

ISF HS 2019

Victor Fernández¹, Hillary Funke², Simon Monai², Estefania C. Otero²,
Pavaskar Parameswaran³, Kevin Soares Correia³, and Johannen Yilmaz²

¹HSLU Informatik

²HSLU Information and Cyber Security

³HSLU Wirtschaftsinformatik

Januar 2020

Vorwort

Diese Zusammenfassung entstand in einer Gruppe während der Lernphase des HS 2019. Alle Fragen aus der Stoffabgrenzung tragen eine **blaue Farbe** und stehen als Unterkapitel. Das Dokument ist Open Source und jeder der möchte und signifikant beiträgt, darf sich als Autor anhängen. Die Source ist [dieses GitHub-Repo¹](#). Dies ist mein erstes L^AT_EX-Dokument überhaupt. Nichts desto trotz wurde auf eine klare Strukturierung und Lesbarkeit des Dokumentes Wert gelegt.

Inhaltsverzeichnis

I Einführung (SW 01)	3
1 Einführung	3
II Kryptographie (SW 02-04)	6
2 Symmetrische Kryptographie	7
3 Asymmetrische Kryptographie	14
4 Zertifikate und SSL-TLS	18
III Angriffe (SW 05-06)	21
5 Angriffe auf Webanwendungen	21
6 Angriffe auf Protokollebene	24
IV Management (SW 07-09)	31
7 Standards & Frameworks, ISMS	31
8 Risiko-Management und IT-Grundschutz	39
9 Awareness	63
V Access Control (SW 10)	65

¹https://github.com/vigi86/HSLU_Zusammenfassungen/tree/master/ISF_HS19

10 Access Control	65
VI Multi-Party-Computation (SW 11)	67
11 Cryptographic Protocols	67
12 Secret Sharing	68
13 Zero-Knowledge-Proof	70
VII Quantum (SW 12)	70
14 Quantum Computing and Quantum Cryptography	70
VIII WAF, Federations (SW 13)	73
15 Firewalls	73
16 Federations	74
IX Talks (SW 14)	79
17 Malware	80
18 WAF	82

Teil I

Einführung (SW 01)

1 Einführung

Einführung in das Thema „Management von Informationssicherheit“

Daten, Information und Wissen Information ist die Verknüpfung von Daten in Form von Zahlen, Worten und Fakten zu interpretierbaren Zusammenhängen. Durch die Vernetzung von Informationen entsteht Wissen, das zunächst personenbezogen ist.

Missbrauch Informationen müssen vor Missbrauch geschützt werden

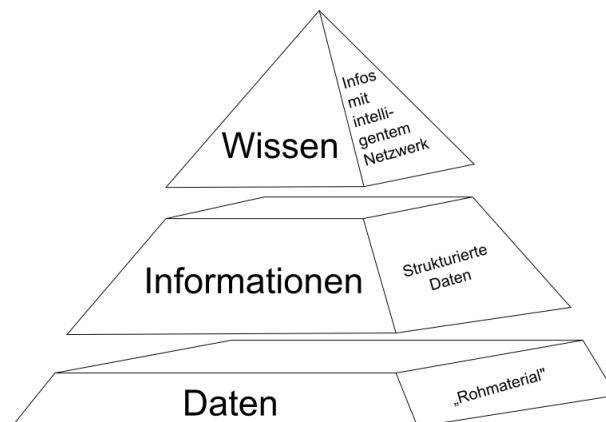


Abbildung 1: Wissenspyramide[1]

Motivation / Bedrohungen

Was gefährdet die Informationen? Welche Gefährdungen/Bedrohungen gibt es?

- Nicht vorsätzliche (zufällige) Gefährdungen/Bedrohungen
 - Naturgewalten (Blitz, Hagel, Unwetter, Erdbeben, Hochwasser, etc.)
 - Ausfall von Strom oder Telekommunikation
 - Technische Pannen, z.B. Fehler von Hard- und/oder Software
 - Bedienerfehler / Fahrlässigkeit der Mitarbeitenden
- Vorsätzliche Gefährdungen/Bedrohungen
 - Bösartiger Code (Viren, Würmer, Trojaner, etc.)
 - Informationsdiebstahl
 - Angriffe (von Skript-Kiddies bis Hacker)
 - Wirtschaftsspionage („was die Konkurrenz wissen möchte“)
 - Missbrauch der IT-Infrastruktur

Menschliches Fehlverhalten durch Fahrlässigkeit, Gleichgültigkeit, Unwissenheit und Leichtgläubigkeit.

Vorsätzliche Manipulation

- Angriffe über das Internet
- Unerlaubter Zugriff auf Systeme
- Abhören und Modifizieren von Daten
- Angriff auf die Verfügbarkeit von Systemen
- Missbrauch von Systemen, Distributed Denial of Service (DDoS)
- Viren, Würmer und Trojanische Pferde
- Drive by Infection²

²unbeabsichtigtes Downloaden von Schadsoftware

Organisatorische Schwachstellen

- Fehlendes Sicherheitsverständnis des Managements
- Unklare Verantwortlichkeiten
- Ungenaue oder fehlende Abläufe / Prozesse
- Mangelhafte Richtlinien
- Fehlende Strategie und Konzepte
- Mangelhafte Awareness der Mitarbeitenden
- Fehlende Kontrollen

Technisches Versagen

- Ungenügende Wartung
- Nicht funktionirende Überwachungssysteme (z.B. IDS³, etc.)
- Falsch dimensionierte Systeme
- Fehlerhafte
 - Konfiguration
 - Applikationen
 - Betriebssysteme
 - Firmware
 - Treiber
 - etc.

Höhere Gewalt

- Ökologisch
 - Unwetter
 - Erdbeben
 - Brände
 - Überschwemmungen
 - Vulkanausbrüche
- Technisch
 - Feuer
 - Wasser
- Sozial
 - Ausschreitungen
 - Geiselnahme
 - Krieg

Verantwortung der Informationssicherheit „Wer die Erfüllung einer Aufgabe befugterweise einem anderen Organ überträgt, haftet für den von diesem verursachten Schaden, sofern er nicht nachweist, dass er bei der Auswahl, Unterrichtung und Überwachung die nach den Umständen gebotene Sorgfalt angewendet hat.“ (OR Art. 754 Absatz 2)

- Fehlende Informationssicherheit kann den Geschäftsfortgang stören oder verunmöglichen
- Der Schutz der Informationen gehört zur Sorgfaltspflicht des Managements
- Verantwortung kann nicht delegiert werden! Denn:

Die Überwachung der Informationssicherheit ist Chefsache!

Ohne Management-Support geht gar nichts!

- Keine Ressourcen (Zeit und Geld)
- Keine Kompetenzen (Befehls- und Umsetzungsgewalt)
- Keine Priorität

Denn das Management trägt die Risiken und entscheidet über die eingesetzten Ressourcen!

Oft gehörte Sicht des Managements

- Was bringt uns Informationssicherheit? ... außer Kosten?
- Wir haben ja schon eine Firewall, oder wie das heißt...
- Unser Unternehmen ist kein lohnendes Ziel für Hacker...
- Bei uns ist noch nie etwas passiert!
- Unsere Mitarbeiter sind zu 100% loyal und wir haben Vertrauen!
- Wir können im Notfall auf unsere Computer problemlos einige Tage verzichten!

³Intrusion Detection System

Was passiert, wenn nichts unternommen wird?

- Kompletter Datenverlust führt in 50% der Fälle zum Konkurs innert 24 Monaten
- Die Beschaffung und Aufbau eines Standard-Ersatzsystems dauert mindestens 36h (falls kein System direkt vor Ort verfügbar)
- Datendiebstahl (wird in den wenigsten Fällen bemerkt)
- Kommen vertrauliche Daten an die Öffentlichkeit, ist der Image-Verlust bei den Kunden je nach Unternehmen immens
- Verletzung gesetzlicher Vorgaben kann strafrechtliche Folgen haben
- Verletzung der Sorgfaltspflicht

Nutzen der Informationssicherheit

- Geringere Verwundbarkeit
- Keine falsche Sicherheit
- Bewussterer Umgang mit Informationen
- Gefahren kennen
- Bewusstes Eingehen von Risiken / Restrisiko bekannt
- Sorgfaltspflicht erfüllt

Umsetzung

- Management ins Boot holen
- Prozess der Informationssicherheit etablieren
- Verantwortlichkeiten festlegen
- Sicherheit allumfassend betrachten
- Schrittweise und stetig umsetzen

Grundbegriffe

Zutritts-, Zugangs-, Zugriffskontrolle

- **Zutrittskontrolle:** Schutz des physischen Systems (Bsp. Serverraum)
- **Zugangskontrolle:** Schutz des logischen Systems (Bsp. Betriebssystem)
- **Zugriffskontrolle:** Daten-bezogen; Schutz der Operationen (Bsp. Dateisystem)

Grundziele (Schutzziele) von Informationssicherheit

Verfügbarkeit

- **Verfügbarkeit** ist gewährleistet, wenn in der vom Benutzer gewünschten Zeit auf Dienste oder Informationen zugegriffen werden kann (Ausfallquote)
- Engl.: **Availability**

Integrität

- **Integrität** ist gewährleistet, wenn Daten oder Systeme nicht unautorisiert oder zufällig manipuliert oder verändert werden können (Datensicherheit)
- Engl.: **Integrity**

Verbindlichkeit

- **Verbindlichkeit** liegt vor, wenn eine Handlung eindeutig einer Person zugeordnet und von dieser nicht geleugnet werden kann
- Engl.: **Non-Repudiation**

Vertraulichkeit

- **Vertraulichkeit** ist gegeben, wenn sichergestellt werden kann, dass Informationen nicht durch unautorisierte Personen, Instanzen oder Prozesse eingesehen werden können
- Engl.: **Confidentiality**

Grundziel



Entdeckung



Abbildung 2: Zeitpunkt der Entdeckung eines Grundziel-Verlustes

Identität / Authentizität

- **Identität:** „Beim Menschen bezeichnet Identität die ihn kennzeichnende und als Individuum von anderen Menschen unterscheidende Eigentümlichkeit seines Wesens.“[1]
- **Authentizität:** „In der Informationssicherheit bezeichnet Authentizität die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit. Die Überprüfung einer behaupteten Eigenschaft wird als Authentifikation bezeichnet. Durch Authentifikation des Datenursprungs wird nachgewiesen, dass Daten einem angegebenen Sender zugeordnet werden können, was durch digitale Signaturen ermöglicht werden kann⁴.“[1]

Risiko Ein Risiko ist ein negativer Ausgang einer Unternehmung, mit dem Nachteile, Verlust, Schäden, usw. verbunden sind.

- Wahrscheinlichkeit, dass eine Gefährdung über eine Schwachstelle zu einem Schaden von bestimmten Ausmass führt
- Wahrscheinlichkeiten sind extrem schwer zu berechnen → Geschätzte Häufigkeiten
- **Risiko = Eintretenshäufigkeit × Schadensausmass**
- Die Eintretenshäufigkeit und Schaden können bewertet werden
- Sicherheit und Risiko sind voneinander abhängig

Integrale⁵, holistische⁶, Informations- und IT-Sicherheit

- Integral: Umfassende Betrachtung aller Sicherheitsaspekte einer Organisation
- Holistisch: Funktionsorientierte und stufengerechte Förderung des Verständnisses für Sicherheit bei Mitarbeitenden, Sicherheitsfachleuten und Management
- Informationssicherheit: Sicherheit in der Verarbeitung von medienunabhängiger Information als solche, also nicht beschränkt auf elektronische Verarbeitung
 - Elektronische Datenträger
 - Papier
 - In den Köpfen der Mitarbeitenden
- IT-Sicherheit: Schutz der Information in ICT-Systemen
 - Server / Hosts
 - Clients / Notebooks
 - Mobile Datenträger (Smartphones, USB-Sticks, Dicams, etc.)

