IT Security

Schutziele:

CIA: 3 Hauptschutzziele

Vertraulichkeit

Nur berechtigte Personen und Systeme dürfen auf Daten zugreifen

Zugriffskontrolle / Verschlüsselung / VPN

Integrität

Daten müssen korrekt und unverändert bleiben, Manipulationen sollen erkannt werden

Prüfsummen / Signaturen / Versionskontrolle

Verfügbarkeit

Anwendungen und Daten müssen zur richtigen Zeit verfügbar sein.

Backups / Raid / Redundanzen / USV

Erweiterte Schutzziele:

Authentizität

Sicherstellen, dass ein Kommunikationspartner oder daten echt sind

SSL/-TLS-Zertifikate

Verbindlichkeit

Niemand kann abstreiten, etwas getan zu haben

Logging / Signaturen

Datenschutz

Schutz der Daten

DSGVO (nur so viele Daten wie nötig speichern)

Merksatz für die Prüfung:

CIA = Confidentiality, Integrity, Availability

Schutzmaßnahmen

Technische Schutzmaßnahmen

Zutrittskontrolle

Zugriffskontrolle

Verschlüsselung

Netzwerk

- IDS = Intrusion Detection System
- Firewalls
- DMZ = Demilitarisierte Zone
- VPN

Backups

- USV, Offline Backups, Raid

System Härtung

- Updates
- Unnötige Software deaktivieren
- Ports schließen
- Patch Management

Organisatorische Schutzmaßnahmen

- Audits – Mitarbeiter Schulungen
- Berechtigungskonzepte
  - Jeder hat die Rechte die er unbedingt braucht
- Penetrationstests
- Awarenesstests
- Sicherheitsrichtlinien
- Notfallmanagement#

Schutzmaßnahmen in der Softwareentwicklung

Versionskontrolle

Änderungen nachvollziehbar machen, Tests zur Qualitätssicherung

Secure Coding

Eingaben validieren und escapen (Schutz vor SQL Injection)

