IT-Security und Betriebssicherheit

Fachbegriff Zero-Day-Exploit

Ein Zero-Day-Exploit ist eine gezielte Ausnutzung einer bislang unbekannten Sicherheitslücke in Software oder Hardware, die dem Hersteller (z. B. Microsoft, Adobe, Apple) noch nicht bekannt ist – und daher noch keine Gegenmaßnahme (Patch) existiert.

"Zero Day" bedeutet: 0 Tage Reaktionszeit seit Bekanntwerden → maximales Risiko.

Aufbau der Begriffsbestandteile

BESTANDTEIL	BEDEUTUNG
ZERO-DAY	Die Schwachstelle ist neu, unbekannt und ungepatcht.
EXPLOIT	Der konkrete Code oder Mechanismus, der die Lücke aktiv ausnutzt.

Wie entsteht ein Zero-Day-Exploit?

1. Ein Sicherheitsforscher, Angreifer oder Hacker entdeckt eine neue Schwachstelle in einer Software (z. B. Browser, Betriebssystem, VPN-Client).
2. Der Entwickler des Produkts weiß noch nichts davon.
3. Der Entdecker nutzt (oder verkauft) den Exploit, bevor ein Sicherheitsupdate veröffentlicht wurde.
4. Nutzer sind wehrlos, da noch kein Schutzmechanismus vorhanden ist.

Warum sind Zero-Day-Exploits so gefährlich?

- Keine Virensignaturen oder Sicherheitsupdates verfügbar
- Antivirus-/EDR-Systeme erkennen sie oft nicht sofort
- Werden oft gezielt gegen Unternehmen, Behörden oder Infrastruktur eingesetzt
- Angriffe sind hochentwickelt, schwer nachweisbar und besonders effektiv

Beispiele aus der Praxis

JAHR	EXPLOIT	ZIEL / AUSWIRKUNG
2010	Stuxnet	Angriff auf iranische Nuklearanlagen
2021	Exchange Server Exploits	Weltweite Angriffe auf Microsoft-Mailserver
2023	MOVEit Transfer Leak	Datenabfluss bei über 100 Firmen weltweit
2024	iOS-Zero-Day (NSO-Pegasus)	Spionagesoftware auf Smartphones

Schutzmaßnahmen (präventiv)

MAßNAHME	ZWECK
REGELMÄßIGE UPDATES	Schließen entdeckter Lücken schnellstmöglich
VERHALTENSBASIERTE ERKENNUNG	EDR/XDR erkennt ungewöhnliche Aktivitäten
LEAST PRIVILEGE-PRINZIP	Rechtevergabe auf Mindestmaß beschränken
NETWORK SEGMENTATION	Schaden begrenzen bei erfolgreichem Angriff
MONITORING & LOGGING	Auffälligkeiten früh erkennen

Fachbegriff Multifaktor-Authentifizierung

Die Multifaktor-Authentifizierung (MFA) ist ein Sicherheitsverfahren, bei dem sich ein Benutzer mithilfe von mindestens zwei unterschiedlichen, unabhängigen Authentifizierungsfaktoren gegenüber einem System ausweisen muss, um Zugriff zu erhalten.

Ziel: Schutz vor unbefugtem Zugriff – auch wenn ein Faktor (z. B. das Passwort) kompromittiert wurde.

Die drei grundlegenden Authentifizierungsfaktoren

FAKTORART	BESCHREIBUNG	BEISPIEL
WISSENSFAKTOR	Etwas, das der Benutzer weiß	Passwort, PIN, Sicherheitsfrage
BESITZFAKTOR	Etwas, das der Benutzer hat	Smartphone, Token, Smartcard
BIOMETRISCHER FAKTOR	Etwas, das der Benutzer ist	Fingerabdruck, Gesicht, Iris, Stimme

MFA erfordert mindestens zwei dieser Kategorien, z. B.:
Passwort (Wissen) + Smartphone-Code (Besitz)

Warum MFA eingesetzt wird

- Schützt Benutzerkonten auch bei gestohlenen oder geleakten Passwörtern
- Erhöht massiv die Sicherheit von Online-Diensten, VPNs, Cloudsystemen, E-Mail-Konten etc.
- Erfüllt gesetzliche Anforderungen (z. B. DSGVO, NIS2, PSD2)
- Verhindert Phishing-Angriffe und Accountübernahmen

Gängige MFA-Methoden im Einsatz

METHODE	FAKTOR(EN)	BESCHREIBUNG
TOTP (Z. B. GOOGLE AUTHENTICATOR)	Besitz	6-stelliger Einmalcode per App
SMS-TAN	Besitz	Einmalcode per SMS – weniger sicher
HARDWARE-TOKEN (Z. B. YUBIKEY)	Besitz	Physisches Gerät generiert oder sendet Code
PUSH-BESTÄTIGUNG (Z. B. MICROSOFT AUTHENTICATOR)	Besitz	Benutzer bestätigt Login auf Mobilgerät
BIOMETRIE	Sein	Fingerabdruck oder Gesichtserkennung
SMARTCARD + PIN	Besitz + Wissen	z. B. im Unternehmen oder E-Government

Risiken bei Einzelfaktoren ohne MFA

Nur Passwort = Unsicher weil:

- Leicht zu erraten (schwache Passwörter)
- Wird oft wiederverwendet
- Kann durch Phishing erbeutet werden
- Kann in Datenleaks auftauchen

MFA schützt auch bei kompromittiertem Passwort!!!

