



Information Security and Privacy

Modul D3.2 – Lecture 1.3

Referent: Dr. Jörg Cosfeld

Lecture 1.2 – Definitionen und Terminologie

Definitionen und Terminologie

Was ist IT Sicherheit?

Mit Hilfe der IT-Sicherheit sollen vorhandene Risiken, die durch Bedrohungen auf IT-Systeme wirken, auf ein angemessenes Maß reduziert werden.

IT-Sicherheit befasst sich daher mit **IT-Sicherheitsmaßnahmen**, die **Informationen** auf IT-Systemen vor dem Verlust von **Vertraulichkeit**, **Authentifikation**, **Authentizität**, **Integrität**, **Verbindlichkeit**, **Verfügbarkeit** und **Anonymisierung/Pseudonymisierung** schützt.

Definitionen und Terminologie

IT-Sicherheit beinhaltet auch die Aspekte der **Softwaresicherheit** und **Zuverlässigkeit** von **IT-Systemen**. IT-Sicherheit schützt IT-Systeme, um Schäden für Unternehmen, Behörden, Organisationen und Personen zu vermeiden.



Verschlüsselung

Verschlüsselung:

Das Ziel der Verschlüsselung besteht darin, Daten in einer solchen Weise einer mathematischen Transformation zu unterziehen, dass es einem Unbefugten unmöglich ist, die Originaldaten aus den transformierten, verschlüsselten Daten zu rekonstruieren.

Damit die verschlüsselten Daten für ihren legitimen Nutzer dennoch verwendbar bleiben, muss es diesem aber möglich sein, durch Anwendung einer inversen Transformation aus ihnen wieder die Originaldaten zu generieren.

Verschlüsselung

Verschlüsselung:

Das Ziel der Verschlüsselung besteht darin, Daten in einer solchen Weise einer mathematischen Transformation zu unterziehen, dass es einem Unbefugten unmöglich ist, die Originaldaten aus den transformierten, verschlüsselten Daten zu rekonstruieren.



Verschlüsselung

Verschlüsselung:

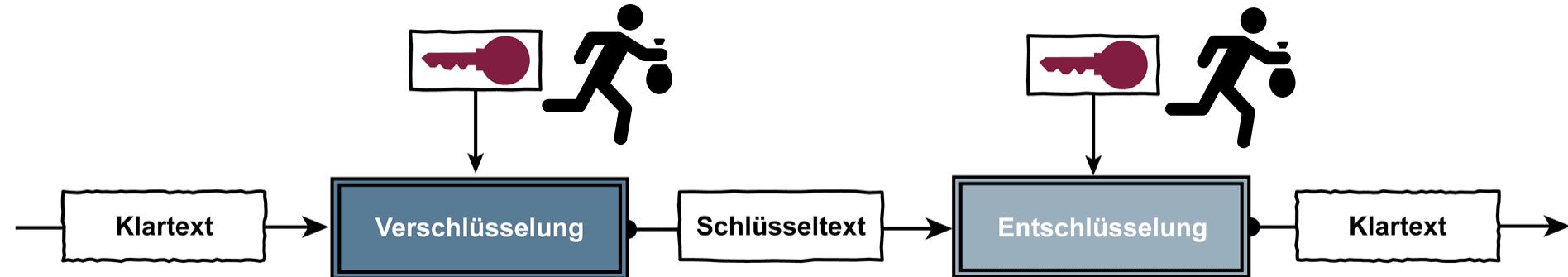
Die Originaldaten werden als Klartext bezeichnet, die transformierten Daten werden **Schlüsseltext** genannt. Die **Transformation** heißt **Verschlüsselung**, ihre Inverse **Entschlüsselung**.



Verschlüsselung

Verschlüsselung:

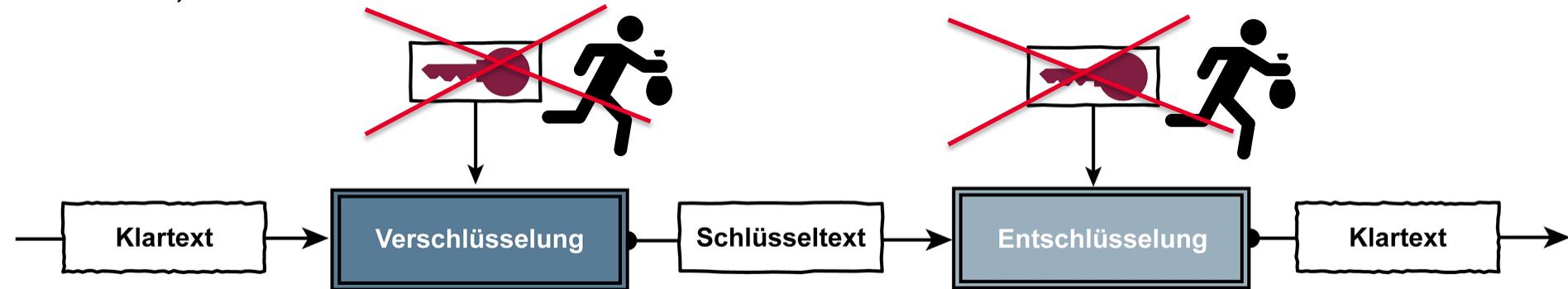
Die **Entschlüsselung** darf nur den **legitimen Empfängern/Besitzern** der übermittelten/gespeicherten Informationen möglich sein, **nicht jedoch anderen Personen** – im Extremfall nicht einmal den Absendern/Initiatoren selbst, die eine Information verschlüsselt haben.



Verschlüsselung

Verschlüsselung:

Die **Entschlüsselung** darf nur den **legitimen Empfängern/Besitzern** der übermittelten/gespeicherten Informationen möglich sein, **nicht jedoch anderen Personen** – im Extremfall nicht einmal den Absendern/Initiatoren selbst, die eine Information verschlüsselt haben.



Public Key – Infrastrukturen

PKI:

Public Key-Infrastrukturen (PKI) dienen der Erstellen und Verwalten von **Zertifikaten mit öffentlichen Schlüsseln** und weiteren Attributen.

Dabei kommt es, außer auf die sichere Erstellung und Speicherung gültiger Schlüssel, auch auf die Verifizierung der **ursprünglichen Identität** ihrer Inhaber – der **PKI-Nutzer** – an.

Public Key – Infrastrukturen

PKI:

Public Key-Infrastrukturen bestehen aus **Hardware**, **Software** und einem abgestimmten **Regelwerk**, der **Leitlinie**. Diese definiert, nach welchen Sicherheitsregeln die Dienstleistungen um die **Zertifikate** erbracht werden.

Räumliche Trennung von PKI Schlüssel und Nutzerverwaltung!

Public Key – Infrastrukturen

PKI:

Public Key-Infrastrukturen bestehen aus **Hardware**, **Software** und einem abgestimmten **Regelwerk**, der **Leitlinie**. Diese definiert, nach welchen Sicherheitsregeln die Dienstleistungen um die **Zertifikate** erbracht werden.

Analogie zu **Standesamt** und **Einwohnermeldeamt**



Max Mustermann existiert
mit richtigen Namen

Public Key – Infrastrukturen

Analogie zu **Standesamt** und **Einwohnermeldeamt**



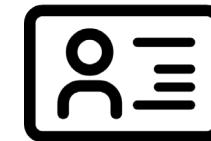
Max Mustermann existiert
mit richtigen Namen

Standesamt



Verwaltet Daten von
Max Mustermann.

Einwohnermeldeamt



Stellt als Dienstleistung den
Ausweis aus

Authentifikation

Authentifikation bezeichnet einen Prozess, in dem überprüft wird, ob „jemand“ oder „etwas“ **echt** ist.

Die digitale Identität wird verifiziert. In **ein** oder **zweiphasigen** Stufen.

Es gibt diverse **Klassen** von **Authentifizierungsverfahren**.

Authentifikation - Klassen

Wissen: Bei dieser Klasse von Authentifizierungsverfahren wird über einen Nachweis der Kenntnis von **Wissen** die **Echtheit eines Nutzers** überprüft.

Passwort, PIN und Sicherheitsfrage

Dies kann passieren:

Wissen vergessen, Wissen kann dupliziert werden, Wissen kann erraten werden, Wissen kann mitgelesen werden

Authentifikation - Klassen

Besitz: Verwendung eines Besitztums für das Authentifizierungsverfahren ist eine weitere Klasse.

Token, SIM-Karte, neuer Personalausweis

Dies kann passieren:

Besitz ist mit Kosten verbunden, Besitz muss mitgeführt werden, Besitz kann verloren gehen, Besitz kann gestohlen werden

Authentifikation - Klassen

Sein: Bei dieser Klasse von Authentifizierungsverfahren muss der Nutzer gegenwärtig sein.

