KEV
Known Exploited Vulnerabilities

Verzeichnis der US-Behörde CISA mit Lücken, die nachweislich aktiv ausgenutzt werden – die höchste Patch-Priorität.

A catalogue run by the US agency CISA listing flaws that are demonstrably exploited in the wild – the highest patching priority.

Key
Geheimer Wert, mit dem verschlüsselt, entschlüsselt oder signiert wird. Seine Sicherheit entscheidet über alles andere.

Secret value used to encrypt, decrypt or sign. Its safety decides everything else.

Keylogger

Schadsoftware oder Hardware, die Tastatureingaben mitschreibt – klassischer Passwortdiebstahl.

Malware or hardware that records keystrokes – classic password theft.

Key Rotation

Schlüssel werden regelmäßig ausgetauscht, damit ein unbemerkt gestohlener Schlüssel nur kurze Zeit nützt.

Keys are replaced regularly so a silently stolen key is only useful for a short time.

Kill Switch

Not-Aus, der einen Dienst, ein Feature oder einen Angriff sofort stoppt.

Emergency stop that halts a service, feature or attack immediately.

KISS

Keep It Simple, Stupid

Prinzip: Die einfachere Lösung ist meist die bessere – sie hat weniger Stellen, an denen etwas kaputtgehen kann.

A principle: the simpler solution is usually better – it has fewer places where things can break.

Konstante

Benannter Wert, der nach dem Setzen nicht mehr geändert werden darf – schützt vor versehentlichen Änderungen.

A named value that must not change after being set – it protects against accidental modification.

Konto

Zugang zu einem Dienst mit eigener Kennung – und der Ort, an dem Rechte und Daten dieser Person hängen.

Access to a service with its own identifier – and where that person's rights and data hang.

Kotlin

Moderne Programmiersprache, die auf der Java-Plattform läuft und für Android-Apps empfohlen wird.

A modern language running on the Java platform and recommended for Android apps.

Kubernetes

Plattform zum Betrieb vieler Container im Verbund, mit eigener Netzwerk- und Rechtewelt.

Platform for running many containers together, with its own networking and permission model.

L

↑ Index

Latency

Verzögerung zwischen Anfrage und Antwort. Hoch bei weiter Entfernung, Überlast oder zusätzlichen Prüfungen.

Delay between request and response. High with distance, overload or extra checks.

Lateral Movement

Ein Angreifer arbeitet sich seitwärts durchs Netz von einem System zum nächsten.

An attacker moves sideways through the network from one system to the next.

Laufzeit

Runtime

Die Umgebung, in der ein Programm tatsächlich läuft – inklusive benötigter Bibliotheken und Systemressourcen.

The environment in which a program actually runs – including required libraries and system resources.

LDAP

Lightweight Directory Access Protocol

Verzeichnisdienst, in dem Benutzer, Gruppen und Rechte liegen – Basis vieler Firmenanmeldungen.

Directory service holding users, groups and permissions – the base of many corporate logins.

LDAP Injection

Lightweight Directory Access Protocol Injection

Angriff, bei dem Eingaben ungefiltert in eine Verzeichnisabfrage fließen – der Angreifer kann damit Bedingungen verändern und etwa Anmeldungen umgehen oder Datensätze auslesen.

An attack where input flows unfiltered into a directory query – letting an attacker alter conditions, bypass logins or extract records.

Least Privilege

Grundsatz: jede Person und jeder Dienst bekommt nur die Rechte, die für die Aufgabe nötig sind.

Principle: every person and service gets only the permissions its task requires.

Legacy Code

Alter Code, der läuft, aber kaum verstanden oder getestet ist – jede Änderung ist riskant.

Old code that runs but is barely understood or tested – every change is risky.

Let's Encrypt

Eine gemeinnützige Zertifizierungsstelle, die Sicherheitszertifikate kostenlos ausstellt.

A non-profit certificate authority that issues security certificates for free.

LFI
Local File Inclusion

Angreifer bringt die Anwendung dazu, lokale Dateien des Servers einzubinden und auszulesen.

Attacker tricks the application into including and reading local files on the server.

LGTM
Looks Good To Me

Freigabe im Code-Review: „sieht für mich gut aus“.

Approval in a code review: “looks good to me”.

Library
Bibliothek

Sammlung fertiger Funktionen, die man gezielt aufruft – ohne dass sie den Aufbau des eigenen Programms bestimmt.

A collection of ready-made functions you call deliberately – without it dictating your program's structure.

Linter

Werkzeug, das Code auf Stilfehler und typische Fehler prüft, ohne ihn auszuführen – findet Unbenutztes, Tippfehler, Muster.

A tool that checks code for style and typical mistakes without running it – unused variables, typos, patterns.

Load Balancer

Verteilt Anfragen auf mehrere Server, damit keiner überlastet und ein Ausfall verkraftbar ist.

Distributes requests across servers so none is overloaded and an outage can be absorbed.

LocalStorage

Kleiner Speicher im Browser für Einstellungen, die bleiben sollen – etwa die gewählte Sprache oder der Dark Mode.

A small browser store for settings that should persist – the chosen language or dark mode, for instance.

Logging

Aufzeichnung von Ereignissen. Ohne Logs gibt es keinen Nachweis, keine Warnung und keine Forensik.

Recording of events. Without logs there is no evidence, no alert and no forensics.

LOL
Laughing Out Loud

Chat-Kürzel für lautes Lachen – in Fachkreisen auch ironisch benutzt, wenn etwas offensichtlich schiefgelaufen ist.

Chat shorthand for laughing out loud – also used ironically in technical circles when something went obviously wrong.

LUKS
Linux Unified Key Setup

Standardverfahren zur vollständigen Verschlüsselung von Festplatten unter Linux.

Standard for full-disk encryption on Linux.

M

↑ Index

Malware
Malicious Software

Sammelbegriff für Schadsoftware: Viren, Würmer, Trojaner, Ransomware, Spyware.

Collective term for harmful software: viruses, worms, trojans, ransomware, spyware.

Mass Assignment

Schwachstelle, bei der eine Anwendung eingereichte Felder ungeprüft in ein Datenmodell übernimmt – der Nutzer kann dadurch Eigenschaften setzen, die er nie setzen sollte.

A flaw where an application copies submitted fields into a data model unchecked – letting a user set properties they should never set.

Media Query

CSS-Regel, die nur unter bestimmten Bedingungen gilt – etwa „ab 720 Pixel Breite“ oder „beim Drucken“.

A CSS rule that applies only under certain conditions – “from 720 pixels wide”, or “when printing”.

Merge

Zusammenführen zweier Zweige – dabei können Konflikte entstehen, wenn dieselbe Stelle in beiden geändert wurde.

Joining two branches – conflicts arise when the same place was changed in both.

MFA
Multi-Factor Authentication

Anmeldung mit mindestens zwei Faktoren: Wissen (Passwort), Besitz (Handy, Schlüssel), Biometrie.

Login with at least two factors: knowledge (password), possession (phone, key), biometrics.

Microservice

Kleiner, eigenständig betreibbarer Dienst mit klarer Aufgabe, meist über APIs verbunden.

Small, independently deployable service with one clear job, usually connected via APIs.

Middleware

Zwischenschicht im Code, die Anfragen vor der eigentlichen Logik prüft, ergänzt oder protokolliert.

Layer in the code that checks, enriches or logs requests before the actual logic runs.

Minify

Code von Leerzeichen, Kommentaren und langen Namen befreien, damit die Datei kleiner wird – Lesbarkeit geht verloren, Funktion nicht.

Stripping code of spaces, comments and long names to shrink the file – readability is lost, behaviour is not.

MITM

Man in the Middle

Angreifer sitzt zwischen den Parteien, liest mit und kann Inhalte unbemerkt verändern.