Anwendung in der Praxis

BEREICH	MFA-EINSATZBEISPIELE
WINDOWS-ANMELDUNG	Smartcard + PIN, Token, Gesicht (Hello)
CLOUD-DIENSTE	Office 365, Google Workspace mit App-Authentifizierung
ONLINE-BANKING	PIN + TAN (z. B. über App oder ChipTAN-Gerät)
VPN-ZUGRIFF	Passwort + Token/Push zur Identitätsprüfung
ADMIN-ZUGÄNGE	Pflicht für Domain-Admins & privilegierte Konten

Kenntnis der Sicherheits-Unterschiede zw. Hardware- und Software-Firewall

Firewalls sind Sicherheitslösungen zur Überwachung, Filterung und Kontrolle des Datenverkehrs zwischen verschiedenen Netzwerken oder innerhalb eines Systems.

Es gibt zwei grundlegende Arten:

TYP	BESCHREIBUNG
HARDWARE-FIREWALL	Ein eigenständiges physisches Gerät im Netzwerk
SOFTWARE-FIREWALL	Eine installierte Anwendung auf einem Betriebssystem

Hardware-Firewall

- Wird zwischen Internet und internem Netzwerk installiert (meist vor dem Router)
- Filtert ein- und ausgehenden Traffic für das gesamte Netzwerk
- Basiert oft auf Stateful Packet Inspection, NAT, Deep Packet Inspection
- Hat ein eigenes Betriebssystem oder eine dedizierte Firmware

Software-Firewall

- Läuft auf dem jeweiligen Endgerät (PC, Server, Notebook)
- Überwacht und steuert einzelne Anwendungen und lokale Ports
- Kann individuell pro Gerät angepasst werden
- Arbeitet auf Betriebssystemebene, z. B. Windows Defender Firewall

Sicherheitsunterschiede im Vergleich

MERKMAL	HARDWARE-FIREWALL	SOFTWARE-FIREWALL
PLATZIERUNG IM NETZWERK	Vor dem internen Netz (zentrale Stelle)	Auf jedem Endgerät individuell
SICHERHEITSNIVEAU (NETZWERK)	Hoch – schützt ganze Netzsegmente	Mittel – schützt nur lokal
SICHERHEITSNIVEAU (APPLIKATION)	Gering (wenig Kontrolle über App-Ebene)	Hoch – erkennt App-spezifischen Traffic
MANIPULATIONSSICHERHEIT	Eigenes System, schwer kompromittierbar	Kann bei Malwarebefall mit kompromittiert werden
AUSFALLSICHERHEIT	Sehr stabil (eigenes System)	Anfällig bei Betriebssystemproblemen
ZUGRIFFSFILTERUNG	IP-/Port-basiert, VLAN, VPN, DoS-Schutz	Programm-/Prozessbasiert (z. B. App X blockieren)
KOSTEN	Höher (Gerät + Einrichtung)	Gering (oft kostenlos, z. B. Windows Firewall)

Kombinierter Einsatz (Best Practice)

In der Praxis gilt:
Defense in Depth: = Kombination beider Typen!

- Hardware-Firewall: schützt Netzübergänge und Firmeninfrastruktur
- Software-Firewall: schützt Endgeräte, insbesondere mobile Clients und BYOD-Systeme

Einsatzbeispiele

SZENARIO	GEEIGNETE FIREWALL
UNTERNEHMENSNETZWERK	Hardware + Software (kombiniert empfohlen)
HOME-OFFICE	Software-Firewall + ggf. Router-Firewall
SERVERRECHENZENTRUM	Dedizierte Hardware-Firewalls (z.B. pfSense, Fortinet)
EINZEL-PC ZU HAUSE	Software-Firewall ausreichend (z.B. Windows Defender)

Funktion einer Hardware-Firewall

Eine Hardware-Firewall ist ein eigenständiges physisches Gerät, das zwischen dem internen Netzwerk und externen Netzwerken (z. B. dem Internet) platziert wird.

Sie filtert und kontrolliert den gesamten ein- und ausgehenden Datenverkehr unabhängig vom Betriebssystem einzelner Geräte.

