IT-Glossar

Stand 1.9.2025

0-9

2FA (Zwei-Faktor-Authentifizierung)
: Zwei-Faktor-Authentifizierung (2FA) ist eine Sicherheitsmaßnahme, die zwei verschiedene Methoden zur Verifizierung der Identität einer Person erfordert. Neben dem Passwort wird ein zusätzlicher Faktor wie ein SMS-Code oder eine App-Bestätigung verwendet. Dies erhöht die Sicherheit, da bei einem Angriff beide Faktoren bekannt sein müssen, um Zugriff zu erhalten.

A

Anhänge
: Anhänge sind Dateien, die an E-Mails angehängt werden. Sie können nützliche Informationen enthalten, aber auch schädliche Software wie Viren oder Trojaner. Es ist wichtig, Anhänge nur von vertrauenswürdigen Quellen zu öffnen und einen Virenscanner zu verwenden.

Authentifizierung
: Authentifizierung ist der Prozess der Überprüfung der Identität einer Person oder eines Systems. Dies geschieht häufig durch Eingabe eines Kontonamens und Passworts. Ziel ist es, sicherzustellen, dass nur autorisierte Personen Zugriff auf bestimmte Daten oder Systeme haben.

Authentifizierungs-App
: Eine Authentifizierungs-App generiert Einmal-Codes, die als zusätzlicher Sicherheitsfaktor bei der Zwei-Faktor-Authentifizierung (2FA) verwendet werden. Diese Apps erhöhen die Sicherheit, indem sie dynamische Codes bereitstellen, die nur kurzzeitig gültig sind.

B

Backup
: Ein Backup ist eine Kopie von Daten, die regelmäßig erstellt wird, um im Falle eines Datenverlusts eine Wiederherstellung zu ermöglichen. Backups sollten sicher gespeichert und regelmäßig aktualisiert werden, um die Datenintegrität zu gewährleisten.

BDSG (Bundesdatenschutzgesetz)
: Das Bundesdatenschutzgesetz (BDSG) ist ein deutsches Gesetz, das den Schutz personenbezogener Daten regelt. Es legt fest, wie Daten erhoben, verarbeitet und genutzt werden dürfen, und gibt den Betroffenen Rechte wie Auskunft und Löschung ihrer Daten.

Betriebssystem

Ein Betriebssystem (OS) ist die grundlegende Software, die Computerhardware und Software verwaltet und steuert. Es ermöglicht die Ausführung von Anwendungen und die Interaktion zwischen Menschen und dem Computer. Zu den Hauptfunktionen gehören die Verwaltung von Speicher, Prozessoren, Dateien und Geräten. Bekannte Betriebssysteme sind Windows, MacOS, Linux und Android. Ein Betriebssystem stellt sicher, dass Programme effizient und sicher laufen und bietet eine einfache Bedienoberfläche des Computers. Es ist essenziell für die Funktionalität und Leistung eines Computersystems.

Betriebssystemprofil

Ein Betriebssystemprofil enthält die Einstellungen und Daten eines Kontos auf einem Computer, wie Desktop-Anordnung, installierte Programme und persönliche Dateien. Es ermöglicht eine personalisierte Nutzung des Systems und sollte regelmäßig gesichert werden.

Browsersicherheit

Bekannte Browser sind Brave, Google Chrome, Mozilla Firefox und Microsoft Edge. Standardmäßig blockieren Brave und Firefox Tracking-Cookies. Chrome und Edge sind aus Datenschutzsicht weniger empfehlenswert, da sie umfangreiche Daten sammeln. Deaktivieren Sie die automatische Ausfüllen-Funktion für Adressen und Zahlungsmethoden, um zu verhindern, dass diese Daten gespeichert werden. Browser können über Erweiterungen wie Passwortmanager neue Funktionen bekommen. Löschen Sie regelmäßig Ihre Cookies und Browserdaten, um Ihre Spuren im Internet zu minimieren.

Brute-Force-Angriffe

Brute-Force-Angriffe sind Versuche, Passwörter oder Verschlüsselungsschlüssel durch systematisches Ausprobieren aller möglichen Kombinationen zu knacken. Diese Angriffe können durch starke Passwörter und Sicherheitsmaßnahmen wie Zwei-Faktor-Authentifizierung erschwert werden.