Attacker sits between the parties, reads along and can alter content unnoticed.

MITRE ATT&CK

Adversarial Tactics, Techniques and Common Knowledge

Öffentliche Wissensbasis über Angriffstaktiken und -techniken; Grundlage für Erkennung und Tests.

Public knowledge base of attacker tactics and techniques; the basis for detection and testing.

Mock

Attrappe einer Funktion oder API, damit Tests ohne echten Server laufen können.

Stand-in for a function or API so tests can run without a real server.

mod_rewrite

Das Apache-Modul, das angefragte Adressen intern umschreibt – Grundlage für schöne URLs und Weiterleitungen.

The Apache module that rewrites requested addresses internally – the basis for pretty URLs and redirects.

Monitoring

Das laufende Beobachten von Verfügbarkeit und Ressourcen, mit Alarm, wenn etwas aus dem Rahmen fällt.

Continuous observation of availability and resources, with alerts when something leaves the normal range.

mTLS

mutual TLS

Beide Seiten einer Verbindung weisen sich mit einem Zertifikat aus – nicht nur der Server, sondern auch der Client.

Both sides of a connection identify themselves with a certificate – not just the server but the client too.

MVP

Minimum Viable Product

Kleinste sinnvoll nutzbare Version eines Produkts – genug Nutzen, um damit zu lernen, nicht mehr.

The smallest useful version of a product – enough value to learn from, no more.

N

↑ Index

NAT
Network Address Translation

Übersetzt interne IP-Adressen in eine öffentliche – so teilen sich viele Geräte eine Adresse.

Translates internal IP addresses to a public one, letting many devices share an address.

Network Segmentation

Das Netz wird in getrennte Zonen aufgeteilt, damit ein Angreifer nicht überallhin kommt.

The network is split into separate zones so an attacker cannot reach everything.

Netzwerk

Mehrere Rechner, die miteinander verbunden sind und Daten austauschen können – im Büro, im Rechenzentrum oder weltweit.

Several machines connected to each other that can exchange data – in an office, a data centre or worldwide.

nginx

Ein weit verbreiteter Webserver und Vermittler (Reverse Proxy), bekannt für Tempo und geringen Speicherverbrauch.

A widely used web server and reverse proxy, known for speed and low memory use.

NIST
National Institute of Standards and Technology

US-Behörde, die viele sicherheitsrelevante Standards setzt, etwa für Passwörter und Kryptografie.

US agency that sets many security-relevant standards, for example for passwords and cryptography.

Node.js

Eine Laufzeitumgebung, die JavaScript auch außerhalb des Browsers ausführt – Grundlage vieler Programmierschnittstellen.

A runtime that executes JavaScript outside the browser – the basis of many APIs.

Nonce
number used once

Einmal-Zahl, damit eine Nachricht nicht wiederverwendet werden kann.

Number used only once so a message cannot be replayed.

Non-Human Identity

Alle Identitäten, die keine Person sind: Service Accounts, Schnittstellen-Schlüssel, Zertifikate, Bots und KI-Agenten.

Every identity that is not a person: service accounts, API keys, certificates, bots and AI agents.

NoSQL Injection

Angriff, bei dem Eingaben in eine Abfrage an eine Dokumentdatenbank wie MongoDB fließen und dort Operatoren einschleusen – etwa ein größer-als, das jedes Passwort akzeptiert.

An attack where input flows into a query for a document database such as MongoDB and smuggles in operators – a greater-than that accepts any password, for instance.

O

↑ Index

OAuth 2.0

Open Authorization

Standard, mit dem eine App im Namen des Nutzers begrenzten Zugriff auf ein fremdes Konto bekommt – ohne das Passwort zu kennen.

Standard letting an app obtain limited access to a user's account elsewhere – without knowing the password.

OAuth Flows

Die vorgesehenen Abläufe, mit denen eine Anwendung ein Token erhält – etwa Authorization Code mit Benutzeranmeldung oder Client Credentials für Maschinen.

The defined flows by which an application obtains a token – authorisation code with a user login, or client credentials for machines.

Obfuscation

Code oder Daten absichtlich unleserlich machen. Erschwert Analyse, ist aber kein Schutz.

Deliberately making code or data unreadable. It hampers analysis but is not protection.

OIDC

OpenID Connect

Login-Schicht auf OAuth 2.0: liefert zusätzlich die bestätigte Identität des Nutzers.

Login layer on top of OAuth 2.0 that also delivers the user's verified identity.

On-Call

Bereitschaft

Bereitschaftsdienst: Jemand ist erreichbar und handlungsfähig, wenn ausserhalb der Arbeitszeit etwas ausfällt.

Being on call: someone is reachable and able to act when something fails outside working hours.

On-Premises

Selbst betrieben im eigenen Rechenzentrum oder Serverraum, im Gegensatz zur Cloud.

Run in-house in your own data centre, as opposed to the cloud.

OpenAPI / Swagger

OpenAPI Specification

Maschinenlesbare Beschreibung einer REST-API; daraus entstehen Doku, Clients und Tests.

Machine-readable description of a REST API; it generates docs, clients and tests.

Open Redirect

Schwachstelle, bei der eine Anwendung auf beliebige, in der Anfrage mitgegebene Adressen weiterleitet – beliebt für Phishing, weil der Link auf die echte, vertrauenswürdige Domain zeigt.

A flaw where an application redirects to any address supplied in the request – popular for phishing because the link points at the real, trusted domain.

OSINT

Open Source Intelligence

Informationen aus öffentlich zugänglichen Quellen, die Angreifer für gezielte Attacken nutzen.

Information from publicly available sources that attackers use to plan targeted attacks.

OTP

One-Time Password

Einmalpasswort, das nur einmal gilt – per SMS, App oder Hardware-Token.

Single-use password valid once only – via SMS, app or hardware token.

OWASP

Open Worldwide Application Security Project

Gemeinnützige Community mit den bekanntesten Sicherheits-Listen: Top 10 für Web und für APIs.

Non-profit community behind the best-known security lists: Top 10 for web and for APIs.

P

↑ Index

Package Manager

Paketverwaltung

Werkzeug, das fremde Bibliotheken samt Versionen herunterlädt, aktualisiert und ihre Abhängigkeiten auflöst.

A tool that downloads third-party libraries with versions, updates them and resolves their dependencies.

Pagination

Große Ergebnislisten werden seitenweise abgeholt, etwa mit page und limit.

Large result sets are fetched page by page, for example with page and limit.

Pair Programming

Zwei Personen an einem Rechner: Eine schreibt, die andere denkt mit und prüft – langsamer im Moment, schneller im Ergebnis.

Two people at one machine: one types, the other thinks along and checks – slower in the moment, faster in the result.

PAM

Privileged Access Management

Verwaltung besonders mächtiger Konten: Zugriff nur auf Zeit, mit Protokoll und Freigabe.

Management of highly privileged accounts: time-limited access with logging and approval.

Parameter

Wert, der an eine Funktion übergeben wird, damit sie damit arbeitet – auch Argument genannt.

A value passed to a function so it can work with it – also called an argument.

Passkey

Passwortloser Login über FIDO2: der private Schlüssel bleibt auf dem Gerät, der Server kennt ihn nie.

Passwordless login via FIDO2: the private key stays on the device and the server never sees it.

Passwordless

Anmeldung ohne Passwort, zum Beispiel per Sicherheitsschlüssel, Passkey oder einmaligem Link.

Signing in without a password – via a security key, a passkey or a one-time link, for example.

Password Manager

Programm, das Passwörter verschlüsselt verwaltet und pro Dienst ein eigenes starkes Passwort ermöglicht.

Program that stores passwords encrypted and enables a unique strong password per service.