Sie bildet die erste Verteidigungslinie gegen Angriffe auf ein Unternehmensnetzwerk.

Grundlegende Funktion
Die Hardware-Firewall überwacht den Netzwerkverkehr in Echtzeit und trifft Entscheidungen auf Basis vordefinierter Regeln, ob Pakete durchgelassen, blockiert oder geprüft werden.

Arbeitsweise in Kurzform:

1. Pakete empfangen (z. B. vom Internet)
2. Regeln prüfen (z. B. Port, IP, Protokoll)
3. Entscheidung treffen:
   - Erlauben (z. B. für Webserver)
   - Blockieren (z. B. unbekannte Zugriffe)
   - Protokollieren oder weiterleiten an Intrusion Detection

Technische Merkmale einer Hardware-Firewall

MERKMAL	BESCHREIBUNG
EIGENE HARDWARE & OS	Läuft unabhängig von PCs – robust und manipulationssicher
STATEFUL PACKET INSPECTION (SPI)	Analysiert Paketstatus & Verbindungszustände
NAT (NETWORK ADDRESS TRANSLATION)	Versteckt interne IPs vor dem Internet
VPN-UNTERSTÜTZUNG	Ermöglicht gesicherte Fernverbindungen
DOS-/DDOS-SCHUTZ	Erkennt und blockiert Massenanfragen oder Angriffe
ZONEN-MANAGEMENT (DMZ)	Isoliert öffentliche Server von internen Netzbereichen
CONTENT-FILTER & APP CONTROL	Kontrolliert Inhalte & Programme, z. B. blockiert Social Media
LOGGING & REPORTING	Zeichnet verdächtige Aktivitäten auf und erstellt Auswertungen

Typischer Aufbau

- WAN-Port: Verbindung zum Internet / Provider
- LAN-Ports oder Switch: Verbindung zu internen Geräten
- DMZ-Port (optional): Separater Zugang für öffentliche Dienste
- Web-GUI oder CLI: Konfiguration durch IT-Admins

Einsatzbereiche

UMGEBUNG	ROLLE DER HARDWARE-FIREWALL
UNTERNEHMEN / KMU	Zentraler Netzwerkschutz gegen Angriffe, Kontrolle & Reporting
SCHULEN / VERWALTUNGEN	Filterung unerwünschter Inhalte, Zugangsbeschränkungen
RECHENZENTREN	Segmentierung, VPN, Redundanz
HEIMNETZWERKE (HIGH-END)	Schutz für Smart-Home, IoT, erweiterte Netzwerkkontrolle

Vorteile einer Hardware-Firewall

VORTEIL	BESCHREIBUNG
SYSTEMUNABHÄNGIG	Kein Einfluss durch installierte Betriebssysteme
ZENTRALISIERT	Kontrolliert alle Geräte gleichzeitig
HOHE LEISTUNG & STABILITÄT	Optimiert für dauerhaften 24/7-Betrieb
BESSERE SICHERHEIT	Schutz auf Netzwerkebene, nicht nur lokal
ERWEITERBAR	Zusatzfunktionen wie VPN, IDS/IPS, Webfilter, VLANs

Einschränkungen

EINSCHRÄNKUNG	BESCHREIBUNG
KOSTENINTENSIVER	Höhere Anschaffungskosten im Vergleich zu Software
KOMPLEXER IN EINRICHTUNG	Fachkenntnisse erforderlich
KEINE ANWENDUNGSKONTROLLE AUF ENDGERÄTEN	Kombi mit Software-Firewall empfohlen

Fachbegriff DMZ

Die DMZ (Demilitarisierte Zone) bezeichnet einen sicherheitskritischen Bereich innerhalb eines Netzwerks, der zwischen dem internen LAN und dem Internet platziert ist.

Sie dient dazu, öffentliche Dienste (z. B. Webserver, Mailserver, FTP) vom internen Netzwerk zu isolieren, ohne sie direkt ungeschützt ins Internet zu stellen.

Die Bezeichnung stammt aus dem militärischen Bereich: Eine DMZ ist ein neutraler Pufferbereich zwischen zwei Parteien – in der IT zwischen Internet und Intranet.

