

WIRTSCHAFTSINFORMATIK 1

INFORMATIONSSICHERHEIT

PROF. DR. CHRISTIAN BOCKERMANN, PROF. DR. JULIAN GROTE, PROF. DR.
VOLKER KLINGSPOR

HOCHSCHULE BOCHUM

WINTERSEMESTER 2026/27

Inhalt

- 1 Motivation
- 2 Schritt 1: Die Daten verschlüsseln
- 3 Schritt 2: Den Schlüssel austauschen
- 4 Schritt 3: Dem Gegenüber vertrauen
- 5 Anwendungen im Alltag
- 6 Passwörter und Authentifizierung
- 7 Der Faktor Mensch

MOTIVATION





Sneaker Shop

Hochschule Bochum
Bochum University
of Applied Sciences



Warenkorb: 0 Artikel, 0,00 €

Kategorien

child
infant
men
preschool
toddler
women
youth

Nike | men



Nike SB Dunk Low April
Skateboards

Preis: 186,00 €

adidas | men



Pharrell x NMD_S1 Mahbs
'Earth Strata'

Preis: 300,00 €

Jordan | youth



Air Jordan 1 Mid SS GS
'Championships'

Preis: 120,00 €

Jordan | infant



Air Jordan 1 Mid SS TD
'Championships'

Preis: 149,00 €

Jordan | men



Jordan 8 Retro Winterized
Gunsmoke

Preis: 238,00 €

adidas | men



Pharrell x NMD_S1 Mahbs
'Pink'

Preis: 400,00 €

Jordan | youth



Air Jordan 1 Mid SS PS
'Championships'

Preis: 183,00 €

Jordan | child



Jordan 8 Retro Winterized
Gunsmoke (GS)

Preis: 226,00 €



Sneaker Shop

Hochschule Bochum
Bochum University
of Applied Sciences



Warenkorb: 0 Artikel, 0,00 €

Kategorien

child
infant
men
preschool
toddler
women
youth

Nike | men



Nike SB Dunk Low April
Skateboards

Preis: 186,00 €

adidas | men



Pharrell x NMD_S1 Mahbs
'Earth Strata'

Preis: 300,00 €

Jordan | youth



Air Jordan 1 Mid SS GS
'Championships'

Preis: 120,00 €

Jordan | infant



Air Jordan 1 Mid SS TD
'Championships'

Preis: 149,00 €

Jordan | men



Jordan 8 Retro Winterized
Gunsmoke

Preis: 238,00 €

adidas | men



Pharrell x NMD_S1 Mahbs
'Pink'

Preis: 400,00 €

Jordan | youth



Air Jordan 1 Mid SS PS
'Championships'

Preis: 183,00 €

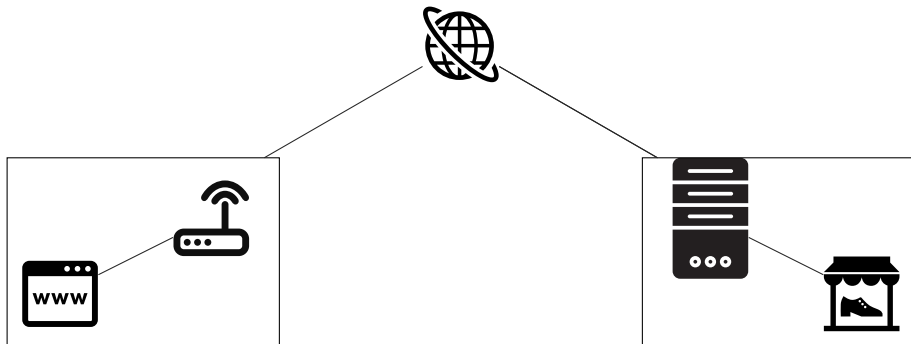
Jordan | child



Jordan 8 Retro Winterized
Gunsmoke (GS)

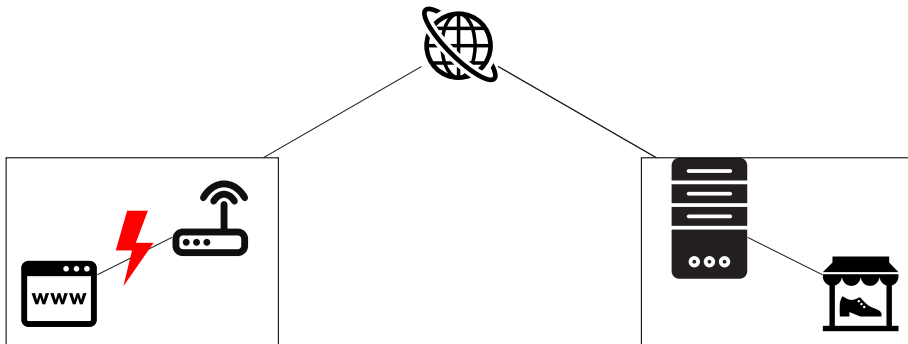
Preis: 226,00 €

Wie können wir Informationen sicher übertragen?



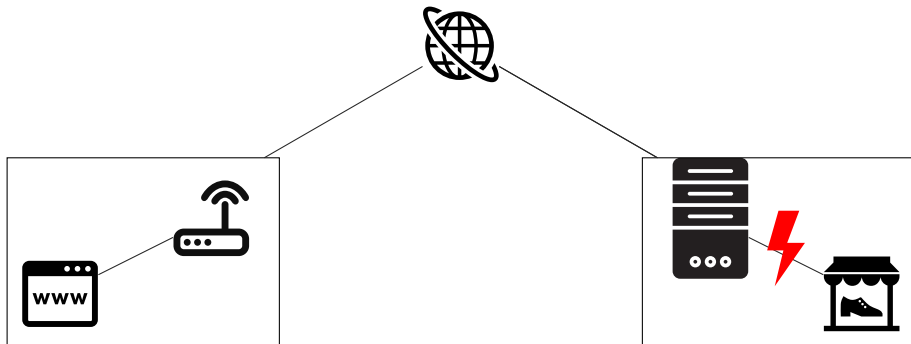
Wo können potentielle Angriffspunkte sein?

Schützen Sie Ihr WLAN!



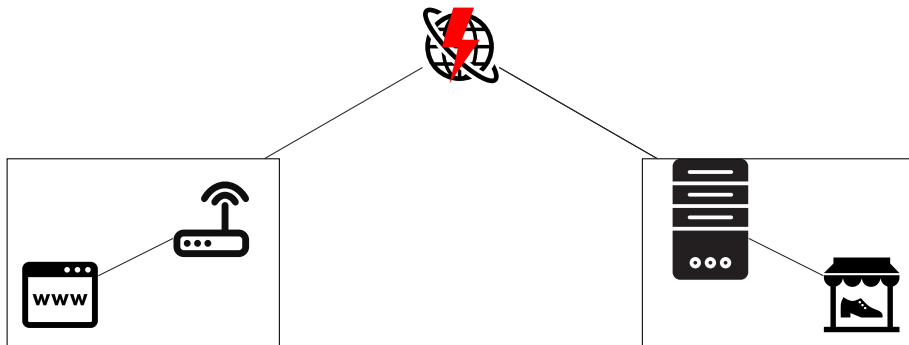
Wo können potentielle Angriffspunkte sein?

Besuchen Sie nur vertrauenswürdige Anbieter!

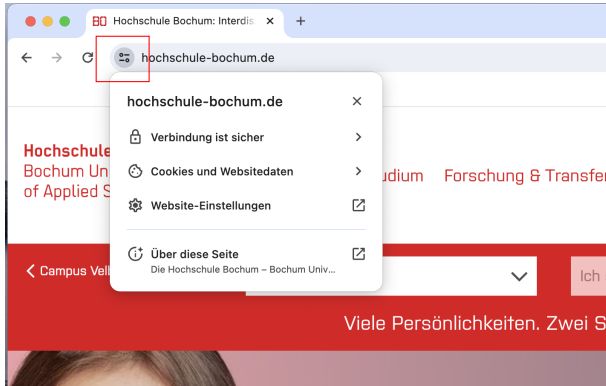


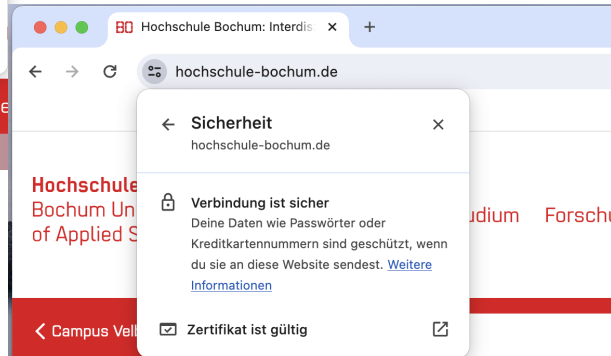
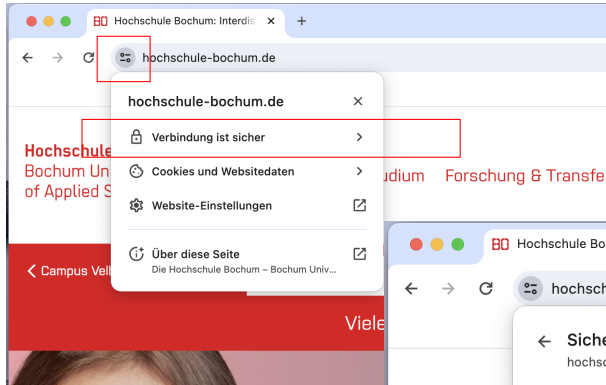
Wo können potentielle Angriffspunkte sein?

Schützen Sie die Internetverbindung!



Wo können potentielle Angriffspunkte sein?





Warum ist die Verbindung zum Web-Server sicher?

Warum ist die Verbindung zum Web-Server sicher?

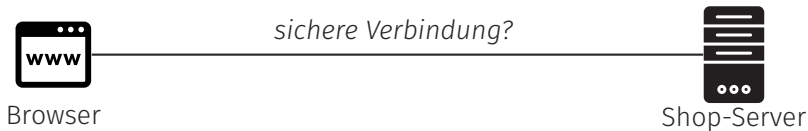
- Die Daten werden verschlüsselt!

Warum ist die Verbindung zum Web-Server sicher?

- Die Daten werden verschlüsselt!
- Der Server kann sich ausweisen!

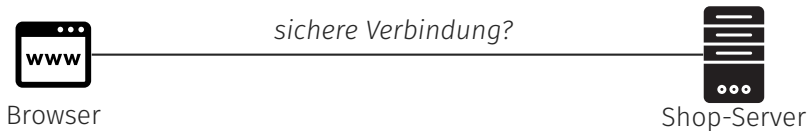


Was brauchen wir, damit die Verbindung zum Shop "sicher" ist?



- ☐ 1. Die Daten verschlüsseln
- ☐ 2. Den Schlüssel austauschen
- ☐ 3. Der Gegenseite vertrauen

Was brauchen wir, damit die Verbindung zum Shop "sicher" ist?



- ☐ 1. Die Daten verschlüsseln
- ☐ 2. Den Schlüssel austauschen
- ☐ 3. Der Gegenseite vertrauen

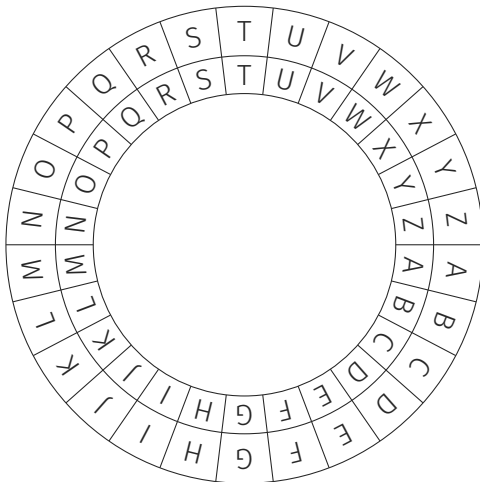
Wir lösen die drei Probleme der Reihe nach.