Biometrische Merkmale, FaceID, Fingerprint

Dies kann passieren:

Merkmale werden immer mitgeführt, Merkmale können nicht weitergegeben werden, keine 100% Aussagekraft,

Authentifikation - Klassen

Weitere unterstützende Faktoren: Es können noch weitere unterstützende Faktoren für die Beurteilung der Echtheit des Nutzers herangezogen werden.

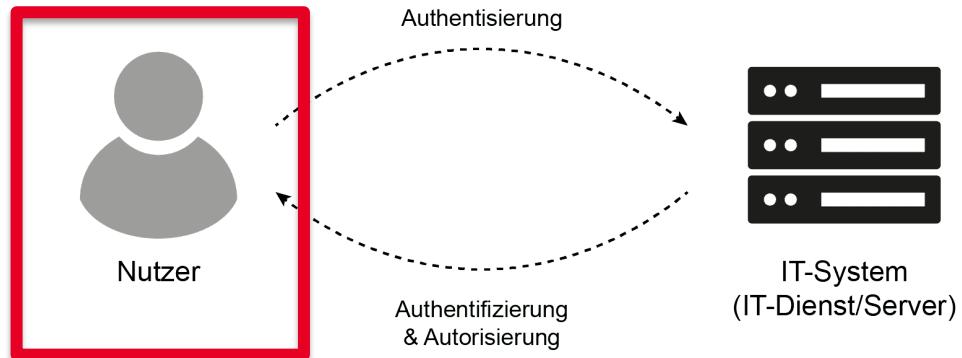
Reputation, Standort, Zeit, Technologie

Authentifikation – Architektur

Ablauf:

Aus der Sicht des Nutzers und des IT-Systems werden **IT-Sicherheitsfunktionen** umgesetzt, die verschiedene **Sicherheitsdienste** erbringen.

Authentisierung (Sichtweise Nutzer): Der Nutzer authentisiert sich gegenüber einem IT-System

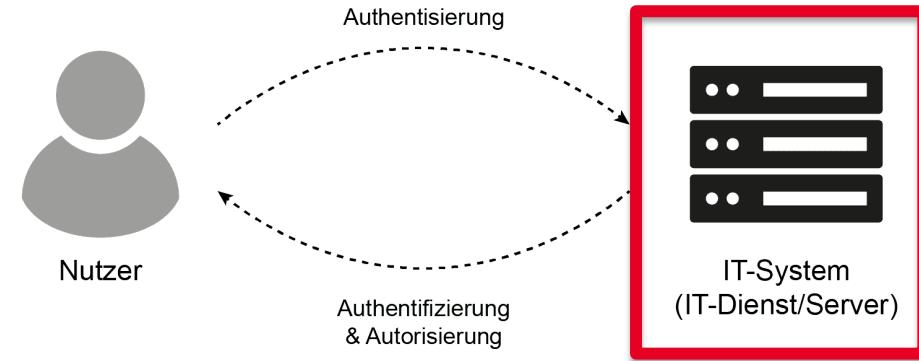


Authentifikation – Architektur

Ablauf:

Aus der Sicht des Nutzers und des IT-Systems werden **IT-Sicherheitsfunktionen** umgesetzt, die verschiedene **Sicherheitsdienste** erbringen.

Authentifizierung (Sichtweise IT-System): Das IT-System (Endgerät, Server, IT-Dienst, Cloud, ...) überprüft den Nachweis, um die Echtheit der digitalen Identität eines Nutzers im Rahmen der Authentifizierung festzustellen.

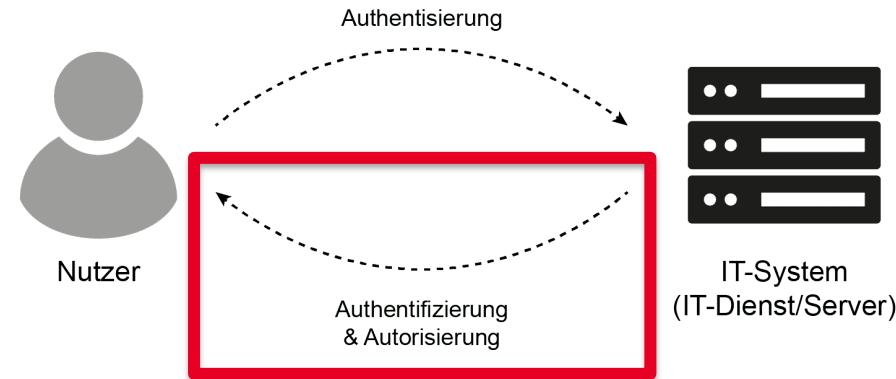


Authentifikation – Architektur

Ablauf:

Aus der Sicht des Nutzers und des IT-Systems werden **IT-Sicherheitsfunktionen** umgesetzt, die verschiedene **Sicherheitsdienste** erbringen.

Autorisierung (Sichtweise IT-System): Wenn die Echtheit der digitalen Identität eines Nutzers erfolgreich verifiziert werden konnte, kann das IT-System (Endgerät, Server, IT-Dienst, Cloud, ...) dem Nutzer definierte Rechte einräumen.

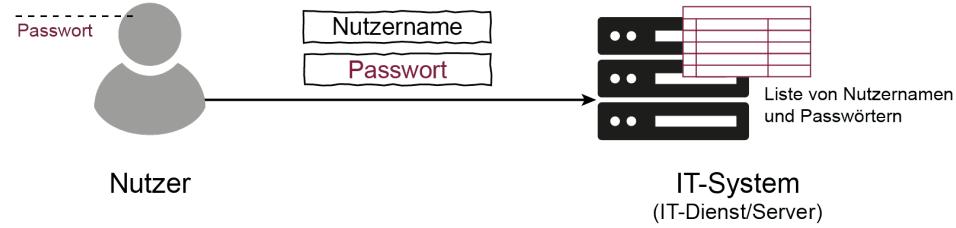


Generelle Authentifikationsverfahren

- Passwort-Verfahren
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren

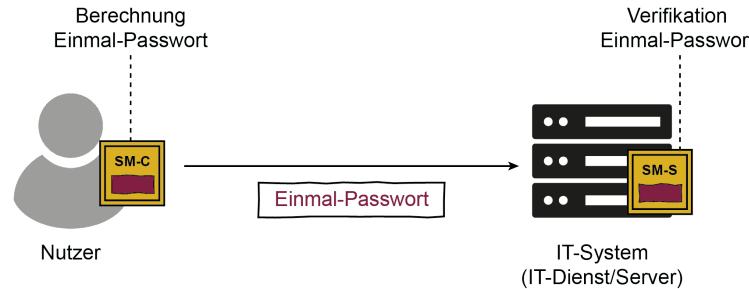
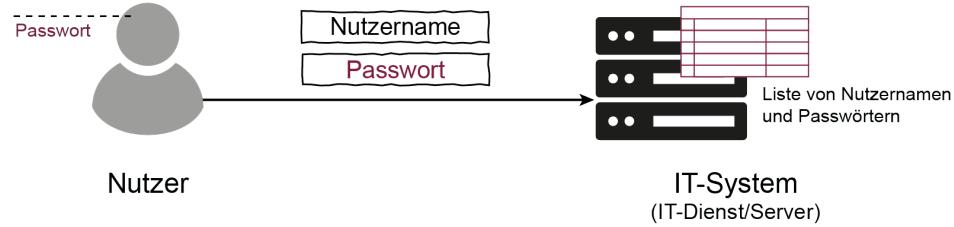
Generelle Authentifikationsverfahren

- Passwort-Verfahren
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren



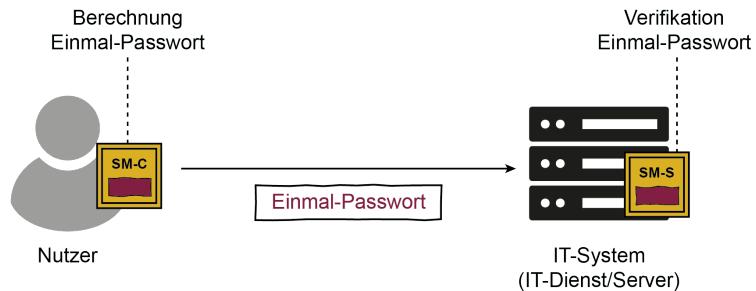
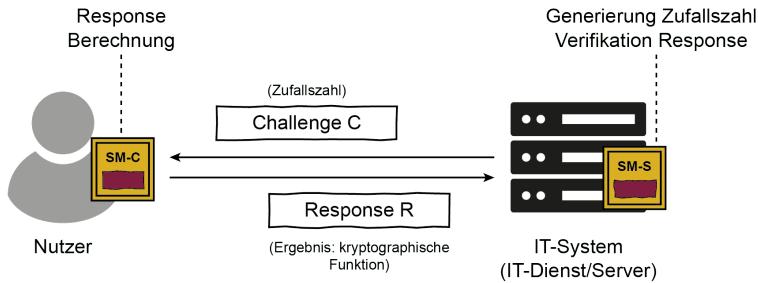
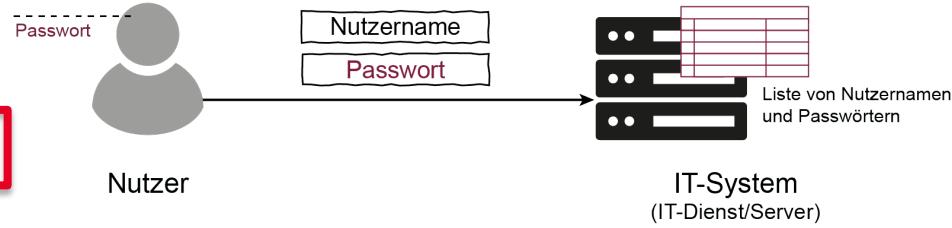
Generelle Authentifikationsverfahren