Zweck und Funktion

- Trennung von Netzwerken mit unterschiedlichen Sicherheitsstufen
- Minimierung von Risiken, falls ein öffentlich zugänglicher Server kompromittiert wird
- Bereitstellung von extern erreichbaren Diensten, ohne interne Systeme zu gefährden

Typischer Aufbau

Internet ← → [Firewall/Router] ← → DMZ ← → [Firewall] ← → Internes LAN

ZONE	INHALT	SICHERHEITSSTUFE
INTERNET	Extern, unkontrolliert	Unsicher
DMZ	Öffentlich erreichbare Server	Eingeschränkt sicher
LAN (INTRANET)	Interne Clients, Datenbanken, AD etc.	Sicher

Typische DMZ-Dienste

DIENST	BESCHREIBUNG
WEBSERVER (HTTP/HTTPS)	Öffentliche Webseiten
MAILSERVER (SMTP/IMAP)	Senden/Empfangen von E-Mails
DNS-SERVER (PUBLIC)	Namensauflösung von außen
VPN-GATEWAY	Remote-Zugänge von Mitarbeitern
REVERSE PROXY	Vermittler zu internen Diensten

Sicherheitsprinzipien der DMZ

- Separate Firewall-Regeln: Ein- und ausgehender Verkehr zur DMZ wird strikt geregelt
- Kein direkter Zugang LAN <--> Internet
- Datenbankserver bleiben im LAN, nicht in der DMZ
- Einbruch in DMZ ≠ direkter Zugriff aufs interne Netz

Varianten der DMZ-Architektur

VARIANTE	BESCHREIBUNG
1-FIREWALL-MODELL	DMZ über eigene Schnittstelle an einer Firewall
2-FIREWALL-MODELL	Zwei getrennte Firewalls (Internet–DMZ, DMZ–LAN)
VIRTUELLE DMZ	VLAN/Segmentierung auf virtuellen Routern/Switches

Vorteile der DMZ

VORTEIL	ERKLÄRUNG
BESSERE KONTROLLE ÜBER EXTERNE ZUGRIFFE	Nur ausgewählte Dienste in der DMZ erreichbar
MINIMIERTES RISIKO FÜR DAS LAN	Eindringlinge in die DMZ bleiben isoliert
HOHE FLEXIBILITÄT	Unterschiedliche Sicherheitsregeln je Zone umsetzbar
BESSERE PROTOKOLLIERUNG	DMZ-Traffic kann gezielt analysiert und überwacht werden

Risiken bei fehlender DMZ

PROBLEM	FOLGE
ÖFFENTLICHE SERVER IM LAN	Kompromittierte Systeme = direkter Zugriff aufs Intranet
KEINE SEGMENTIERUNG	Sicherheitsverletzungen schwerer zu isolieren
FEHLKONFIGURIERTE REGELN	Ungewollter Traffic zwischen LAN und Internet

Fachbegriff Stateful Packet Inspection

Stateful Packet Inspection (SPI) – auch bekannt als zustandsorientierte Paketprüfung – ist eine Firewall-Technologie, die nicht nur einzelne Netzwerkpakete überprüft, sondern den Zustand einer gesamten Verbindung analysiert.

Im Gegensatz zur einfachen „stateless“ Filterung erkennt SPI, ob ein Paket Teil einer gültigen, etablierten Verbindung ist – und trifft erst dann eine Filterentscheidung.

Funktionsweise von SPI (vereinfacht)

- Ein Client (z. B. ein PC) startet eine Verbindung zum Server (z. B. eine Website).
- Die Firewall prüft das erste Paket, erkennt den Verbindungsaufbau und merkt sich die Session (IP-Adressen, Ports, Protokoll, Status).
- Nachfolgende Pakete derselben Verbindung werden automatisch erlaubt, solange sie zum erwarteten Status gehören.
- Unerwartete oder manipulierte Pakete (z. B. ohne vorherigen Handshake) werden geblockt.

Beispielhafte Informationen, die SPI speichert:

MERKMAL	BEISPIEL
QUELL-IP / ZIEL-IP	z. B. 192.168.0.2 → 8.8.8.8
PORTNUMMERN	z. B. 50483 → 443
VERBINDUNGSSTATUS	z. B. SYN gesendet, ACK empfangen, ESTABLISHED
PROTOKOLL	TCP, UDP, ICMP
SESSION-ZEIT	Ablauf bei Inaktivität oder Verbindungsende

Vorteile von SPI gegenüber stateless Packet Filtering

VORTEIL	ERKLÄRUNG
VERBINDUNGSERKENNUNG	Erkennt, ob ein Paket zu einer zulässigen Session gehört
WENIGER REGELBEDARF	Kein manuelles Öffnen von Rückporten für Antworten nötig
EFFEKTIVER GEGEN SPOOFING	Blockiert nicht-autorisierte Pakete mit gefälschter Herkunft
DYNAMISCHE REAKTION	Anpassung an temporäre Sessions wie FTP, VoIP, HTTPS
SICHERER ALS EINFACHE PORTFILTER	Erkennt anomalen Verkehr auch auf bekannten Ports

Grenzen / Nachteile

EINSCHRÄNKUNG	BESCHREIBUNG
RESSOURCENVERBRAUCH	Speicher und CPU-Belastung durch Tracking aller Sessions
KEIN ANWENDUNGSFILTER	Kennt keine Inhalte (dafür braucht es DPI/NGFW)
NICHT 100 % GEGEN MALWARE	Malware kann auch gültige Verbindungen nutzen

Kenntnisse über Sicherheitstechnologie TLS

TLS (Transport Layer Security) ist ein netzwerkbasierter Sicherheitsstandard, der die vertrauliche, authentifizierte und integritätsgeschützte Kommunikation über unsichere Netzwerke (z. B. das Internet) ermöglicht.