C

Cloud

Die Cloud bezeichnet die Bereitstellung von IT-Ressourcen wie Speicherplatz und Rechenleistung über das Internet. Cloud-Dienste ermöglichen den Zugriff auf Daten und Anwendungen von überall und bieten Skalierbarkeit und Flexibilität für Unternehmen und Privatpersonen. Bekannte Cloudsysteme sind z. B. Nextcloud, Microsoft SharePoint, Google Cloud.

D

Datei- und Ordnerberechtigungen

Datei- und Ordnerberechtigungen legen fest, wer auf bestimmte Dateien und Ordner zugreifen, sie ändern oder löschen darf. Diese Berechtigungen helfen, die Sicherheit und Integrität von Daten zu gewährleisten, indem sie den Zugriff auf autorisierte Personen beschränken.

Dateiendungen

Dateiendungen sind die letzten Zeichen im Dateinamen, die den Dateityp anzeigen, wie .docx für Word-Dokumente oder .jpg für Bilder. Sie helfen, die richtige Anwendung zum Öffnen der Datei zu bestimmen, und können Hinweise auf potenziell gefährliche Dateien geben.

Dateikomprimierung

Dateikomprimierung ist ein Verfahren, bei dem die Größe von Dateien reduziert wird, um Speicherplatz zu sparen oder die Übertragung zu beschleunigen. Komprimierte Dateien haben Endungen wie .zip oder .rar und können durch spezielle Software entpackt werden.

Datenerfassung

Datenerfassung ist der Prozess des Sammelns und Speicherns von Informationen. Dies kann manuell oder automatisch erfolgen und umfasst verschiedene Methoden wie Umfragen, Sensoren oder Software. Ziel ist es, Daten für Analysen, Berichte oder die Entscheidungsfindung bereitzustellen.

Datenintegrität

Datenintegrität bezieht sich auf die Genauigkeit und Vollständigkeit von Daten. Maßnahmen zur Sicherstellung der Datenintegrität umfassen regelmäßige Backups, Fehlerprüfungen und Zugriffskontrollen. Ziel ist es, sicherzustellen, dass Daten korrekt und unverändert bleiben.

Datenmanipulation

Datenmanipulation ist die absichtliche Veränderung von Daten mit betrügerischer Absicht. Dies kann durch unbefugten Zugriff oder schädliche Software erfolgen. Schutzmaßnahmen umfassen Zugriffskontrollen, Verschlüsselung und regelmäßige Überprüfungen der Datenintegrität.

Datenschutz

Datenschutz bezieht sich auf den Schutz persönlicher Daten vor unbefugtem Zugriff und Missbrauch. Dies umfasst Maßnahmen wie Verschlüsselung, sichere Speicherung und die Einhaltung gesetzlicher Vorschriften. Ziel ist es, die Privatsphäre und Sicherheit der Daten zu gewährleisten.

Datenschutzbeauftragte

Datenschutzbeauftragte sind Personen, die für die Einhaltung der Datenschutzgesetze und Vorschriften in einer Organisation verantwortlich sind. Sie beraten das Unternehmen in Datenschutzfragen, überwachen die Datenverarbeitung und schulen Mitarbeitende im Umgang mit personenbezogenen Daten.

Datensicherheit

Datensicherheit umfasst Maßnahmen zum Schutz von Daten vor Verlust, Diebstahl oder Beschädigung. Dazu gehören regelmäßige Backups, Verschlüsselung und sichere Netzwerke. Ziel ist es, die Integrität und Verfügbarkeit der Daten zu gewährleisten.

Datensparsamkeit

Datensparsamkeit ist ein Prinzip des Datenschutzes, bei dem nur die unbedingt notwendigen Daten erhoben und verarbeitet werden. Ziel ist es, das Risiko von Datenmissbrauch zu minimieren und die Privatsphäre der betroffenen Personen zu schützen.

Datenverlust

Datenverlust bezeichnet den Verlust von Daten durch Hardwarefehler, Softwareprobleme, menschliches Versagen oder schädliche Angriffe. Maßnahmen zur Vermeidung von Datenverlust umfassen regelmäßige Backups, sichere Speicherung und Schutz vor Malware.