- Passwort-Verfahren
- **Einmal-Passwort-Verfahren**
- Challenge-Response-Verfahren
- Biometrische Verfahren



Generelle Authentifikationsverfahren

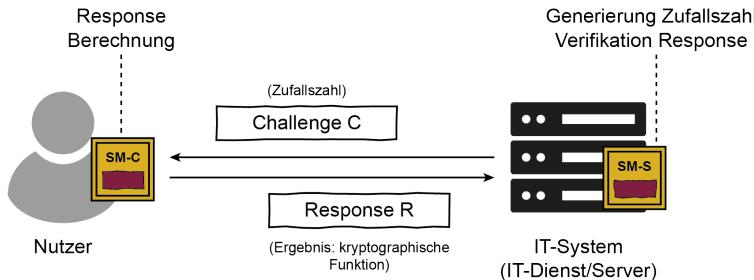
- Passwort-Verfahren
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren



Generelle Authentifikationsverfahren

- Passwort-Verfahren
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren

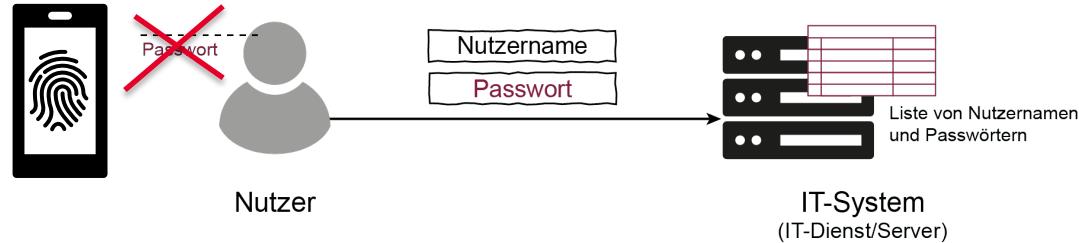
Beim Challenge-Response-Verfahren wird festgelegt, dass ein Nutzer sich gegenüber dem IT-System kryptografisch beweisen muss.



Beispiel: AppleID

Generelle Authentifikationsverfahren

- Passwort-Verfahren
- Einmal-Passwort-Verfahren
- Challenge-Response-Verfahren
- Biometrische Verfahren



Hardware Sicherheitsmodul

Definition:

Das Ziel eines **Hardware-Sicherheitsmodules** ist ein hoher **Schutz** vor **Auslesen** und **Manipulation** von besonders sensiblen, sicherheitsrelevanten Informationen.

- **Geheime Schlüssel**
 - Die nicht kopiert werden dürfen
 - **Programme**
 - Die nicht manipuliert werden dürfen
 - **Daten**
 - Von besonderen Wert
- Aber wie?

Hardware Sicherheitsmodul

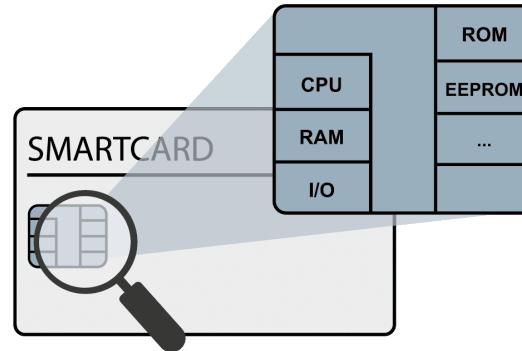
Definition:

Das Ziel eines **Hardware-Sicherheitsmodules** ist ein hoher **Schutz** vor **Auslesen** und **Manipulation** von besonders sensiblen, sicherheitsrelevanten Informationen.

- **Smartcards**

Karte von EC Kartengröße. Ist im Besitz einer ROM CPU und einem Arbeitsspeicher.

Geheimer **RSA-Schlüssel** oder andere symmetrische **Schlüssel** sowie **persönliche Daten (Passwörter etc.)** sicher gespeichert sind.



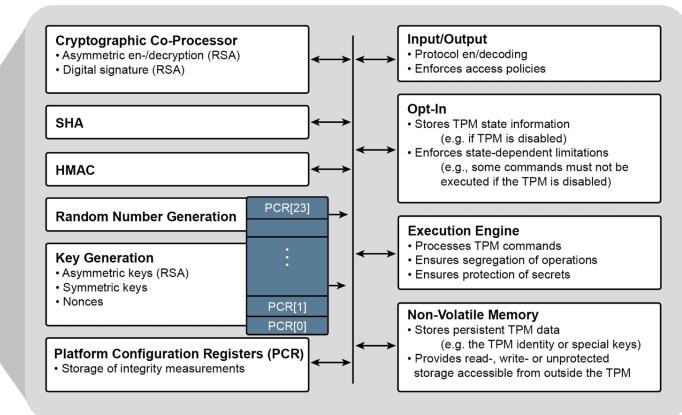
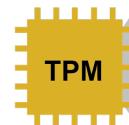
Hardware Sicherheitsmodul

Definition:

Das Ziel eines **Hardware-Sicherheitsmodules** ist ein hoher **Schutz** vor **Auslesen** und **Manipulation** von besonders sensiblen, sicherheitsrelevanten Informationen.

- **Trusted Platform Module**

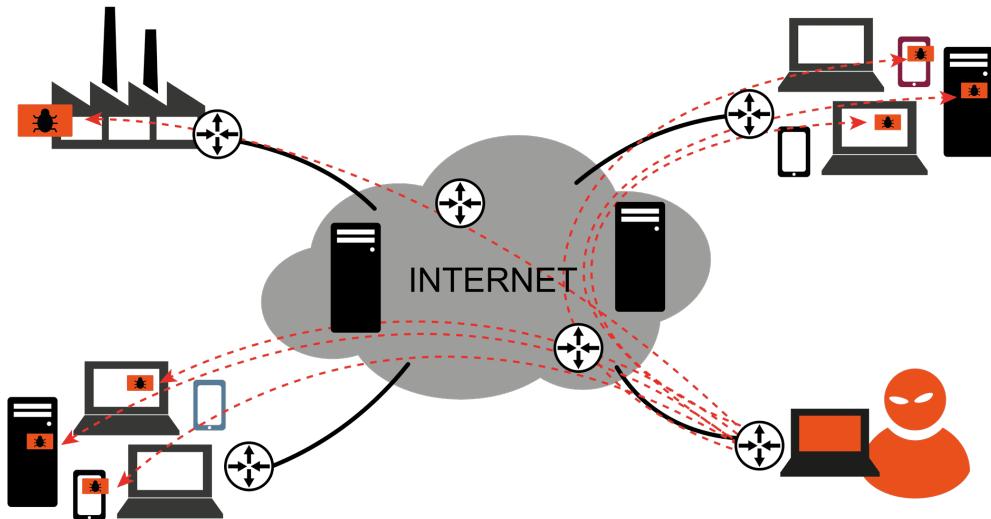
Onboard Smartcard in Notebooks.



Anti Maleware

Definition:

Malware ist der Oberbegriff für „Schadsoftware“ wie Viren, Würmer, trojanische Pferde und Ähnlichem.