TLS ist der Nachfolger von SSL und wird bei HTTPS, E-Mail, VPN, VoIP und vielen anderen Diensten eingesetzt.

TLS schützt Daten auf der Transportschicht (Layer 4/5 OSI-Modell) – zwischen Anwendungen und Netzwerkprotokollen wie TCP.

Ziele von TLS

SICHERHEITSZIEL	BESCHREIBUNG
VERTRAULICHKEIT	Daten werden verschlüsselt, damit Dritte sie nicht lesen können
AUTHENTIZITÄT	Der Kommunikationspartner wird per Zertifikat überprüft
INTEGRITÄT	Sicherstellung, dass Daten nicht manipuliert wurden
FORWARD SECRECY	Selbst bei späterem Key-Leak bleiben alte Sessions sicher

Funktionsweise (vereinfacht)

Ablauf des TLS-Handshakes:

1. Client Hello
   → Client sendet TLS-Version, unterstützte Verschlüsselungsverfahren, Zufallszahl
2. Server Hello
   → Server antwortet mit Zertifikat (inkl. Public Key), Zufallszahl, Chiffre-Auswahl
3. Schlüsselvereinbarung
   → Per RSA oder Diffie-Hellman wird ein sicherer Sitzungsschlüssel erzeugt
4. Verschlüsselung aktiv
   → Ab hier ist die Verbindung vollständig verschlüsselt

Wichtige Begriffe im TLS-Kontext

BEGRIFF	BEDEUTUNG
ZERTIFIKAT	Nachweis der Server-Identität (meist X.509, ausgestellt von CA)
PUBLIC KEY / PRIVATE KEY	Asymmetrisches Schlüsselpaar zur Authentifizierung & Verschlüsselung
SESSION KEY	Temporärer symmetrischer Schlüssel für die eigentliche Kommunikation
CIPHER SUITE	Kombination aus Verschlüsselung, Signatur und Hash-Verfahren
TLS-VERSIONEN	Aktuell: **TLS 1.3** (seit 2018), veraltet: SSL 3.0, TLS 1.0/1.1

Anwendung von TLS

ANWENDUNG	PROTOKOLL MIT TLS	BEISPIEL
WEBBROWSER	HTTPS	Webseiten mit Schloss-Symbol
E-MAIL-VERSCHLÜSSELUNG	SMTPS, IMAPS, POP3S	Postausgang/-eingang mit TLS
VPN	TLS-basierte VPNs	OpenVPN
VOIP	SIP over TLS	Sprachdaten verschlüsselt
DATEIÜBERTRAGUNG	FTPS (nicht FTP!)	Sicheres FTP über TLS

Aktuelle Sicherheitsanforderungen (Best Practices)

EMPFEHLUNG	BESCHREIBUNG
NUR TLS 1.2 ODER TLS 1.3 NUTZEN	Ältere Versionen (TLS 1.0/1.1) sind unsicher
ZERTIFIKATE VON VERTRAUENSWÜRDIGEN CAS	z. B. Let's Encrypt, DigiCert
FORWARD SECRECY AKTIVIEREN	Schutz vergangener Sessions bei Key-Leak
STARKE CIPHER SUITES VERWENDEN	Keine RC4-, DES- oder MD5-basierten Algorithmen
REGELMÄßIGE ERNEUERUNG & PRÜFUNG	Zertifikatslaufzeiten verkürzen, automatische Erneuerung

Risiken bei fehlender oder falsch konfigurierter TLS-Nutzung

RISIKO	MÖGLICHE FOLGE
KEINE VERSCHLÜSSELUNG	Passwörter, Daten im Klartext → Mitlesen möglich
FALSCHES ZERTIFIKAT	Man-in-the-Middle-Angriff durch gefälschte Seiten
VERALTETE PROTOKOLLE	Anfällig für Angriffe wie BEAST, POODLE, Heartbleed

Fachbegriff CA in Zusammenhang mit Zertifikaten

Eine CA – Certificate Authority (Zertifizierungsstelle) ist eine vertrauenswürdige Organisation, die digitale Zertifikate ausstellt, überprüft und signiert, um die Identität von Personen, Servern oder Organisationen im Internet oder in Netzwerken zu bestätigen.