SCHRITT 1: DIE DATEN VERSCHLÜSSELN

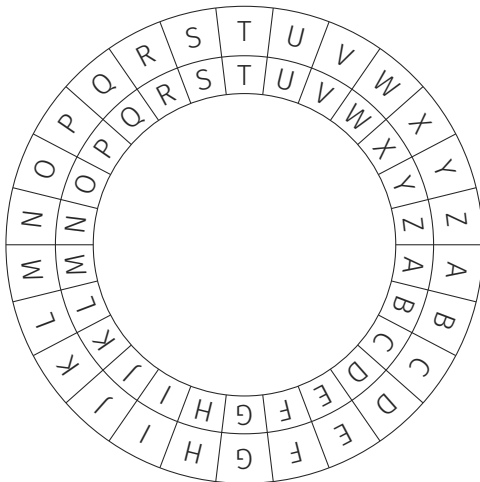
SCHRITT 1: DIE DATEN VERSCHLÜSSELN

CAESAR-CHIFFRE

Verschlüsselung vor 2000 Jahren: Jeder Buchstabe wird im Alphabet verschoben

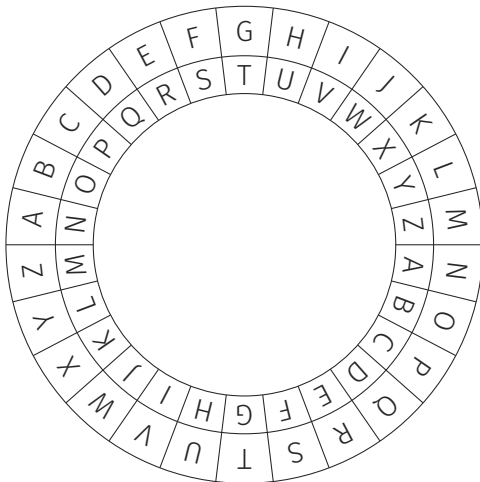


Verschlüsselung vor 2000 Jahren: Jeder Buchstabe wird im Alphabet verschoben



Benutzername: fritz
Kennwort: geheim

Geheimer Schlüssel = 13: Sender und Empfänger kennen ihn, sonst niemand



Benutzername: sevgm
Kennwort: **trurvz**

Der geheime Schlüssel ist 13 — nutzen Sie die Scheibe von eben.

va qre urhgvtra trfpuäsgfjryg vfg qvr vasbezngvx rva hairemvpugonerf jrexm-
rht süe qvr orgevrofjvegfpung. fvr rezötyvpug rssvmvrgrf qngraznantrzrag,
nanylfra haq nhgbzngvfvrehat, jnf mh shaqvregra ragfpurvqhatra haq jrggor-
jreofibegrvyra süueg.

Der geheime Schlüssel ist 13 — nutzen Sie die Scheibe von eben.

va qre urhgvtra trfpuäsgfjryg vfg qvr vasbezngvx rva hairemvpugonerf jrexm-
rht süe qvr orgevrofjvegfpung. fvr rezötyvpug rssvmvrgrf qngraznantrzrag,
nanylfra haq nhgbzngvfvrehat, jnf mh shaqvregra ragfpurvqhatra haq jrggor-
jreofibegrvyra süueg.

Wie sicher ist das?

- Es gibt nur 25 sinnvolle Schlüssel

- Es gibt nur 25 sinnvolle Schlüssel
- Alle durchprobieren (Brute Force): von Hand Minuten, für den Computer Mikrosekunden

- Es gibt nur 25 sinnvolle Schlüssel
- Alle durchprobieren (Brute Force): von Hand Minuten, für den Computer Mikrosekunden
- Noch schneller: Der häufigste Buchstabe im Deutschen ist fast immer das E (Häufigkeitsanalyse)

- Es gibt nur 25 sinnvolle Schlüssel
- Alle durchprobieren (Brute Force): von Hand Minuten, für den Computer Mikrosekunden
- Noch schneller: Der häufigste Buchstabe im Deutschen ist fast immer das E (Häufigkeitsanalyse)

- Es gibt nur 25 sinnvolle Schlüssel
- Alle durchprobieren (Brute Force): von Hand Minuten, für den Computer Mikrosekunden
- Noch schneller: Der häufigste Buchstabe im Deutschen ist fast immer das E (Häufigkeitsanalyse)

Moderne Verfahren machen im Kern dasselbe — nur ist der Schlüssel nicht 1 aus 26, sondern 1 aus $2^{128} \approx 3,4 \cdot 10^{38}$

- Es gibt nur 25 sinnvolle Schlüssel
- Alle durchprobieren (Brute Force): von Hand Minuten, für den Computer Mikrosekunden
- Noch schneller: Der häufigste Buchstabe im Deutschen ist fast immer das E (Häufigkeitsanalyse)

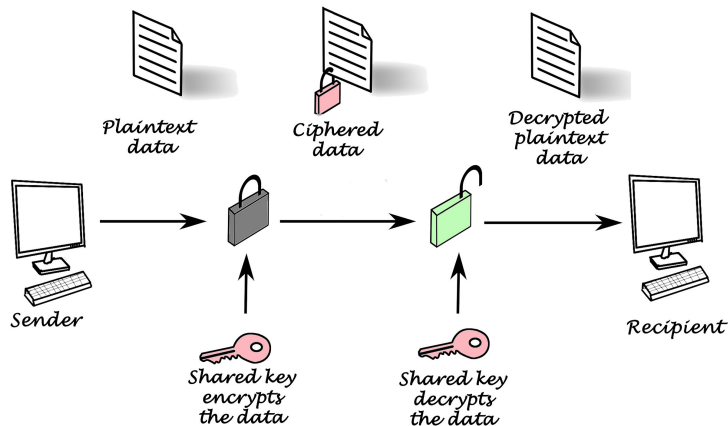
Moderne Verfahren machen im Kern dasselbe — nur ist der Schlüssel nicht 1 aus 26, sondern 1 aus $2^{128} \approx 3,4 \cdot 10^{38}$

Alle Computer der Welt zusammen bräuchten zum Durchprobieren länger, als das Universum alt ist.

SCHRITT 1: DIE DATEN VERSCHLÜSSELN

SYMMETRISCHE VERSCHLÜSSELUNG

Private Key Encryption



Herausforderungen:

- der Schlüssel muss beiden Seiten bekannt sein
- der Schlüssel darf niemandem anderen bekannt sein

Herausforderungen:

- der Schlüssel muss beiden Seiten bekannt sein
- der Schlüssel darf niemandem anderen bekannt sein

Beispiel für (super einfache) Verschlüsselung: die Caesar-Chiffre — gerade selbst ausprobiert!

Zum Nachspielen:

<https://www.kryptowissen.de/caesar-chiffre-praxis.php>

Herausforderungen:

- der Schlüssel muss beiden Seiten bekannt sein
- der Schlüssel darf niemandem anderen bekannt sein

Beispiel für (super einfache) Verschlüsselung: die Caesar-Chiffre — gerade selbst ausprobiert!

Zum Nachspielen:

<https://www.kryptowissen.de/caesar-chiffre-praxis.php>

Beispiele für sichere Verschlüsselungsalgorithmen: AES, Triple-DES, Twofish

https://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem

Wofür eignet sich symmetrische Verschlüsselung?

Wofür eignet sich symmetrische Verschlüsselung?

- Verschlüsselung von Dokumenten

Wofür eignet sich symmetrische Verschlüsselung?

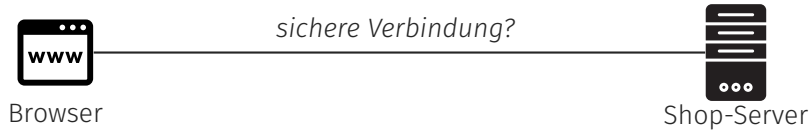
- Verschlüsselung von Dokumenten
- Verschlüsselung von Festplatten

Wofür eignet sich symmetrische Verschlüsselung?

- Verschlüsselung von Dokumenten
- Verschlüsselung von Festplatten
- Verschlüsselung der WLAN-Verbindung

Wofür eignet sich symmetrische Verschlüsselung?

- Verschlüsselung von Dokumenten
- Verschlüsselung von Festplatten
- Verschlüsselung der WLAN-Verbindung
- Immer dann sinnvoll, wenn der Schlüssel einfach und sicher geteilt werden kann.



1. Die Daten verschlüsseln

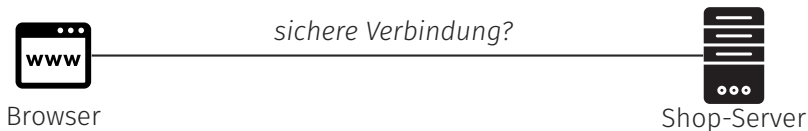


2. Den Schlüssel austauschen



3. Der Gegenseite vertrauen

- Verschlüsseln können wir jetzt — aber **beide Seiten brauchen denselben Schlüssel**



1. Die Daten verschlüsseln



2. Den Schlüssel austauschen



3. Der Gegenseite vertrauen

- Verschlüsseln können wir jetzt — aber **beide Seiten brauchen denselben Schlüssel**
- Wie kommt der Schlüssel vom Browser zum Server, ohne dass jemand auf der Leitung mitliest?

SCHRITT 2: DEN SCHLÜSSEL AUSTAUSCHEN

Können wir den geheimen Schlüssel einfach über das Internet schicken?

Können wir den geheimen Schlüssel einfach über das Internet schicken?



Wer mitliest, kennt den Schlüssel — und liest ab jetzt **alles** mit!

Können wir den geheimen Schlüssel einfach über das Internet schicken?



Wer mitliest, kennt den Schlüssel — und liest ab jetzt **alles** mit!

- Wir brauchen ein Verfahren, bei dem der **Entschlüsselungs-Schlüssel** nie **verschickt** wird

SCHRITT 2: DEN SCHLÜSSEL AUSTAUSCHEN

ASYMMETRISCHE VERSCHLÜSSELUNG

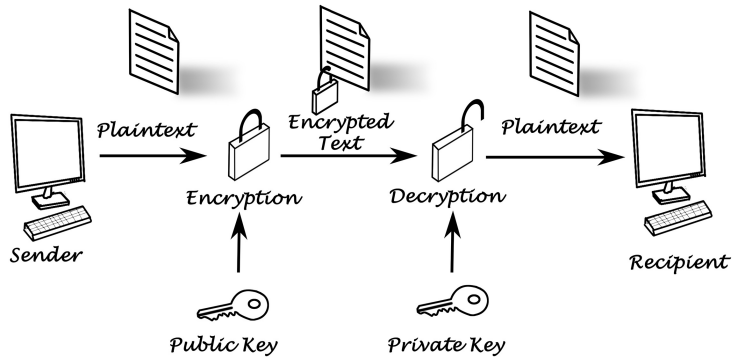
- Einwerfen kann **jeder** — der Schlitz ist öffentlich

- Einwerfen kann **jeder** — der Schlitz ist öffentlich
- Herausholen kann **nur einer** — wer den Briefkastenschlüssel besitzt

- Einwerfen kann **jeder** — der Schlitz ist öffentlich
- Herausholen kann **nur einer** — wer den Briefkastenschlüssel besitzt
- Genauso funktioniert asymmetrische Verschlüsselung:
der **öffentliche Schlüssel** verschlüsselt (einwerfen),
nur der **private Schlüssel** entschlüsselt (herausholen)

- Einwerfen kann **jeder** — der Schlitz ist öffentlich
- Herausholen kann **nur einer** — wer den Briefkastenschlüssel besitzt
- Genauso funktioniert asymmetrische Verschlüsselung:
der **öffentliche Schlüssel** verschlüsselt (einwerfen),
nur der **private Schlüssel** entschlüsselt (herausholen)
- Der private Schlüssel verlässt seinen Besitzer **nie**

Der Empfänger besitzt ein Schlüsselpaar



Herausforderungen:

- der private Schlüssel muss geheim bleiben
- der öffentliche Schlüssel muss sicher zugeordnet werden können
- die Verschlüsselung ist relativ langsam

Herausforderungen:

- der private Schlüssel muss geheim bleiben
- der öffentliche Schlüssel muss sicher zugeordnet werden können
- die Verschlüsselung ist relativ langsam

Bekanntestes Verfahren: **RSA** (benannt nach Rivest, Shamir und Adleman, 1977)

Wofür eignet sich asymmetrische Verschlüsselung?