DSGVO (Datenschutz-Grundverordnung)

Die Datenschutz-Grundverordnung (DSGVO) ist ein EU-Gesetz, das den Schutz personenbezogener Daten regelt. Es legt strenge Anforderungen an die Verarbeitung und Speicherung von Daten fest und gibt Einzelpersonen Rechte wie Auskunft und Löschung ihrer Daten. Unternehmen müssen DSGVO-konform handeln.

E

E-Mail-Header

Ein E-Mail-Header enthält technische Informationen über die E-Mail, wie Absender, Empfänger, Datum und Serverpfade. Er hilft, die Herkunft und Authentizität der E-Mail zu überprüfen, und kann bei der Identifizierung von SPAM oder betrügerischen Nachrichten nützlich sein.

Ende-zu-Ende-Verschlüsselung

Ende-zu-Ende-Verschlüsselung ist eine Methode, bei der Daten während der Übertragung verschlüsselt und nur vom Absender und Empfänger entschlüsselt werden können. Dies schützt die Daten vor unbefugtem Zugriff und stellt sicher, dass nur die vorgesehenen Parteien die Informationen lesen können.

F

FIDO2-USB-Schlüssel

Ein FIDO2-USB-Schlüssel ist ein physisches Gerät, das zur sicheren Authentifizierung verwendet wird. Es ermöglicht eine starke Zwei-Faktor-Authentifizierung, indem es einen kryptografischen Schlüssel speichert, der nur durch physisches Einstecken des Schlüssels in den Computer verwendet werden kann.

Firewall

Eine Firewall ist eine Sicherheitsvorrichtung, die den Datenverkehr zwischen einem internen Netzwerk und dem Internet überwacht und kontrolliert. Sie blockiert unerwünschte Zugriffe und schützt das Netzwerk vor Angriffen und schädlicher Software.

H

HTML (Hypertext Markup Language)

HTML ist die Standardsprache zur Erstellung von Webseiten. Sie ermöglicht die Strukturierung von Inhalten durch Tags, die Text, Bilder, Links und andere Elemente definieren. HTML ist die Grundlage des Webdesigns und wird von Browsern interpretiert, um Webseiten darzustellen.

HTTPS (Hypertext Transfer Protocol Secure)

HTTPS ist eine sichere Version des HTTP-Protokolls, das zur Übertragung von Daten im Internet verwendet wird. Es verschlüsselt die Datenübertragung zwischen dem Browser und der Webseite, um die Vertraulichkeit und Integrität der Daten zu gewährleisten.

I

IMAP (Internet Message Access Protocol)

IMAP ist ein Protokoll, das den Zugriff auf E-Mails auf einem Server ermöglicht. Es erlaubt das Synchronisieren von E-Mails auf mehreren Geräten, sodass Nachrichten auf dem Server gespeichert bleiben und von verschiedenen Geräten aus abgerufen werden können.

L

LAN-Verbindung

Eine LAN-Verbindung (Local Area Network) ist eine kabelgebundene Netzwerkverbindung, die Geräte innerhalb eines begrenzten Bereichs verbindet. Sie bietet hohe Geschwindigkeit und Sicherheit, da sie weniger anfällig für externe Angriffe ist als drahtlose Verbindungen.

Links

Links sind Verweise auf andere Webseiten oder Dokumente, die durch Anklicken geöffnet werden. Sie können jedoch auch auf schädliche Seiten führen. Es ist wichtig, Links vor dem Anklicken zu überprüfen, insbesondere in E-Mails von unbekannten Absendern.

M

Makros

Makros sind kleine Programme oder Skripte, die in Office-Dokumenten wie Word oder Excel eingebettet sind. Sie automatisieren Aufgaben, können aber auch schädlichen Code enthalten. Daher ist es sicherer, Makros zu deaktivieren.