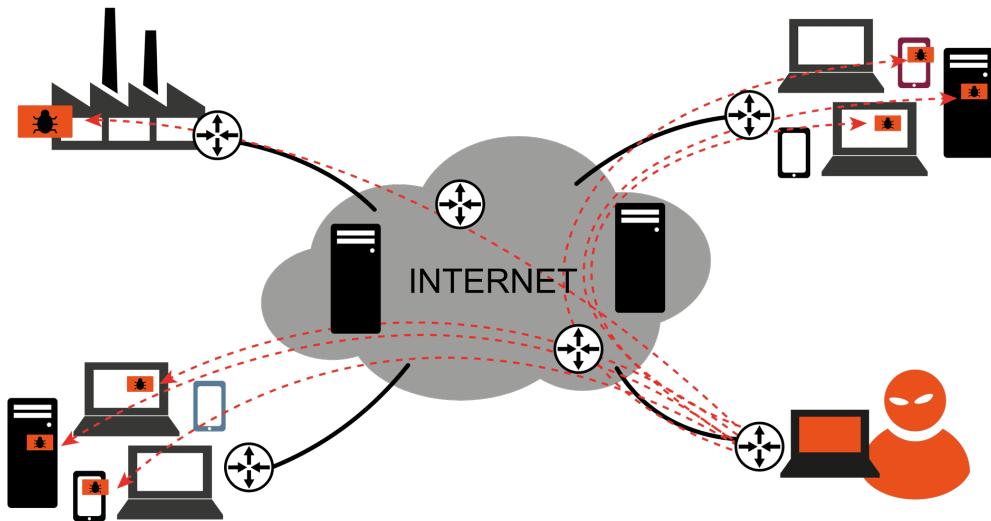
Ransomware

böswillige Schadfunktion in Malware, die wichtige Daten auf dem kompromittierten IT-System verschlüsselt, um Lösegeld verlangen zu können.

Anti Maleware

Definition:

Malware ist der Oberbegriff für „Schadsoftware“ wie Viren, Würmer, trojanische Pferde und Ähnlichem.



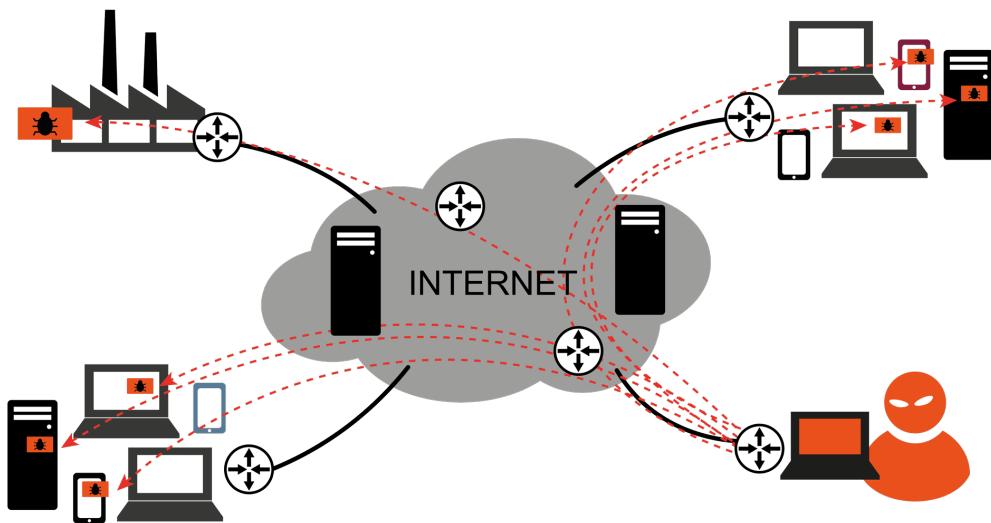
Keylogger

Ein Keylogger ist eine Schadfunktion in einer Malware, die alle Informationen (Nutzernamen/Passwörter, Bankdaten, Kreditdaten usw.), die über die Tastatur oder andere Eingabegeräte vom Nutzer in das eigene IT-System eingegeben werden, stiehlt.

Anti Maleware

Definition:

Malware ist der Oberbegriff für „Schadsoftware“ wie Viren, Würmer, trojanische Pferde und Ähnlichem.



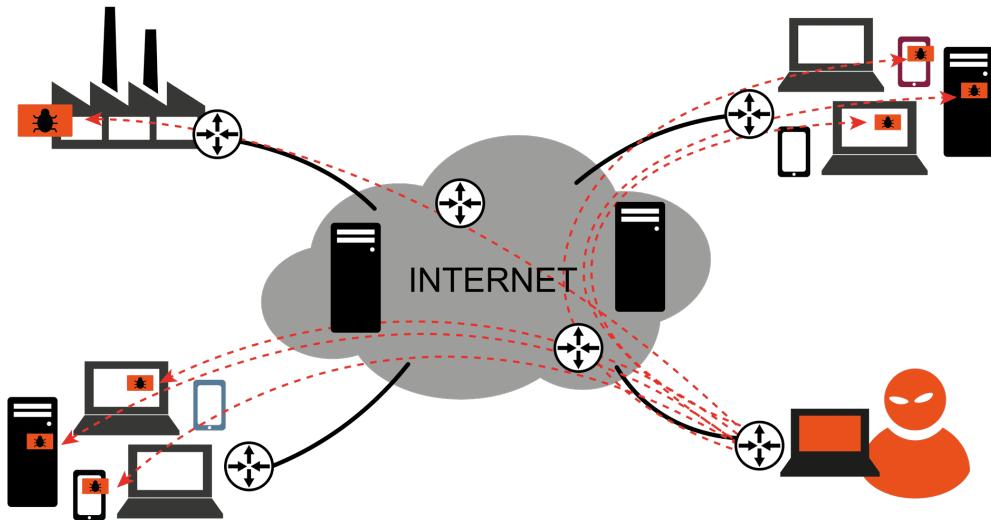
Click-Fraud

Eine Klickbetrug-Schadfunktion in Malware klickt auf kommerzielle Werbeflächen, um das genutzte Abrechnungssystem zum Vorteil des Angreifers zu manipulieren und damit Geld zu verdienen.

Anti Maleware

Definition:

Malware ist der Oberbegriff für „Schadsoftware“ wie Viren, Würmer, trojanische Pferde und Ähnlichem.



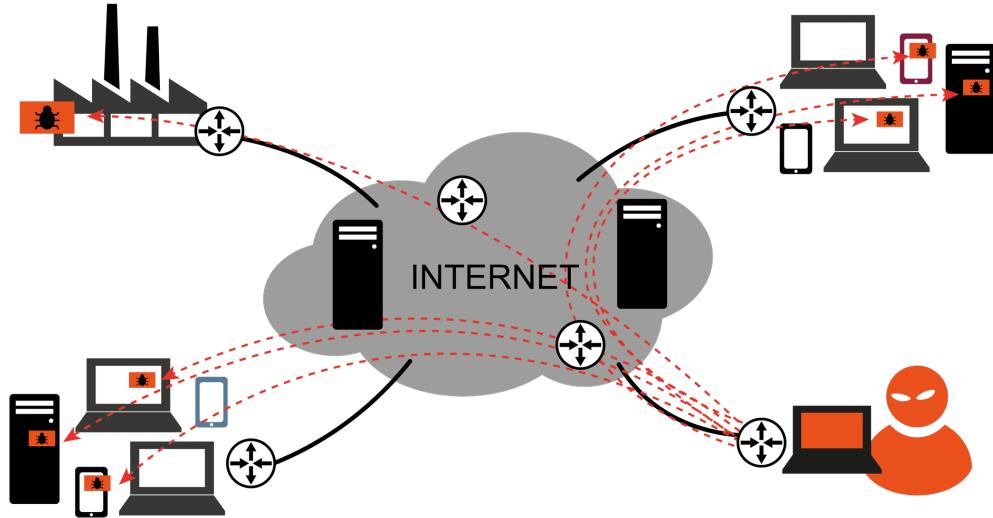
Adware

Eine Adware ist eine Schadfunktion in Malware, die auf dem eigenen IT-System unerlaubt Werbung anzeigen, private Daten stiehlt und Suchanfragen umleitet.

Anti Maleware

Definition:

Malware ist der Oberbegriff für „Schadsoftware“ wie Viren, Würmer, trojanische Pferde und Ähnlichem.

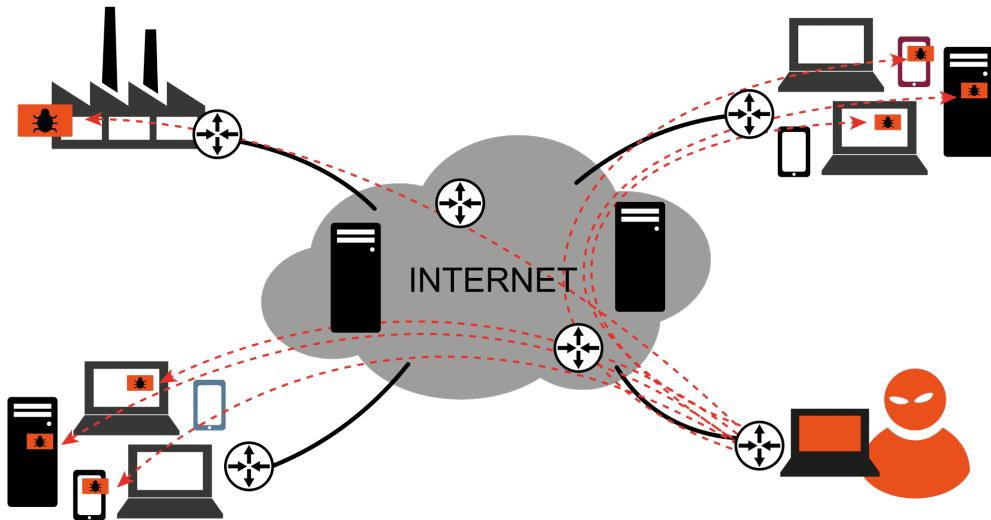


Was kann man tun?