Wofür eignet sich asymmetrische Verschlüsselung?

- Verschlüsseltes Versenden von Emails

Wofür eignet sich asymmetrische Verschlüsselung?

- Verschlüsseltes Versenden von Emails
- Verschlüsseltes Versenden von geheimen Schlüsseln

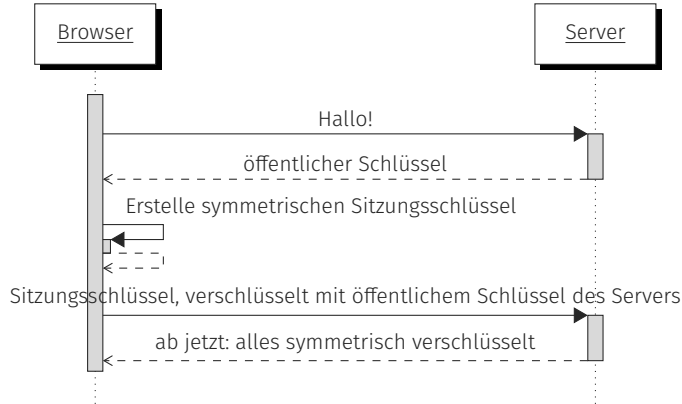
Wofür eignet sich asymmetrische Verschlüsselung?

- Verschlüsseltes Versenden von Emails
- Verschlüsseltes Versenden von geheimen Schlüsseln
- ...

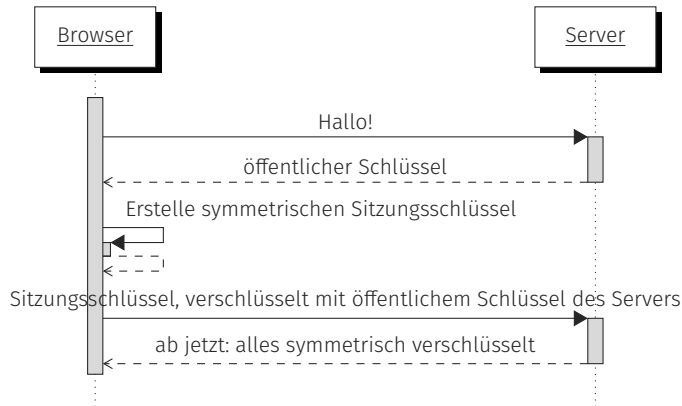
Wofür eignet sich asymmetrische Verschlüsselung?

- Verschlüsseltes Versenden von Emails
- Verschlüsseltes Versenden von geheimen Schlüsseln
- ...
- Immer dann sinnvoll, wenn der Schlüssel nicht einfach und sicher geteilt werden kann.

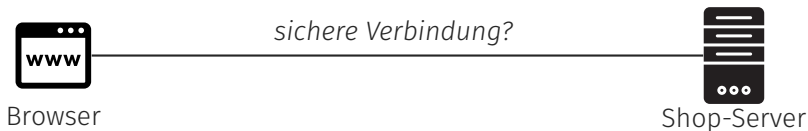
Asymmetrisch ist langsam — deshalb nur für den **Schlüsseltausch**:



Asymmetrisch ist langsam — deshalb nur für den **Schlüsseltausch**:



Nur der Server kann den Sitzungsschlüssel entschlüsseln — mit seinem **privaten** Schlüssel.



1. Die Daten verschlüsseln

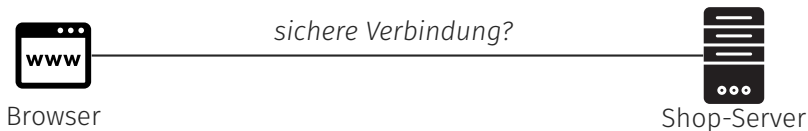


2. Den Schlüssel austauschen



3. Der Gegenseite vertrauen

- Der Schlüsseltausch funktioniert — **wenn** der öffentliche Schlüssel wirklich vom Shop stammt



1. Die Daten verschlüsseln



2. Den Schlüssel austauschen



3. Der Gegenseite vertrauen

- Der Schlüsseltausch funktioniert — **wenn** der öffentliche Schlüssel wirklich vom Shop stammt
- Woher wissen wir das? Auf der Leitung könnte **jemand dazwischensitzen** ...

SCHRITT 3: DEM GEGENÜBER VERTRAUEN

Ein Angreifer sitzt auf der Leitung und fängt unsere Anfrage ab:



Ein Angreifer sitzt auf der Leitung und fängt unsere Anfrage ab:



Ein Angreifer sitzt auf der Leitung und fängt unsere Anfrage ab:



- Der Browser verschlüsselt den Sitzungsschlüssel — mit dem Schlüssel des Angreifers

Ein Angreifer sitzt auf der Leitung und fängt unsere Anfrage ab:



- Der Browser verschlüsselt den Sitzungsschlüssel — mit dem Schlüssel des **Angreifers**
- Der Angreifer liest alles mit und reicht es weiter: **niemand merkt etwas**

Ein Angreifer sitzt auf der Leitung und fängt unsere Anfrage ab:



- Der Browser verschlüsselt den Sitzungsschlüssel — mit dem Schlüssel des **Angreifers**
- Der Angreifer liest alles mit und reicht es weiter: **niemand merkt etwas**
- Verschlüsselung allein genügt nicht — wir müssen **wissen, mit wem wir reden**

Dafür brauchen wir zwei neue Werkzeuge:

- **Hash-Funktionen** — ein Fingerabdruck für Dokumente

Dafür brauchen wir zwei neue Werkzeuge:

- **Hash-Funktionen** — ein Fingerabdruck für Dokumente
- **Signaturen** — eine fälschungssichere Unterschrift

Dafür brauchen wir zwei neue Werkzeuge:

- **Hash-Funktionen** — ein Fingerabdruck für Dokumente
- **Signaturen** — eine fälschungssichere Unterschrift

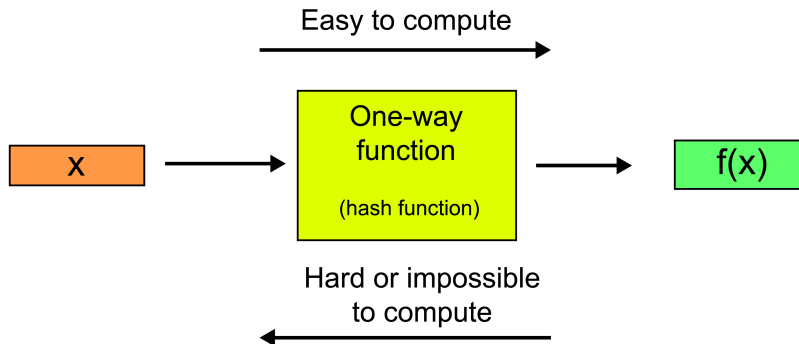
Dafür brauchen wir zwei neue Werkzeuge:

- **Hash-Funktionen** — ein Fingerabdruck für Dokumente
- **Signaturen** — eine fälschungssichere Unterschrift

Aus beiden zusammen entsteht das **Zertifikat** — der digitale Ausweis des Servers.

SCHRITT 3: DEM GEGENÜBER VERTRAUEN

HASH-FUNKTIONEN



- Der Hashwert $f(x)$ für ein Dokument/ x ist immer gleich
- Ändert sich das Dokument/ x auch nur ein wenig, ist der Hashwert $f(x)$ vollständig anders
- Zwei unterschiedliche Dokumente/ x haben unterschiedliche Hashwerte $f(x)$

Wozu dienen Hash-Funktionen?

Wozu dienen Hash-Funktionen?

- Überprüfen, ob ein Dokument verändert wurde

Wozu dienen Hash-Funktionen?

- Überprüfen, ob ein Dokument verändert wurde
- Speichern von Passwörtern

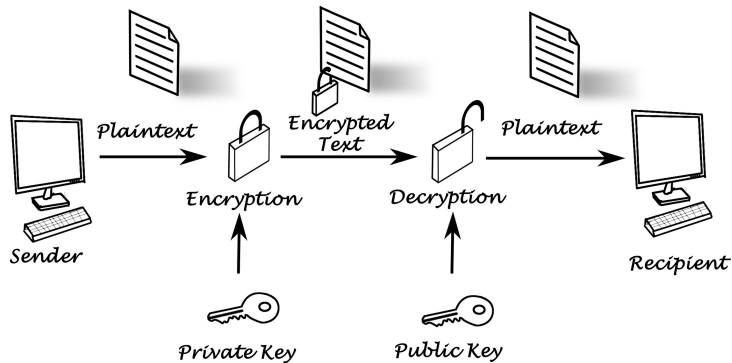
Wozu dienen Hash-Funktionen?

- Überprüfen, ob ein Dokument verändert wurde
- Speichern von Passwörtern
- ...

SCHRITT 3: DEM GEGENÜBER VERTRAUEN

SIGNIERUNG

Der **Sender** besitzt ein **Schlüsselpaar**



- Der "verschlüsselte" Text ist *nicht* geheim
- Jeder kann den Text mit dem öffentlichen Schlüssel lesen
- Da nur der Besitzer des privaten Schlüssels den Text verschlüsseln konnte, kann dieser als Verfasser verifiziert werden.

- Der "verschlüsselte" Text ist *nicht* geheim
- Jeder kann den Text mit dem öffentlichen Schlüssel lesen
- Da nur der Besitzer des privaten Schlüssels den Text verschlüsseln konnte, kann dieser als Verfasser verifiziert werden.

Herausforderungen:

- der private Schlüssel muss geheim bleiben
- der öffentliche Schlüssel muss sicher zugeordnet werden können

Wofür eignet sich Signierung?

Wofür eignet sich Signierung?

- Sicherstellen, dass ein Dokument von einem bestimmten Verfasser stammt
- ...

SCHRITT 3: DEM GEGENÜBER VERTRAUEN

ZERTIFIKATE

Ein **Zertifikat** bestätigt den Eigentümer sowie weitere Eigenschaften eines öffentlichen Schlüssels.

Es beinhaltet i.d.R

- Den Namen des Eigentümers (engl. subject) des öffentlichen Schlüssels.
- Informationen zur Gültigkeitsdauer
- Den öffentlichen Schlüssel
- Den Namen und weitere Informationen des Ausstellers (engl. issuer) des Zertifikates
- Weitere Informationen zum Eigentümer des öffentlichen Schlüssels.
- Angaben zum zulässigen Anwendungs- und Geltungsbereich des öffentlichen Schlüssels.