Malware

Malware, kurz für „malicious software“, bezeichnet schädliche Programme, die darauf abzielen, Computersysteme zu beschädigen, Daten zu stehlen oder unbefugt Zugriff zu erlangen. Zu den häufigsten Arten gehören Viren, Würmer, Trojaner und Ransomware. Malware kann über infizierte E-Mails, Downloads oder kompromittierte Websites verbreitet werden. Sie verursacht erhebliche Schäden und Sicherheitsrisiken. Der Schutz vor Malware erfordert regelmäßige Updates, starke Passwörter und Vorsicht beim Öffnen unbekannter Dateien und Links.

Messenger-Dienst

Ein Messenger-Dienst ermöglicht die Echtzeitkommunikation über Textnachrichten, Bilder und Dateien. Für Unternehmen ist es wichtig, datenschutzkonforme Messenger zu nutzen, um die DSGVO einzuhalten. Diese Dienste müssen sicherstellen, dass personenbezogene Daten geschützt und nur auf Servern innerhalb der EU gespeichert werden. Beispiele für DSGVO-konforme Messenger sind Threema, Signal und Wire. Unternehmen müssen sicherstellen, dass die Nutzung dieser Dienste transparent ist und die Zustimmung aller Beteiligten eingeholt wird.

N

Netzwerkkabel

Ein Netzwerkkabel ist ein Kabel, das Geräte in einem Netzwerk verbindet, um Daten zu übertragen. Es bietet eine stabile und schnelle Verbindung und ist weniger anfällig für Störungen als drahtlose Verbindungen. Netzwerkkabel sind wichtig für die Infrastruktur von Unternehmensnetzwerken.

Nur-Text-Format

Das Nur-Text-Format ist eine E-Mail-Einstellung, bei der Nachrichten nur aus einfachem Text bestehen, ohne Bilder, Links oder Formatierungen. Es bietet mehr Sicherheit, da keine versteckten Links oder Skripte ausgeführt werden können. Der Nachteil ist, dass die E-Mails weniger ansprechend und funktional sind.

O

Öffentlicher Schlüssel

Ein öffentlicher Schlüssel ist Teil eines kryptografischen Schlüsselpaares, das zur Verschlüsselung von Daten verwendet wird. Er kann frei verteilt werden und ermöglicht es anderen, Nachrichten zu verschlüsseln, die nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden können.

P

Passkey

Ein Passkey ist eine moderne Authentifizierungsmethode, die auf kryptografischen Schlüsseln basiert. Er ersetzt Passwörter und ermöglicht eine sichere Anmeldung durch biometrische Daten oder Geräte, die den Passkey speichern. Dies erhöht die Sicherheit und erleichtert die Bedienung.

Passphrasen

Passphrasen sind längere und komplexere Versionen von Passwörtern, die aus mehreren Wörtern bestehen. Sie sind leichter zu merken und bieten höhere Sicherheit, da sie schwerer zu knacken sind. Eine gute Passphrase sollte mindestens vier Wörter enthalten und zufällig gewählt sein.

Passwort

Ein Passwort ist eine geheime Zeichenfolge, die zur Authentifizierung einer Person verwendet wird. Es sollte stark und einzigartig sein, um unbefugten Zugriff zu verhindern. Regelmäßige Änderungen und die Verwendung von Kombinationen aus Buchstaben, Zahlen und Sonderzeichen erhöhen die Sicherheit.

Passwortmanager

Ein Passwortmanager ist eine Software, die Menschen hilft, starke und einzigartige Passwörter für verschiedene Online-Konten zu erstellen, zu speichern und zu verwalten. Diese Programme speichern Passwörter sicher in einer verschlüsselten Datenbank und ermöglichen den einfachen Zugriff darauf durch ein Master-Passwort. Passwortmanager können auch Passwörter automatisch ausfüllen und generieren, was die Sicherheit erhöht und die Verwaltung vereinfacht. Bekannte Passwortmanager sind LastPass, 1Password, Protonpass und Bitwarden. Sie sind essenziell, um die Sicherheit persönlicher und sensibler Daten zu gewährleisten.

Personenbezogene Daten

Personenbezogene Daten sind Informationen, die sich auf eine identifizierbare Person beziehen, wie Name, Adresse, Geburtsdatum und Kontodaten. Der Schutz dieser Daten ist entscheidend, um die Privatsphäre und Sicherheit der betroffenen Personen zu gewährleisten.