Anti Maleware

Definition:

Malware ist der Oberbegriff für „Schadsoftware“ wie Viren, Würmer, trojanische Pferde und Ähnlichem.

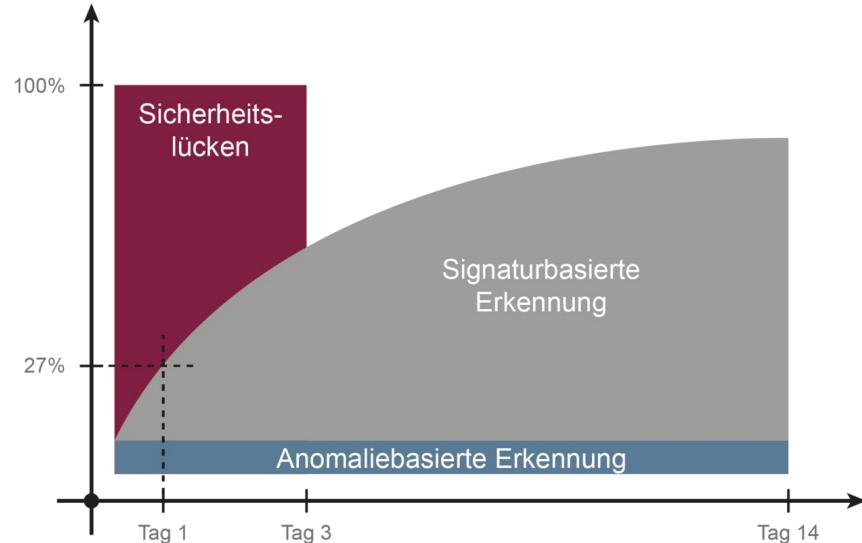


Anti-Malware-Lösungen haben das Ziel, Malware zu erkennen und damit entsprechende Angriffe zu verhindern. Die Anti-Malware-Lösungen haben heute bei **Massen-Angriffen mit 75 % bis 95 % eine zu schwache Erkennungsrate.**

Anti Maleware

Definition:

Malware ist der Oberbegriff für „Schadsoftware“ wie Viren, Würmer, trojanische Pferde und Ähnlichem.



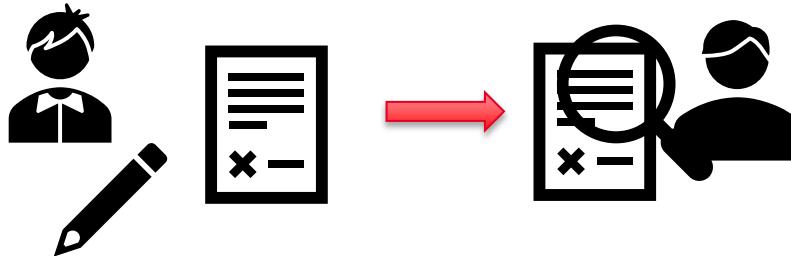
Anti-Malware-Lösungen haben das Ziel, Malware zu erkennen und damit entsprechende Angriffe zu verhindern. Die Anti-Malware-Lösungen haben heute bei **Massen-Angriffen mit 75 % bis 95 % eine zu schwache Erkennungsrate.**

Mail Sicherheit

Definition:

Der Austausch von E-Mails ist eine sehr häufig genutzte Anwendung im Internet.

- Hohe Werte
 - Vertragsentwürfe
 - Entwicklungsunterlagen
 - Kundendaten



OK

Oder

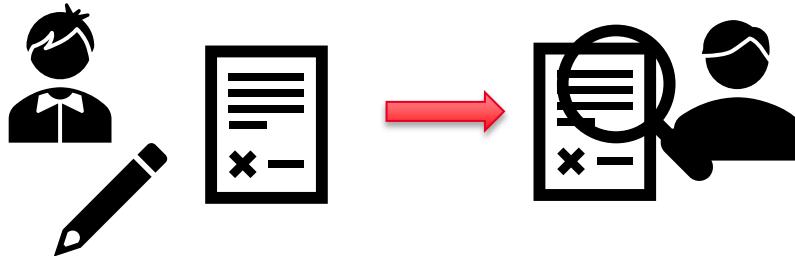
Nicht OK

Mail Sicherheit

Definition:

Der Austausch von E-Mails ist eine sehr häufig genutzte Anwendung im Internet.

- Hohe Werte
 - Vertragsentwürfe
 - Entwicklungsunterlagen
 - Kundendaten



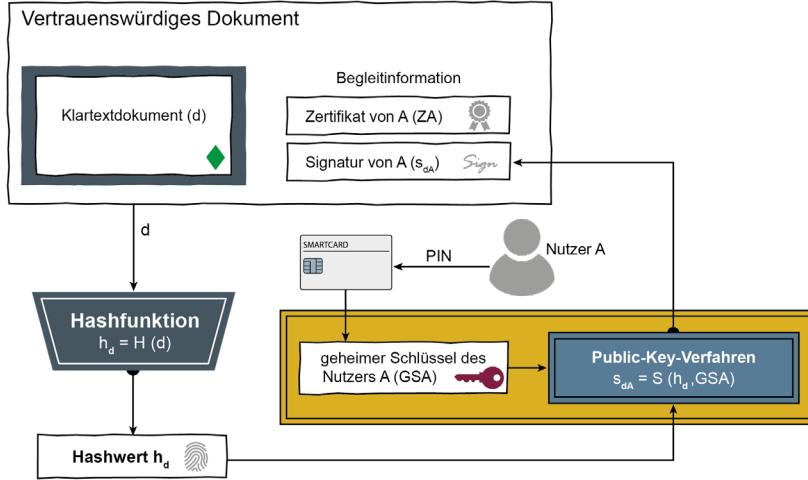
OK

Oder

Nicht OK

**Gleiche Sicherheit soll
im Mailversand
erreicht werden.**

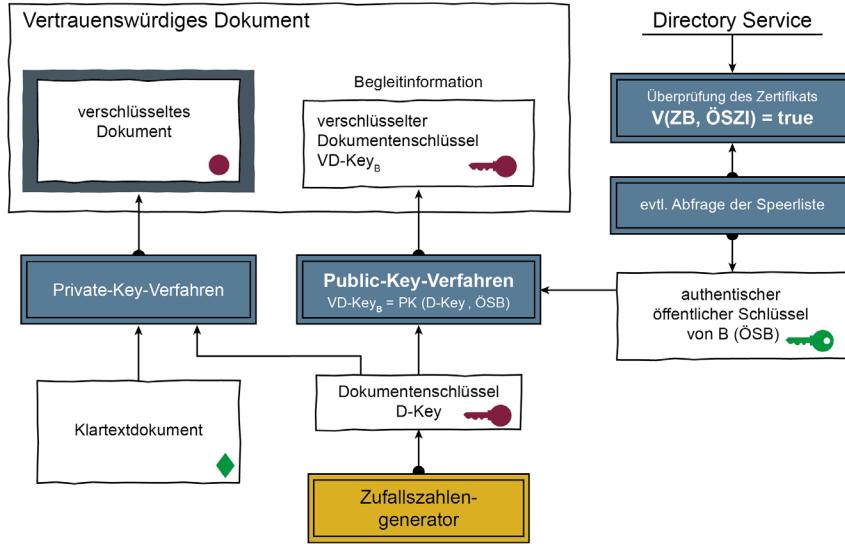
Mail Sicherheit



- Erstellung einer elektronischen Information.
- Nutzer ruft Signatur Funktion auf
- Dokument wird eine Signatur beigelegt
- Ein Zertifikat des Nutzers wird der Mail beigelegt