Datensicherheit & Datenschutz

- **Datensicherheit** (–Informationssicherheit): Schutz von Daten und Informationen
- **Datenschutz:** Schutz der Persönlichkeit und er Grundrechte von Personen, über die Daten bearbeitet werden

⁴Siehe Authentifizierung, Seite 67

⁵Die Integrale Sicherheit überprüft Personen und Unternehmen mit Zugang zu vertraulichen oder geheimen Informationen, Materialien oder Anlagen. - <https://www.sbis.ch>

⁶ganzheitlich

Teil II

Kryptographie (SW 02-04)

2 Symmetrische Kryptographie

Sie verstehen was Steganographie ist

Steganographie Verstecken von Information, z.B. in Bildern oder Audiofiles. Siehe Link⁷

Sie verstehen was Private-Key-Kryptographie ist, welche Arten von Sicherheit es gibt und welche Angriffsarten auf Verschlüsselung existieren

Zeichencodierung Kodierung (*Encoding*) heisst, einen Wert mit Symbolen eines Zeichensatzes darzustellen. Beispiel:

Dezimalsystem	100
Binärsystem	1100100
Hexadezimalsystem ('hex')	64
ASCII	hello
Base64	aGVsbG8=

Achtung: Kodierung ≠ Verschlüsselung

Symmetrische Verschlüsselung Bei symmetrischen Verschlüsselungsverfahren gibt es im Gegensatz zu den asymmetrischen Verfahren, **nur einen einzigen Schlüssel**. Dieser Schlüssel ist für die Verschlüsselung, als auch für die Entschlüsselung zuständig.

Secret Key Verschlüsselung Secret Key ('Symmetrische') Verschlüsselung wird zwischen zwei Parteien verwendet, welche einen **gemeinsamen Schlüssel** besitzen. Ausserdem wird sie oft verwendet, wenn der gleiche Benutzer ein Dokument verschlüsseln und zu einem späteren Zeitpunkt wieder entschlüsseln muss.

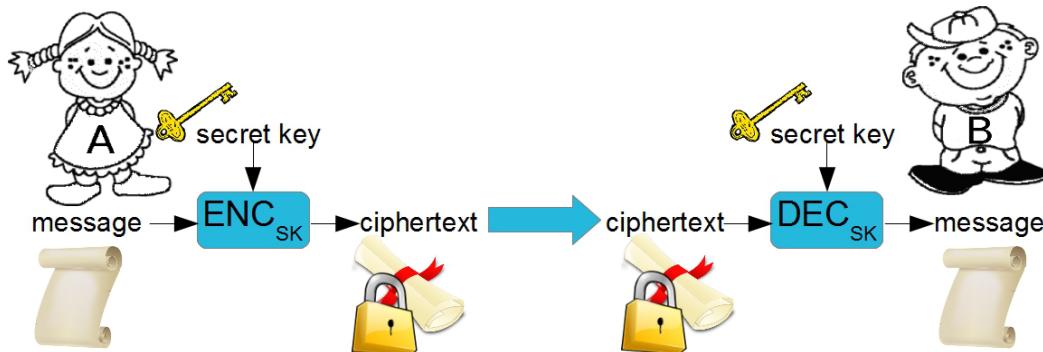


Abbildung 3: Alice verschlüsselt, Bob entschlüsselt mit dem gemeinsamen Schlüssel

Informationstheoretische Sicherheit Das Ziel informationstheoretischer Sicherheit ist der Schutz von Daten vor unbefugtem Zugriff während der Übertragung. Im Unterschied zur Kryptographie basiert informationstheoretische Sicherheit nicht auf der Annahme, dass die Rechenleistung eines unberechtigten Empfängers nicht gross genug ist, um die Daten zu decodieren. Vielmehr garantiert informationstheoretische Sicherheit, dass ein unberechtigter Empfänger selbst bei beliebig grosser Rechenleistung nicht in der Lage ist, solcherart geschützte Nachrichten zu decodieren. Mit anderen Worten erhält ein Angreifer durch den Geheimtext keinerlei (zusätzliche) Information über den Klartext[2]. Beispielsweise ist OTP⁸ informationstheoretisch sicher. Formal: $P(M = m) = P(M = m | C = c)$

Berechenmässige Sicherheit Der sicheren Übertragung und Aufbewahrung vertraulicher Daten kommt in unserer von Information dominierten Gesellschaft immer grössere Bedeutung zu. Die heute gebräuchlichen Verfahren zur Datenverschlüsselung bieten allerdings nur beschränkte, sogenannt berechenmässige Sicherheit.

⁷<https://www.petitcolas.net/steganography/index.html>

⁸Siehe One-time pad, Seite 11

Das bedeutet, dass diese prinzipiell von einem Angreifer, der über genügend Rechenleistung (zum Beispiel einen, heute noch hypothetischen, Quantencomputer) verfügt, gebrochen werden können[2].

Kerckhoff's Prinzip Der Angreifer kennt den Algorithmus und alle Details des Systems. Nur der Schlüssel ist geheim.

Angriffsarten Bei der Sicherheit von modernen Verschlüsselungssystemen wird zwischen den Angriffsmöglichkeiten des Angreifers unterschieden:

- **Ciphertext only attack:** Angreifer erhält nur den zu entschlüsselnden Geheimtext

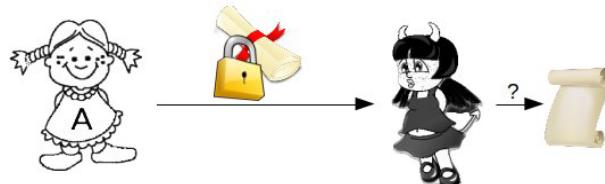


Abbildung 4: Nur Geheimtext

- **Known plaintext attack:** Angreifer erhält zusätzlich andere Klartext-Geheimtext-Paare

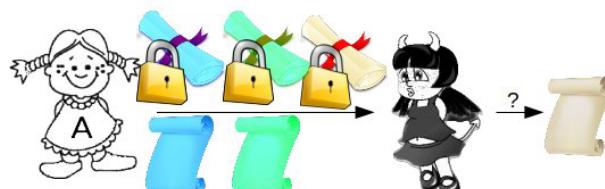


Abbildung 5: Klartext-Geheimtext-Paare

- **Chosen plaintext attack:** Angreifer kann zusätzliche Klartexte wählen, zu denen er auch die Geheimtexte erhält

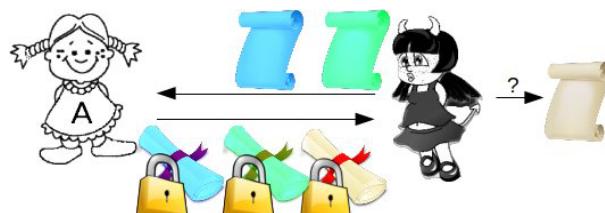


Abbildung 6: Klartexte und Geheimtexte

Sie können „klassische“ symmetrische Verschlüsselungverfahren wie Caesar cipher, Vigenère cipher, one-time pad anwenden und verstehen die Vor- und Nachteile bzw. Schwachstellen dieser Verfahren

Caesar cipher Caesar-Verschlüsselung ist ein einfaches symmetrisches Verschlüsselungsverfahren, das auf der monographischen und monoalphabetischen Substitution basiert.

Vorteil: es ist **einfach**.

Nachteil: es ist **unsicher**, da es sehr schnell geknackt werden kann.

Schwachstelle: Die in der natürlichen Sprache ungleiche Verteilung der Buchstaben wird durch diese Art der Verschlüsselung nicht verborgen, so dass eine Häufigkeitsanalyse (Frequenzanalyse) das Wirken einer einfachen monoalphabetischen Substitution enthüllt.

Caesar cipher: Vorgang

- Verschiebt jeden Buchstaben des Alphabets um eine bestimmte Anzahl Stellen
- Soll bereits von Julius Caesar verwendet worden sein, daher der Name
- Der Schlüssel wird entweder als Anzahl Stellen, um die verschoben wird, oder als Buchstaben, auf den 'A' verschoben wird angegeben
- Variante: ROT13 (Verschlüsselung = Entschlüsselung)
- Problem 1: Schlüssellänge (nur 26 verschiedene Schlüssel)
- Problem 2: Frequenzanalyse

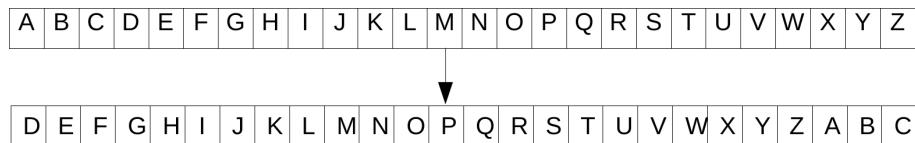


Abbildung 7: Caesar cipher mit Verschiebung um 3 Stellen

Das folgende Diagramm zeigt die Häufigkeitsverteilung der Buchstaben in einem längeren Text in deutscher Sprache:

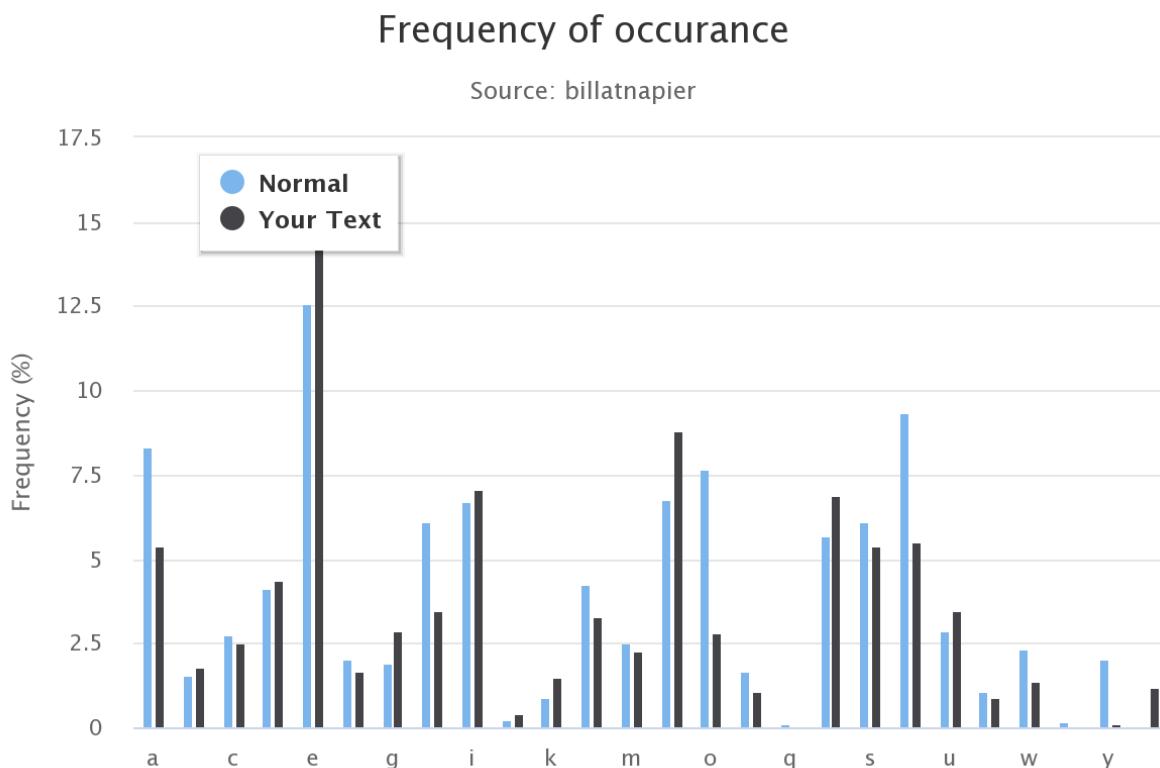


Abbildung 8: Frequenzanalyse unchiffriert

Wie zu erwarten, ist der häufigste Buchstabe E, gefolgt von N und I, wie es im Deutschen üblicherweise der Fall ist. Wird der Text mit dem Schlüssel 10 (oder anders gesagt, mit dem Schlüsselbuchstaben J) chiffriert, erhält man einen Geheimtext, der folgende Häufigkeitsverteilung besitzt:

Frequency of occurrence

Source: billatnapier

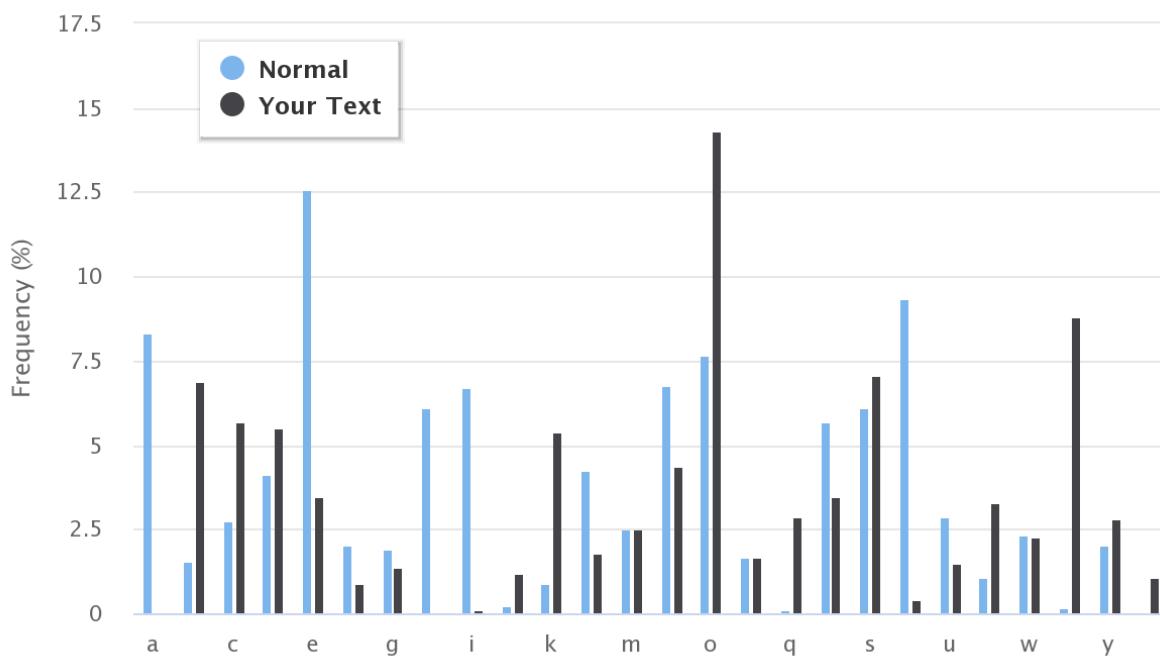


Abbildung 9: Frequenz um 10 Stellen verschoben

Der häufigste Buchstabe ist hier O, gefolgt von X und S. Man erkennt auf den ersten Blick die Verschiebung des deutschen „Häufigkeitsgebirges“ um zehn Stellen nach hinten und besitzt damit den Schlüssel. Voraussetzung ist lediglich, dass man die Verteilung der Zeichen des Urtextes vorhersagen kann.

Besitzt man diese Information nicht oder möchte man auf die Häufigkeitsanalyse verzichten, kann man auch die Tatsache ausnutzen, dass bei der Cäsar-Chiffre nur eine sehr kleine Anzahl möglicher Schlüssel in Frage kommt. Da die Grösse des Schlüsselraums nur 25 beträgt, was einer „Schlüssellänge“ von nicht einmal 5 bit entspricht, liegt nach Ausprobieren spätestens nach dem 25. Versuch der Klartext vor.

Vigenère cipher

- Schlüssel: Wort der Länge L
- Jeder Buchstabe im Text wird mit der Caesar cipher des entsprechenden Schlüsselwortes verschlüsselt
- Anzahl mögliche Schlüssel: 26^L
- Problem: Frequenzanalyse jeder L 'ten Stelle

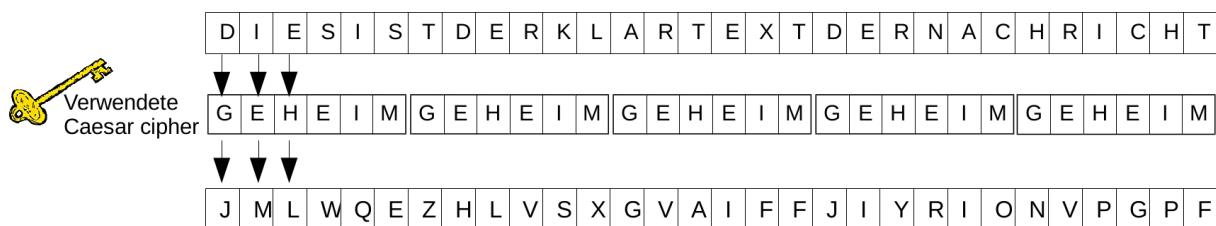


Abbildung 10: Vigenère cipher

One-time pad

- Jede Stelle wird mit einem anderen Schlüssel verschlüsselt
- Darf nur 1 Mal verwendet werden!
- Anzahl möglicher Schlüssel = Anzahl möglicher Nachrichten
- Ist sicher, d.h. Geheimtext verrät keinerlei (zusätzliche) Information über den Klartext
- Intuitiv: Für einen bestimmten Geheimtext sind alle Klartexte (dieser Länge) möglich

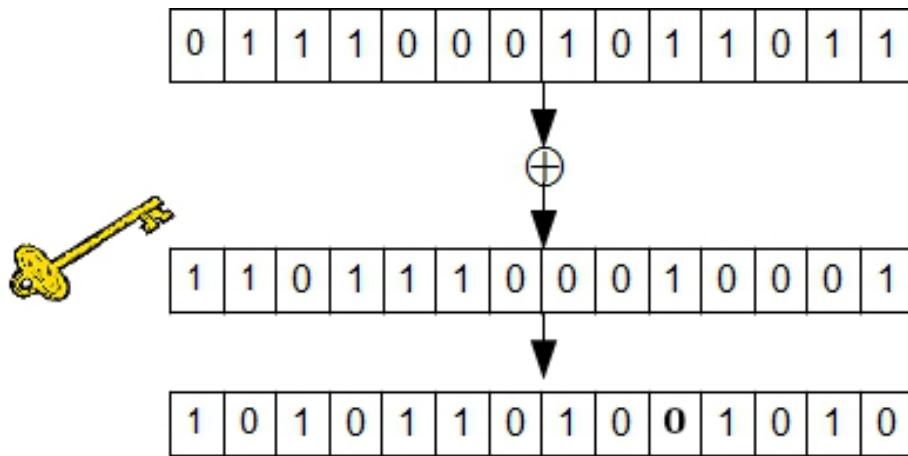


Abbildung 11: Funktionsweise des OTP

Sie wissen welche modernen Verschlüsselungsalgorithmen in der Praxis verwendet werden und was deren Eigenschaften sind

Secret Key Verschlüsselung: Algorithmen Beispiele für symmetrische Verschlüsselung

Name	Blocklänge	Schlüssellänge	Jahr	Kommentar
DES	64 Bit	56 Bit	1970	gebrochen
Triple DES	64 Bit	112 Bit (3 × 56 Bit)		nicht mehr empfohlen
RC4	stream cipher	8-2040	1987	gebrochen
IDEA	64 Bit	128 Bit	1990	nicht mehr empfohlen
RC5	64 oder 128 Bit	4-256 Bit	1994	nicht mehr empfohlen
Camellia	128 Bit	128, 192 oder 256 Bit	2000	
Twofish	128 Bit	128, 192 oder 256 Bit	1998	
AES (Rijndal)	128 Bit	128, 192 oder 256 Bit	2000	

Sie verstehen was eine Hashfunktion ist und welche Eigenschaften eine kryptographische Hashfunktion ausmachen, bzw. was es heisst, wenn eine Hashfunktion gebrochen ist

Hashfunktion Eine Hashfunktion ist eine Abbildung, die eine grosse Eingabemenge (die Schlüssel) auf eine kleinere Zielmenge (die Hashwerte) abbildet. Die Eingabemenge kann Elemente unterschiedlicher Längen enthalten, die Elemente der Zielmenge haben dagegen meist eine feste Länge.

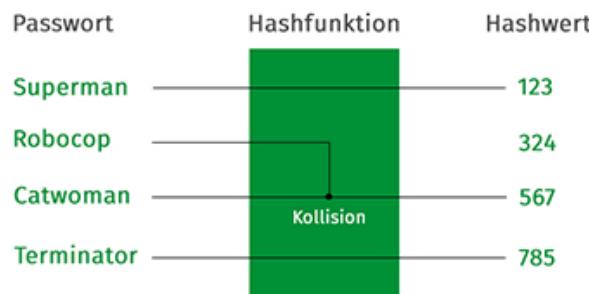


Abbildung 12: Einfaches Beispiel einer Hashfunktion

Auf der linken Seite sehen wir 4 Passwörter von beispielsweise 4 Mitarbeitern eines Unternehmens. Die Hashfunktion wandelt nun diese Passwörter in eine Zeichenfolge (dem Hashwert) mit einer festen Länge (hier 3 Zeichen) um. Für das Passwort „Superman“ bekommt man den Hashwert 123, dem Passwort „Robocop“ wird der Hashwert 567 zugeordnet, genauso wie dem Passwort „Catwoman“ und „Terminator“ bekommt 785. Hashfunktionen reduzieren zunächst nur Zeichen beliebiger Länge (unterschiedliche Passwörter) auf Zeichen fester Länge (im Beispiel 3 Zeichen). Sie werden also in eine kleine, kompakte Form gebracht.

Zusatzinfo zum Hashwert Der Hashwert ist das Ergebnis, das mittels einer Hashfunktion berechnet wurde. Man definiert eine feste Länge, wie lang ein Hashwert immer sein darf. Oft wird der Hashwert als eine hexadezimale Zeichenkette codiert, d.h. der Hashwert besteht aus einer Kombination von Zahlen und Buchstaben zwischen 0 und 9 sowie A bis F (als Ersatz für die Zahlen 10 bis 15). Ein Hashwert aus 10 hexadezimalen Zeichen könnte so aussehen: „3d180ab86e“.

Eigenschaft einer Hashfunktion

- Einwegfunktion: Aus dem Hashwert darf nicht der originale Inhalt erzeugt werden können. In unserem Beispiel darf es nicht möglich sein, aus dem Hashwert „123“ den Ursprungstext „Superman“ zu erzeugen.
- Kollisionssicherheit: Den unterschiedlichen Texten darf nicht derselbe Hashwert zugeordnet sein. Ist diese Voraussetzung erfüllt, so spricht man auch von **kryptographischen Hashfunktionen**. In unserem Beispiel (Abbildung 12) liegt eine Kollision vor, da die Passwörter „Robocop“ und „Catwoman“ denselben Hashwert haben. Damit ist die Hashfunktion im Bild nicht kollisionssicher und es handelt sich nicht um eine kryptografische Hashfunktion.
- Schnelligkeit: Das Verfahren zu Berechnung des Hashwertes muss schnell sein.

Algorithmen für Passwortspeicherung Um Passwörter zu speichern werden sog. **Password Based Key Derivation Functions (PBKDF)** verwendet, d.h. **kryptographische Hashfunktionen** welche zusätzlich resourcen-intensiv (langsam) zu berechnen sind.