PGP (Pretty Good Privacy)

PGP ist eine Verschlüsselungssoftware, die zur sicheren Kommunikation und Datenübertragung verwendet wird. Sie nutzt ein Schlüsselpaar aus öffentlichem und privatem Schlüssel, um Nachrichten zu verschlüsseln und zu entschlüsseln. PGP bietet hohe Sicherheit und wird häufig für E-Mail-Verschlüsselung verwendet.

Phishing

Phishing ist eine Betrugsmethode, bei der versucht wird, persönliche Daten wie Passwörter oder Kreditkarteninformationen zu stehlen, indem eine Person sich als vertrauenswürdig ausgibt. Dies geschieht durch gefälschte E-Mails oder Webseiten. Wachsamkeit und Überprüfung der Quellen sind entscheidend.

Privater Schlüssel

Ein privater Schlüssel ist Teil eines kryptografischen Schlüsselpaares und wird zur Entschlüsselung von Daten verwendet, die mit dem öffentlichen Schlüssel verschlüsselt wurden. Er muss geheim gehalten werden, da er den Zugriff auf die verschlüsselten Informationen ermöglicht.

R

Ransomware

Ransomware ist eine schädliche Software, die Daten auf einem infizierten System verschlüsselt und Lösegeld fordert, um die Entschlüsselung zu ermöglichen. Schutzmaßnahmen umfassen regelmäßige Backups, Antiviren-Software und vorsichtiges Verhalten beim Öffnen von Dateien und E-Mails.

Recht auf Löschung

Das Recht auf Löschung ist ein Datenschutzrecht, das Einzelpersonen das Recht gibt, die Löschung ihrer personenbezogenen Daten zu verlangen. Unternehmen müssen diesem Antrag nachkommen, sofern keine rechtlichen Gründe dagegensprechen. Dies hilft, die Privatsphäre der Betroffenen zu schützen.

S

Sicherer Ort

Ein sicherer Ort ist ein physischer oder digitaler Speicherplatz, der vor unbefugtem Zugriff geschützt ist. Beispiele sind verschlossene Schränke, sichere Server oder verschlüsselte Cloud-Speicher. Daten und wichtige Dokumente sollten an sicheren Orten aufbewahrt werden, um ihre Integrität zu gewährleisten.

Sicherheitszertifikat

Ein Sicherheitszertifikat ist eine digitale Datei, die die Identität einer Webseite oder eines Servers bestätigt und die verschlüsselte Kommunikation ermöglicht. Zertifikate werden von vertrauenswürdigen Zertifizierungsstellen ausgestellt und helfen, die Sicherheit von Online-Transaktionen zu gewährleisten.

Signal App

Signal ist eine Messaging-App, die Ende-zu-Ende-Verschlüsselung für sichere Kommunikation bietet. Sie ermöglicht das Senden von Nachrichten, Bildern und Videos sowie Sprach- und Videoanrufe. Signal ist bekannt für seine starken Sicherheitsfunktionen und den Schutz der Privatsphäre.

SMTP (Simple Mail Transfer Protocol)

SMTP ist ein Protokoll, das zum Senden von E-Mails verwendet wird. Es regelt den Austausch von E-Mails zwischen Servern und ermöglicht die Zustellung von Nachrichten an die Empfänger. SMTP ist ein grundlegender Bestandteil der E-Mail-Kommunikation.

SPAM

SPAM sind unerwünschte E-Mails, die in großen Mengen versendet werden. Sie können Werbung, Betrugsversuche oder schädliche Links enthalten. SPAM-Filter helfen, diese E-Mails zu erkennen und zu blockieren, um die Sicherheit und Ordnung im Posteingang zu gewährleisten.

T

Terminalserver

Ein Terminalserver ist ein Server, der Personen den Zugriff auf Anwendungen und Daten über ein Netzwerk ermöglicht. Er zentralisiert die Verwaltung und bietet eine sichere Umgebung für die Nutzung von Software und Daten, insbesondere in Unternehmensnetzwerken.

TLS (Transport Layer Security)

TLS ist ein Protokoll, das die Sicherheit der Datenübertragung im Internet gewährleistet. Es verschlüsselt die Kommunikation zwischen Client und Server und schützt die Daten vor Abhörversuchen und Manipulation. TLS wird häufig bei HTTPS-Verbindungen verwendet.