Digitalen Signatur in Verbindung mit einem digitalen Zeitstempel

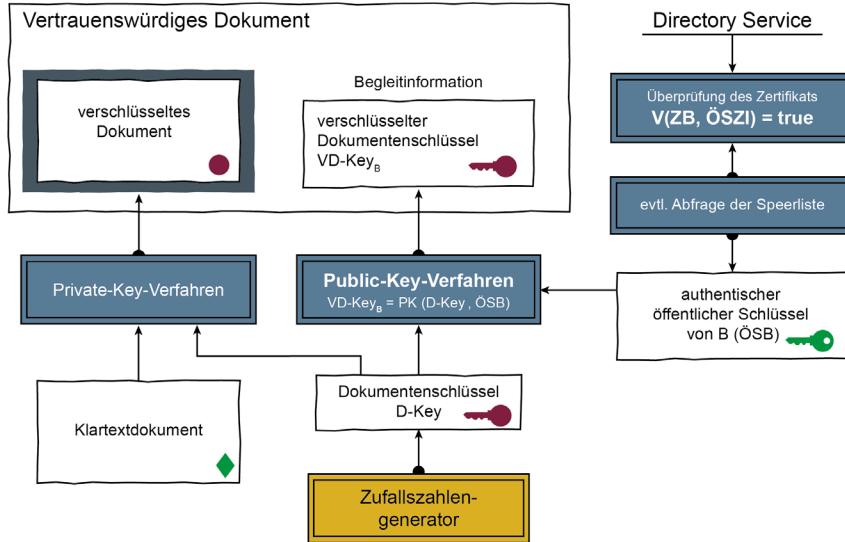
Mail Sicherheit



- Eine Verschlüsselungsfunktion verschlüsselt das Dokument
- Der Brief wird verschlossen und versiegelt.

Digitalen Signatur in Verbindung mit einem digitalen Zeitstempel

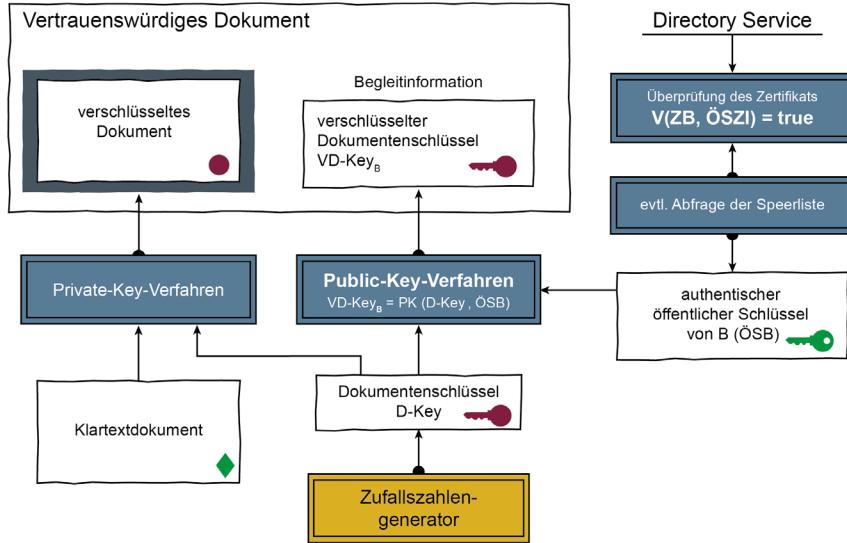
Mail Sicherheit



- Eine Verschlüsselungsfunktion verschlüsselt das Dokument
- Der Brief wird verschlossen und versiegelt.
- Dokumentenschlüssel (D-Key) eine qualitative Zufallszahl

Digitalen Signatur in Verbindung mit einem digitalen Zeitstempel

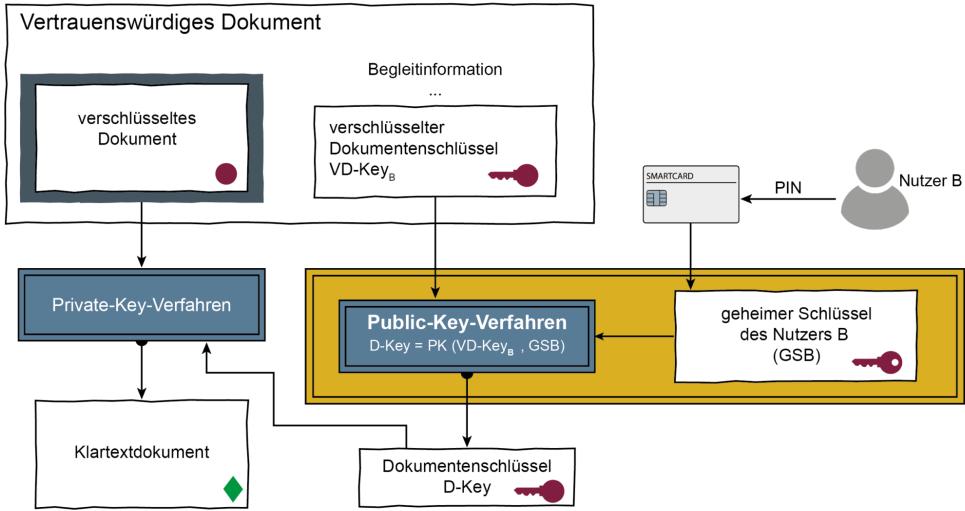
Mail Sicherheit



Digitale Signatur in Verbindung mit einem digitalen Zeitstempel

- Eine Verschlüsselungsfunktion verschlüsselt das Dokument
- **Der Brief wird verschlossen und versiegelt.**
- Dokumentenschlüssel (D-Key) eine qualitative Zufallszahl
- Das **Klartext-Dokument** wird dann unter Verwendung des **Dokumentenschlüssels** mit dem **Private Key-Verfahren** verschlüsselt

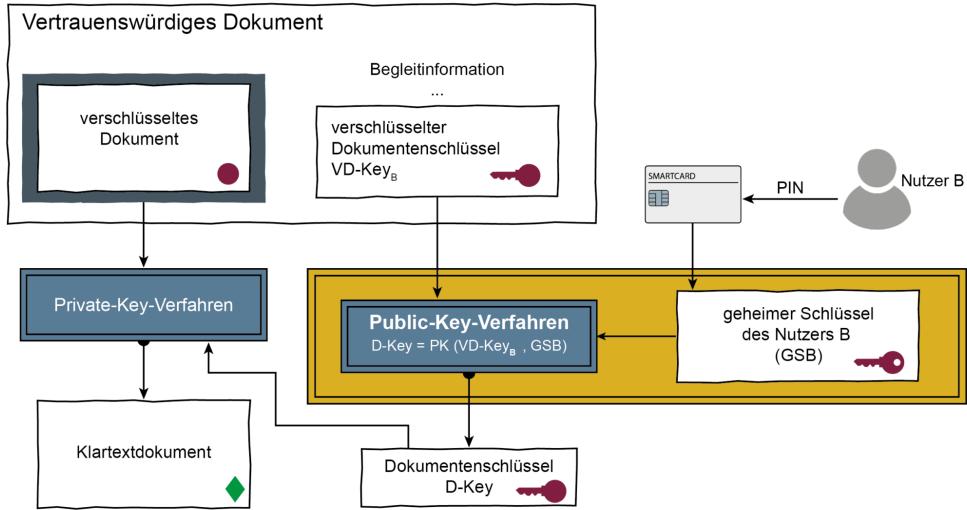
Mail Sicherheit



- Zuerst wird der Empfänger B aufgefordert, mithilfe seiner PIN seine Smartcard zu aktivieren

Entschlüsselung der Mail

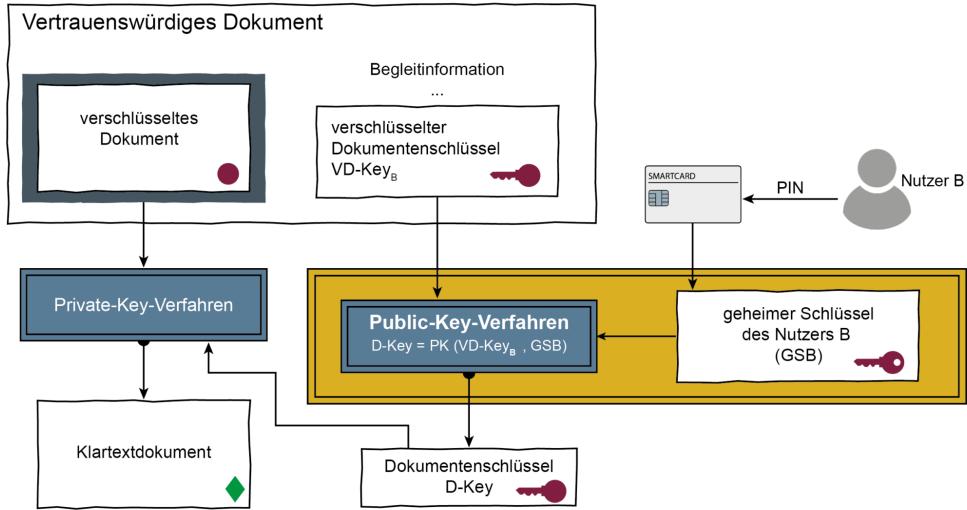
Mail Sicherheit



- Zuerst wird der Empfänger B aufgefordert, mithilfe seiner PIN seine Smartcard zu aktivieren
- Anschließend wird das Dokument unter **Verwendung des Private Key-Verfahrens** mit dem **Dokumentenschlüssel (D-Key)** entschlüsselt und steht im Klartext zur Verfügung