Clean Code

Quellcode kommentieren, Dokumentation schreiben

Code Reviews

Fehler frühzeitig erkennen

Typische Bedrohungen

Malware

Ransomware – verschlüsselt Daten und fordert Lösegeld

Trojaner – Tarnt sich als nützliche Software, enthält aber Schadcode

Rootkit – Tief im System verankert, das Admin Rechte hat

Spyware – Sammelt Informationen und gibt diese unbemerkt an Dritte weiter

Viren – Befallen Dateien, verbreiten sich durch Öffnen

Würmer – verbreitet sich Selbstständig über Netzwerke

Social-Engineering

Shoulder-Surfing – Durch beobachten an Informationen kommen

Phishing – Emails mit Links auf gefälschten Seiten

CEO Fraud – Gibt sich als Chef aus, um Mitarbeiter zu Überweisungen zu bewegen

Pretexting – Täuschung durch erfundene Geschichten, um an Zugangsdaten zu kommen

Vertrauen Missbrauchen

Angriffe auf Anwendungen

SQL-Injection – Einschleusen von schädlichen SQL Befehlen über Eingabefelder

Buffer Overflow – Ausnutzen von Programmierfehlern

Netzwerkangriffe

Dos/DDos – Server wird mit Anfragen überlastet, bis er nicht mehr antwortet

ARP-Sppofing/DNS-Spoofing – Umleitung von Netzwerkverkehr auf falsche Ziele

Man in the Middle – Angreifer klingt sich in die Kommunikation ein

Insider Threads

Absichtlich – Unzufriedene Mitarbeiter stehlen Daten

Unabsichtlich – Mitarbeiter klickt unvorsichtig auf einen Phishing Link

Backups

Vollbackup

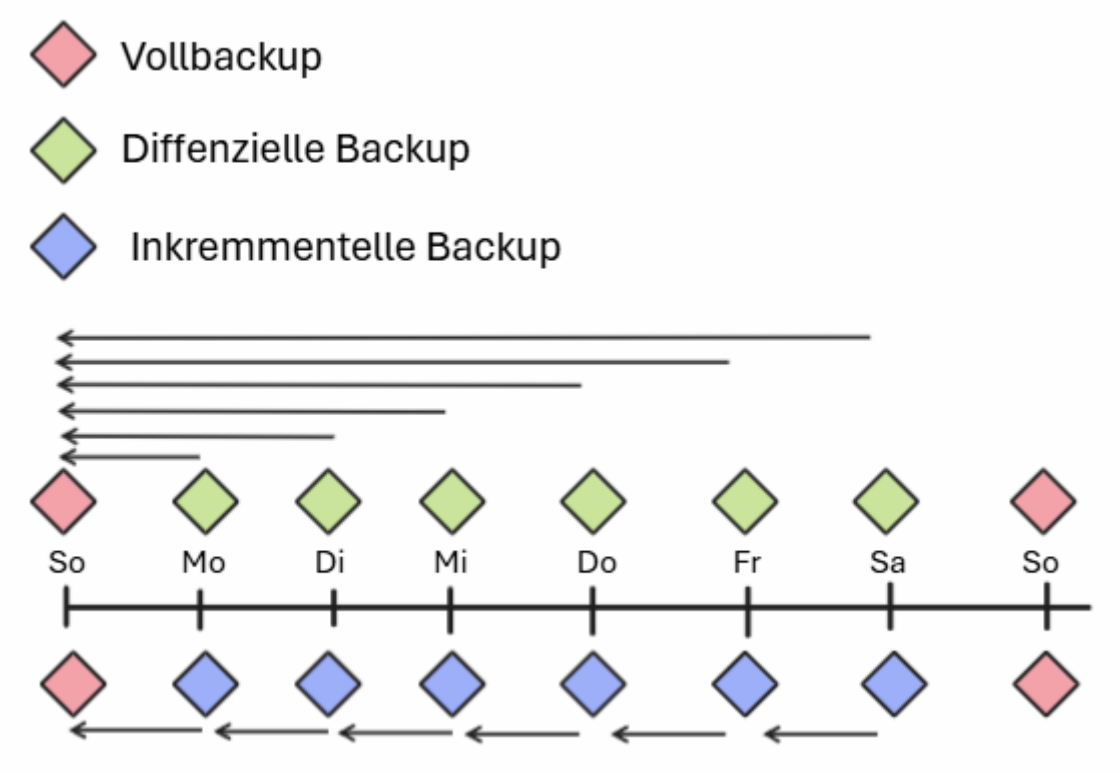
Vollständige Sicherung aller Daten

Inkrementelles Backup

Alle Änderungen seit dem letzten Backup

Differenzielles Backup

Alle Änderungen seit dem letzten Vollbackup



Verschlüsselung

Symmetrische Verschlüsselung

1 Key zum verschlüsseln und endschlüsseln

Schnell und weniger Rechenleistung benötigt

Schlüsselaustauschproblem

Schlüsselverwaltung sehr aufwendig

A-Symmetrische Verschlüsselung

2 Keys = 1 Privater & 1 Öffentlicher

Öffentliche für verschlüsseln

Private zum entschlüsseln

Kein Schlüsselaustauschproblem

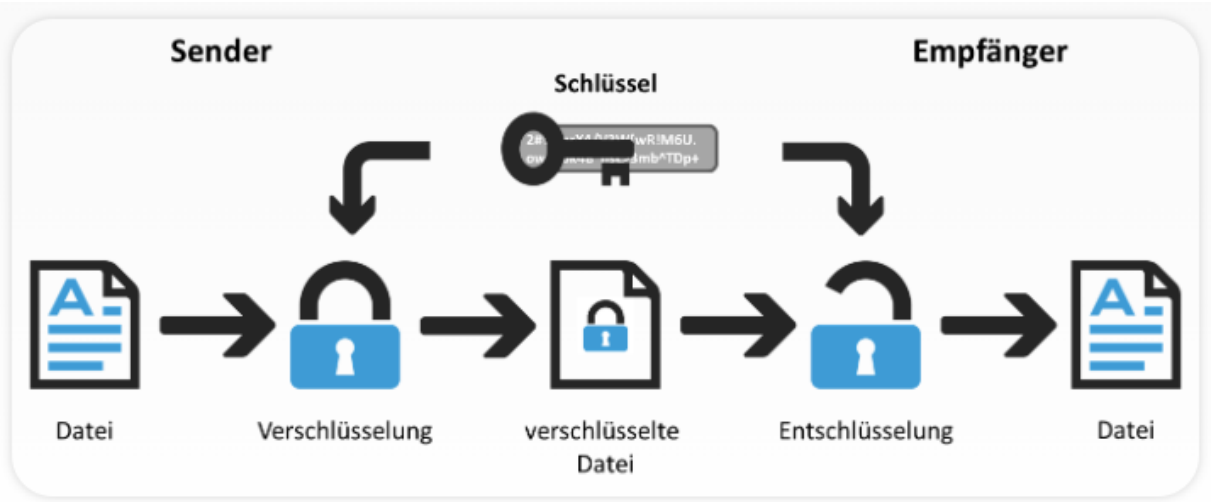
Langsamer und mehr Rechenleistung

Mit dem Privaten Schlüssel wird eine Signatur erstellt, mit dem öffentlich Schlüssel wird Sie dann überprüft.