TOTP (Time-Based-One-Time Password)

TOTP ist ein Algorithmus, der zeitbasierte Einmal-Codes für die Zwei-Faktor-Authentifizierung (2FA) generiert. Diese Codes sind nur für kurze Zeit gültig und erhöhen die Sicherheit, da sie regelmäßig aktualisiert werden. TOTP wird häufig von Authentifizierungs-Apps verwendet.

Tracker

Tracker sind Technologien oder Skripte, die das Verhalten von Personen auf Webseiten verfolgen. Sie sammeln Daten über Seitenaufrufe, Klicks und andere Aktivitäten, um Analysen und personalisierte Werbung zu ermöglichen. Datenschutzmaßnahmen können helfen, die Verfolgung zu begrenzen.

Trojaner

Ein Trojaner ist eine Art von Malware, die sich als nützliche Software tarnt, um Menschen zur Installation der Software zu verleiten. Einmal installiert, kann er Daten stehlen, Systeme beschädigen oder anderen schädlichen Code nachladen. Vorsicht beim Herunterladen und Installieren von Software ist wichtig.

U

Update

Ein Update ist eine Aktualisierung von Software, die Fehler behebt, Sicherheitslücken schließt und neue Funktionen hinzufügt. Regelmäßige Updates sind wichtig, um die Sicherheit und Leistung von Systemen und Anwendungen zu gewährleisten.

USB Stick

Ein USB-Stick ist ein tragbares Speichermedium, das über den USB-Anschluss mit einem Computer verbunden wird. Er ermöglicht den einfachen Transport und Austausch von Daten, kann aber auch Malware enthalten. Vorsicht beim Einstecken unbekannter USB-Sticks ist wichtig.

V

Verschlüsselung

Verschlüsselung ist ein Verfahren, bei dem Daten in eine unlesbare Form umgewandelt werden, die nur mit einem speziellen Schlüssel wieder entschlüsselt werden kann. Dies schützt die Daten vor unbefugtem Zugriff und ist besonders wichtig für sensible Informationen.

Virus

Ein Virus ist eine schädliche Software, die sich selbst verbreitet und Dateien oder Systeme infiziert. Viren können Daten beschädigen, stehlen oder das System funktionsunfähig machen. Schutzmaßnahmen umfassen Antivirussoftware und vorsichtiges Verhalten beim Öffnen von Dateien und E-Mails.

VPN (Virtual Private Network)

Ein VPN ist eine Technologie, die eine sichere und verschlüsselte Verbindung über das Internet ermöglicht. Es schützt die Datenübertragung und die Privatsphäre, indem es die IP-Adresse der Person verbirgt und den Datenverkehr verschlüsselt.

W

W-LAN Verbindung

Eine W-LAN-Verbindung ermöglicht drahtlosen Internetzugang über ein lokales Netzwerk. Sie ist praktisch, aber auch anfällig für Sicherheitsrisiken wie unbefugten Zugriff. Verschlüsselung und sichere Passwörter sind wichtig, um die Verbindung zu schützen.

Wiederherstellungscode

Ein Wiederherstellungscode ist ein spezieller Code, der verwendet wird, um den Zugriff auf ein Konto oder System wiederherzustellen, wenn das Passwort vergessen wurde oder der Zugang verloren gegangen ist. Er sollte sicher aufbewahrt werden, um im Notfall die Wiederherstellung zu ermöglichen.

Z

Zugangsdaten

Zugangsdaten sind Informationen, die benötigt werden, um sich bei einem System oder Dienst anzumelden, wie Kontoname und Passwort. Sie sollten sicher aufbewahrt und regelmäßig geändert werden, um unbefugten Zugriff zu verhindern.

Zugriffskontrolle

Zugriffskontrolle umfasst Maßnahmen, die den Zugang zu Daten und Systemen auf autorisierte Personen beschränken. Dies kann durch Passwörter, biometrische Daten oder andere Authentifizierungsmethoden erfolgen. Ziel ist es, die Sicherheit und Integrität der Daten zu gewährleisten.