- basieren auf einer herkömmlichen Hashfunktion, welche mehrmals verknüpft ausgeführt wird
- die Geschwindigkeit wird durch einen Parameter bestimmt, welcher die Anzahl Runden angibt
- damit werden Angriffe mittels speziell für die Berechnung von Hashfunktionen optimierte Hard- und Software erschwert

Beispiele sind PBKDF2 und bcrypt (Blowfish-Algorithmus), welche zusätzlich viel Memory benötigen, oder scrypt (Entwicklung motiviert durch Verwundbarkeit von PBKDF2 und bcrypt durch Brute-Force-Angriffen) und Argon2.

Sie kennen moderne Hashfunktionen und wissen welche Eigenschaften diese haben

Hashfunktionen Algorithmen

Name	Block Länge	Output Länge	Bemerkung
MD5	512	128	gebrochen
SHA-1	512	160	gebrochen
SHA-256	512	256	
SHA-384	1024	384	
SHA-512	1024	512	
SHA3-256	1088	256	
SHA3-384	832	384	
SHA3-512	576	512	

Gebrochene Hashfunktionen „Gebrochen“ = „geknackt“. Dies war z.B. bei LinkedIn und Dropbox der Fall. Wie können aber Passwörter geknackt werden, wenn man wegen der Einweg-Eigenschaften der Hashfunktionen nicht auf den ursprünglichen Text zurückschliessen kann? Zunächst muss man wissen, dass fast alle Algorithmen „offen“ liegen, diese also auch von Angreifern genutzt werden können. Das hat zur Folge, dass der Hashwert von einem Passwort immer gleich ist, egal ob es die Plattform oder der Angreifer berechnet. Passwort „Superman“ = MD5-Hash: „527d60cd4715db174ad56cda34ab2dce“. Ein Angreifer kann sich also eine Liste mit typischen unsicheren Passwörtern erstellen und es durch den Hashgenerator jagen. Wenn er nun die Datenbank mit den Hashwerten der Plattform stiehlt, kann er die Hashwerte mit seiner Liste vergleichen. Findet er in der geklauten Liste den Hashwert „527d60cd4715db174ad56cda34ab2dce“, so weiss er, dass dieser Hashwert dem Passwort „Superman“ zugeordnet ist. Solche Listen nennt man **rainbow tables**.

Sie kennen Anwendungen von Hashfunktionen

Verwendung von Hashfunktionen

- Identifikation einer Datei in peer-to-peer Netzwerken
- Fehlererkennung
- Integritätsprüfung
 - Symmetric Key Solution: Message Authentication Code (MAC) durch einen ‘keyed hash’
 - Asymmetric Key Solution: Digital Signature durch Signatur des Hashwertes
- „Proof of work“ in Blockchain

Sie wissen was ein keyed Hash (HMAC) ist und wofür dieser verwendet werden kann

HMAC Ein Keyed-Hash Message Authentication Code (HMAC) ist ein Message Authentication Code (MAC), dessen Konstruktion auf einer kryptografischen Hash-Funktion, wie z.B. MD5 und einem geheimen Schlüssel basiert. Der Hashwert wird aus dem Message-Body und einem angehängtem Key erstellt. Es ist eine **symmetrische** Kryptographie, d.h. beide Parteien müssen den Key besitzen.

- Authentifizieren einer Nachricht
- Sicherstellen des Ursprungs einer Nachricht (**Authentizität**)
- Sicherstellen der **Integrität** einer Nachricht
- Im Gegensatz zu einem normalen Hash (z.B. MD5) ist ein HMAC zusätzlich „keyed“, also abhängig von einem Schlüssel
- HMAC wird z.B. im Rahmen von IPSEC verwendet
 - IPSEC ist ein Protokoll, welches mehrere Elemente vereint
(Schlüsselaustausch, symmetrische Verschlüsselung, Authentifizierung von Nachrichten, etc.)
 - der Schlüsselaustausch von HMAC erfolgt im Rahmen von IPSEC (IKE⁹) via Diffie-Hellman

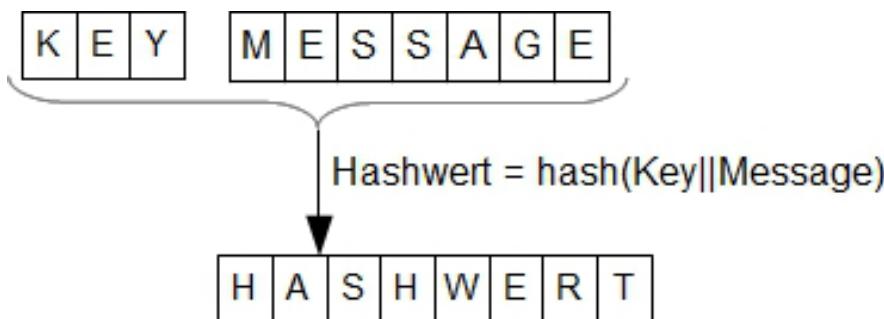


Abbildung 13: Funktionsweise eines Keyed-Hash Message Authentication Codes

Sie kennen die „Best-practices“ zu Passwortsicherheit und wissen, gegen welche Angriffe diese schützen

Passwortsicherheit Best practices

- Gespeichert wird nur der **Hashwert** des Passwortes
 - Ziel: Admin oder Angreifer mit Zugang zur DB erhalten das Passwort nicht
- Oder noch besser:
- Das Passwort wird gemeinsam mit einem **Salt** gehasht. Dieser neue Hash wird in der DB abgelegt. Der Salt muss nicht geheim, aber einzigartig (*unique*) sein.
 - Ziel: Aufgrund der einzigartigen DB-Einträge ist nicht erkennbar, ob zwei Benutzer dasselbe Passwort haben. Zusätzlich kann ein Angreifer nicht die häufigsten Passwörter hashen und danach vergleichen, welcher Benutzer in der DB dieses Passwort verwendet hat. Er muss jeden Eintrag einzeln angreifen.
 - Als Hashfunktion wird eine langsame und resourcen-intensive Hashfunktion verwendet, z.B. scrypt.
 - Ziel: Verlangsamen einer Offline-Attacke auf die Passwort-Hashes.

⁹Internet Key Exchange

3 Asymmetrische Kryptographie

Asymmetrische Verschlüsselung In der asymmetrischen Kryptographie (Verschlüsselung) arbeitet man nicht mit einem einzigen Schlüssel, sondern mit einem **Schlüsselpaar**. Bestehend aus einem **öffentlichen** und einem **privaten Schlüssel**. Man bezeichnet diese Verfahren als asymmetrische Verfahren oder Public-Key-Verfahren.

Sie verstehen was Public-Key-Kryptographie ist, worauf deren Sicherheit basiert und wie sie zur Verschlüsselung, für Signaturen und zur Authentisierung verwendet werden kann

Public Key Verschlüsselung Basiert auf Funktionen, welche einfach zu berechnen sind, deren Umkehrfunktion aber (vermutlich) schwierig zu berechnen ist. Beispiel:

Multiplikation (einfach):	$97 \times 84 = 8051$
Faktorisieren (schwierig):	$8051 = ?$

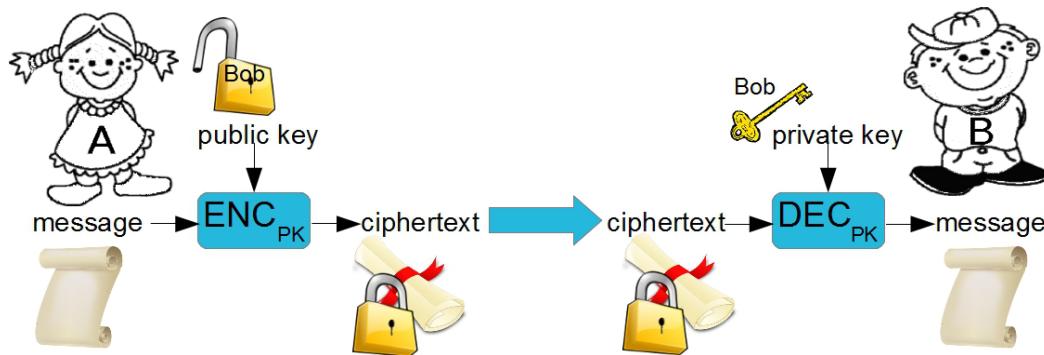


Abbildung 14: Alice verschlüsselt mittels Bob's Public Key asymmetrisch

Sie kennen die gängigen asymmetrischen Verschlüsselungs- und Signaturalgorithmen und wissen, worauf deren Sicherheit basiert

Name	Unterliegende 'schwierige' Funktion
RSA	Faktorisieren grosser Zahlen
Diffie-Hellman	Diskrete Logarithmen berechnen
Elliptic Curve DH (ECDH)	Diskrete Logarithmen berechnen
ElGamal Verschlüsselung	Diskrete Logarithmen berechnen

Sie wissen wie Diffie-Hellman-Schlüsselaustausch bzw. ElGamal-Verschlüsselung funktioniert

Diffie-Hellman (DH) Schlüsselaustausch Diffie-Hellman ist ein Schlüsselvereinbarungsprotokoll. Der vereinbarte gemeinsame geheime Schlüssel kann danach zur Verschlüsselung der Nachricht verwendet werden. Diffie-Hellman nutzt eine diskrete Exponentialfunktion (modulare Exponentiation) $b^x \bmod m$. Der Vorteil einer solchen Funktion ist, dass man schnell ein Ergebnis (Secret Key) ausrechnen kann, während die Umkehrfunktion, der diskrete Logarithmus, um den Exponenten (Private Key) zu erhalten, nur sehr schwer auszurechnen ist.

$$5 \equiv 4^2 \equiv 4^7 \equiv 4^{12} \equiv 4^{17} \pmod{11} \dots$$

Rest 5 ist schnell ausgerechnet, aber es ist praktisch nicht möglich herauszufinden, ob der Exponent nun 317, 27·142 oder doch 1·492·967 ist. Weiter wird nicht der Secret Key selber versendet, sondern vor Ort berechnet.

Sicherer Schlüsselaustausch mittels DH¹⁰

- Alice wählt eine zufällige Primzahl p und zufällige Basis $g \in [1, p - 1]$
 p und g werden nicht geheim gehalten
- Alice wählt zufällige Zahl für Private Key $a \in [0, p - 2]$
- Berechnet ihren Public Key $A = g^a \bmod p$
Alice hält a geheim und schickt (A, g, p) an → Bob
- Bob wählt zufällige Zahl für Private Key $b \in [0, p - 2]$
- Berechnet $B = g^b \bmod p$
Bob hält b geheim und schickt B an → Alice
- Alice berechnet $B^a \bmod p = g^{b \cdot a} \bmod p$
- Bob berechnet $A^b \bmod p = g^{a \cdot b} \bmod p$
- Gemeinsamer Secret Key $K = g^{a \cdot b} \bmod p$ ist nur Alice und Bob bekannt, ohne das Alice b kennt und Bob a

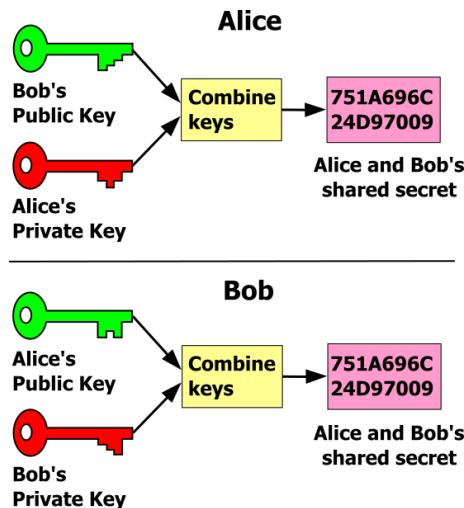


Abbildung 15: Identischer Geheimschlüssel wird erzeugt[1]

Beispiel für $p = 17$ und $g = 3$

- Alice wählt $a = 7$ und berechnet $A = g^a \bmod 17 = 2187 \bmod 17 \equiv 11$
- Bob wählt $b = 4$ und berechnet $B = g^b \bmod 17 = 81 \bmod 17 \equiv 13$
- Der gemeinsame Schlüssel ist $K = A^b \bmod 17 = 14641 \bmod 17 \equiv 4$

ElGamal-Verschlüsselung ElGamal verwendet DH um einen asymmetrischen Verschlüsselungsalgorithmus zu erstellen. Daher ist es sicherer als RSA, welches ‘nur’ Faktorisieren grosser Zahlen als unterliegende Funktion hat. Im Vergleich zu DH gibt es bei ElGamal weitere Teilschritte und feine Unterschiede. Die zu verschlüsselnde Nachricht x wird nämlich in den Secret Key verschmelzt.