Password Spraying

Angriff, bei dem wenige häufige Passwörter gegen viele Konten probiert werden – gerade so oft, dass keine Sperre greift.

An attack that tries a few common passwords against many accounts – just rarely enough to avoid lockouts.

Patch

Software-Update, das Fehler und Sicherheitslücken schließt. Je schneller eingespielt, desto besser.

Software update that fixes bugs and vulnerabilities. The faster it is applied, the better.

Patch Management

Geregelter Ablauf, wie Updates geprüft, getestet und eingespielt werden – mit Fristen je nach Schwere der Lücke.

A controlled process for reviewing, testing and installing updates – with deadlines depending on severity.

Path Traversal

Angriff, bei dem über relative Pfadangaben aus dem vorgesehenen Verzeichnis ausgebrochen wird – etwa mit ../../, um Systemdateien zu erreichen.

An attack that escapes the intended directory using relative paths – ../../ for example – to reach system files.

Payload

Die eigentliche Nutzlast einer Anfrage – oder der schädliche Teil eines Angriffs.

The actual payload of a request – or the harmful part of an attack.

PCI DSS

Payment Card Industry Data Security Standard

Sicherheitsstandard für alle, die Kreditkartendaten verarbeiten.

Security standard for anyone handling credit card data.

Pentest

Penetration Test

Bezahlter, ausdrücklich erlaubter Angriffsversuch, um Schwachstellen vor echten Angreifern zu finden.

Paid, explicitly authorised attack to find weaknesses before real attackers do.

Pepper

Zusätzliches Geheimnis, das vor dem Hashen an Passwörter gehängt wird und nicht in der Datenbank liegt.

Extra secret appended before hashing that is kept outside the database.

Phishing

Gefälschte Mails oder Webseiten, die Zugangsdaten, Karten oder Überweisungen abgreifen sollen.

Fake mails or websites meant to harvest credentials, card data or payments.

PHP-FPM

Der Dienst, der PHP-Code für den Webserver ausführt – getrennt vom Webserver, damit ein PHP-Absturz nicht alles mitreißt.

The service that executes PHP code for the web server – separate from it, so a PHP crash does not take everything down.

PII

Personally Identifiable Information

Personenbezogene Daten, mit denen sich eine Person direkt oder indirekt identifizieren lässt.

Personal data that can identify a person directly or indirectly.

PKCE

Proof Key for Code Exchange

Erweiterung von OAuth für öffentliche Clients wie Apps, damit ein abgefangener Code wertlos ist.

OAuth extension for public clients such as apps so an intercepted code is worthless.

PKI

Public Key Infrastructure

Gesamtsystem aus Zertifizierungsstellen, Zertifikaten und Regeln für öffentliche Schlüssel.

Overall system of certificate authorities, certificates and rules for public keys.

Plaintext

Unverschlüsselter Klartext – genau das, was niemand bei Passwörtern oder Tokens speichern sollte.

Unencrypted clear text – exactly what nobody should store for passwords or tokens.

POC

Proof of Concept

Machbarkeitsnachweis: ein kleiner, schnell gebauter Prototyp, der zeigt, ob ein Ansatz überhaupt funktioniert.

A feasibility proof: a small, quickly built prototype showing whether an approach works at all.

Polyfill

Nachbau einer modernen Funktion für ältere Browser, damit derselbe Code überall läuft.

A backport of a modern feature for older browsers so the same code runs everywhere.

Port

Eine nummerierte Tür an einem Rechner. Über sie entscheidet sich, welches Programm eine ankommende Verbindung bekommt – 443 ist zum Beispiel die Tür für verschlüsselte Webseiten.

A numbered door on a machine. It decides which program receives an incoming connection – 443, for example, is the door for encrypted websites.

PostgreSQL

Eine leistungsfähige Datenbank für Anwendungen mit vielen gleichzeitigen Zugriffen und hohen Ansprüchen an Konsistenz.

A powerful relational database for applications with many concurrent users and strict consistency needs.

Postmortem

Auswertung nach einem Vorfall: Was ist passiert, wie konnte es passieren, was verhindert die Wiederholung?

A review after an incident: what happened, how could it happen, what prevents a repeat?

Post-Quantum-Kryptographie

Verfahren, die auch gegen künftige Quantencomputer sicher sein sollen. Migration läuft bereits.

Algorithms meant to remain secure against future quantum computers. Migration is already underway.

POST-Request

POST

HTTP-Methode, die Daten anlegt oder verändert. Nicht idempotent: zweimal gesendet heißt oft zweimal angelegt.

HTTP method that creates or changes data. Not idempotent: sending it twice often creates twice.

Privileged Account

Konto mit weitreichenden Rechten wie Administrator oder Root – das bevorzugte Ziel von Angreifern.

An account with far-reaching rights such as administrator or root – the preferred target of attackers.

Privilege Escalation

Ausweitung von Rechten, meist durch eine Lücke: aus einem normalen Konto wird ein Administrator.

Escalating privileges, usually through a flaw: a normal account becomes an administrator.

Protokoll

Feste Verabredung, wie zwei Systeme miteinander reden – welche Reihenfolge, welche Befehle, welche Antworten.

A fixed agreement on how two systems talk – which order, which commands, which replies.

Prototype Pollution

Angriff auf JavaScript-Anwendungen: Über präparierte Objekt-Schlüssel werden Grundeigenschaften verändert, die dann für alle Objekte gelten – bis hin zur Codeausführung.

An attack on JavaScript applications: crafted object keys modify base properties that then apply to all objects – sometimes up to code execution.

Proxy

Vermittler zwischen Client und Ziel, der Anfragen weiterleitet und dabei prüfen oder filtern kann.

Intermediary between client and target that forwards requests and can inspect or filter them.

Prozess

Ein laufendes Programm im Speicher, mit eigenem Zustand und eigenen Rechten – sichtbar in der Prozessliste des Systems.

A running program in memory with its own state and rights – visible in the system's process list.

Pseudonymisierung

Personenbezug wird durch ein Kennzeichen ersetzt und bleibt mit Zusatzwissen auflösbar – anders als bei Anonymisierung.

Personal reference is replaced by a token that stays reversible with extra knowledge, unlike anonymisation.

PTAL

Please Take Another Look

Bitte noch einmal ansehen – Standardfloskel, wenn ein Review überarbeitet wurde.

Please take another look – the standard phrase after a review was revised.

Public Key

Öffentlicher Schlüssel eines Schlüsselpaars. Er darf geteilt werden; der private Gegenpart bleibt geheim.

The public half of a key pair. It may be shared; the private counterpart stays secret.

Pull Request

Vorschlag, Änderungen aus einem Branch in den Hauptstand zu übernehmen – mit Diff, Diskussion und Freigabe.

A proposal to bring changes from a branch into the main line – with diff, discussion and approval.

Purple Team

Rotes und blaues Team arbeiten zusammen, damit Angriffssimulationen direkt bessere Erkennung erzeugen.

Red and blue teams work together so attack simulations directly improve detection.

Push Notification

Kurze Nachricht, die der Hersteller-Dienst an ein Gerät schickt, auch wenn die App geschlossen ist.

A short message the vendor service sends to a device even when the app is closed.

PWA

Progressive Web App

Webseite, die sich wie eine App installieren lässt: eigenes Icon, offline nutzbar, Push-Nachrichten – ohne App Store.

A website that installs like an app: own icon, works offline, push messages – without an app store.

Q

↑ Index

Quarantäne

Abgesonderter Bereich, in dem verdächtige Dateien liegen, ohne Schaden anrichten zu können.

Segregated area where suspicious files are held without being able to cause harm.

Query

Abfrage an eine Datenbank oder API, etwa „gib alle Bestellungen von heute“ als SQL oder JSON.

A request to a database or API, e.g. „all orders from today“ expressed in SQL or JSON.