Die CA ist das Zentrum der Vertrauenskette (Trust Chain) im Bereich der IT-Sicherheit – ohne sie wären digitale Zertifikate nicht überprüfbar.

Aufgaben einer Certificate Authority

AUFGABE	BESCHREIBUNG
ZERTIFIKATSAUSTELLUNG	Generiert und signiert X.509-Zertifikate
IDENTITÄTSPRÜFUNG	Prüft, ob der Antragsteller tatsächlich der Inhaber der Domain/Identität ist
DIGITALE SIGNATUR	Signiert Zertifikate mit dem privaten Schlüssel der CA
ZERTIFIKATSGÜLTIGKEIT VERWALTEN	Festlegen von Laufzeiten, Sperrung (z. B. über CRL/OCSP)
VERTRAUENSANKER BEREITSTELLEN	Root- und Intermediate-Zertifikate in Browsern/Clients verankern

Aufbau eines digitalen Zertifikats (X.509)
Ein Zertifikat enthält:

- Name des Antragstellers (Subject) – z. B. www.firma.de
- Öffentlicher Schlüssel (Public Key)
- Name der ausstellenden CA
- Seriennummer und Gültigkeitszeitraum
- Digitale Signatur der CA

Nur durch die Signatur der CA kann ein Browser überprüfen, ob das Zertifikat echt und gültig ist.

Arten von Cas

TYP	BESCHREIBUNG
ROOT-CA	Oberste Zertifizierungsstelle – höchste Vertrauensstufe
INTERMEDIATE-CA	Wird von Root-CA zertifiziert und stellt Zertifikate aus
PRIVATE CA (IN-HOUSE)	Wird intern im Unternehmen betrieben (z. B. Active Directory CA)
PUBLIC CA	Öffentliche, weltweit anerkannte Anbieter (z. B. Let's Encrypt, DigiCert, GlobalSign)

Bekannte öffentliche Cas

CA-ANBIETER	BESONDERHEIT
LET'S ENCRYPT	Kostenlos, automatisiert, sehr verbreitet
DIGICERT	Kommerziell, hohe Vertrauensstufe
SECTIGO	Früher Comodo, große Kompatibilität
GLOBALSIGN	Weit verbreitet, besonders im Business

Vertrauensprüfung durch Browser/Clients
Wenn du eine HTTPS-Seite öffnest:

- Browser prüft das Zertifikat (Domain, Gültigkeit, Signatur)
- Er vergleicht die CA im Zertifikat mit den hinterlegten vertrauenswürdigen Root-CAs
- Wenn alles passt → Schloss-Symbol / sichere Verbindung
  Wenn nicht → Warnung: „Verbindung nicht sicher“

Risiken bei unzuverlässiger CA

RISIKO	AUSWIRKUNG
KOMPROMITTIERTE CA	Gefälschte Zertifikate können ausgestellt werden
UNZUREICHENDE PRÜFUNG	Identitätsfälschung trotz gültigem Zertifikat möglich
NICHT VERTRAUENSWÜRDIG	Browser akzeptieren Zertifikate nicht

Fachbegriffe Private Key und Public Key

Die Begriffe Private Key (privater Schlüssel) und Public Key (öffentlicher Schlüssel) stammen aus der asymmetrischen Kryptographie. Dabei handelt es sich um ein Verfahren, bei dem zwei Schlüssel mathematisch zusammengehören, jedoch unterschiedliche Rollen übernehmen:

BEGRIFF	KURZDEFINITION
PUBLIC KEY	Wird öffentlich verteilt – zum Verschlüsseln oder Prüfen
PRIVATE KEY	Wird streng geheim gehalten – zum Entschlüsseln oder Signieren

Zusammen bilden sie ein sogenanntes Schlüsselpaar, das nur in eine Richtung verschlüsselt und in der anderen entschlüsselt werden kann.

Funktionsprinzip der asymmetrischen Verschlüsselung

ANWENDUNG	WAS PASSIERT?
VERSCHLÜSSELUNG	Der Absender verschlüsselt mit dem Public Key des Empfängers
ENTSCHLÜSSELUNG	Nur der Empfänger kann die Nachricht mit seinem Private Key entschlüsseln
DIGITALE SIGNATUR	Der Absender signiert mit seinem Private Key
SIGNATURPRÜFUNG	Jeder Empfänger kann sie mit dem Public Key des Absenders verifizieren

Eigenschaften der Schlüssel

MERKMAL	PUBLIC KEY	PRIVATE KEY
VERBREITUNG	Öffentlich – kann jeder kennen	Geheim – darf niemals geteilt werden
VERWENDUNG	Zum Verschlüsseln oder Prüfen	Zum Entschlüsseln oder Signieren
SICHERHEIT	Sicher durch mathematische Einwegfunktion	Muss vor Diebstahl oder Leak geschützt werden
SPEICHERORT	Zertifikate, Websites, DNS, E-Mail	Geschützt im Gerät, Token, HSM, Datei mit Passwort