Zertifikats-Viewer: www.hs-bochum.de

Allgemein

Details

Ausgestellt für

Allgemeiner Name (CN)	www.hs-bochum.de
Organisation (O)	Hochschule Bochum
Organisationseinheit (OU)	<Gehört nicht zum Zertifikat>

Ausgestellt von

Allgemeiner Name (CN)	GEANT OV RSA CA 4
Organisation (O)	GEANT Vereiniging
Organisationseinheit (OU)	<Gehört nicht zum Zertifikat>

Gültigkeitsdauer

Ausgestellt am	Mittwoch, 28. Februar 2024 um 01:00:00
Gültig bis	Freitag, 28. Februar 2025 um 00:59:59

SHA-256-Fingerabdrücke

Zertifikat	f20241a8744081a370c3d6741195957a339fdc04e8b69d55dc779ff512d7ef51
Öffentlicher Schlüssel	054996c5ffed6bea9d18a65162a82150a6e5e1cdf38e5e4a837fe0956cfc88b0

Zertifikats-Viewer: www.hs-bochum.de

Allgemein

Details

Zertifikathierarchie

USERTrust RSA Certification Authority

GEANT OV RSA CA 4

www.hs-bochum.de

Zertifikatsfelder

www.hs-bochum.de

Zertifikat

Version

Seriennummer

Algorithmus für Zertifikatsignatur

Aussteller

Gültigkeit

Nicht vor

Feldwert

CN = GEANT OV RSA CA 4

O = GEANT Vereiniging

C = NL

- Das Zertifikat ist **signiert** — von einer **Zertifizierungsstelle** (engl. Certificate Authority, CA)

- Das Zertifikat ist **signiert** — von einer **Zertifizierungsstelle** (engl. Certificate Authority, CA)
- Die öffentlichen Schlüssel der großen CAs sind im Browser **vorinstalliert**

- Das Zertifikat ist **signiert** — von einer **Zertifizierungsstelle** (engl. Certificate Authority, CA)
- Die öffentlichen Schlüssel der großen CAs sind im Browser **vorinstalliert**
- Der Browser prüft die Signatur-Kette:
Shop-Zertifikat → Zwischenstelle → Wurzel-Zertifizierungsstelle

- Das Zertifikat ist **signiert** — von einer **Zertifizierungsstelle** (engl. Certificate Authority, CA)
- Die öffentlichen Schlüssel der großen CAs sind im Browser **vorinstalliert**
- Der Browser prüft die Signatur-Kette:
Shop-Zertifikat → Zwischenstelle → Wurzel-Zertifizierungsstelle
- Der Angreifer aus der Mitte bekommt für seinen Schlüssel **kein** Zertifikat für den Namen des Shops

- Das Zertifikat ist **signiert** — von einer **Zertifizierungsstelle** (engl. Certificate Authority, CA)
- Die öffentlichen Schlüssel der großen CAs sind im Browser **vorinstalliert**
- Der Browser prüft die Signatur-Kette:
Shop-Zertifikat → Zwischenstelle → Wurzel-Zertifizierungsstelle
- Der Angreifer aus der Mitte bekommt für seinen Schlüssel **kein** Zertifikat für den Namen des Shops

- Das Zertifikat ist **signiert** — von einer **Zertifizierungsstelle** (engl. Certificate Authority, CA)
- Die öffentlichen Schlüssel der großen CAs sind im Browser **vorinstalliert**
- Der Browser prüft die Signatur-Kette:
Shop-Zertifikat → Zwischenstelle → Wurzel-Zertifizierungsstelle
- Der Angreifer aus der Mitte bekommt für seinen Schlüssel **kein** Zertifikat für den Namen des Shops

So schließt sich der Kreis: Signatur + Zertifikat = **Vertrauen** in den öffentlichen Schlüssel.

SCHRITT 3: DEM GEGENÜBER VERTRAUEN

HTTPS

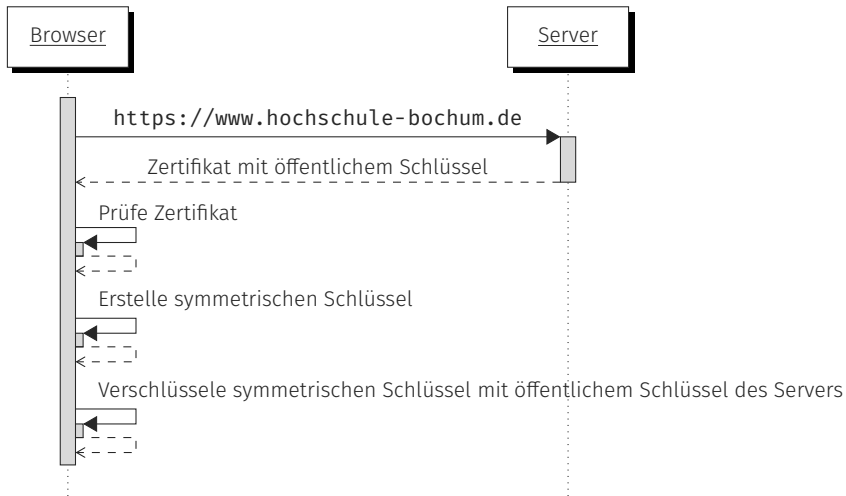
Alle drei Schritte zusammen ergeben das Verfahren, das jede **https://**-Seite nutzt:

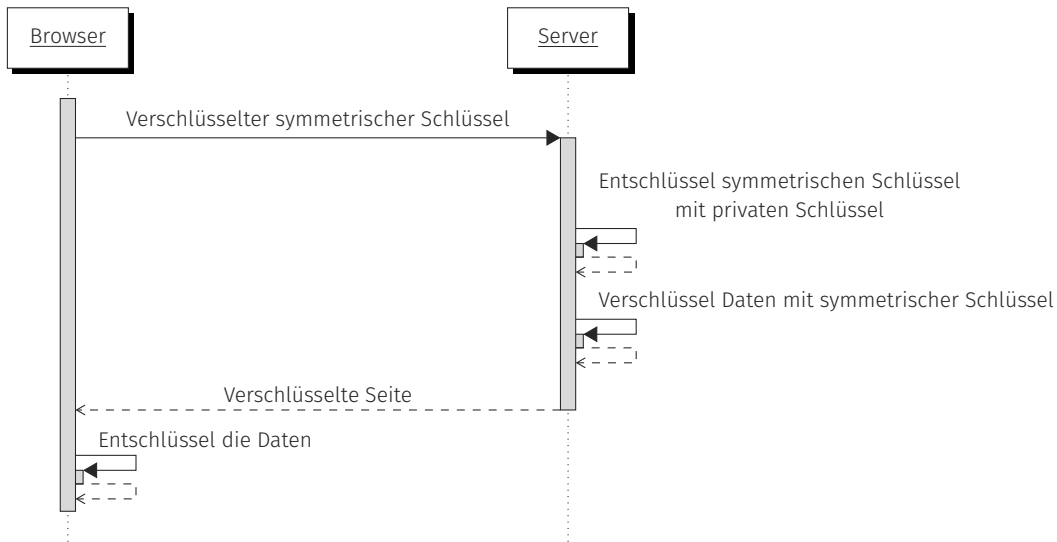
- **HTTPS** = HTTP + **TLS** (Transport Layer Security, Nachfolger von SSL)
- Das Schloss im Browser bedeutet: die TLS-Verbindung steht

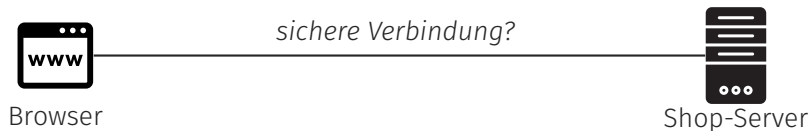
Alle drei Schritte zusammen ergeben das Verfahren, das jede **https://**-Seite nutzt:

- **HTTPS** = HTTP + **TLS** (Transport Layer Security, Nachfolger von SSL)
- Das Schloss im Browser bedeutet: die TLS-Verbindung steht

Wie wird beim Aufruf einer Web-Seite ein Schlüssel generiert und ausgetauscht?







1. Die Daten verschlüsseln



2. Den Schlüssel austauschen

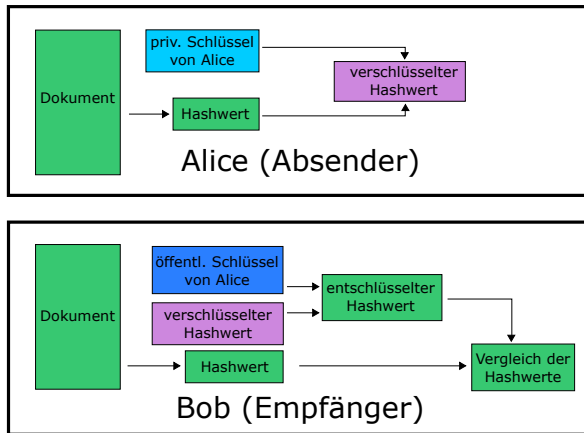


3. Der Gegenseite vertrauen

Das **Schloss im Browser** bedeutet: alle drei Schritte erledigt — bei **jedem** Aufruf einer **https://**-Seite, in Millisekunden.

ANWENDUNGEN IM ALLTAG

Eine **Signatur (elektronische Unterschrift)** stellt sicher, dass ein Dokument von einer bestimmten Person erstellt und nicht geändert wurde.



https://de.wikipedia.org/wiki/Elektronische_Signatur


Unterschrieben und alle Unterschriften sind gültig.
Unterschriftsfenster

Können Sie mit Hilfe des Internets für die folgenden Hashwerte wieder das Originalwort bestimmen?
Wieso ist bei manchen Hashwerten der Originaltext wieder bestimmbar? Was ergibt sich daraus für die Wahl von Passwörtern?

Hochschule Bochum
Bochum University
of Applied Sciences

BO

Fachbereich Wirtschaft
Prof. Blumet, Prof. Bockermann, Prof. Klingspor

Aufgabe 6 (Elektronische Signaturen)

Diese Datei ist elektronisch unterzeichnet. Können Sie nachprüfen, durch wen sie unterzeichnet wurde und ob die die Unterschrift vertrauenswürdig ist?
(Unter MacOs geht dies auf jeden Fall mit Adobe Acrobat. Ob und wie das auf anderen Computern funktioniert, können wir in der Übung klären).

**Volker
Klingspor**

*Digital
unterschrieben von
Volker Klingspor
Datum: 2024.04.24
10:46:58 +02'00'*

× Unterschriften



Revision 1: Unterschrieben von Volker Klingspor <volker.klingspor@hs-bochum.de>

Unterschrift ist gültig:

Dokument wurde nach dem Unterschreiben nicht mehr geändert.

Unterschrieben vom aktuellen Benutzer.

Die Signatur ist mit einem eingebetteten Zeitstempel versehen.

Unterschrift ist LTV-fähig

> Unterschriftsinformationen

Zuletzt geprüft: 2026.05.05 10:19:32 +02'00'

Feld: Signature2 auf Seite 2

[Klicke, um diese Version anzuzeigen.](#)

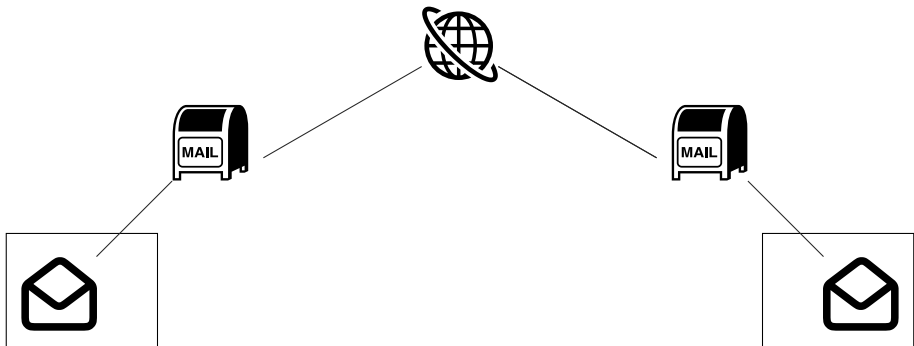
Rahmenbedingungen für Signaturen

- Technisch sicher, wenn
 - der öffentliche Schlüssel eindeutig zugeordnet werden kann
 - der private Schlüssel sicher gespeichert ist
- Erfordert "Trust Service Provider" der Person verifiziert und Zertifikat ausstellt
- Für Deutschland aktuell unter
<https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tl/DE>
zu finden
- Gesetzlich geregelt in: Verordnung (EU) Nr. 910/2014 (eIDAS-Verordnung) und Vertrauensdienstegesetz (VDG)
- Für PDF-Dokumente: PAdES (PDF Advanced Electronic Signatures)