- Diffie-Hellman: $K = g^{a \cdot b} \bmod p$
- ElGamal: $C = x \cdot g^{a \cdot b} \bmod p$

ElGamal-Verfahren im Detail

Schlüsselerzeugung

- Alice wählt eine grosse Primzahl p und ein Gruppenelement g der Ordnung p ($0 < g < p$)
- Wählt für den Private Key eine zufällige Zahl $a \in [0, p - 2]$
- Berechnet ihren Public Key $A = g^a \bmod p$

Alice hält a geheim und schickt (A, g, p) an → Bob

Bis hierhin verlief das Ganze ziemlich ähnlich zum DH-Schlüsselaustausch.

¹⁰<https://www.cs.uni-potsdam.de/ti/lehre/07-Kryptographie/slides/slides-5.1-anim.pdf>

Verschlüsselung

- Bob hat die zu verschlüsselnde Nachricht x
- Wählt für den *Private Key* eine zufällige Zahl $b \in [0, p - 2]$
- Berechnet seinen *Public Key* $B = g^b \bmod p$
- Erstellt *Secret Key* $K = A^b \bmod p$
- Bob verschlüsselt x zu $C = x \cdot K \bmod p$
Bob hält b geheim und schickt (B, C) an → Alice

Entschlüsselung

- Alice entschlüsselt Ciphertext C mit $x = (B^{p-a-1} \bmod p) \cdot C \bmod p$

Sie wissen was kryptographisch sichere Zufallszahlen sind und wo diese verwendet werden

Sichere Zufallszahlen Kryptographisch sichere Zufallszahlen können im Gegensatz zu Zahlen in einer gewöhnlichen Random-Funktion anhand des Seeds nicht vorausgesagt werden. Java bietet beispielsweise neben der Random-Klasse die SecureRandom-Klasse¹¹. Kryptographisch sichere Zufallszahlen braucht man z.B. in den oben beschriebenen Schlüsselaustauschprotokollen.

Normaler Zufallszahlengenerator

- Zahlen sollen uniform (gleichmäßig verteilt sein)
- Wenn möglich: hohe Rate

Beispiel: `java.util.Random.nextInt()`

$$RN1 = InitialSeed$$

$$RN2 = (A \cdot RN1 + C) \bmod M$$

$$RN3 = (A \cdot RN2 + C) \bmod M$$

Kryptographisch sicherer Zufallszahlengenerator

- Zusätzlich: Zufallszahlen sollen nicht vorhersagbar sein

Beispiel: `java.security.SecureRandom.nextInt()`

Vorsicht Mit 2 Zahlen können alle weiteren vorhergesagt werden!

Sie wissen was eine elektronische Signatur ausmacht

Signatur Die elektronische Signatur ist ein technisches Verfahren zur Überprüfung der Echtheit eines Dokuments, einer elektronischen Nachricht oder anderer elektronischer Daten sowie der Identität des Unterzeichnenden. Sie basiert auf einer Zertifizierungsinfrastruktur, die von vertrauenswürdigen Dritten verwaltet wird: den Anbieterinnen von Zertifizierungsdiensten. Die elektronische Signatur und die handschriftliche Unterschrift werden zudem mit dem neuen Gesetz unter bestimmten Bedingungen als gleichwertig betrachtet.

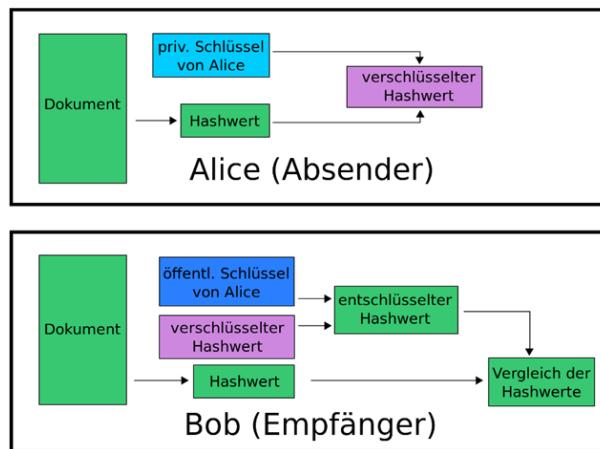


Abbildung 16: Signatur im Detail

¹¹Siehe `Random` und `SecureRandom`

Beispiel Max Meier erhält von seinem Kunden den Geschäftsvertrag – digital als PDF, wie es heutzutage üblich ist. Vergleichsweise altmodisch geht es aber nachher weiter: Meier druckt das Dokument aus und unterzeichnet es handschriftlich. Den unterschriebenen Vertrag steckt er schliesslich in einen Umschlag und wirft diesen in den nächstgelegenen Briefkasten. Viele Schritte für eine Unterschrift. Was Max Meier nicht weiss: Dokumente lassen sich auch digital unterzeichnen. Jede digitale Signatur basiert auf der sogenannten asymmetrischen Verschlüsselung. Sie wird auch als Public-Key-Verfahren bezeichnet und nutzt einen öffentlichen und einen privaten (geheimen) Schlüssel. Mit dem privaten Schlüssel wird die digitale Signatur erzeugt, während mit dem öffentlichen Schlüssel die Authentizität der Unterschrift überprüft wird.

Eigenschaft einer Signatur

1. **Fälschungssicherheit:** Nach dem Unterschreiben kann das Dokument nicht mehr (unerkannt) verändert werden.
2. **Authentizität:** Die Unterschrift kann zweifelsfrei (überprüfbar) einer bestimmten Person zugeordnet werden.
3. **Unleugbarkeit:** Der Unterzeichner kann später nicht abstreiten, das Dokument unterschrieben zu haben.
4. **Willenserklärend:** Die Unterschrift kann nur willentlich (bewusst) unter das Dokument gesetzt worden sein.

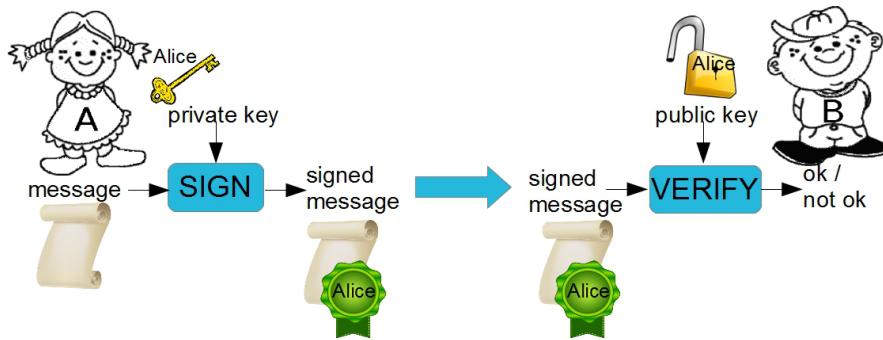


Abbildung 17: Alice verschickt eine signierte Nachricht an Bob

Sie wissen wie hybride Verschlüsselung bzw. hybride Signaturen funktionieren

Hybridverschlüsselung Eine Hybridverschlüsselung ist eine Kombination von symmetrischer und asymmetrischer Verschlüsselung. Dabei werden die Vorteile beider Verschlüsselungsverfahren genutzt. Symmetrische Verschlüsselung ist deutlich schneller, asymmetrische haben den Vorteil eines deutlich einfacheren Schlüsselaustausches. Der Ablauf ist folgendermassen:

- Sender Alice wählt einen zufälligen symmetrischen Schlüssel, einen Session-Key
- Der Session-Key verschlüsselt die Daten/Nachricht symmetrisch
- Der Session-Key wird asymmetrisch mit Bob's Public-Key verschlüsselt
- Die verschlüsselten Sachen werden an Bob gesendet
- Bob entschlüsselt asymmetrisch den Session-Key mit seinem Private-Key
- Der Session-Key entschlüsselt nun die Nachricht symmetrisch

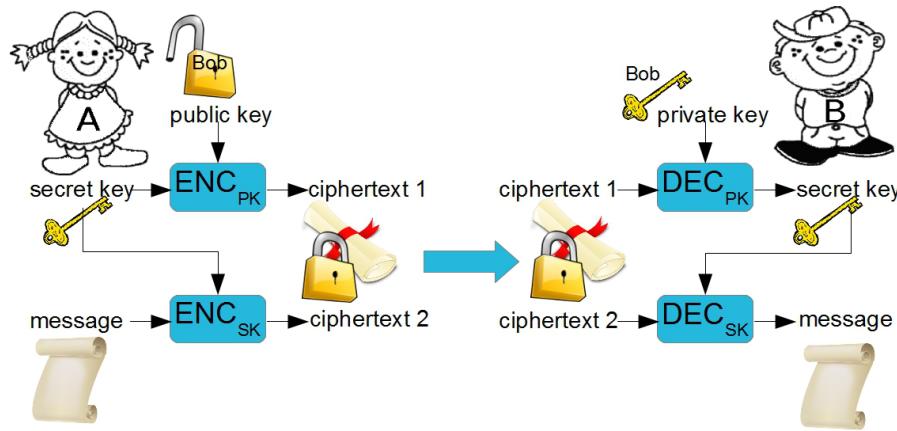


Abbildung 18: Hybridverschlüsselung einer Nachricht

Man erkennt schnell den Vorteil dieser Methode. Ein symmetrisches Verschlüsselungsverfahren ist sehr effizient auch im Verschlüsseln von grossen Datenmengen

Hybride Signatur Digitale Signaturen verwenden oft ähnliche oder sogar die gleichen Algorithmen wie Public Key Verschlüsselung. Das Signieren eines Dokuments entspricht dann einer Entschlüsselung mit dem Private Key, die Verifikation der Signatur entspricht der Verschlüsselung mit dem Public Key.

Name	Unterliegende 'schwierige' Funktion
RSA	Faktorisieren grosser Zahlen
Digital Signature Algorithm	Diskrete Logarithmen Berechnen
Elliptic DSA	Diskrete Logarithmen Berechnen
ElGamal Signature	Diskrete Logarithmen Berechnen

4 Zertifikate und SSL-TLS

Sie kennen die verschiedenen Arten von „Trust“

Problematik: Wie ordnet man ein Public Key einer bestimmten Person / Entität zu?

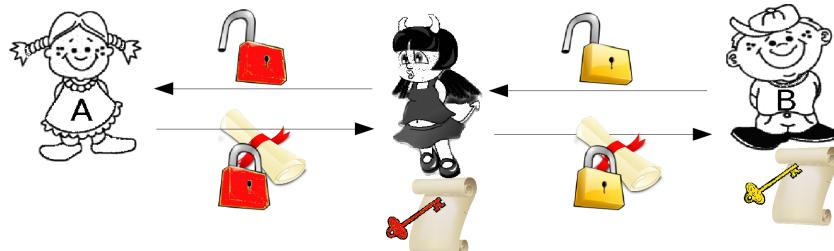


Abbildung 19: Eve als man in the middle

Direct Trust Alice vertraut der Authentizität von Bob's Public Key, durch direktes Überprüfen, normalerweise über den Fingerprint des Key's.