Beispielanwendung: HTTPS (TLS/SSL)

1. Browser ruft Webseite auf
2. Server sendet Zertifikat mit seinem Public Key
3. Browser prüft das Zertifikat
4. Sitzungsschlüssel wird mit dem Public Key des Servers verschlüsselt
5. Nur der Server kann ihn mit seinem Private Key entschlüsseln

Weitere Einsatzgebiete

EINSATZBEREICH	ROLLE VON PUBLIC/PRIVATE KEY
E-MAIL-VERSCHLÜSSELUNG (S/MIME, PGP)	Nur Empfänger kann Mails entschlüsseln (Private Key)
DIGITALE SIGNATUREN	Sicherstellung der Absenderidentität
SSH-ZUGRIFFE	Private Key bleibt beim Admin, Server prüft mit Public Key
SOFTWARE-UPDATES	Code-Signierung schützt vor Manipulationen

Technische Standards

- RSA, ECDSA, EdDSA – gängige Algorithmen für Schlüsselpaarerzeugung
- Schlüssellänge (z. B. 2048 oder 4096 Bit) beeinflusst Sicherheit
- Public Keys werden meist in Zertifikaten eingebettet (X.509)

Sicherstellen von Datenvertraulichkeit bei gemeinsamen Netzlaufwerken

Die Datenvertraulichkeit auf gemeinsamen Netzlaufwerken bedeutet:

Nur berechtigte Personen sollen Zugriff auf bestimmte Daten erhalten – alle anderen sollen weder lesen, ändern noch sehen können, dass diese existieren.

Gemeinsame Netzlaufwerke (z. B. „H:\Projekte“) werden oft von mehreren Benutzern und Gruppen genutzt – eine saubere Zugriffskontrolle ist essenziell.

Wichtige Schutzmaßnahmen für Vertraulichkeit

MAßNAHME	BESCHREIBUNG
NTFS-BERECHTIGUNGEN (DATEISYSTEM)	Feingranulare Rechte auf Ordner- und Dateiebene (z. B. „Lesen“, „Ändern“)
FREIGABEBERECHTIGUNGEN	Kontrolle auf Netzwerkebene (z. B. \Server\Projekte)
GRUPPENBASIERTES BERECHTIGUNGSKONZEPT	Vermeidung individueller Rechte – einfacher, sicherer
ZUGRIFFSPROTOKOLLIERUNG	Aktivieren von Auditing bei Zugriffen (z. B. über GPO)
VERSCHLÜSSELUNG (EFS, BITLOCKER)	Schutz vor unbefugtem Zugriff bei Diebstahl/Sicherung
SICHERHEITSRICHTLINIEN ÜBER GPO	Einschränkung des Zugriffs z. B. nach Standort, Uhrzeit, Gerätetyp
NETZWERKSEGMENTIERUNG / VLAN	Trennung sensibler Abteilungen auf Netzwerkebene

NTFS- und Freigabeberechtigungen richtig einsetzen

- NTFS-Berechtigungen:
  Werden auf dem lokalen Dateisystem des Servers vergeben – z. B. für:
  - Ordner: „Lesen“, „Schreiben“, „Ändern“, „Vollzugriff“
  - Vererbung gezielt deaktivieren oder einschränken
- Freigabeberechtigungen:
  Gültig nur über das Netzwerk – zusätzliche Sicherheitsebene
  - Meist: „Jeder – Lesen“ oder restriktiv je nach Gruppe

Prinzip: Die strengste Kombination aus Freigabe + NTFS gilt!

Beispiel: Projektlaufwerk mit Gruppenrichtlinien

ORDNERSTRUKTUR	ZUGRIFF (BEISPIELGRUPPEN)
\\SERVER\PROJEKTE\HR	Nur Gruppe „HR“: Vollzugriff
\\SERVER\PROJEKTE\IT	Nur „IT“: Vollzugriff, „GF“: Lesen
\\SERVER\PROJEKTE\GF	Nur „GF“: Vollzugriff

Keine direkten Benutzerrechte! Nur Gruppen verwenden (Best Practice)

Weitere technische Maßnahmen

MAßNAHME	FUNKTION
ZUGRIFFSPROTOKOLLIERUNG (AUDIT POLICY)	Wer hat wann welche Datei geöffnet/gelöscht?
DFS-NAMENSRÄUME (DOMAIN-BASED)	Benutzer erhalten nur ihre Bereichsansicht
VERSCHLÜSSELUNG (EFS, BITLOCKER TO GO)	Schutz bei mobilen Endgeräten oder Backups
QUOTA-MANAGEMENT (FSRM)	Schutz vor Datenüberflutung / Missbrauch