Query-Parameter

Werte in der URL nach dem Fragezeichen, etwa ?status=offen&limit=50. Sichtbar in Logs, also keine Geheimnisse.

Values in the URL after the question mark, e.g. ?status=open&limit=50. Visible in logs, so no secrets.

Quota

Erlaubtes Kontingent, etwa Anfragen pro Minute, Speicherplatz oder Nutzer pro Lizenz.

An allowed allowance, such as requests per minute, storage or users per licence.

R

↑ Index

Race Condition

Fehler, bei dem zwei Vorgänge gleichzeitig denselben Zustand prüfen und beide durchkommen – etwa wenn zwei Abbuchungen gleichzeitig das Guthaben prüfen und beide als gedeckt gelten.

A bug where two operations check the same state at the same moment and both pass – two withdrawals checking the balance at once and both looking covered.

Ransomware

Erpressungssoftware, die Daten verschlüsselt und für die Entschlüsselung Geld verlangt. Backup ist die beste Abwehr.

Extortion software that encrypts data and demands money for decryption. Backups are the best defence.

RASP

Runtime Application Self-Protection

Schutz, der direkt in der laufenden Anwendung sitzt und Angriffe im Moment der Ausführung erkennt.

Protection built into the running application that detects attacks at execution time.

Rate Limit Bypass

Umgehen einer Anfrage-Bremse durch wechselnde Adressen, Konten, Kopfzeilen oder Zeitfenster – der Schutz existiert, greift aber nicht.

Circumventing a request throttle by rotating addresses, accounts, headers or time windows – the protection exists but does not bite.

Rate Limiting

Bremse pro Client: nur eine bestimmte Zahl Anfragen pro Minute oder Stunde, darüber kommt 429.

Per-client throttle: only a fixed number of requests per minute or hour, otherwise 429.

RBAC

Role-Based Access Control

Rechte werden Rollen zugeordnet (Buchhaltung, Support, Admin) und Rollen den Benutzern.

Permissions are attached to roles (accounting, support, admin) and roles to users.

RCE

Remote Code Execution

Schwerwiegendste Klasse von Lücken: ein Angreifer führt aus der Ferne eigenen Code auf dem Server aus.

The most severe class of flaw: an attacker runs their own code on the server from a distance.

RDP

Remote Desktop Protocol

Microsofts Protokoll für Fernzugriff auf Windows-Oberflächen; im Internet ein häufiges Angriffsziel.

Microsoft's protocol for remote Windows desktops; a frequent target when exposed to the internet.

React Native

Framework, mit dem man Apps für Android und iOS in JavaScript schreibt und die Oberflächen des Systems nutzt.

A framework for writing Android and iOS apps in JavaScript while using the system's own interface elements.

Rechenzentrum

Ein Gebäude voller Server mit Strom, Kühlung und Netzanbindung – dort stehen die Maschinen, die Webseiten ausliefern.

A building full of servers with power, cooling and connectivity – where the machines serving websites stand.

Redirect

Eine Weiterleitung des Webservers auf eine andere Adresse; 301 gilt dauerhaft, 302 vorübergehend.

A web server redirect to another address; 301 is permanent, 302 temporary.

Redis

Ein sehr schneller Zwischenspeicher im Arbeitsspeicher – für Sitzungen, Zwischenergebnisse und Warteschlangen.

A very fast in-memory cache – for sessions, cached results and queues.

Red Team

Angreifer-Team, das ein System absichtlich wie ein echter Gegner attackiert, um Schwächen zu finden.

An attacking team that deliberately assaults a system like a real adversary to find weaknesses.

Refresh Token

Langlebiges Token, mit dem ein Client neue, kurzlebige Access Tokens holt – ohne neue Anmeldung.

Long-lived token a client uses to obtain new, short-lived access tokens without logging in again.

Regex

Regular Expression

Muster zum Durchsuchen und Prüfen von Text. Mächtig, aber fehleranfällig und bei Angreifern als Rechenbombe beliebt.

Pattern for searching and validating text. Powerful but error-prone, and popular as a CPU bomb.

Regression

Funktion, die vorher lief und durch eine Änderung kaputtgegangen ist – der häufigste Grund für automatisierte Tests.

A feature that worked before and broke due to a change – the most common reason for automated tests.

Rekursion

Eine Funktion, die sich selbst aufruft, um ein Problem in kleinere Teilprobleme zu zerlegen – braucht immer eine Abbruchbedingung.

A function that calls itself to break a problem into smaller ones – it always needs a stopping condition.

Responsible Disclosure

Verfahren, bei dem Sicherheitsforscher eine Lücke vertraulich melden und dem Hersteller Zeit zur Reparatur lassen, bevor Details öffentlich werden.

A process where security researchers report a flaw confidentially and give the vendor time to fix it before details become public.

Responsive Design

Gestaltung, bei der sich eine Seite an Bildschirmgröße und Gerät anpasst – ein Layout für Handy, Tablet und Desktop.

A design approach where a page adapts to screen size and device – one layout for phone, tablet and desktop.

REST

Representational State Transfer

Verbreiteter API-Stil: Ressourcen unter festen URLs, gesteuert über HTTP-Methoden, zustandslos.

Widely used API style: resources under fixed URLs, driven by HTTP methods, stateless.

Retrospektive

Retro

Rückblick am Ende eines Sprints: Was lief gut, was nicht, was ändern wir konkret?

A review at the end of a sprint: what went well, what did not, what do we change concretely?

Retry / Backoff

Nach einem Fehler wird die Anfrage wiederholt – aber mit wachsender Pause (1 s, 2 s, 4 s, 8 s) und zufälliger Streuung (Jitter). So bricht ein überlasteter Server nicht unter gleichzeitigen Wiederholungen zusammen. Nur bei Fehlern sinnvoll, die ein zweiter Versuch lösen kann (429, 500, 503, Timeout) und nur bei idempotenten Aufrufen.

After a failure the request is retried – but with a growing wait (1 s, 2 s, 4 s, 8 s) and random jitter, so an overloaded server is not hit by thousands of simultaneous retries. Only useful for errors a retry can fix (429, 500, 503, timeout), and only for idempotent calls.

Reverse Engineering

Aus fertiger Software oder aus Datenverkehr herausfinden, wie etwas funktioniert – Werkzeug von Angreifern und Forschern.

Working out how something functions from finished software or traffic – a tool for attackers and researchers alike.

Reverse Proxy

Vorgeschalteter Server (z. B. nginx), der Anfragen annimmt, prüft, verschlüsselt und an die Anwendung weiterleitet.

Front server (e.g. nginx) that receives, checks, encrypts and forwards requests to the application.

RFC

Request For Comments

Vorschlag zur Diskussion, bevor gebaut wird – bei grossen Änderungen ein Dokument mit Begründung und Alternativen.

A proposal for discussion before building – for large changes a document with rationale and alternatives.

RFI

Remote File Inclusion

Angreifer lässt die Anwendung eine Datei von einem fremden Server einbinden und ausführen.

Attacker makes the application include and execute a file from a foreign server.

robots.txt

Eine Textdatei im Wurzelverzeichnis, die Suchmaschinen-Crawlern sagt, welche Bereiche sie nicht durchsuchen sollen.

A text file in the root directory telling search engine crawlers which areas not to index.

Rootkit

Schadsoftware, die sich tief im System versteckt und vor Erkennung tarnt – oft nur mit Neuinstallation entfernbar.

Malware hidden deep in the system that masks itself from detection – often removable only by reinstalling.

Router

Gerät, das Daten zwischen Netzen weiterleitet und den richtigen Weg wählt – die Weiche zwischen deinem Heimnetz und dem Internet.

A device that forwards data between networks and picks the route – the junction between your home network and the internet.