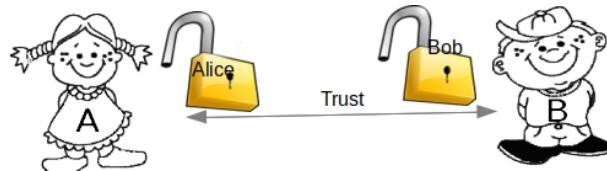


Abbildung 20: Alice vertraut Bob durch direkte Überprüfung

- Persönliche Überprüfung
 - Vorinstalliert in System oder Software (z.B. Public Key von Google-Server in Chrome, Apps, VPN-Clients)
 - Publiziert auf Webseite oder in Zeitung
- Benötigt jedoch einen authentischen Kanal zum Etablieren des Trust.

Web of Trust (WOT) Alice vertraut der Authentizität von Daves Public Key, weil dieser von Charlie signiert wurde, dessen Public Key wiederum von Bob signiert wurde, dem sie vertraut.

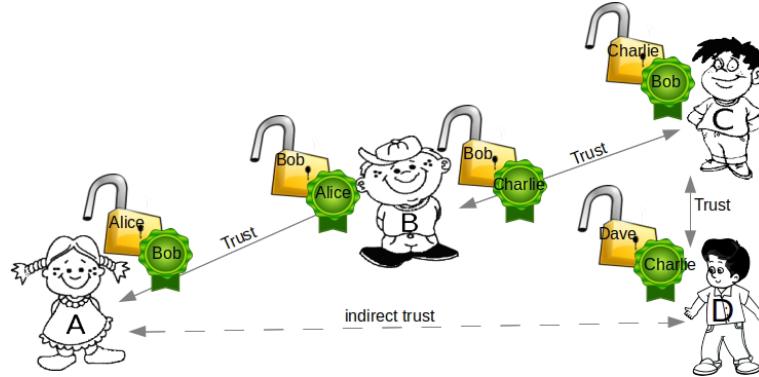


Abbildung 21: Alice vertraut Dave indirekt durch Vertrauensnetz

Hierarchial Trust (PKI) Eine *Public Key Infrastructure (PKI)* ist ein System, das digitale Zertifikate ausstellen, verteilen und Prüfen kann. Im Gegensatz zum WOT ist eine PKI hierarchisch aufgebaut und bedingt deshalb Root Certification Authorities, welche über alle anderen Zertifizierungstellen steht.

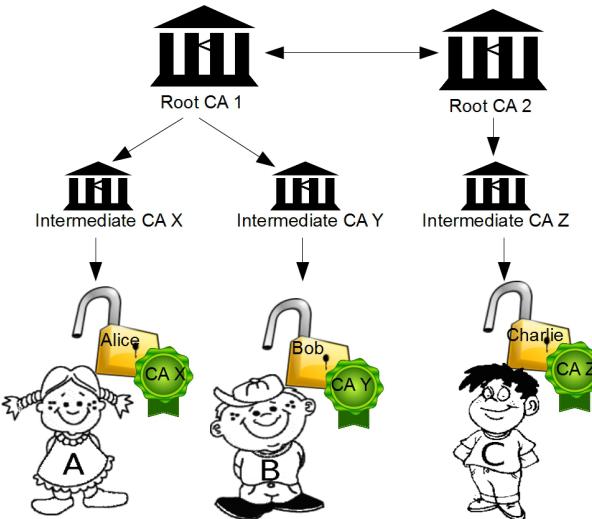


Abbildung 22: Hierarchical Trust durch Certificate Authorities

Sie wissen was eine Public-Key-Infrastruktur, eine Certificate Authority und ein Zertifikat ist, wofür und wie diese verwendet werden und wie Zertifikate ausgestellt und revoziert werden

Grundbegriffe PKI Die Zertifizierungstelle *Certificate Authority (CA)*

Eine CA ist eine Organisation, welche digital eZertifikate ausstellt. Ein digitales Zertifikat ordnet einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zu. Diese Zuordnung wird von der Zertifizierungstelle beglaubigt, indem sie sie mit ihrer eigenen digitalen Unterschrift versieht.

Ein Zertifikat wird durch eine sog. *Chain of Trust* beglaubigt. Eine *intermediate CA* signiert das Zertifikat (Public Key) des Endbenutzers. Das Zertifikat der intermediate CA wird wiederum von einer anderen CA unterschrieben. Das letzte Zertifikat in dieser Kette heisst *Root Certificate* und enthält den Public Key der *root CA*. Dieses Zertifikat ist normalerweise *self signed*, also von der root CA selbst unterschrieben.

Prüfung der Authentisierung mittels Zertifikat

- Ist das Zertifikat gültig? (Nicht abgelaufen, nicht revoziert)
- Ist das Zertifikat und die gesamte Zertifikatskette korrekt signiert?
- Traue ich der Root-CA der Zertifikatskette?
- Besitzt „Bob“ den zum Zertifikat gehörenden Private Key?
– $VERIFY_{public\ key\ Bob}(response)$

Sie wissen was SSL/TLS ist, welche Funktionalität es erreicht und wie das Protokoll konzeptionell abläuft

SSL-TLS erreicht

- Authentisierung des Servers gegenüber dem Client
- Optional: Authentisierung des Clients gegenüber dem Server ('mutual SSL')
- Verschlüsselung und Authentisierung der Daten

Das SSL/TLS-Protokoll läuft in zwei Phasen ab:

- **Handshake:** vereinbart mittels Public-Key-Kryptographie einen Schlüssel
- **Datenaustausch:** verwendet Secret-Key-Kryptographie zum Verschlüsseln und Authentisieren

Beispiele für SSL/TLS-ciphers:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

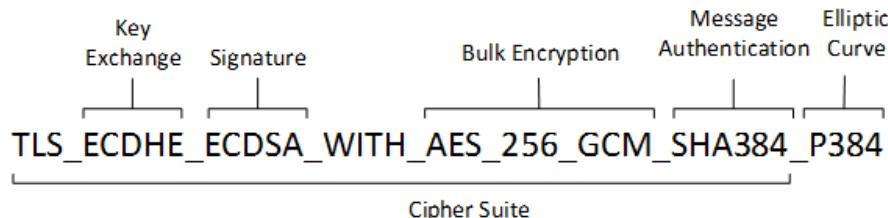


Abbildung 23: TLS Cipher im Detail

SSL im Detail

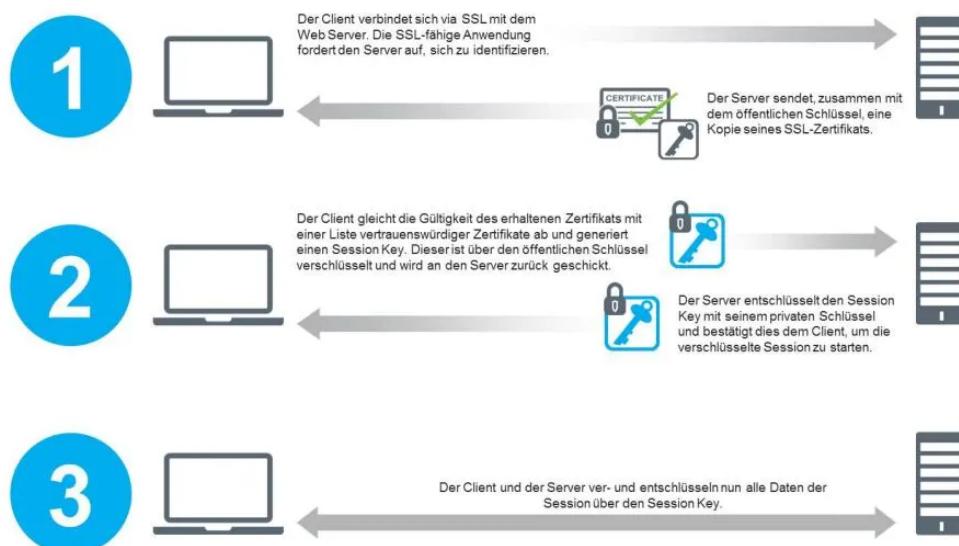


Abbildung 24: SSL / TLS

Teil III

Angriffe (SW 05-06)

5 Angriffe auf Webanwendungen

Bedrohungen auf Anwendungsebene Webanwendung, Session, Headers, CSRF

Sie wissen was eine Webanwendung ausmacht, wie HTTP funktioniert

Was unterscheidet eine Webanwendung aus Sicherheitssicht zu anderen Anwendungen?

- Kommuniziert über HTTP mit einem Server
 - zustandsloses Protokoll
- Läuft in einem Browser
 - Mehrere Webanwendungen können parallel im gleichen Browser laufen
 - Die Webanwendung erbt vom Browser implementierte Features bzw. muss diese richtig ansprechen

HTTP Der Browser kommuniziert mit dem Webserver über das **Hypertext Transfer Protokoll (HTTP)**. HTTP besteht aus *Requests* und *Responses*.

HTTP-Request-Methoden Die häufigsten HTTP-Request-Methoden sind **GET** und **POST**. Es existieren aber auch **PUT**, **HEAD**, **DELETE**, **PATCH**, **OPTIONS**.

GET `https://www.hslu.ch/?p=5` HTTP/1.1

User-Agent: Mozilla/5.0

- Message Body: kein
- Ruft Daten vom Server ab
- Sollte Serverzustand nicht verändern

POST `https://www.hslu.ch/` HTTP/1.1

User-Agent: Mozilla/5.0

- Message Body: `id=123&pwd=password`
- Darf Serverzustand verändern
- Wird nicht gecachet

Häufigste Response-Codes

- 200 OK
- 204 No Content
- 301 Moved Permanently
- 302 Found (Vorher: „Moved temporarily“)
- 304 Not Modified
- 400 Bad Request
- 403 Forbidden
- 404 Not Found
- 500 Internal Server Error

HTTP Zustand HTTP ist ein zustandsloses Protokoll, d.h. es hat kein ‘Gedächtnis’, bzw. Erinnerung.

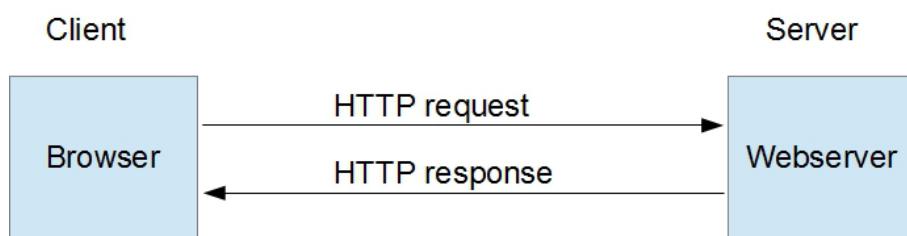


Abbildung 25: HTTP zustandslos

Die einzige Möglichkeit einen Zustand an den Client zu übergeben ist, diesen per weiteren Requests mitzuschicken. Die Zustände werden mit einem Cookie oder einem „Hidden field“ erfasst.