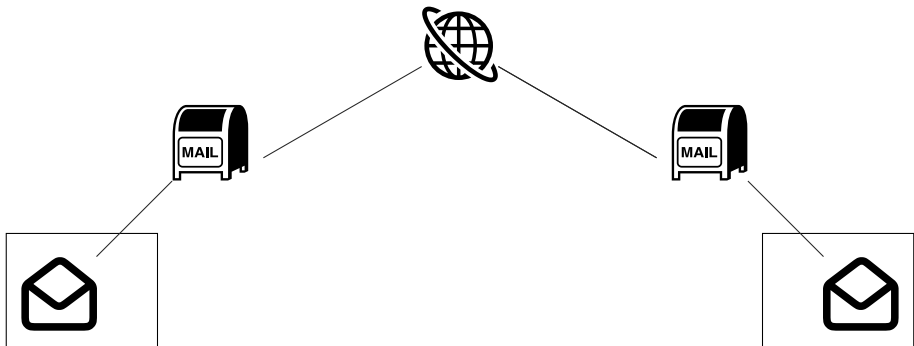
ANWENDUNGEN IM ALLTAG

EMAIL

Emails sind wie Postkarten – für jeden lesbar

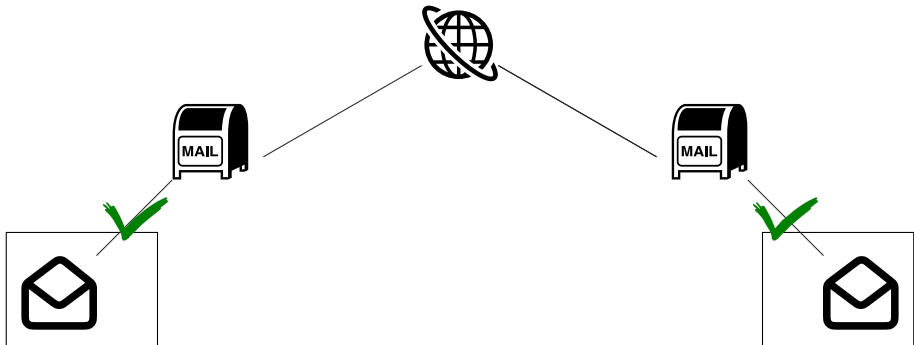


Emails sind wie Postkarten – für jeden lesbar



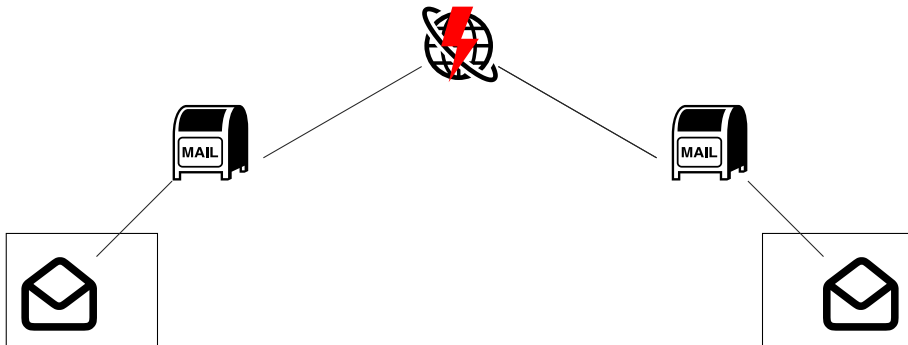
Emails sind wie Postkarten – für jeden lesbar

Die Verbindung zum Mail-Server ist i.d.R. sicher!

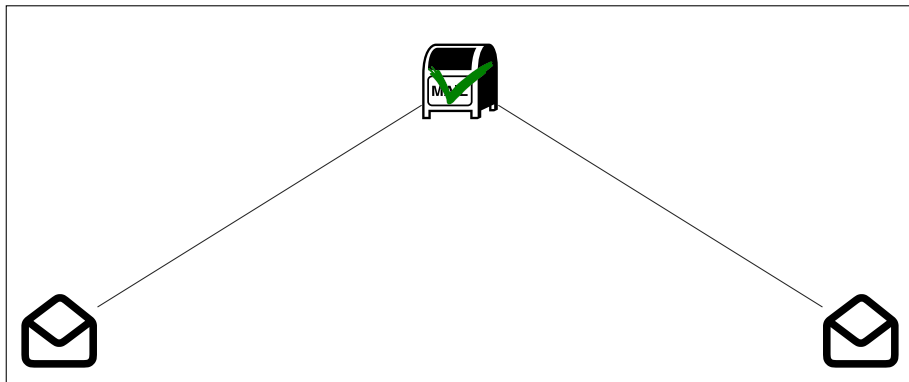


Emails sind wie Postkarten – für jeden lesbar

Im Internet wird die Mail unverschlüsselt weitergereicht!



Emails innerhalb einer Organisation sind sicher!



Alle Nachrichten, die Sie außerhalb kontrollierter Infrastruktur verschicken, sollten Ende-zu-Ende-verschlüsselt sein.

Email: OpenPGP, S/MIME

<https://www.bsi.bund.de/dok/11486410>

- Kein einheitlicher Standard für alle
- Keine für Privatpersonen einfache Infrastruktur zum Schlüsselaustausch

WhatsApp: Meta und amerikanische Geheimdienste haben vermutlich Zugriff

Signal, Threema: Server in EU, OpenSource → vermutlich sicher

Verschicken Sie als Unternehmen keine schützenswerten Informationen
(Rechnungen, Verträge, Kundendaten, ...) per Email.

PASSWÖRTER UND AUTHENTIFIZIERUNG

PASSWÖRTER UND AUTHENTIFIZIERUNG

PASSWÖRTER

Die 10 häufigsten (privaten) Passwörter in Deutschland 2023 (Hasso Platter Institut):

Die 10 häufigsten (privaten) Passwörter in Deutschland 2023 (Hasso Platter Institut):

1. 123456789
2. 12345678
3. hallo
4. 1234567890
5. 1234567
6. password
7. password1
8. target123
9. iloveyou
10. gwerly123

Beruflich wird auch gerne der Firmenname verwendet (Platz 1 lt. Wikipedia in Deutschland)

Wie sollten Sie Passwörter behandeln?

- Gutes Passwort wählen
 - 8–12 Zeichen bei vier verschiedenen Zeichenarten
 - mehr als 25 Zeichen bei 2 Zeichenarten
- Individuelles Passwort pro Account
- Das Passwort sollte im Wörterbuch nicht vorkommen
- Vermeiden Sie Namen und Geburtsdaten
- Vermeiden Sie Wiederholungs- und Tastaturmuster (*qwrtz*)
- Vermeiden Sie Ziffern und Sonderzeichen am Anfang oder Ende eines sonst einfachen Passworts (*password1*)
- Nutzen Sie Mehr-Faktor-Authentifizierung → gleich mehr dazu
- Nutzen Sie Passwort-Manager

<https://www.bsi.bund.de/dok/6596574>

Wie werden Passwörter in den Web-Anwendungen gespeichert?

- Passwörter werden mit einer Hashfunktion "Ein-Weg-Verschlüsselt"
 - Nicht umkehrbar
 - Kollisionsfrei
- "iloveyou" → Hashfunktion (SHA-1) →
"ee8d8728f435fd55of83852aabab5234ce1da528"
- Der Hashwert wird gespeichert
- Bei der Prüfung der Passworts werden die Hashwerte verglichen

PASSWÖRTER UND AUTHENTIFIZIERUNG

ZWEI-FAKTOR-AUTHENTIFIZIERUNG

Drei **Faktoren** können Sie ausweisen:

Drei **Faktoren** können Sie ausweisen:

Wissen

Passwort, PIN,
Sicherheitsfrage

Drei **Faktoren** können Sie ausweisen:

Wissen

Passwort, PIN,
Sicherheitsfrage

Besitz

Smartphone,
Chipkarte,
TAN-Generator

Drei **Faktoren** können Sie ausweisen:

Wissen

Passwort, PIN,
Sicherheitsfrage

Besitz

Smartphone,
Chipkarte,
TAN-Generator

Biometrie

Fingerabdruck,
Gesicht

- 2FA = Kombination aus **zwei verschiedenen** Faktoren

- 2FA = Kombination aus **zwei verschiedenen** Faktoren
- Geldautomat: Karte (**Besitz**) + PIN (**Wissen**) — 2FA seit Jahrzehnten!

- 2FA = Kombination aus **zwei verschiedenen** Faktoren
- Geldautomat: Karte (**Besitz**) + PIN (**Wissen**) — 2FA seit Jahrzehnten!
- Online-Banking: Passwort + Freigabe in der Banking-App

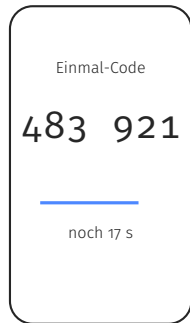
- 2FA = Kombination aus **zwei verschiedenen** Faktoren
- Geldautomat: Karte (**Besitz**) + PIN (**Wissen**) — 2FA seit Jahrzehnten!
- Online-Banking: Passwort + Freigabe in der Banking-App
- Passwort + Sicherheitsfrage ist **keine** 2FA — zweimal Wissen

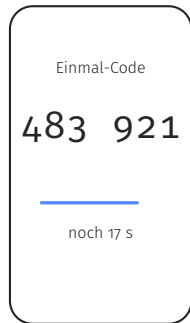
- 2FA = Kombination aus **zwei verschiedenen** Faktoren
- Geldautomat: Karte (**Besitz**) + PIN (**Wissen**) — 2FA seit Jahrzehnten!
- Online-Banking: Passwort + Freigabe in der Banking-App
- Passwort + Sicherheitsfrage ist **keine** 2FA — zweimal Wissen

- 2FA = Kombination aus **zwei verschiedenen** Faktoren
- Geldautomat: Karte (**Besitz**) + PIN (**Wissen**) — 2FA seit Jahrzehnten!
- Online-Banking: Passwort + Freigabe in der Banking-App
- Passwort + Sicherheitsfrage ist **keine** 2FA — zweimal Wissen

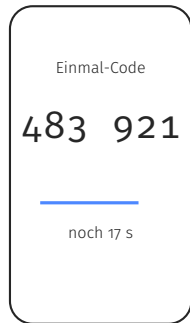
Ein gestohlenes Passwort allein reicht dem Angreifer nicht mehr.

- App und Server teilen ein Geheimnis

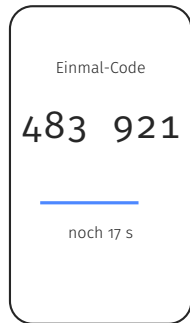




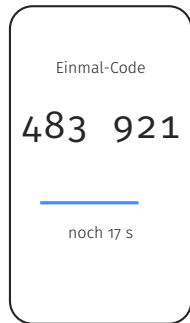
- App und Server teilen ein Geheimnis
- Daraus entsteht alle 30 Sekunden ein neuer 6-stelliger Code (TOTP)



- App und Server teilen ein Geheimnis
- Daraus entsteht alle 30 Sekunden ein neuer 6-stelliger Code (TOTP)
- Funktioniert ohne Internet und ohne Mobilfunk

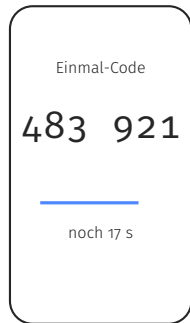


- App und Server teilen ein Geheimnis
- Daraus entsteht alle 30 Sekunden ein neuer 6-stelliger Code (TOTP)
- Funktioniert ohne Internet und ohne Mobilfunk
- Beispiele: Microsoft/Google Authenticator



- App und Server teilen ein Geheimnis
- Daraus entsteht alle 30 Sekunden ein neuer 6-stelliger Code (TOTP)
- Funktioniert ohne Internet und ohne Mobilfunk
- Beispiele: Microsoft/Google Authenticator

Warum ist SMS als zweiter Faktor schwächer?



- App und Server teilen ein Geheimnis
- Daraus entsteht alle 30 Sekunden ein neuer 6-stelliger Code (TOTP)
- Funktioniert ohne Internet und ohne Mobilfunk
- Beispiele: Microsoft/Google Authenticator

Warum ist SMS als zweiter Faktor schwächer?

- **SIM-Swapping**: Angreifer übernimmt die Rufnummer beim Mobilfunkanbieter
- Trotzdem: besser als gar kein zweiter Faktor

DER FAKTOR MENSCH

Die erfolgreichsten Angriffe knacken keine Verschlüsselung —
sie überlisten Menschen.

Die erfolgreichsten Angriffe knacken keine Verschlüsselung —
sie überlisten Menschen.