Entschlüsselung der Mail

Mail Sicherheit



- Zuerst wird der Empfänger B aufgefordert, mithilfe seiner PIN seine Smartcard zu aktivieren
- Anschließend wird das Dokument unter **Verwendung des Private Key-Verfahrens** mit dem **Dokumentenschlüssel (D-Key)** entschlüsselt und steht im Klartext zur Verfügung

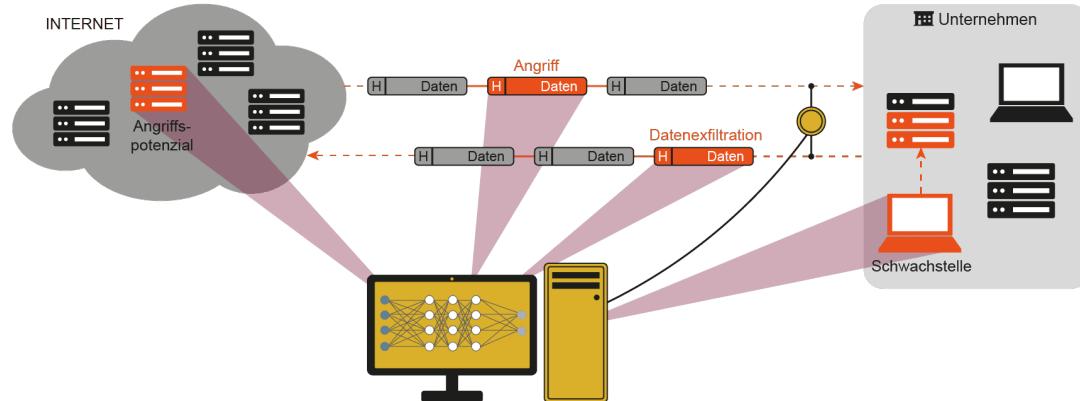
Entschlüsselung der Mail

Das gleiche kann für Dokumente verwendet werden.
Beispiel: Adobe Acrobat

Frühwarnsysteme – Angriffe erkennen

Definition:

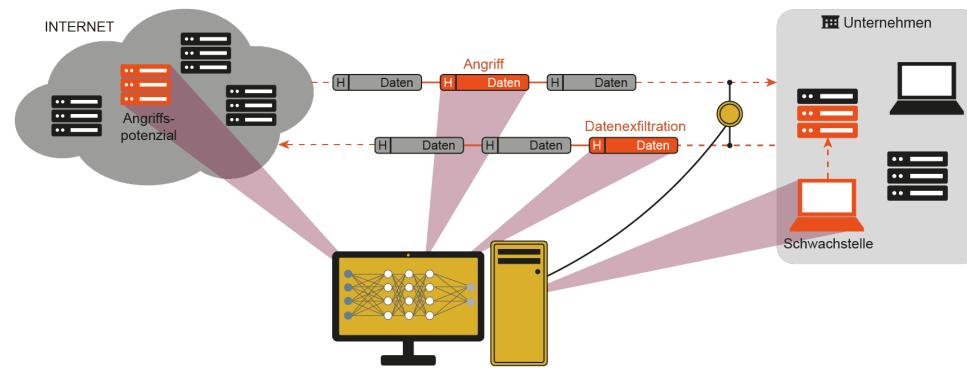
- Früh Angriffspotenziale und reale Angriffe zu erkennen, um rechtzeitig Warnhinweise zu geben.
- Sicherheit und Vertrauenswürdigkeit von IT-Systemen und IT-Infrastruktur nachhaltig zu erhöhen und widerstandsfähiger zu gestalten



Frühwarnsysteme – Angriffe erkennen

Ansprüche an das System:

- Früh genug reagieren
 - Auch bei unbekannten Vorgängen
 - Bildung eines Expertensystems
 - Bessere Entscheidungsfindung
 - Sammlung von Beweismitteln
 - Matching zu bekannten Fällen

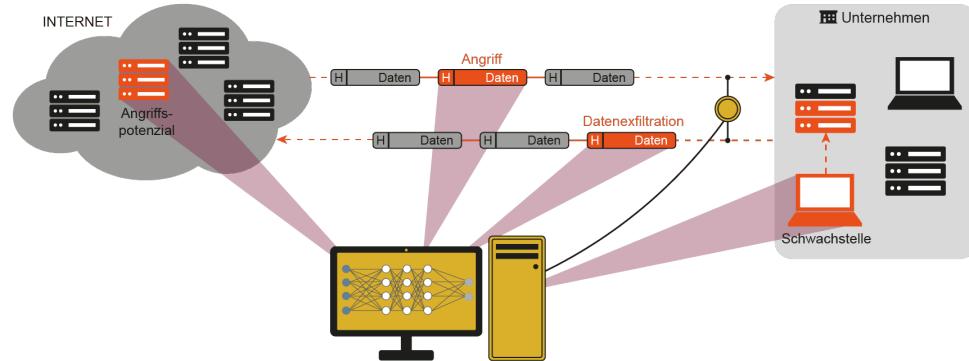


Frühwarnsysteme – Angriffe erkennen

Ansprüche an das System:

- Früh genug reagieren
 - Auch bei unbekannten Vorgängen
- Bildung eines Expertensystems
 - Bessere Entscheidungsfindung
- Sammlung von Beweismitteln
 - Matching zu bekannten Fällen

Reaktion



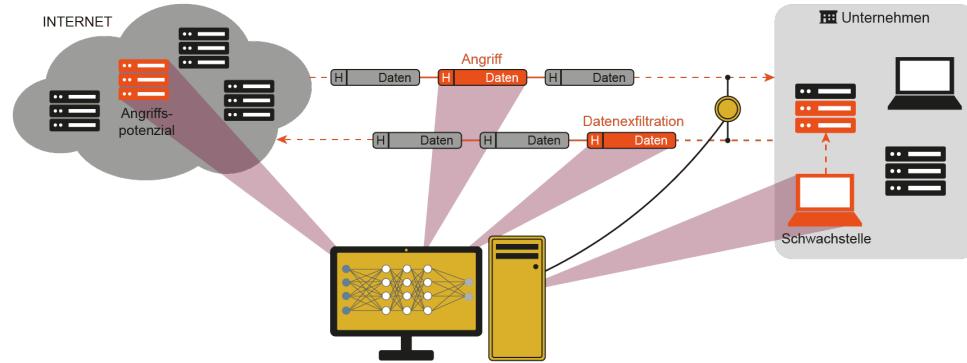
Frühwarnsysteme – Angriffe erkennen

Ansprüche an das System:

- Früh genug reagieren
 - Auch bei unbekannten Vorgängen
- Bildung eines Expertensystems
 - Bessere Entscheidungsfindung
- Sammlung von Beweismitteln
 - Matching zu bekannten Fällen

Reaktion

Aktueller Status muss ständig verifiziert werden.



Backup

Definition:

Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.

Fall von Datenverlust: Rückkopieren der Sicherung auf das Kernlaufwerk.

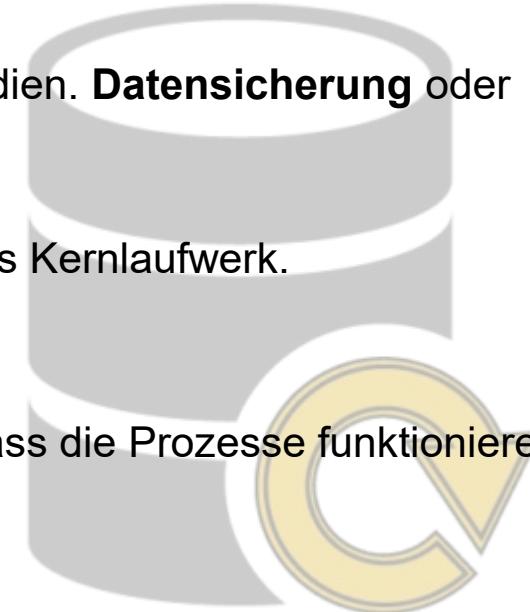
Prozessname: **Recovery**



Backup

Definition:

Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.



Fall von Datenverlust: Rückkopieren der Sicherung auf das Kernlaufwerk.