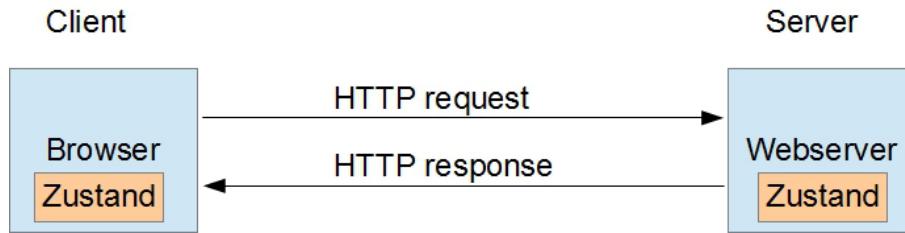


Abbildung 26: HTTP Zustand per Request (hidden field)

Cookies Cookies sind kurze Textdaten, welche vom Server als Header an den Browser übermittelt werden und von diesem ebenso als Header bei requests wieder mitgesendet werden. Cookies werden vom Browser verwaltet. Die meistgenutzte Möglichkeit ist es, ein Cookie zu setzen. Jedoch dürfen auch Cookies nicht client-seitig angepasst werden können!

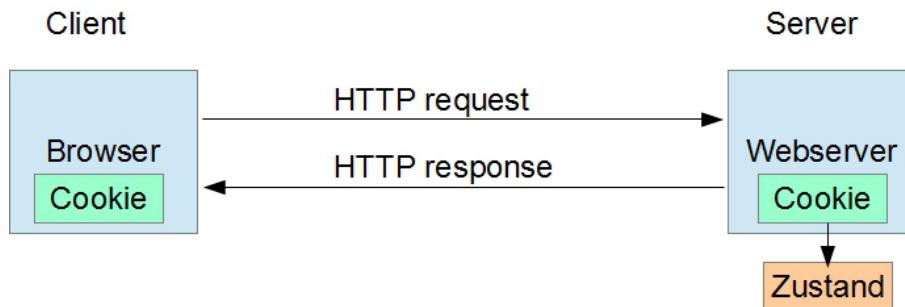


Abbildung 27: Einsatz eines Cookies

Cookie Eigenschaften Die Eigenschaften von Cookies sind:

- **Persistent** (mit Ablaufdatum) oder **Session-Cookie** (ohne Ablaufdatum)
- **Secure** (wird nur über HTTPS übertragen)
- **HTTP Only** (darf nur von HTTP gelesen werden)
- **Same Site** (wird nicht bei Cross-Domain-Aufrufen mitgesendet, z.B. ‘embedded’ Link, Image)

Sie wissen was eine Session ist und welche Eigenschaften einer Session bei welchen Angriffen wichtig sind bzw wie sie gegen gewisse Angriffe Schutz bieten

Session Eine Session ist der Zeitraum, in dem ein Client eine stehende Verbindung mit einem Server hat; vom Login bis zum Logout. Der Server vergibt dem Client eine eindeutige Session-ID. Die Sitzungsdaten (z.B. Warenkorb) werden im Server gespeichert. Bei jedem Request gibt der Client seine Session-ID mit, damit der Server beim Response die zugehörigen Daten dieser ID übermitteln kann. Es gibt auch Sessions ohne stehende Verbindung (ohne Login). Dies wird zu Statistikzwecken verwendet, z.B. um die Bewegung des Besuchers auf der Website zu verfolgen. Oder aber auch um einen Warenkorb ohne Login verwenden zu können.

Schwaches Session-Management Was ist das?

- der Sessionwert ist vorhersagbar
- der Sessionwert kann vom Client gesetzt werden
- die Cookie-Attribute ‘Secure’, ‘HttpOnly’ oder ‘Same Site’ sind nicht gesetzt
- Cookie-Domain oder -Pfad sind nicht so eingeschränkt wie möglich
- die Session wird bei einem Logout nicht invalidiert
- die Session hat kein server-seitiges Timeout (Inaktivitäts- und absolutes Timeout)

Schwaches Session-Management Was kann dagegen tun?

- lange und kryptographisch zufällige Sessionwerte wählen
- nur vom Server gewählte Sessionwerte akzeptieren
- Cookies als ‘Secure’, ‘HttpOnly’ oder ‘Same Site’ mit so eingeschränkter Domain und Pfad wie möglich setzen
- Session **server-seitig** bei einem Logout oder Timeout invalidieren

Same Origin Policy Mehrere Webanwendungen können im gleichen Browser parallel laufen. Die Same-Origin-Policy verhindert, dass eine parallel laufende Webanwendungen uneingeschränkt

- auf die Daten einer anderen Anwendung zugreifen
- die Cookies einer anderen Anwendung lesen oder mitschicken
- Requests auf die andere Anwendung absetzen

kann.

Same Origin Policies im Browser gibt es z.B. für Cookies, DOM access (Zugang zu document.cookie), HTML5Storage, XMLHttpRequests.

Same Origin Policy: Cookies Cookies haben eine **domain** und **path**.

- **Setzen des Cookies:** Nur Domain-Suffix des URL-Hostname dürfen gesetzt werden. (Aber keine Top-Level Domains!) Path kann beliebig gesetzt werden.
- **Senden des Cookies:** Cookies werden nur dann mitgeschickt, wenn die Cookie-Domain ein Domain-Suffix der URL-Domain und der Cookie-Path ein Prefix des URL-Path ist.

Session Fixation Was ist das?

Der Sessionwert wird nach einem Login oder Loginschritt nicht geändert. Ein Angreifer mit Zugang zu einer unauthentisierten Session kann warten bis ein Benutzer sich einloggt und ist damit selbst eingeloggt.

Session Fixation Was kann dagegen tun?

Sessionwert nach jedem Authentisierungsschritt ändern.

Sie kennen sicherheitsrelevante Header

Sicherheitsrelevante Response-Header

1. **HSTS: Strict-Transport-Security:** max-age=31536000; includeSubDomains
Seite wird nur via HTTPS aufgerufen. max-age muss hoch gesetzt werden!
2. **Frame-Options: X-Frame-Options: deny**
Verbietet das Einbinden der Seite in einem Frame oder erlaubt es nur für bestimmte Domains
3. **XSS-Protection: X-XSS-Protection: 1; mode=block**
Filtert und säubert oder blockiert die Anzeige der Seite, wenn ein XSS-Angriff entdeckt wird
4. **Content-Type-Options: X-Content-Type-Options: nosniff**
Verhindert, dass der Content als einen anderen MIME-Type interpretiert wird als angegeben
5. **CSP: Content-Security-Policy: script-src \textquotesingle self\textquotesingle**
Definiert, welche Ressourcen (z.B. Bilder, Scripts, Fonts, etc.) von wo eingebunden werden können
6. **CORS Access-Control-Allow-Origin: http://foo.example**
Cross-Origin Resource Sharing (CORS) ist ein Mechanismus, der Webbrowsers oder auch anderen Webclients Cross-Origin-Requests ermöglicht. Zugriffe dieser Art sind normalerweise durch die Same-Origin-Policy (SOP) untersagt. CORS ist ein Kompromiss zugunsten größerer Flexibilität im Internet unter Berücksichtigung möglichst hoher Sicherheitsmaßnahmen.
7. **Caching-Options Last-Modified: Mon, 08 Dec 2014 19:23:51 GMT; ETag: "5485fac7-ae74"; Cache-Control: (Nicht sicherheitsrelevant)** Ist ein Mechanismus, der den Umgang mit dem Inhalt von Seiten Browser um Proxy steuert. So können z.B. unnötige Request und erneute Downloads vermieden werden, ohne die Aktualität des Inhalts zu beeinträchtigen. Unter HTTP/1.0 mit dem Header **Pragma**
8. **HPKP (deprecated!): Public-Key-Pins:**
pin-sha256="d6qzRu9z0ECb90Uez27xWltNsj0e1Md7GkYYkVoZWmM=";
pin-sha256="E9CZ9INDbd+2eRQozYqqbQ2yXLVKB9+xcprMF+44U1g=";
report-uri=http://example.com/pkp-report;
max-age=10000; includeSubDomains
HTTP Public Key Pinning: Nur das Serverzertifikat mit dem korrekten Fingerprint wird akzeptiert. Wurde wieder abgekündigt und die meisten Browser unterstützen es nicht mehr.

Sie verstehen wie ein Cross-Site-Request-Forgery-Angriff abläuft und wie man sich dagegen schützen kann

CSRF - Cross-Site Request Forgery Was ist das?

Der Angreifer bringt einen Benutzer dazu, einen Request aus seinem Browser abzusetzen und dadurch eine Aktion auf dem Server auszulösen. Ist der Benutzer zu dem Zeitpunkt eingeloggt, wird das Cookie automatisch mitgeschickt.

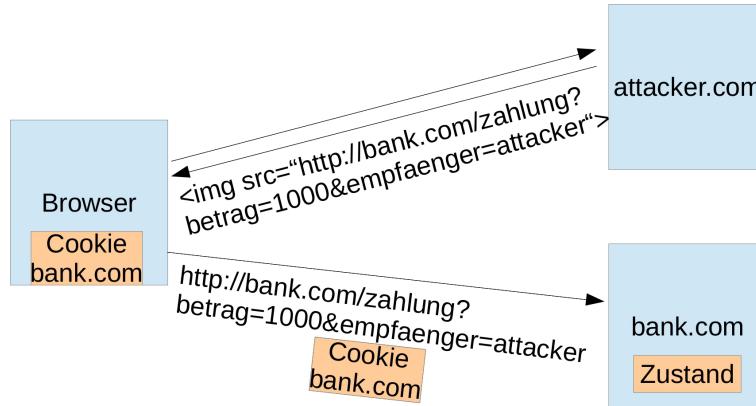


Abbildung 28: Cross-Site Request Forgery

CSRF - Cross-Site Request Forgery Was kann man dagegen tun?

- **CSRF-Token:** ein Secret als Teil des Form Field oder Header mitgeben (Secret darf nicht vorhersagbar sein)
- **Zusätzlich:** Same-Site-Attribut setzen

6 Angriffe auf Protokollebene

Sie kennen die Grundbegriffe der Anwendungssicherheit

Bedrohungen auf Protokollebene Begriffe: Social Engineering, Angriffe auf ARP, TCP/IP, DNS, SSL, HTTP

Kurzübersicht

- **Bedrohungen auf Link-Layer:** Spoofing
- **Bedrohungen auf Transport-Layer:** Denial of Service (DoS)
- **Bedrohungen auf SSL / TLS:** Preisgabe Sensitiver Daten
- **Bedrohungen auf Anwendungslayer:** Cross Site Scripting (XSS), Code Injection
- **Bedrohungen auf Layer 8 (Mensch):** Social Engineering

Flaws vs. Bugs Bei Softwaredefekten wird unterschieden zwischen Flaws und Bugs

- **Flaw:** Ein Flaw ist ein Defekt im Design der Software
- **Bug:** Ein Bug ist ein Defekt in der Implementation

Grundbegriffe: Bedrohung

- **Threat:** Möglicher Grund für einen ungewollten Vorfall, der das System oder die Organisation schädigen kann.
- **Threat Agent:** Individuum oder Gruppe welche eine Bedrohung darstellt.

Aktive vs. passive Angriffe

Bei einem **passiven Angriff** hält sich der Angreifer an das protokoll. Er verändert z.B. die ausgetauschten Nachrichten nicht hört aber die Kommunikation ab. Bei einem **aktiven Angriff** hält sich der Angreifer nicht an das Protokoll. Er verändert z.B. Nachrichten.