- Schäden durch Cyberangriffe auf die deutsche Wirtschaft:
mehr als 200 Milliarden Euro pro Jahr (Bitkom)

Die erfolgreichsten Angriffe knacken keine Verschlüsselung —
sie überlisten Menschen.

- Schäden durch Cyberangriffe auf die deutsche Wirtschaft: mehr als 200 Milliarden Euro pro Jahr (Bitkom)
- Häufigster Einstiegsweg laut BSI-Lagebericht: Phishing-E-Mails

Warum den Tresor knacken, wenn man nach dem Schlüssel fragen kann?

Warum den Tresor knacken, wenn man nach dem Schlüssel fragen kann?

Social Engineering: Angriff auf den Menschen statt auf die Technik. Ausgenutzt werden:

- Hilfsbereitschaft ("Kollege" braucht dringend Zugriff)

Warum den Tresor knacken, wenn man nach dem Schlüssel fragen kann?

Social Engineering: Angriff auf den Menschen statt auf die Technik. Ausgenutzt werden:

- Hilfsbereitschaft ("Kollege" braucht dringend Zugriff)
- Respekt vor Autorität (Anruf "vom Chef", "von der Bank")

Warum den Tresor knacken, wenn man nach dem Schlüssel fragen kann?

Social Engineering: Angriff auf den Menschen statt auf die Technik. Ausgenutzt werden:

- Hilfsbereitschaft ("Kollege" braucht dringend Zugriff)
- Respekt vor Autorität (Anruf "vom Chef", "von der Bank")
- Zeitdruck und Angst ("Ihr Konto wird gesperrt!")

Warum den Tresor knacken, wenn man nach dem Schlüssel fragen kann?

Social Engineering: Angriff auf den Menschen statt auf die Technik. Ausgenutzt werden:

- Hilfsbereitschaft ("Kollege" braucht dringend Zugriff)
- Respekt vor Autorität (Anruf "vom Chef", "von der Bank")
- Zeitdruck und Angst ("Ihr Konto wird gesperrt!")
- Neugier (gefundener USB-Stick, Datei "Gehaltsliste.xlsx")

Warum den Tresor knacken, wenn man nach dem Schlüssel fragen kann?

Social Engineering: Angriff auf den Menschen statt auf die Technik. Ausgenutzt werden:

- Hilfsbereitschaft ("Kollege" braucht dringend Zugriff)
- Respekt vor Autorität (Anruf "vom Chef", "von der Bank")
- Zeitdruck und Angst ("Ihr Konto wird gesperrt!")
- Neugier (gefundener USB-Stick, Datei "Gehaltsliste.xlsx")

Warum den Tresor knacken, wenn man nach dem Schlüssel fragen kann?

Social Engineering: Angriff auf den Menschen statt auf die Technik. Ausgenutzt werden:

- Hilfsbereitschaft ("Kollege" braucht dringend Zugriff)
- Respekt vor Autorität (Anruf "vom Chef", "von der Bank")
- Zeitdruck und Angst ("Ihr Konto wird gesperrt!")
- Neugier (gefundener USB-Stick, Datei "Gehaltsliste.xlsx")

"Hier IT-Support — wir brauchen kurz Ihr Passwort für das Update."

Von: Paket Service <service@paket-zustellung-info.xyz>

Betreff: Ihr Paket konnte nicht zugestellt werden!!

Sehr geehrter Kunde,

Ihr Paket Nr. 83921 liegt im Verteilzentrum. Bezahlen Sie die Zollgebühr von 1,99 Euro innerhalb von 24 Stunden, sonst wird das Paket kostenpflichtig zurückgesand.

[» Jetzt bezahlen: paket-zustellung-info.xyz/pay «](#)

Von: Paket Service <service@paket-zustellung-info.xyz> Absender

Betreff: Ihr Paket konnte nicht zugestellt werden!!

Sehr geehrter Kunde,

Ihr Paket Nr. 83921 liegt im Verteilzentrum. Bezahlen Sie die Zollgebühr von 1,99 Euro innerhalb von 24 Stunden, sonst wird das Paket kostenpflichtig zurückgesand.

[» Jetzt bezahlen: paket-zustellung-info.xyz/pay «](#)

Von: Paket Service <service@paket-zustellung-info.xyz> Absender

Betreff: Ihr Paket konnte nicht zugestellt werden!!

Sehr geehrter Kunde,

2 Anrede

Ihr Paket Nr. 83921 liegt im Verteilzentrum. Bezahlen Sie die Zollgebühr von 1,99 Euro innerhalb von 24 Stunden, sonst wird das Paket kostenpflichtig zurückgesand.

[» Jetzt bezahlen: paket-zustellung-info.xyz/pay «](#)

Von: Paket Service <service@paket-zustellung-info.xyz> 1 Absender

Betreff: Ihr Paket konnte nicht zugestellt werden!!

Sehr geehrter Kunde, 2 Anrede

Ihr Paket Nr. 83921 liegt im Verteilzentrum. Bezahlen Sie die Zollge-
buhr von 1,99 Euro innerhalb von 24 Stunden, sonst wird das Paket
kostenpflichtig zurückgesand. 3 Zeitdruck

[» Jetzt bezahlen: paket-zustellung-info.xyz/pay «](#)

Von: Paket Service <service@paket-zustellung-info.xyz>

Betreff: Ihr Paket konnte nicht zugestellt werden!

Sehr geehrter Kunde,

Ihr Paket Nr. 83921 liegt im Verteilzentrum. Bezahlen Sie die Zollgebühren von 1,99 Euro innerhalb von 24 Stunden, sonst wird das Paket kostenpflichtig zurückgesandt.

[» Jetzt bezahlen: paket-zustellung-info.xyz/pay «](#)

- 1 Absender
- 4 Tippfehler
- 2 Anrede
- 3 Zeitdruck

Von: Paket Service <service@paket-zustellung-info.xyz>

Betreff: Ihr Paket konnte nicht zugestellt werden!

Sehr geehrter Kunde,

Ihr Paket Nr. 83921 liegt im Verteilzentrum. Bezahlen Sie die Zollgebühren von 1,99 Euro innerhalb von 24 Stunden, sonst wird das Paket kostenpflichtig zurückgesandt.

» [Jetzt bezahlen: paket-zustellung-info.xyz/pay](https://paket-zustellung-info.xyz/pay) «

- 1 Absender
- 4 Tippfehler
- 2 Anrede
- 3 Zeitdruck
- 5 Link

- Absenderadresse genau lesen — entscheidend ist die **Domain** hinter dem @

- Absenderadresse genau lesen — entscheidend ist die **Domain** hinter dem @
- Link-Ziel prüfen: Maus darüber halten, **nicht** klicken

- Absenderadresse genau lesen — entscheidend ist die **Domain** hinter dem @
- Link-Ziel prüfen: Maus darüber halten, **nicht** klicken
- Niemals Passwörter oder TANs nach einer E-Mail-Aufforderung eingeben

- Absenderadresse genau lesen — entscheidend ist die **Domain** hinter dem @
- Link-Ziel prüfen: Maus darüber halten, **nicht** klicken
- Niemals Passwörter oder TANs nach einer E-Mail-Aufforderung eingeben
- **Zeitdruck ist ein Alarmsignal** — seriöse Anbieter drohen nicht mit Fristen

- Absenderadresse genau lesen — entscheidend ist die **Domain** hinter dem @
- Link-Ziel prüfen: Maus darüber halten, **nicht** klicken
- Niemals Passwörter oder TANs nach einer E-Mail-Aufforderung eingeben
- **Zeitdruck ist ein Alarmsignal** — seriöse Anbieter drohen nicht mit Fristen
- Im Zweifel: die Webseite selbst im Browser aufrufen oder anrufen

- Absenderadresse genau lesen — entscheidend ist die **Domain** hinter dem @
- Link-Ziel prüfen: Maus darüber halten, **nicht** klicken
- Niemals Passwörter oder TANs nach einer E-Mail-Aufforderung eingeben
- **Zeitdruck ist ein Alarmsignal** — seriöse Anbieter drohen nicht mit Fristen
- Im Zweifel: die Webseite selbst im Browser aufrufen oder anrufen

- Absenderadresse genau lesen — entscheidend ist die **Domain** hinter dem @
- Link-Ziel prüfen: Maus darüber halten, **nicht** klicken
- Niemals Passwörter oder TANs nach einer E-Mail-Aufforderung eingeben
- **Zeitdruck ist ein Alarmsignal** — seriöse Anbieter drohen nicht mit Fristen
- Im Zweifel: die Webseite selbst im Browser aufrufen oder anrufen

<https://www.bsi.bund.de/dok/6595724>

"Streng vertraulich! Überweisen Sie heute noch 240.000 Euro für die Firmenübernahme. Keine Rückfragen — ich bin in Verhandlungen.

— Der Geschäftsführer"

"Streng vertraulich! Überweisen Sie heute noch 240.000 Euro für die Firmenübernahme. Keine Rückfragen — ich bin in Verhandlungen.

— Der Geschäftsführer"

- Autorität + Vertraulichkeit + Zeitdruck: **Social Engineering im Paket**

"Streng vertraulich! Überweisen Sie heute noch 240.000 Euro für die Firmenübernahme. Keine Rückfragen — ich bin in Verhandlungen.

— Der Geschäftsführer"

- Autorität + Vertraulichkeit + Zeitdruck: **Social Engineering im Paket**
- Reale Schäden in Millionenhöhe
(z.B. Automobilzulieferer Leoni 2016: ca. 40 Millionen Euro)

"Streng vertraulich! Überweisen Sie heute noch 240.000 Euro für die Firmenübernahme. Keine Rückfragen — ich bin in Verhandlungen.

— Der Geschäftsführer"

- Autorität + Vertraulichkeit + Zeitdruck: **Social Engineering im Paket**
- Reale Schäden in Millionenhöhe
(z.B. Automobilzulieferer Leoni 2016: ca. 40 Millionen Euro)

"Streng vertraulich! Überweisen Sie heute noch 240.000 Euro für die Firmenübernahme. Keine Rückfragen — ich bin in Verhandlungen.

— Der Geschäftsführer"

- Autorität + Vertraulichkeit + Zeitdruck: **Social Engineering im Paket**
- Reale Schäden in Millionenhöhe
(z.B. Automobilzulieferer Leoni 2016: ca. 40 Millionen Euro)

Gegenmaßnahmen:

- **Vier-Augen-Prinzip** bei Überweisungen

"Streng vertraulich! Überweisen Sie heute noch 240.000 Euro für die Firmenübernahme. Keine Rückfragen — ich bin in Verhandlungen.

— Der Geschäftsführer"

- Autorität + Vertraulichkeit + Zeitdruck: **Social Engineering im Paket**
- Reale Schäden in Millionenhöhe
(z.B. Automobilzulieferer Leoni 2016: ca. 40 Millionen Euro)

Gegenmaßnahmen:

- **Vier-Augen-Prinzip** bei Überweisungen
- Rückruf über die **bekannte** Nummer, nie über die aus der Mail

"Streng vertraulich! Überweisen Sie heute noch 240.000 Euro für die Firmenübernahme. Keine Rückfragen — ich bin in Verhandlungen.