RTFM

Read The Fucking Manual

Derber Hinweis, erst die Dokumentation zu lesen – heute oft freundlicher als „siehe Doku“ formuliert.

A blunt hint to read the documentation first – today often softened to “see the docs”.

Rubber Duck Debugging

Technik, bei der man das Problem laut einem Gegenstand erklärt – beim Formulieren fällt der Fehler oft von selbst auf.

A technique of explaining the problem aloud to an object – often the bug reveals itself while you phrase it.

Rückgabewert

Ergebnis, das eine Funktion an die aufrufende Stelle zurückliefert – kann ein Wert, ein Objekt oder auch nichts sein.

The result a function hands back to the caller – it may be a value, an object or nothing at all.

S

↑ Index

Salt

Zufallszusatz, der vor dem Hashen an jedes Passwort gehängt wird, damit gleiche Passwörter verschieden aussehen.

Random value appended before hashing so identical passwords produce different hashes.

SAML

Security Assertion Markup Language

XML-Standard für Single Sign-on zwischen Firmensystemen: Der zentrale Anmeldedienst stellt eine signierte Bestätigung über die Identität aus.

An XML standard for single sign-on between enterprise systems: the central login service issues a signed assertion about identity.

Sandbox

Abgeschottete Umgebung, in der unbekannter Code laufen kann, ohne das echte System zu gefährden.

Isolated environment where unknown code can run without endangering the real system.

SAST

Static Application Security Testing

Automatische Code-Prüfung auf Sicherheitsfehler, ohne die Anwendung auszuführen.

Automated inspection of source code for security bugs without running the application.

SBOM

Software Bill of Materials

Stückliste aller Bestandteile und Versionen einer Software – nötig, um bei einer Lücke sofort zu wissen, ob man betroffen ist.

Inventory of all components and versions in a piece of software – needed to know instantly whether a flaw affects you.

SCA

Software Composition Analysis

Automatische Prüfung, welche fremden Bibliotheken im Projekt stecken und ob für sie bekannte Lücken gemeldet sind.

Automated checking of which third-party libraries a project uses and whether known flaws are reported for them.

Schleife

Sprachkonstrukt, das einen Block mehrfach ausführt – entweder eine feste Anzahl oft oder solange eine Bedingung gilt.

A language construct that runs a block repeatedly – either a fixed number of times or while a condition holds.

SCIM

System for Cross-domain Identity Management

Standard, mit dem Benutzerkonten automatisch zwischen Anmeldedienst und Anwendungen angelegt, geändert und gelöscht werden.

A standard for automatically creating, changing and deleting user accounts between the login service and applications.

Scope

Umfang einer Berechtigung: was ein Token, ein Test oder ein Auftrag ausdrücklich abdecken darf.

The extent of a permission: what a token, a test or an engagement is explicitly allowed to cover.

Scrum

Vorgehensmodell mit festen Rollen, Sprints und Ritualen (Planung, Daily, Review, Retro) für die Produktentwicklung.

A process model with fixed roles, sprints and ceremonies (planning, daily, review, retro) for product development.

SDK

Software Development Kit

Paket aus Werkzeugen, Bibliotheken und Dokumentation, mit dem man für eine bestimmte Plattform entwickelt.

A bundle of tools, libraries and documentation for building software for a specific platform.

Secret

Geheimer Wert wie Passwort, API-Key oder privater Schlüssel. Gehört in einen Secrets-Speicher, nie ins Repository.

A secret value such as a password, API key or private key. Belongs in a secret store, never in a repository.

Secrets Management

Geordnete Verwaltung von Geheimnissen: zentral gespeichert, verschlüsselt, mit Rotation und Zugriffsprotokoll.

Disciplined handling of secrets: stored centrally, encrypted, rotated and access-logged.

Secure by Design

Sicherheit ist von Anfang an Teil des Entwurfs – nicht eine Prüfung kurz vor der Veröffentlichung.

Security is part of the design from the start, not a check just before release.

Security Awareness

Schulung und Sensibilisierung der Mitarbeiter, weil die meisten Angriffe beim Menschen ansetzen.

Training and awareness for staff, because most attacks start with a person.

Security Baseline

Der verbindliche Mindeststand, den jedes System erfüllen muss, bevor es produktiv geht – und der regelmäßig nachgeprüft wird.

The mandatory minimum standard every system must meet before going live – and which is reviewed regularly.

Security by Obscurity

Sicherheit durch Geheimhalten des Aufbaus. Allein reicht das nie, als zusätzliche Schicht ist es in Ordnung.

Security by hiding how something works. Never enough on its own, acceptable as an extra layer.

Security Misconfiguration

Fehlkonfiguration: Standardpasswörter, unnötige Dienste, offene Verzeichnisse oder zu weite Rechte – oft die einfachste Eintrittstür.

Misconfiguration: default passwords, unnecessary services, open directories or over-broad permissions – often the easiest way in.

SEO

Search Engine Optimization

Maßnahmen, damit eine Seite in Suchmaschinen gefunden wird – Inhalte, Struktur, Ladezeit, technische Angaben.

Measures that help a page be found in search engines – content, structure, load time, technical metadata.

Separation of Duties

Aufgabentrennung: Wer eine Zahlung anlegt, darf sie nicht selbst freigeben – Fehler und Betrug brauchen immer zwei.

The separation of tasks: whoever creates a payment may not approve it – mistakes and fraud always require two people.

Server

Ein Rechner, der für andere da ist: Er nimmt Anfragen an und antwortet – rund um die Uhr, ohne dass jemand davorsitzt.

A machine that is there for others: it accepts requests and answers – around the clock, with nobody sitting in front of it.

Service Account

Technisches Konto für ein Programm statt für einen Menschen – mit eigenen, eng begrenzten Rechten.

A technical account for a program rather than a person – with its own, tightly limited permissions.

Service Worker

Skript, das im Hintergrund zwischen Seite und Netz sitzt – cached Inhalte und macht sie offline verfügbar.

A script sitting between page and network in the background – it caches content and makes it available offline.

Session

Sitzung eines eingeloggten Nutzers, meist über ein Cookie oder Token gehalten; sollte ablaufen können.

A logged-in user's session, usually held by a cookie or token; it must be able to expire.

Session Fixation

Angriff, bei dem der Angreifer dem Opfer vor der Anmeldung eine bekannte Sitzungskennung unterschiebt; nach dem Login ist dieselbe Kennung gültig – und der Angreifer mit im Boot.

An attack where the attacker plants a known session identifier on the victim before login; after login the same identifier stays valid – and the attacker is along for the ride.

Session Hijacking

Übernahme einer bestehenden Sitzung durch Diebstahl der Sitzungskennung – etwa über unsauberes WLAN, Schadsoftware oder ein nicht geschütztes Cookie.

Taking over an existing session by stealing its identifier – via insecure Wi-Fi, malware or an unprotected cookie.

Session Token

Die Kennung, die eine angemeldete Sitzung repräsentiert – meist in einem Cookie oder im Authorization-Kopf der Anfrage.

The identifier representing a logged-in session – usually in a cookie or the Authorization header of the request.

SHA-256

Secure Hash Algorithm 256 Bit

Hash-Verfahren mit 256 Bit; Standard für Signaturen, Zertifikate und Prüfsummen.

256-bit hashing algorithm; the standard for signatures, certificates and checksums.

SIEM

Security Information and Event Management

System, das Logs aus vielen Quellen sammelt, korreliert und bei verdächtigen Mustern Alarm schlägt.

System that collects and correlates logs from many sources and alerts on suspicious patterns.

Simulator

Nachbildung einer Umgebung ohne die echte Hardware – schneller als ein Emulator, aber weniger realitätsnah.

An imitation of an environment without the real hardware – faster than an emulator but less faithful.