Prozessname: **Recovery**

Regelmäßige Tests sind empfohlen um sicherzustellen, dass die Prozesse funktionieren.

Backup

Definition:

Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.



Endgültigen Verlust des Datenbestands durch Software- oder Hardwareausfälle, Angriffe mittels Ransomware, Naturkatastrophen, Diebstahl oder aktiver Sabotage zu schützen.

Backup

Definition:

Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.



Backup

Definition:

Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.



Der Verlust von Datenbeständen verursacht in der Regel einen hohen **finanziellen Schaden**.

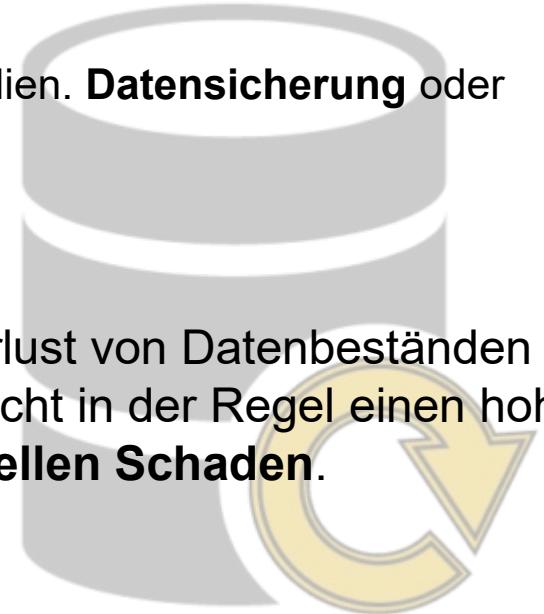
Backup

Definition:

Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.

Welches Speichermedium sollte verwendet werden?

Der Verlust von Datenbeständen verursacht in der Regel einen hohen **finanziellen Schaden**.



Backup

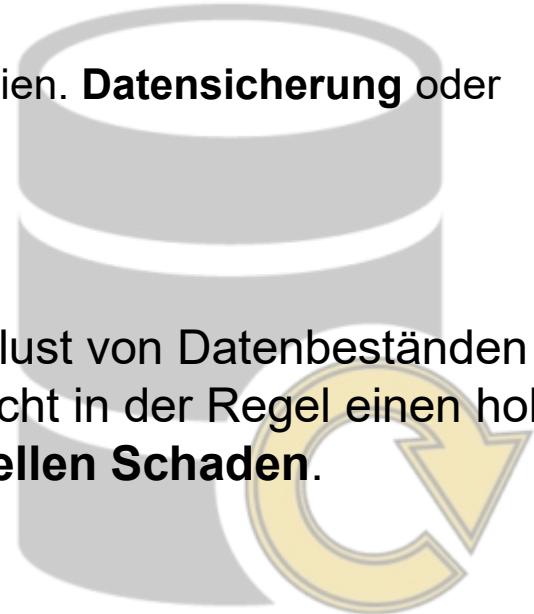
Definition:

Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.

Welches Speichermedium sollte verwendet werden?

Externe Festplatte, USB-Stick, DVDs/CDs, aber auch Tapes (Bänder)

Der Verlust von Datenbeständen verursacht in der Regel einen hohen **finanziellen Schaden**.



Backup

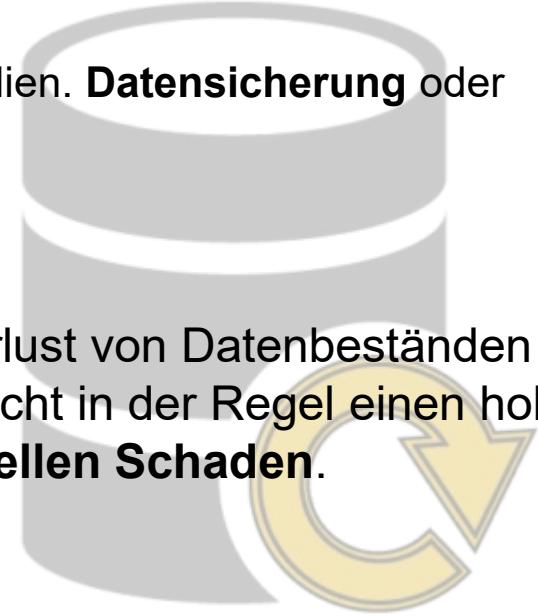
Definition:

Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.

Welches Speichermedium sollte verwendet werden?

Externe Festplatte, USB-Stick, DVDs/CDs, aber auch Tapes (Bänder)

Der Verlust von Datenbeständen verursacht in der Regel einen hohen **finanziellen Schaden**.



Immutable Backup

Nicht ständig an das System angeschlossen.

Backup

Definition:

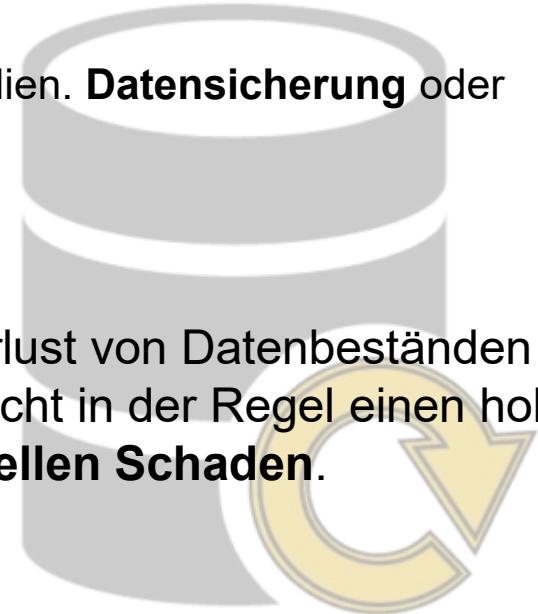
Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.

Welches Speichermedium sollte verwendet werden?

Cloud-Storage



Der Verlust von Datenbeständen verursacht in der Regel einen hohen **finanziellen Schaden**.



Backup

Definition:

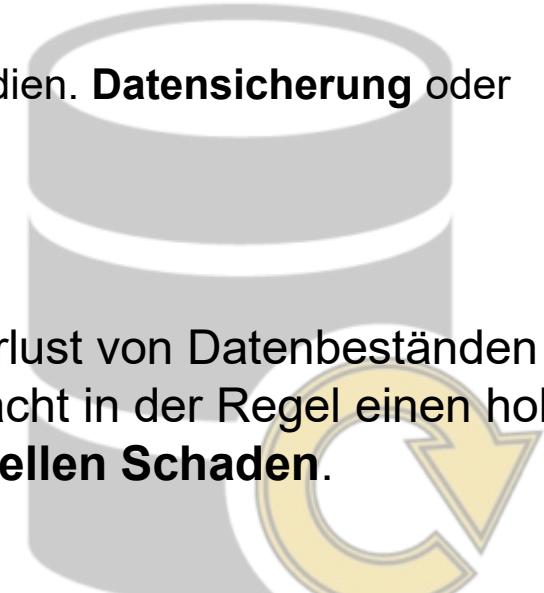
Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.

Welches Speichermedium sollte verwendet werden?

Cloud-Storage



Der Verlust von Datenbeständen verursacht in der Regel einen hohen **finanziellen Schaden**.



Was ist mit dem Datenschutz?
Wo liegen die Daten?

Backup

Definition:

Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.

Welches Speichermedium sollte verwendet werden?

Cloud-Storage



Was ist mit dem Datenschutz?
Wo liegen die Daten?

Backup

Definition:

Erstellung von Sicherheitskopien auf externe Speichermedien. **Datensicherung** oder **Backup**.

Welches Speichermedium sollte verwendet werden?

Cloud-Storage

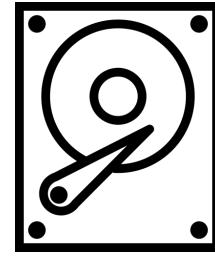


Was ist mit dem Datenschutz?
Wo liegen die Daten?

Backup

Definition:

Vollständige Backups



Backup

Definition:

Vollständige Backups

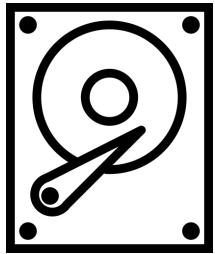
Vollständiges Abbild der Daten.



Backup

Definition:

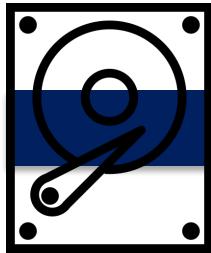
Inkrementelle Backups



Backup

Definition:

Inkrementelle Backups



Dieser Bereich hat sich nach dem letzten Backup geändert.

Backup

Definition:

Inkrementelle Backups



Nur der geänderte Bereich wird in das Backup geschrieben.