Risiken bei fehlender Kontrolle

RISIKO	BEISPIEL
UNBEFUGTER ZUGRIFF	Azubi kann Personalakten einsehen
FEHLENDE PROTOKOLLIERUNG	Zugriff nicht nachvollziehbar bei Datenleck
KEINE GRUPPENSTRATEGIE	Chaos bei Rechten, „Rechte-Wildwuchs“
OFFENE FREIGABEN	„Jeder: Vollzugriff“ auf \Server\Daten

Erarbeiten von Berechtigungskonzepten im Active Directory

Ein Berechtigungskonzept im Active Directory legt systematisch fest, welche Benutzer(gruppen) auf welche Ressourcen mit welchen Rechten zugreifen dürfen.

Es dient der IT-Sicherheit, Nachvollziehbarkeit und rechtssicheren Verwaltung von Zugriffsrechten.

Ziel: So viel wie nötig, so wenig wie möglich (Prinzip der minimalen Rechte)

Bestandteile eines Berechtigungskonzepts

BESTANDTEIL	BESCHREIBUNG
BENUTZERSTRUKTUR	Einzelne Benutzerkonten – eindeutig identifizierbar
GRUPPENKONZEPT	Rollenbasiert, nach Funktion oder Abteilung gegliedert
RESSOURCENGRUPPEN	Für Ordner, Drucker, Applikationen, Shares
RECHTE-DEFINITION	Genaue Festlegung: Lesen, Schreiben, Ändern, Löschen
ZUGRIFFSREGELN	Welche Gruppen dürfen was auf welche Ressourcen?
DOKUMENTATION	Schriftliches Regelwerk mit Änderungsprotokoll

Best Practices im Active Directory

A-G-DL-P-Modell (Microsoft Empfehlung)

EBENE	BEDEUTUNG
A	Account = Benutzer (z. B. Max Mustermann)
G	In globale Gruppen einordnen (z. B. „Mitarbeiter HR“)
DL	Globale Gruppen in Domänenlokale Gruppen (z. B. „Zugriff HR-Freigabe“)
P	**Ressource auf Datei-/Serverebene** wird mit DL-Gruppe verknüpft

Trennung von Person, Rolle und Ressource → Übersichtlicher, skalierbar, revisionssicher

Gruppentypen in AD gezielt nutzen

GRUPPENTYP	EINSATZBEREICH
GLOBALE GRUPPEN	Benutzer mit gleicher Rolle/Funktion
DOMÄNENLOKALE GRUPPEN	Zugriff auf konkrete Ressourcen
UNIVERSELLE GRUPPEN	domänenübergreifend – nur bei Bedarf verwenden
VERTEILERGRUPPEN	Nur für E-Mail, nicht für Zugriffsrechte

Beispiel für ein Konzept (HR-Abteilung)

OBJEKT	BEISPIELGRUPPE	BERECHTIGUNG
BENUTZERKONTO	mustermann.m	-
GLOBALE GRUPPE	G_HR_Mitarbeiter	Mitglied: mustermann.m
DOMÄNENLOKALE GRUPPE	DL_HR_Ordner_RW	Zugriff auf \srv\hr
FREIGABE	\srv\hr	DL_HR_Ordner_RW = „Ändern“

Technische Umsetzungsschritte

- Analyse: Wer benötigt welche Daten?
- Planung: Gruppenstruktur (A-G-DL-P), Namenskonventionen definieren
- Erstellung: Gruppen im AD anlegen, Benutzer zuordnen
- Freigaben: Rechte auf NTFS- & Freigabeebene setzen
- Dokumentation: Protokollierte Zuordnung, Änderungsnachweise
- Überprüfung: Regelmäßiges Rechtemanagement (z. B. jährlich)

Vorteile eines durchdachten Berechtigungskonzepts

VORTEIL	WIRKUNG
HOHE SICHERHEIT	Keine unnötigen oder gefährlichen Berechtigungen
ZENTRALE ÜBERSICHTLICHKEIT	Wenige Gruppen, klare Zuordnung
EINFACHES MANAGEMENT	Neue Benutzer schnell zuordenbar
COMPLIANCE UND AUDITFÄHIGKEIT	Erfüllung von ISO, DSGVO, BSI-Grundschutz
SKALIERBARKEIT	Für wachsende Teams, Standorte, Rollen leicht anpassbar

Häufige Fehler vermeiden

FEHLER	RISIKO
EINZELRECHTE AUF BENUTZEROBJEKTE	Unübersichtlich, fehleranfällig
KEIN GRUPPENKONZEPT	Rechtechaos, Sicherheitslücken
BENUTZER IN MEHRERE GRUPPEN MIT WIDERSPRÜCHLICHEN RECHTEN	Unklare Effektivberechtigung