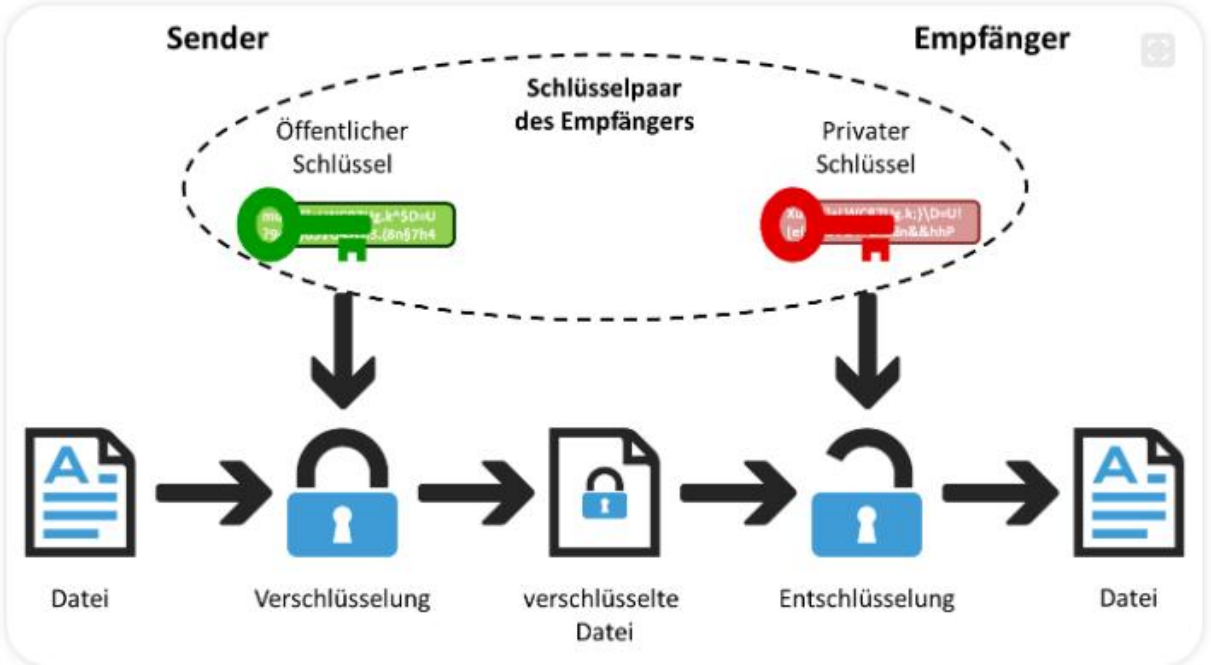
Hybride Verschlüsselung

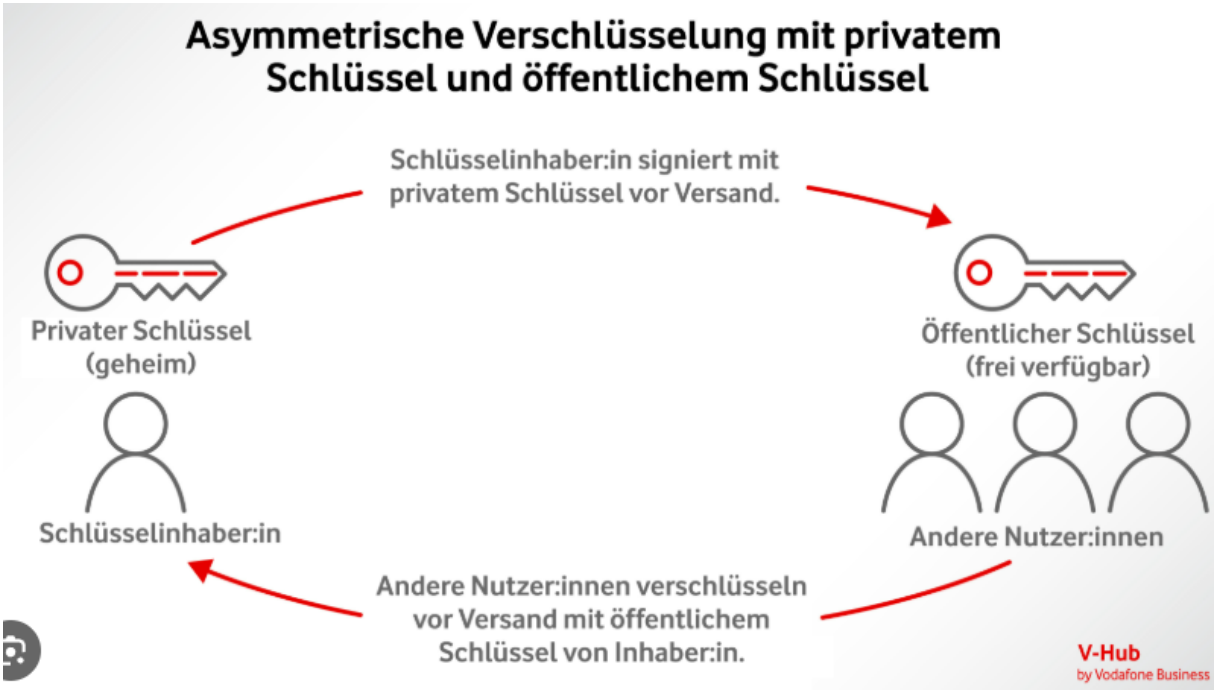
Wir nutzen die A-Symmetrische Verschlüsselung, um den Symmetrischen Schlüssel auszutauschen, die weitere Kommunikation findet dann symmetrisch statt.

Symmetrische Verschlüsselung



A-Symmetrische Verschlüsselung





Caesar Verschlüsselung

Versetzen der Buchstaben des Alphabets

Rene +3 Uhqh -3 Rene

BSI = Bundesamt für Sicherheit in der Informationstechnik

Sitz: Bonn

Gegründet: 1991

Zuständig für: IT-Sicherheit für Staat, Wirtschaft, Gesellschaft

Untersteht: Bundesministerium des Inneren und für Heimat (BMI)

Aufgaben:

Sicherheitsberatung für Behörden und Unternehmen

- Entwicklung von Standrads und Empfehlungen (IT-Grundschutz)
- Sicherheitsbewertungen von IT-Produkten

IT Grundschutzkatalog

- Sammlungen von Best Practices und Maßnahmen zur Informationssicherheit

Warnungen und Informationen

- Herausgabe von Sicherheitswarnungen bei aktuellen IT-Bedrohungen
- Betreiben der Plattform – bsi-fuer-buerger.de

Krypto & Zertifizierung

- Entwickeln und Prüfung von Verschlüsselungsverfahren
- Zulassung von Sicherheitsprodukten für Behörden

Betreiber von CERT-Bund