Smoke Test

Kurzer Funktionstest nach dem Ausrollen: Läuft die Anwendung überhaupt, antwortet die Startseite, klappt die Anmeldung?

A quick check after a rollout: does the application run at all, does the home page answer, does login work?

SOAR
Security Orchestration, Automation and Response

Automatisierung von Reaktionen: erkannte Angriffe werden nach festem Plan selbsttätig eingedämmt.

Automation of responses: detected attacks are contained automatically by a fixed playbook.

SOC
Security Operations Center

Team und Ort, das Sicherheitsereignisse rund um die Uhr beobachtet und bewertet.

Team and place that monitors and assesses security events around the clock.

Social Engineering

Angriffe über den Menschen: Vortäuschen einer Identität, Zeitdruck, Hilfsbereitschaft ausnutzen.

Attacks that target people: impersonation, time pressure, abusing helpfulness.

Software

Programme und ihre Daten – alles, was nicht greifbar ist, sondern auf der Hardware läuft.

Programs and their data – everything not tangible that runs on the hardware.

SPA
Single Page Application

Webanwendung, die nur einmal geladen wird und danach Inhalte im Browser nachlädt, statt neue Seiten aufzurufen.

A web application loaded once that then loads content in the browser instead of requesting new pages.

Spaghetti-Code

Code ohne klare Struktur, in dem alles von überall abhängt – kleine Änderungen haben unvorhersehbare Folgen.

Code without clear structure where everything depends on everything – small changes have unpredictable effects.

Spalte

Eine Eigenschaft über alle Datensätze hinweg – senkrecht gelesen: alle Namen, alle Beträge, alle Daten.

One attribute across all records – read vertically: every name, every amount, every date.

Spoofing

Vortäuschen einer falschen Identität, etwa Absenderadresse, IP oder Domain.

Pretending to be someone else, for example a sender address, IP or domain.

Sprint

Fester Arbeitsabschnitt, meist zwei Wochen, in dem ein Team eine vereinbarte Menge Aufgaben erledigt.

A fixed work period, usually two weeks, in which a team completes an agreed set of tasks.

Spyware

Software, die heimlich Daten sammelt und nach außen schickt.

Software that secretly collects data and sends it out.

SQL-Injection

Structured Query Language Injection

Angreifer schleust SQL-Befehle über Eingabefelder ein und liest oder verändert die Datenbank. Abwehr: Prepared Statements.

Attacker injects SQL through input fields to read or change the database. Defence: prepared statements.

SSH

Secure Shell

Verschlüsselter Fernzugang zur Kommandozeile eines Servers, heute Standard für Administration.

Encrypted remote access to a server's command line, today's standard for administration.

SSL

Secure Sockets Layer

Vorgänger von TLS. „SSL-Zertifikat“ sagt man umgangssprachlich noch, technisch läuft heute TLS.

Predecessor of TLS. People still say „SSL certificate“, but technically TLS is what runs today.

SSO

Single Sign-On

Ein Login gilt für viele Anwendungen; ein zentraler Anbieter prüft die Anmeldung.

One login works for many applications; a central provider verifies the sign-in.

SSR

Server-Side Rendering

Verfahren, bei dem der Server die fertige Seite ausliefert, statt sie erst im Browser zusammenzubauen – gut für Ladezeit und Suchmaschinen.

An approach where the server delivers the finished page instead of the browser assembling it – good for load time and search engines.

SSRF

Server-Side Request Forgery

Der eigene Server wird dazu gebracht, interne Adressen aufzurufen – so werden Firewalls umgangen.

Your own server is tricked into calling internal addresses, thereby bypassing firewalls.

SSTI

Server-Side Template Injection

Schwachstelle, bei der Nutzereingaben als Teil einer Vorlage ausgewertet werden, mit der der Server Seiten baut – im schlimmsten Fall lassen sich damit Befehle auf dem Server ausführen.

A flaw where user input is evaluated as part of the template the server uses to build pages – in the worst case allowing commands to run on the server.

Stack
Stapelspeicher

Speicherbereich für lokale Variablen und Funktionsaufrufe, streng in fester Reihenfolge verwaltet – schnell, aber begrenzt.

A memory area for local variables and function calls, managed strictly in order – fast but limited.

Stateless

Der Server merkt sich zwischen zwei Anfragen nichts. Jede Anfrage bringt ihren Ausweis selbst mit, etwa ein Token.

The server remembers nothing between requests. Each request brings its own credential, such as a token.

Steganographie

Informationen werden in Bildern, Ton oder anderen Daten versteckt – nicht verschlüsselt, sondern getarnt.

Information is hidden inside images, audio or other data – disguised rather than encrypted.

Story Points

Relative Schätzung des Aufwands in Punkten statt Stunden – vergleicht Aufgaben miteinander statt Zeit zu versprechen.

A relative estimate of effort in points rather than hours – compares tasks instead of promising time.

String
Zeichenkette

Datentyp für Text – eine Folge von Zeichen. In den meisten Sprachen unveränderlich, Änderungen erzeugen einen neuen Wert.

A data type for text – a sequence of characters. Immutable in most languages, so changes produce a new value.

Subdomain Takeover

Übernahme einer Subdomain, die auf einen nicht mehr existierenden fremden Dienst zeigt – der Angreifer registriert den Dienst und liefert unter der vertrauten Adresse eigene Inhalte aus.

Taking over a subdomain that points at a foreign service which no longer exists – the attacker registers that service and serves their own content under the familiar address.

Subnetz

Teilnetz eines IP-Bereichs, etwa 192.168.178.0/24 für ein Heimnetz mit 256 Adressen.

A part of an IP range, e.g. 192.168.178.0/24 for a home network with 256 addresses.

sudo

Ein Befehl, mit dem ein normaler Benutzer eine einzelne Aktion mit Administratorrechten ausführt – statt dauerhaft als Administrator zu arbeiten.

A command that lets a normal user perform one single action with administrator rights instead of working as root all the time.

Supply Chain Attack

Angriff über die Zulieferkette: Nicht das Ziel selbst wird gehackt, sondern ein Baustein, dem es vertraut – eine Bibliothek, ein Update-Mechanismus, ein Dienstleister.

An attack through the supply chain: instead of hacking the target, an element it trusts is compromised – a library, an update mechanism, a service provider.

Swift

Programmiersprache von Apple für iOS, macOS und verwandte Systeme – löst Objective-C ab.

Apple's programming language for iOS, macOS and related systems – the successor to Objective-C.

Switch

Gerät, das Rechner innerhalb eines Netzes miteinander verbindet und Daten gezielt an den richtigen Anschluss schickt.

A device connecting machines inside one network and sending data to the right socket.

Symmetric Encryption

Verschlüsselung mit demselben Schlüssel zum Ver- und Entschlüsseln; schnell, aber der Schlüssel muss sicher geteilt werden.

Encryption with the same key for locking and unlocking; fast, but the key must be shared securely.

systemctl

Das Kommando, mit dem man systemd bedient: starten, stoppen, neu laden, Status abfragen, Autostart schalten.

The command used to drive systemd: start, stop, reload, query status, enable at boot.

systemd

Der Start- und Aufsichtsdienst moderner Linux-Systeme: Er startet beim Booten alle Dienste, überwacht sie und startet abgestürzte neu.

The start-up and supervision service of modern Linux systems: it starts all services at boot, watches them and restarts crashed ones.

T

↑ Index

Tabelle

Geordnete Sammlung von Datensätzen in Zeilen und Spalten – die Grundform, in der Datenbanken Daten ablegen.

An ordered collection of records in rows and columns – the basic shape databases use to store data.

TBD

To Be Determined

Noch offen und später zu entscheiden – Platzhalter in Aufgabenlisten und Spezifikationen.