— Der Geschäftsführer"

- Autorität + Vertraulichkeit + Zeitdruck: **Social Engineering im Paket**
- Reale Schäden in Millionenhöhe
(z.B. Automobilzulieferer Leoni 2016: ca. 40 Millionen Euro)

Gegenmaßnahmen:

- **Vier-Augen-Prinzip** bei Überweisungen
- Rückruf über die **bekannte** Nummer, nie über die aus der Mail
- Feste Freigabeprozesse — auch wenn "der Chef" drängelt

- Awareness-Schulungen und **Phishing-Simulationen** (Test-Mails an die eigene Belegschaft)

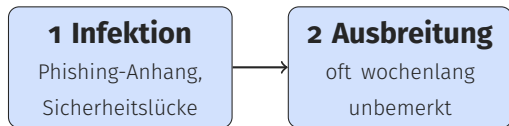
- Awareness-Schulungen und **Phishing-Simulationen** (Test-Mails an die eigene Belegschaft)
- Klare Meldewege: lieber einmal zu viel melden als einmal zu wenig

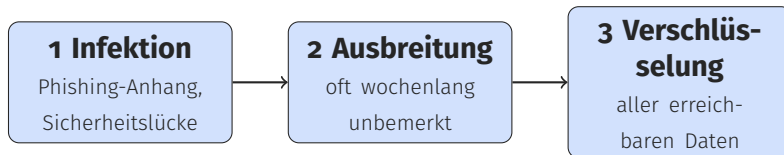
- Awareness-Schulungen und **Phishing-Simulationen** (Test-Mails an die eigene Belegschaft)
- Klare Meldewege: lieber einmal zu viel melden als einmal zu wenig
- **Fehlerkultur**: Wer klickt und es meldet, wird nicht bestraft — sonst meldet es niemand mehr

RANSOMWARE UND BACKUPS

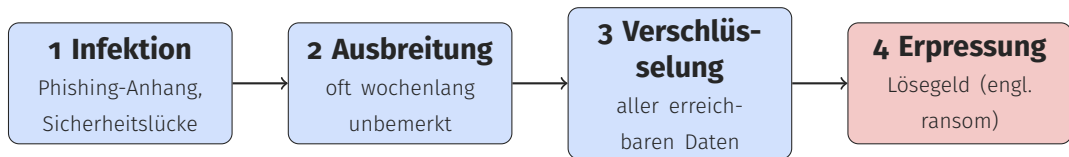
1 Infektion

Phishing-Anhang,
Sicherheitslücke

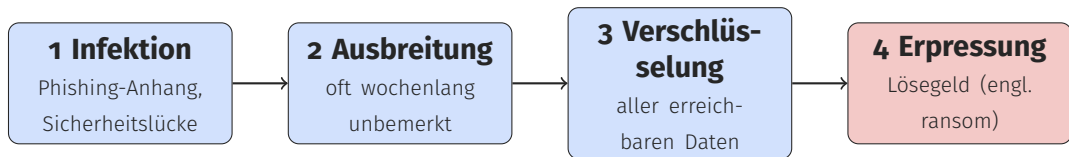




- Die Angreifer nutzen **symmetrische Verschlüsselung** — die kennen Sie schon!



- Die Angreifer nutzen **symmetrische Verschlüsselung** — die kennen Sie schon!



- Die Angreifer nutzen **symmetrische Verschlüsselung** — die kennen Sie schon!
- Oft zusätzlich: Drohung, gestohlene Daten zu veröffentlichen (**Double Extortion**)

Die Daten sind verschlüsselt, der Betrieb steht still. Zahlen?

Die Daten sind verschlüsselt, der Betrieb steht still. Zahlen?

Empfehlung von BSI und Polizei: Nein!

Die Daten sind verschlüsselt, der Betrieb steht still. Zahlen?

Empfehlung von BSI und Polizei: Nein!

- Keine Garantie, dass die Daten wiederkommen

Die Daten sind verschlüsselt, der Betrieb steht still. Zahlen?

Empfehlung von BSI und Polizei: Nein!

- Keine Garantie, dass die Daten wiederkommen
- Jede Zahlung finanziert die nächsten Angriffe

Die Daten sind verschlüsselt, der Betrieb steht still. Zahlen?

Empfehlung von BSI und Polizei: Nein!

- Keine Garantie, dass die Daten wiederkommen
- Jede Zahlung finanziert die nächsten Angriffe
- Wer zahlt, gilt als lohnendes Ziel — und wird wieder angegriffen

Die Daten sind verschlüsselt, der Betrieb steht still. Zahlen?

Empfehlung von BSI und Polizei: Nein!

- Keine Garantie, dass die Daten wiederkommen
- Jede Zahlung finanziert die nächsten Angriffe
- Wer zahlt, gilt als lohnendes Ziel — und wird wieder angegriffen

Die Daten sind verschlüsselt, der Betrieb steht still. Zahlen?

Empfehlung von BSI und Polizei: Nein!

- Keine Garantie, dass die Daten wiederkommen
- Jede Zahlung finanziert die nächsten Angriffe
- Wer zahlt, gilt als lohnendes Ziel – und wird wieder angegriffen

Stattdessen: Anzeige erstatten, Systeme neu aufsetzen, **aus Backups wiederherstellen.**

3

Kopien der Daten (Original + zwei Sicherungen)

- 3** Kopien der Daten (Original + zwei Sicherungen)
- 2** verschiedene Speichermedien

- 3 Kopien der Daten (Original + zwei Sicherungen)
- 2 verschiedene Speichermedien
- 1 Kopie außer Haus — und **offline**

- 3 Kopien der Daten (Original + zwei Sicherungen)
- 2 verschiedene Speichermedien
- 1 Kopie außer Haus — und **offline**

- Warum offline? Ransomware verschlüsselt auch das angeschlossene Backup-Laufwerk!

3 Kopien der Daten (Original + zwei Sicherungen)

2 verschiedene Speichermedien

1 Kopie außer Haus — und **offline**

- Warum offline? **Ransomware verschlüsselt auch das angeschlossene Backup-Laufwerk!**
- Gilt übrigens auch für Ihre Bachelorarbeit ...

Was verletzt ein Ransomware-Angriff eigentlich?

Was verletzt ein Ransomware-Angriff eigentlich?

- Die Daten sind unbrauchbar → die **Verfügbarkeit** ist weg

Was verletzt ein Ransomware-Angriff eigentlich?

- Die Daten sind unbrauchbar → die **Verfügbarkeit** ist weg
- Bei Double Extortion zusätzlich: Daten veröffentlicht → die **Vertraulichkeit** ist weg

Was verletzt ein Ransomware-Angriff eigentlich?

- Die Daten sind unbrauchbar → die **Verfügbarkeit** ist weg
- Bei Double Extortion zusätzlich: Daten veröffentlicht → die **Vertraulichkeit** ist weg

Was verletzt ein Ransomware-Angriff eigentlich?

- Die Daten sind unbrauchbar → die **Verfügbarkeit** ist weg
- Bei Double Extortion zusätzlich: Daten veröffentlicht → die **Vertraulichkeit** ist weg

Verfügbarkeit? Vertraulichkeit? — Diese **Schutzziele** schauen wir uns jetzt systematisch an.

INFORMATIONSSICHERHEIT

Sicherstellung der Schutzziele

Vertraulichkeit: Informationen sind nur für den vorgesehenen Empfängerkreis einsehbar

Verfügbarkeit: Informationen stehen mit hoher Wahrscheinlichkeit zur Verfügung

Integrität: Informationen können nicht unautorisiert verändert werden

- Schutz vor unbefugter Preisgabe von Informationen
 - Eigenschaft einer Information, nur für einen beschränkten Empfängerkreis vorgesehen zu sein.
 - Weitergabe und Veröffentlichung sind nicht erwünscht.
- Schutzmaßnahmen
 - Zugangskontrolle (Bsp.: Tresor, Passwörter, etc.)
 - Verschlüsselung (Bsp.: HTTPS)

- Gewährleistung, dass die Daten/das System
 - zugänglich und
 - funktionsfähig sind/ist.
- Schutz vor
 - Ausfällen (Schutz gegen Stromausfall, Brand, Wasser, ...)
 - Datenverlust (Erstellen von Sicherungen → 3-2-1-Regel)
 - Diebstahl / Ransomware (siehe vorige Sektion)
 - Denial-of-Service-Attacken

- Gewährleistung, dass die Daten nur von befugten Personen geändert werden
- Schutz vor unbefugtem
 - Löschen
 - Ändern
 - Hinzufügen

- Zurechenbarkeit
 - Es kann jederzeit nachgewiesen werden, wer welche Änderungen durchgeführt hat
- Verbindlichkeit/Nichtabstreitbarkeit (engl. non-repudiation)
 - Es ist kein unzulässiges Abstreiten durchgeführter Handlungen
- Rechtssicherheit
 - Die Informationen können rechtskräftig nachgewiesen werden
 - Ein Vertragsabschluss muss z.B. nachgewiesen werden können

- Gesetzliche Anforderungen
 - Datenschutzgrundverordnung (DSGVO)
 - BSI-Gesetz §8a: Sicherheit in der Informationstechnik Kritischer Infrastrukturen
 - BSI-Gesetz §8c: Anforderungen an Anbieter digitaler Dienste
 - Basel II, SOX, Richtlinien zur Buchführung lassen Anforderungen erschließen

- Gesetzliche Anforderungen
 - Datenschutzgrundverordnung (DSGVO)
 - BSI-Gesetz §8a: Sicherheit in der Informationstechnik Kritischer Infrastrukturen
 - BSI-Gesetz §8c: Anforderungen an Anbieter digitaler Dienste
 - Basel II, SOX, Richtlinien zur Buchführung lassen Anforderungen erschließen
- Externe Anforderungen
 - Geschäftspartner erwarten die vertrauliche/sichere Verwendung von Daten
 - BP: Teilefertigung für Automobile erfordern genaue Kenntnisse über Automobil-Design

- Gesetzliche Anforderungen
 - Datenschutzgrundverordnung (DSGVO)
 - BSI-Gesetz §8a: Sicherheit in der Informationstechnik Kritischer Infrastrukturen
 - BSI-Gesetz §8c: Anforderungen an Anbieter digitaler Dienste
 - Basel II, SOX, Richtlinien zur Buchführung lassen Anforderungen erschließen
- Externe Anforderungen
 - Geschäftspartner erwarten die vertrauliche/sichere Verwendung von Daten
 - BP: Teilefertigung für Automobile erfordern genaue Kenntnisse über Automobil-Design
- Interne Anforderungen
 - Daten stellen wirtschaftlichen Wert dar
 - Personaldaten sind für Headhunter interessant
 - Produktdaten für Konkurrenzunternehmen/Plagierer
 - Verlust von vertraulichen Daten kann zu Vertrauensverlust führen (weniger Kunden, Kursverluste, ...)

Kein System kann 100% die Anforderungen erfüllen

- schon früher nicht → Panzerknackerbande
- Risiken:
 - analysieren
 - bewerten (Schaden im Eintrittsfall vs. Eintrittswahrscheinlichkeit vs. Kosten der Schutzmaßnahmen)
 - dokumentieren
 - Schutzmaßnahmen ergreifen

Die Sicherstellung der Informationssicherheit ist ein fortlaufender Prozess

- IT-Grundschutz-Katalog des Bundesamts für Sicherheit in der Informationstechnik (BSI)

Sie liegt in der Verantwortung der Geschäftsleitung, diese kann nicht delegiert werden.

DATENSCHUTZ

Grundrecht auf informationelle Selbstbestimmung

- Jeder kann selbst darüber entscheiden, wem er welche persönlichen Informationen zur Verfügung stellt
- *Volkszählungsurteil* (BVerfG, vom 15. Dezember 1983)
- Verordnung (EU) 2016/679: Datenschutz-Grundverordnung (DSGVO)

Die DSGVO schützt personenbezogene Daten (Art. 4):

- alle Informationen über eine identifizierte oder identifizierbare Person

Die DSGVO schützt **personenbezogene Daten** (Art. 4):

- alle Informationen über eine **identifizierte oder identifizierbare** Person

Besondere Kategorien (Art. 9, streng geschützt):

- Gesundheit, Religion, politische Meinung, Biometrie, Sexualleben, Herkunft

Ein Online-Shop speichert über jeden Kunden sechs Felder. **Sortieren Sie: heikel oder harmlos?**

Name

Adresse

Geburtsdatum

Geschlecht

Bestellhistorie

Zahlungsart

Ein Online-Shop speichert über jeden Kunden sechs Felder. **Sortieren Sie: heikel oder harmlos?**

Name	Adresse	Geburtsdatum
Geschlecht	Bestellhistorie	Zahlungsart

- **Name, Adresse:** identifizieren direkt — klar schützenswert

Ein Online-Shop speichert über jeden Kunden sechs Felder. **Sortieren Sie: heikel oder harmlos?**

Name	Adresse	Geburtsdatum
Geschlecht	Bestellhistorie	Zahlungsart

- **Name, Adresse:** identifizieren direkt — klar schützenswert
- Der Rest ist harmlos? **Die Kombination macht's:**
Geburtsdatum + Postleitzahl + Geschlecht identifizieren die meisten Menschen eindeutig

Ein Online-Shop speichert über jeden Kunden sechs Felder. **Sortieren Sie: heikel oder harmlos?**

Name	Adresse	Geburtsdatum
Geschlecht	Bestellhistorie	Zahlungsart

- **Name, Adresse:** identifizieren direkt — klar schützenswert
- Der Rest ist harmlos? **Die Kombination macht's:**
Geburtsdatum + Postleitzahl + Geschlecht identifizieren die meisten Menschen eindeutig
- Und die Bestellhistorie kann Sensibles verraten (Medikamente, ...)