- Das „Computer Emergency Response Team“ für Bundesbehörden

Merksatz:

Das BSI ist die zentrale staatliche Stelle für IT-Sicherheit in Deutschland

Kreuzreferenztabelle

DSGVO

Daten Schutz Grund Ver Ordnung

Gültigkeitsbereich: Europäische Gesetzgebung

Gegründet: 2018

Die DSGVO regelt bzw. legt fest, wie mit Personenbezogenen Daten umgegangen werden muss.

Rechte:

- Recht auf vergessen (Löschung)
- Auskunftsrecht
- Änderungsrecht
- Informationsrecht (was wird mit den Daten gemacht)
- Wie werden meine Daten behandelt und weitergegeben
- Recht auf Übertragbarkeit

Was genau sind personenbezogene Daten?

- Alle Daten, die direkt oder auch indirekt auf eine Person zurückzuführen sind.

Direkte Identifikation:

- Name, Vorname
- Adresse
- Telefonnummer
- Email Adresse
- Kundennummer, Personalausweisnummer

Indirekte Identifikation:

- IP-Adresse
- Standortdaten (GPS)
- Cookies & Online ID ´s
- Fahrzeugkennzeichen

Besondere Kategorie: besonders Schützenswert

- Gesundheitsdaten
- Biometrische Daten
- Politische Meinung
- Gewerkschaftszugehörigkeit
- Religion
- Ethische Herkunft

- Nicht personenbezogen:
- Anonymisiert
- Aggregierte Daten
- Pseudonymisiert