Still open and to be decided later – a placeholder in task lists and specifications.

TCP/IP

Transmission Control Protocol / Internet Protocol

Die Basis des Internets: IP adressiert Pakete, TCP sorgt für Reihenfolge und Vollständigkeit.

The foundation of the internet: IP addresses packets, TCP guarantees order and completeness.

Technische Schulden

Tech Debt

Abkürzungen, die kurzfristig Zeit sparen und später Zinsen kosten – fehlende Tests, Umgehungen, Provisorien.

Shortcuts that save time now and cost interest later – missing tests, workarounds, temporary fixes.

Thread

Ein Ausführungsstrang innerhalb eines Programms. Mehrere Threads können gleichzeitig arbeiten – und sich dabei in die Quere kommen.

A single path of execution inside a program. Several threads can work at the same time – and get in each other's way.

Threat Actor

Die handelnde Bedrohung: Gelegenheitskriminelle, organisierte Banden, Insider oder staatliche Gruppen.

The actor behind a threat: opportunistic criminals, organised gangs, insiders or state groups.

Threat Hunting

Aktive, gezielte Suche nach Angreifern im eigenen Netz – bevor eine automatische Warnung auslöst.

Actively and deliberately hunting for attackers in your own network before an alert fires.

Threat Intelligence

Aufbereitetes Wissen über aktuelle Angreifer, Werkzeuge und Ziele, das die Verteidigung vorbereitet.

Curated knowledge about current attackers, tools and targets that prepares defences.

Threat Model

Systematische Frage: Was baue ich, was kann schiefgehen, wer würde es angreifen und was tue ich dagegen?

Systematic question: what am I building, what can go wrong, who would attack it and what do I do about it?

Throughput

Durchsatz: wie viele Anfragen oder Datenmengen ein System pro Zeit verarbeitet.

Throughput: how many requests or how much data a system processes per unit of time.

TL;DR
Too Long; Didn't Read

Zusammenfassung am Anfang oder Ende eines langen Textes – „kurz gesagt“.

A summary at the start or end of a long text – “in short”.

TLS
Transport Layer Security

Verschlüsselungsschicht unter HTTPS, Mail und vielen APIs; prüft per Zertifikat, mit wem man spricht.

Encryption layer beneath HTTPS, mail and many APIs; certificates verify who you are talking to.

Token
Digitaler Ausweis mit Ablaufdatum, der bei jeder Anfrage mitgeschickt wird.

A digital credential with an expiry that is sent along with every request.

Tokenization
Sensible Werte werden durch wertlose Platzhalter ersetzt, etwa Kartennummern durch ein Token.

Sensitive values are replaced by worthless placeholders, e.g. card numbers by a token.

Token Revocation
Möglichkeit, ein ausgestelltes Token sofort ungültig zu machen – nach einem Diebstahl, beim Logout oder beim Verdacht auf Missbrauch.

The ability to invalidate an issued token immediately – after theft, at logout or when abuse is suspected.

Tor
The Onion Router

Anonymisierungsnetz, das Verbindungen über mehrere Stationen leitet – auch von Angreifern genutzt.

Anonymity network routing connections through several relays – also used by attackers.

TOTP
Time-based One-Time Password

Sechsstelliger Code aus einer Authenticator-App, der 30 Sekunden gilt und aus Uhrzeit und geheimem Startwert berechnet wird.

Six-digit code from an authenticator app, valid for 30 seconds, computed from the time and a shared secret.

Trojaner
Schadsoftware, die sich als nützliches Programm tarnt und im Hintergrund Schaden anrichtet.

Malware disguised as a useful program that causes damage in the background.

TTL
Time to Live

Haltbarkeitsdauer eines Eintrags oder Tokens, etwa 300 Sekunden für einen DNS-Cache.

How long an entry or token stays valid, e.g. 300 seconds for a DNS cache entry.

Typosquatting

Taktik, bei der Namen von Paketen, Domains oder Programmen mit kleinen Tippfehlern nachgebaut werden – in der Hoffnung, dass jemand danebengreift.

A tactic that clones package, domain or program names with small typos – hoping someone grabs the wrong one.

U

↑ Index

UDP

User Datagram Protocol

Paket-Protokoll ohne Verbindung und ohne Garantie – schnell, aber unzuverlässig; Basis von DNS und VoIP.

Connectionless packet protocol without guarantees – fast but unreliable; the base of DNS and VoIP.

ufw

Ein einfacher Vorbau für die Linux-Firewall: Erlaubt oder verbietet Ports mit einem einzigen Befehl.

A simple front end for the Linux firewall: allow or block ports with a single command.

Unicode

Weltweiter Zeichensatz, der jedem Schriftzeichen eine eindeutige Nummer gibt – über 150.000 Stück, inklusive Emoji und Sonderzeichen.

A worldwide character set assigning a unique number to every character – more than 150,000, including emoji and symbols.

Unit Test

Automatischer Test einer einzelnen Funktion oder Klasse, der bei jeder Änderung erneut läuft und Fehler sofort meldet.

An automated test of a single function or class that reruns on every change and reports failures immediately.

Universal Link

Link, der auf iOS direkt in die App führt und auf dem Desktop auf die Webseite – ohne Zwischenseite.

A link that opens the app directly on iOS and the website on desktop – no interstitial page.

Uptime

Anteil der Zeit, in der ein Dienst verfügbar ist; 99,9 Prozent erlaubt rund 43 Minuten Ausfall im Monat.

Share of time a service is available; 99.9 percent allows about 43 minutes of downtime per month.

URI

Uniform Resource Identifier

Eindeutige Bezeichnung einer Ressource; eine URL ist ein URI, der auch sagt, wie man sie erreicht.

Unique identifier of a resource; a URL is a URI that also says how to reach it.

User-Agent

Kennung von Browser oder Client in der Anfrage. Leicht fälschbar, darum nie als Sicherheitsmerkmal nutzen.

Identifier of the browser or client in a request. Easily faked, so never use it as a security check.

UTF-8

Unicode Transformation Format 8 Bit

Kodierung, die jedes Zeichen aus dem Unicode-Zeichensatz als ein bis vier Bytes speichert – heute der Standard im Web.

An encoding that stores every Unicode character in one to four bytes – today's standard on the web.

UUID

Universally Unique Identifier

Praktisch weltweit eindeutige Kennung wie 550e8400-e29b-41d4-a716-446655440000.

Practically worldwide unique identifier such as 550e8400-e29b-41d4-a716-446655440000.

V

↑ Index

Variable

Benannter Speicherplatz für einen Wert, der sich während des Programmlaufs ändern kann.

A named storage location for a value that may change while the program runs.

Versioning

Mehrere API-Stände parallel betreiben (v1, v2), damit bestehende Clients weiterlaufen, während Neues entsteht.

Running several API versions side by side (v1, v2) so existing clients keep working while new ones appear.

Versionskontrolle

Versionsverwaltung

System, das jede Änderung an Dateien festhält, sodass man zu jedem Stand zurückkehren kann – meist Git.

A system that records every change to files so you can return to any state – usually Git.

Verzeichnis

Ordner

Behälter für Dateien und weitere Verzeichnisse – die Struktur, in der Daten auf einem Rechner geordnet sind.

A container for files and further directories – the structure that orders data on a machine.

Viewport

Der sichtbare Bereich einer Seite im Browser. Ohne die richtige Angabe zoomt ein Handy die Desktop-Ansicht klein.

The visible area of a page in the browser. Without the right setting a phone zooms out the desktop view.

Virtual Host

Ein Eintrag im Webserver, der einer Domain ihr eigenes Verzeichnis und ihre eigenen Einstellungen zuweist – mehrere Webseiten auf einem Server.

An entry in the web server that gives a domain its own directory and settings – several websites on one server.