Datenschutz-Grundverordnung (DSGVO)

- **Einwilligung/Rechtsgrundlage:** Unternehmen dürfen Daten nur speichern, wenn
 - es eine gesetzliche Verpflichtung dazu gibt (z.B. Vertragsdaten, Abrechnungsdaten, ...), oder
 - der Betroffene seine explizite Einwilligung dazu gegeben hat

Datenschutz-Grundverordnung (DSGVO)

- **Einwilligung/Rechtsgrundlage**: Unternehmen dürfen Daten nur speichern, wenn
 - es eine gesetzliche Verpflichtung dazu gibt (z.B. Vertragsdaten, Abrechnungsdaten, ...), oder
 - der Betroffene seine explizite Einwilligung dazu gegeben hat
- **Datenminimierung** (Minimalitätsprinzip): Nur die Daten speichern, die unbedingt erforderlich sind

Datenschutz-Grundverordnung (DSGVO)

- **Einwilligung/Rechtsgrundlage**: Unternehmen dürfen Daten nur speichern, wenn
 - es eine gesetzliche Verpflichtung dazu gibt (z.B. Vertragsdaten, Abrechnungsdaten, ...), oder
 - der Betroffene seine explizite Einwilligung dazu gegeben hat
- **Datenminimierung** (Minimalitätsprinzip): Nur die Daten speichern, die unbedingt erforderlich sind
- **Zweckbindung**: Daten dürfen nur für den Zweck genutzt werden, für den sie erhoben wurden

Datenschutz-Grundverordnung (DSGVO)

- **Einwilligung/Rechtsgrundlage**: Unternehmen dürfen Daten nur speichern, wenn
 - es eine gesetzliche Verpflichtung dazu gibt (z.B. Vertragsdaten, Abrechnungsdaten, ...), oder
 - der Betroffene seine explizite Einwilligung dazu gegeben hat
- **Datenminimierung** (Minimalitätsprinzip): Nur die Daten speichern, die unbedingt erforderlich sind
- **Zweckbindung**: Daten dürfen nur für den Zweck genutzt werden, für den sie erhoben wurden
- Gespeicherte Daten müssen auf Anfrage
 - herausgegeben werden
 - korrigiert werden
 - gelöscht werden (wenn rechtlich zulässig)

Datenschutz-Grundverordnung (DSGVO)

- **Einwilligung/Rechtsgrundlage**: Unternehmen dürfen Daten nur speichern, wenn
 - es eine gesetzliche Verpflichtung dazu gibt (z.B. Vertragsdaten, Abrechnungsdaten, ...), oder
 - der Betroffene seine explizite Einwilligung dazu gegeben hat
- **Datenminimierung** (Minimalitätsprinzip): Nur die Daten speichern, die unbedingt erforderlich sind
- **Zweckbindung**: Daten dürfen nur für den Zweck genutzt werden, für den sie erhoben wurden
- Gespeicherte Daten müssen auf Anfrage
 - herausgegeben werden
 - korrigiert werden
 - gelöscht werden (wenn rechtlich zulässig)
- Die Prinzipien müssen auch eingehalten werden, wenn die Daten an Dritte weitergegeben werden

Ein Online-Händler erhebt Kundendaten "zur Bestellabwicklung und für Serviceanfragen" — so haben die Kunden eingewilligt.

Später gibt er die **komplette Kundentabelle** an einen Werbedienstleister weiter.

Ein Online-Händler erhebt Kundendaten "zur Bestellabwicklung und für Serviceanfragen" — so haben die Kunden eingewilligt.

Später gibt er die **komplette Kundentabelle** an einen Werbedienstleister weiter.

Welche Grundsätze sind verletzt?

Ein Online-Händler erhebt Kundendaten "zur Bestellabwicklung und für Serviceanfragen" — so haben die Kunden eingewilligt.

Später gibt er die **komplette Kundentabelle** an einen Werbedienstleister weiter.

Welche Grundsätze sind verletzt?

- **Zweckbindung**: Werbung war nicht der Zweck der Erhebung

Ein Online-Händler erhebt Kundendaten "zur Bestellabwicklung und für Serviceanfragen" — so haben die Kunden eingewilligt.

Später gibt er die **komplette Kundentabelle** an einen Werbedienstleister weiter.

Welche Grundsätze sind verletzt?

- **Zweckbindung**: Werbung war nicht der Zweck der Erhebung
- **Einwilligung**: deckt die Weitergabe nicht ab

Ein Online-Händler erhebt Kundendaten "zur Bestellabwicklung und für Serviceanfragen" — so haben die Kunden eingewilligt.

Später gibt er die **komplette Kundentabelle** an einen Werbedienstleister weiter.

Welche Grundsätze sind verletzt?

- **Zweckbindung**: Werbung war nicht der Zweck der Erhebung
- **Einwilligung**: deckt die Weitergabe nicht ab
- **Datenminimierung**: komplette Tabelle statt der nötigen Felder

- Separate, **spezifische Einwilligung** für Werbung einholen

- Separate, **spezifische Einwilligung** für Werbung einholen
- Nur die **benötigten Felder** übermitteln

- Separate, **spezifische Einwilligung** für Werbung einholen
- Nur die **benötigten Felder** übermitteln
- **Pseudonymisieren**: Name durch Kundennummer ersetzen

- Separate, **spezifische Einwilligung** für Werbung einholen
- Nur die **benötigten Felder** übermitteln
- **Pseudonymisieren**: Name durch Kundennummer ersetzen
- **Auftragsverarbeitungsvertrag** (Art. 28 DSGVO) mit dem Dienstleister schließen

Anna Meier, 44801 Bochum, 12.03.2004

Anna Meier, 44801 Bochum, 12.03.2004



Pseudonymisierung: Name → Kundennummer

K-4711, 44801 Bochum, 12.03.2004

- Die Zuordnungstabelle (K-4711 → Anna Meier) wird **getrennt** aufbewahrt

Anna Meier, 44801 Bochum, 12.03.2004



Pseudonymisierung: Name → Kundennummer

K-4711, 44801 Bochum, 12.03.2004



Anonymisierung: Details vergrößern/löschen

448xx, Jahrgang 2004

- Die Zuordnungstabelle (K-4711 → Anna Meier) wird **getrennt** aufbewahrt

Anna Meier, 44801 Bochum, 12.03.2004



Pseudonymisierung: Name → Kundennummer

K-4711, 44801 Bochum, 12.03.2004



Anonymisierung: Details vergrößern/löschen

448xx, Jahrgang 2004

- Die Zuordnungstabelle (K-4711 → Anna Meier) wird **getrennt** aufbewahrt
- Pseudonymisierte Daten bleiben **personenbezogen**:
PLZ + Geburtsdatum reichen oft zur **Re-Identifikation** (siehe eben!)

Anna Meier, 44801 Bochum, 12.03.2004



Pseudonymisierung: Name → Kundennummer

K-4711, 44801 Bochum, 12.03.2004



Anonymisierung: Details vergrößern/löschen

448xx, Jahrgang 2004

- Die Zuordnungstabelle (K-4711 → Anna Meier) wird **getrennt** aufbewahrt
- Pseudonymisierte Daten bleiben **personenbezogen**:
PLZ + Geburtsdatum reichen oft zur **Re-Identifikation** (siehe eben!)
- Erst **anonymisierte** Daten fallen nicht mehr unter die DSGVO

Ein Händler schätzt mit einem Modell das **Retourenrisiko** jeder Bestellung. Das Merkmal **Postleitzahl** verbessert die Vorhersage deutlich — Kunden aus manchen Vierteln bekommen nur noch Vorkasse.

Ein Händler schätzt mit einem Modell das **Retourenrisiko** jeder Bestellung. Das Merkmal **Postleitzahl** verbessert die Vorhersage deutlich — Kunden aus manchen Vierteln bekommen nur noch Vorkasse.

Was ist daran problematisch?

Ein Händler schätzt mit einem Modell das **Retourenrisiko** jeder Bestellung. Das Merkmal **Postleitzahl** verbessert die Vorhersage deutlich — Kunden aus manchen Vierteln bekommen nur noch Vorkasse.

Was ist daran problematisch?

- Die PLZ korreliert mit Einkommen und Herkunft → **Proxy-Diskriminierung**

Ein Händler schätzt mit einem Modell das **Retourenrisiko** jeder Bestellung. Das Merkmal **Postleitzahl** verbessert die Vorhersage deutlich — Kunden aus manchen Vierteln bekommen nur noch Vorkasse.

Was ist daran problematisch?

- Die PLZ korreliert mit Einkommen und Herkunft → **Proxy-Diskriminierung**
- Formal wird kein "verbotenes" Merkmal benutzt — die Wirkung ist trotzdem diskriminierend

Ein Händler schätzt mit einem Modell das **Retourenrisiko** jeder Bestellung. Das Merkmal **Postleitzahl** verbessert die Vorhersage deutlich — Kunden aus manchen Vierteln bekommen nur noch Vorkasse.

Was ist daran problematisch?

- Die PLZ korreliert mit Einkommen und Herkunft → **Proxy-Diskriminierung**
- Formal wird kein "verbotenes" Merkmal benutzt — die Wirkung ist trotzdem diskriminierend

Ein Händler schätzt mit einem Modell das **Retourenrisiko** jeder Bestellung. Das Merkmal **Postleitzahl** verbessert die Vorhersage deutlich — Kunden aus manchen Vierteln bekommen nur noch Vorkasse.

Was ist daran problematisch?

- Die PLZ korreliert mit Einkommen und Herkunft → **Proxy-Diskriminierung**
- Formal wird kein "verbotenes" Merkmal benutzt — die Wirkung ist trotzdem diskriminierend

Diskussion: Sollte ein Shop sein Angebot am Kundenverhalten personalisieren?

Auskunft: kostenlose Kopie aller gespeicherten Daten (Art. 15)

Auskunft: kostenlose Kopie aller gespeicherten Daten (Art. 15)

Berichtigung: falsche Daten müssen korrigiert werden (Art. 16)

Auskunft: kostenlose Kopie aller gespeicherten Daten (Art. 15)

Berichtigung: falsche Daten müssen korrigiert werden (Art. 16)

Löschung: "Recht auf Vergessenwerden" (Art. 17)

Auskunft: kostenlose Kopie aller gespeicherten Daten (Art. 15)

Berichtigung: falsche Daten müssen korrigiert werden (Art. 16)

Löschung: "Recht auf Vergessenwerden" (Art. 17)

Widerspruch: z.B. gegen Werbung (Art. 21)

Auskunft: kostenlose Kopie aller gespeicherten Daten (Art. 15)

Berichtigung: falsche Daten müssen korrigiert werden (Art. 16)

Löschung: "Recht auf Vergessenwerden" (Art. 17)

Widerspruch: z.B. gegen Werbung (Art. 21)

Auskunft: kostenlose Kopie aller gespeicherten Daten (Art. 15)

Berichtigung: falsche Daten müssen korrigiert werden (Art. 16)

Löschung: "Recht auf Vergessenwerden" (Art. 17)

Widerspruch: z.B. gegen Werbung (Art. 21)

- Probieren Sie es aus: Auskunftsanfrage per E-Mail an einen Online-Shop — Antwortfrist: ein Monat
- Beschwerdestelle: Landesbeauftragte für Datenschutz (in NRW: LDI NRW)