VPN

Virtual Private Network

Verschlüsselter Tunnel zwischen Gerät und Netz, damit Daten unterwegs nicht mitgelesen werden können.

Encrypted tunnel between device and network so data cannot be read in transit.

Vulnerability

Sicherheitslücke: eine Schwäche, die ein Angreifer ausnutzen kann, um Schaden anzurichten.

A weakness an attacker can exploit to cause damage.

Vulnerability Management

Lücken systematisch finden, bewerten, priorisieren und schließen – ein dauerhafter Prozess, kein Einzelakt.

Finding, rating, prioritising and closing vulnerabilities systematically – an ongoing process, not a one-off.

W

↑ Index

WAF

Web Application Firewall

Filter vor der Webanwendung, der bösartige Anfragen wie SQL-Injection-Muster abweist.

Filter in front of the web application that rejects malicious requests such as SQL-injection patterns.

Watering Hole

Angriff, bei dem eine Webseite infiziert wird, die die Zielgruppe regelmäßig besucht – der Angreifer wartet am Wasserloch, statt jeden einzeln anzugreifen.

An attack that infects a website the target group visits regularly – the attacker waits at the watering hole instead of hunting individuals.

Webhook

Umgekehrter Aufruf: ein Dienst meldet sich per HTTP bei deiner URL, sobald etwas passiert.

Reverse call: a service calls your URL over HTTP as soon as something happens.

Webserver

Das Programm, das Anfragen aus dem Internet annimmt und Antworten zurückschickt – Seiten, Bilder, Daten.

The program that accepts requests from the internet and sends answers back – pages, images, data.

WebSocket

Dauerhafte, beidseitige Verbindung zwischen Browser und Server, für Live-Daten statt ständiger neuer Anfragen.

Persistent two-way connection between browser and server for live data instead of repeated requests.

WebView

Eingebetteter Browser innerhalb einer App, der Webseiten anzeigt – bequem, aber eine eigene Angriffsfläche.

An embedded browser inside an app that displays web pages – convenient, but an attack surface of its own.

Wert

Value

Eine einzelne Information, die gespeichert oder übergeben wird – eine Zahl, ein Text, ein Ja/Nein. Zusammen mit einem Namen ergibt sie ein Datenfeld.

A single piece of information that is stored or passed – a number, a text, a yes/no. Together with a name it forms a data field.

Whitelist

Erlaubnisliste. Der Begriff wurde weitgehend durch Allowlist ersetzt (und Blocklist statt Blacklist).

Allow-list. The term has largely been replaced by allowlist (and blocklist instead of blacklist).

Wildcard-Zertifikat

Ein Zertifikat für *.example.com gilt für alle direkten Subdomains; praktisch, aber ein Leck betrifft alle.

*One certificate for *.example.com covers all direct subdomains; convenient, but one leak affects them all.*

WIP

Work In Progress

In Arbeit, noch nicht fertig – oft als Sperre im Ticket oder als Hinweis im Branch-Namen.

In progress, not finished – often a ticket state or a hint in the branch name.

WSGI

Eine einheitliche Schnittstelle zwischen Webserver und Python-Anwendung, damit beide zusammenarbeiten können.

A standard interface between web server and Python application so the two can work together.

X

↑ Index

X.509-Zertifikat

Standardformat für digitale Zertifikate; darin steht, zu welcher Domain welcher öffentliche Schlüssel gehört.

Standard format for digital certificates, stating which public key belongs to which domain.

XDR
Extended Detection and Response

Erkennung über mehrere Quellen hinweg – Endgeräte, Netz, Mail, Cloud – statt nur einzeln pro Werkzeug.

Detection across several sources – endpoints, network, mail, cloud – instead of per tool in isolation.

XML
Extensible Markup Language

Ältere Auszeichnungssprache für strukturierte Daten; bei XML-APIs auf XXE-Angriffe achten.

Older markup language for structured data; XML APIs must guard against XXE attacks.

XSS
Cross-Site Scripting

Fremdes JavaScript wird in eine Webseite eingeschleust und läuft im Browser anderer Nutzer. Abwehr: Encoding und CSP.

Foreign JavaScript is injected into a page and runs in other users' browsers. Defence: output encoding and CSP.

XXE
XML External Entity

Angriff auf Programme, die XML einlesen: Über einen präparierten Verweis im Dokument bringt der Angreifer den Server dazu, lokale Dateien zu lesen oder Anfragen an fremde Systeme zu schicken.

An attack on software that parses XML: a crafted reference inside the document makes the server read local files or send requests to foreign systems.

Y

↑ Index

YAGNI
You Aren't Gonna Need It

Prinzip: Baue nichts auf Vorrat, was heute niemand braucht – die Annahme über morgen ist meist falsch.

A principle: build nothing in advance that nobody needs today – assumptions about tomorrow are usually wrong.

Yak Shaving

Ketten von Vorarbeiten, die eigentlich nichts mit der Aufgabe zu tun haben – man rasiert den Yak, statt das Problem zu lösen.

Chains of preparatory work unrelated to the actual task – shaving the yak instead of solving the problem.

YAML
YAML Ain't Markup Language

Menschenlesbares Format für Konfigurationen, etwa in Kubernetes oder CI-Pipelines. Einrückung ist bedeutsam.

Human-readable format for configuration, e.g. in Kubernetes or CI pipelines. Indentation matters.

YARA
Regelsprache, um Schadsoftware anhand von Mustern zu erkennen, etwa in Forensik und Virenscannern.
Rule language for spotting malware by patterns, used in forensics and scanners.

YubiKey
Hardware-Schlüssel der Firma Yubico für Zwei-Faktor-Anmeldung und FIDO2.
Hardware key made by Yubico for two-factor login and FIDO2.

Z

↑ Index

ZAP
Zed Attack Proxy
Kostenloses Open-Source-Werkzeug zum Testen von Webanwendungen auf Sicherheitslücken.
Free open-source tool for testing web applications for security weaknesses.

Zeile
Ein einzelner Datensatz in einer Tabelle – waagerecht gelesen gehört alles zu einem Fall.
A single record in a table – read horizontally, everything belongs to one case.

Zero-Day
Lücke, für die es noch keinen Patch gibt und die der Hersteller oft noch nicht kennt.
A flaw with no patch yet, often unknown to the vendor.

Zero-Knowledge
Der Anbieter erfährt den Inhalt nie, weil Ver- und Entschlüsselung nur beim Nutzer passiert – etwa bei Passwort-Managern.
The provider never learns the content because encryption happens only at the user, e.g. in password managers.

Zero Trust
Sicherheitsmodell: niemandem wird allein aufgrund seiner Netzposition vertraut, alles wird jedes Mal geprüft.
Security model: nobody is trusted just because of network position; everything is verified every time.

Zombie
Gekaperter Rechner, der ferngesteuert Befehle ausführt – Baustein eines Botnets.
A hijacked machine executing remote commands – a building block of a botnet.

ZTNA
Zero Trust Network Access
Zugriff auf Anwendungen nur nach Prüfung von Identität und Gerätezustand – ohne Vertrauen ins Netz selbst.
Access to applications only after checking identity and device state – without trusting the network itself.

Quellen & Hinweis

Alle Erklärungen sind eine Zusammenstellung allgemein zugänglicher Informationen aus dem Internet (u. a. Wikipedia, Hersteller- und Projektdokumentationen) in eigenen Formulierungen – ohne Anspruch auf Vollständigkeit oder Richtigkeit und ohne Gewähr. Verlinkte Inhalte gehören ihren jeweiligen Urhebern.

All explanations compile publicly available information from the internet (Wikipedia, vendor and project documentation) in our own wording – no claim of completeness or accuracy, no warranty. Linked content belongs to its respective authors.