Sie kennen Beispiele von Angriffen auf verschiedenen Ebenen des Protokollstacks und wissen was diese bewirken

OSI-Layers

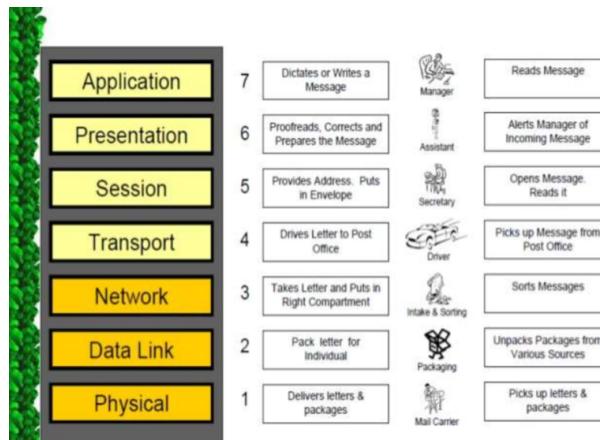


Abbildung 29: OSI-Layers

OSI vs Internet Reference Model

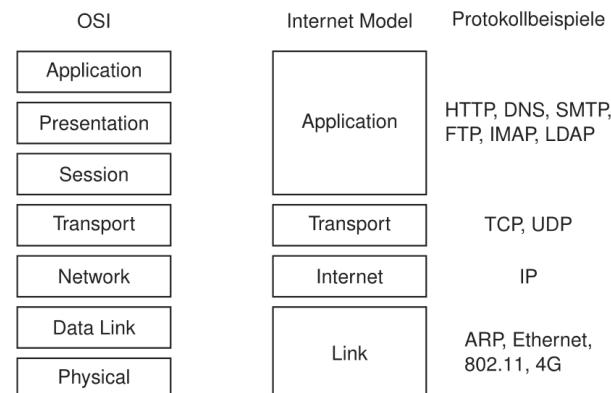


Abbildung 30: OSI vs. Internet Reference Model

Encapsulation (Datenkapselung)

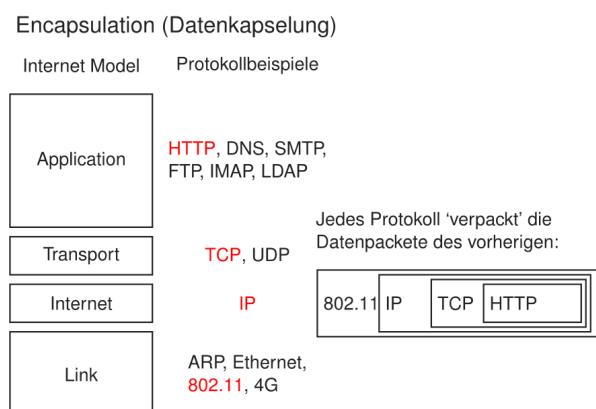


Abbildung 31: TCP-Encapsulation

Beispiel: ARP-Spoofing auf dem Link-Layer

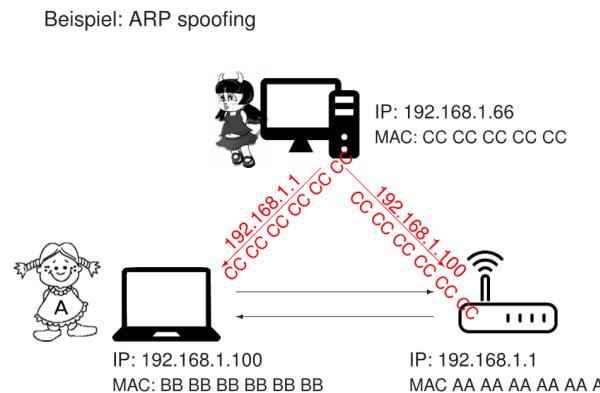


Abbildung 32: ARP Spoofing

Spoofing: Was ist das? Eine Person oder ein Programm gibt sich als jemand anderen oder etwas anderes aus.

Beispiele:

- Telefonnummern-Spoofing (Call Centers etc.)
- Email-Adressen-Spoofing
- IP Spoofing
- DNS Spoofing
- ARP Spoofing
- Content Spoofing

„ARP-Spoofing (vom engl. *to spoof* – dt. täuschen, reinlegen) oder auch ARP Request Poisoning (zu dt. etwa Anfrageverfälschung) bezeichnet das Senden von gefälschten ARP-Paketen. Es wird benutzt, um die ARP-Tabellen in einem Netzwerk so zu verändern, dass anschliessend der Datenverkehr zwischen zwei (oder mehr) Systemen in einem Computernetz abgehört oder manipuliert werden kann. Es ist eine Möglichkeit, einen Man-in-the-Middle-Angriff im lokalen Netz durchzuführen.“[1]

Spoofing: Was kann man dagegen tun?

Je nach Situation unterschiedlich, zB.:

- Authentisieren
- Angaben überprüfen

Repetition: TCP Verbindungsauftbau (vereinfacht)

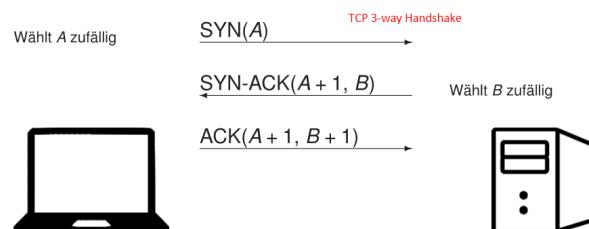


Abbildung 33: 3-Way Handshake

Bedrohungen auf Transport-Layer: Denial of Service (DoS)

Denial of Service Syn-Nachrichten werden mit gespoofter IP gesendet. Syn-Acknowledgements Nachrichten gehen nirgendwo hin. Server wird überflutet mit Abfragen und kann nicht schneller abarbeiten als Sie reinkommen. Als Resultat kann somit von den meisten Benutzern die Seite nicht angezeigt werden.

Beispiel: SYN Flood

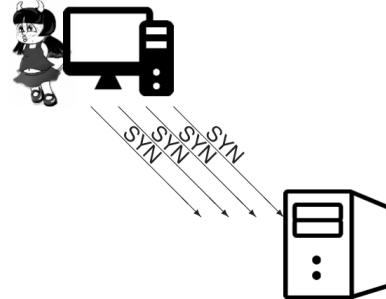


Abbildung 34: SYN Flood

Beispiel: Distributed Reflection Denial of Service „Hierbei adressiert der Angreifer seine Datenpakete nicht direkt an das Opfer, sondern an regulär arbeitende Internetdienste, trägt jedoch als Absenderadresse die des Opfers ein (IP-Spoofing). Die Antworten auf diese Anfragen stellen dann für das Opfer den eigentlichen DoS-Angriff dar. Durch diese Vorgehensweise ist der Ursprung des Angriffs für den Angegriffenen nicht mehr direkt ermittelbar.“ - Wikipedia

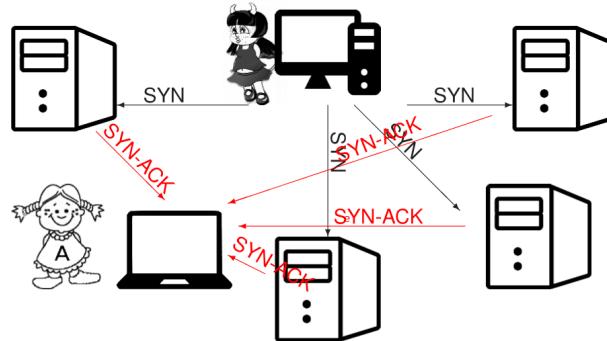


Abbildung 35: DRDoS

Denial of Service: Was kann man dagegen tun? Jedes System bricht irgendwann zusammen! Es geht darum sicherzustellen, dass dabei keine bleibenden Schäden am Kernsystem entstehen und das System nach einem Angriff schnell wieder funktionsfähig zu machen.

Schutzbeispiele

- Beschränkung der Anzahl (Web-) Requests pro Zeiteinheit / IP
- Sicherstellen, dass der „Flaschenhals“ weit vorne auftritt (z.B. Firewall) um Kernsysteme zu schützen
- Sicherstellen, dass das System sich nicht selbst überlastet durch freigeben nicht mehr verwendeter Ressourcen, vermeiden von undendlichen Loops etc.
- Disaster Recovery Plan

SSL/TLS im internet Modell

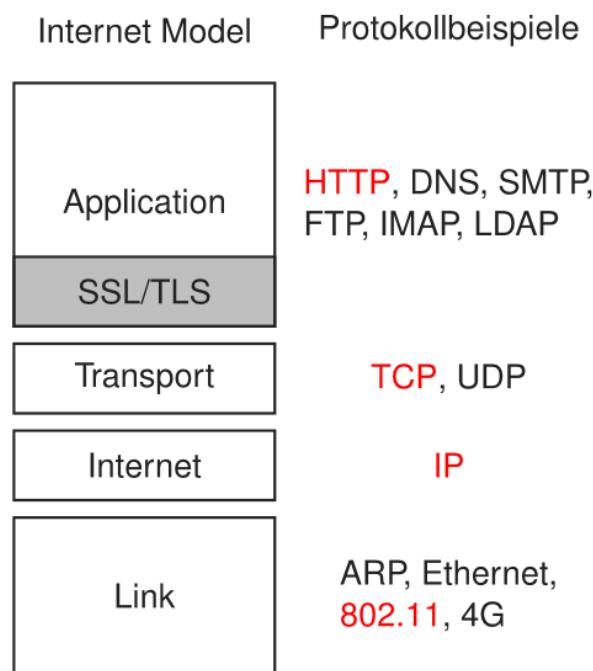


Abbildung 36: SSL/TLS

Bedrohung auf SSL / TLS (Preisgabe Sensitiver Daten)

Preisgeber Sensitiver Daten: Was ist das? Angreifer stehlen Schlüssel, Passwörter, Geschäftsheimnisse, Personendaten oder andere sensitive Daten vom Server, bei der Übertragung oder vom Client

Preisgabe sensitiver Daten: Was kann man dagegen tun?

- Keine Daten speichern oder übertragen, welche nicht benötigt werden.
- Daten nach ihrer Sensivität klassifizieren und entsprechend behandeln
- Sensitive Daten nur gespeichert auf dem Server ablegen
- Passwörter mit Salt und Pepper und einer starken Passwort-Hashfunktion gehasht ablegen.
- Daten verschlüsselt übertragen (FTP⇒SFTP, HTTP⇒HTTPS, etc). Zertifikat überprüfen!
- Sicherstellen, dass sichere Ciphers verwendet werden
- Keine sensitiven Daten auf der Clientseite cachen.

Bedrohungen auf Anwendungslayer: Cross Site Scripting (XSS) und Code Injection

XSS: Was ist das? Ein Angreifer bringt den legitimen Server dazu ein Script an den Browser zu senden. Dieses wird im Kontext des legitimen Servers ausgeführt. Es wird zwischen **stored** und **reflected** XSS unterschieden

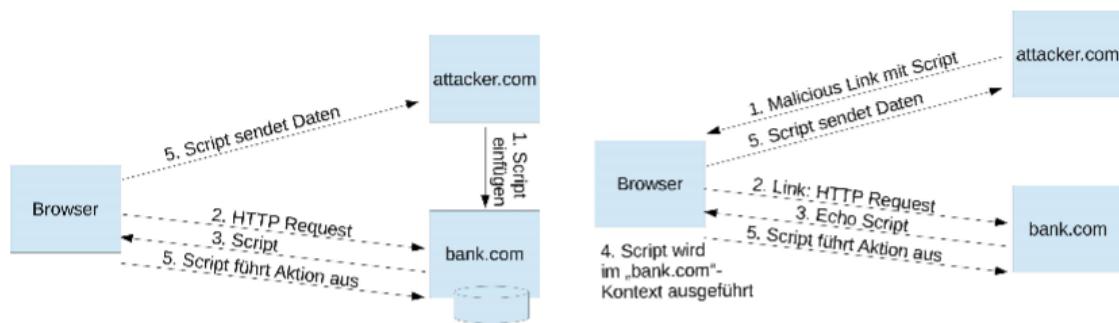


Abbildung: 'Stored' und 'reflected' XSS.

Abbildung 37: XSS

XSS: was kann man dagegen tun?

- Escaping aller unsicheren Daten (z.B. vom Benutzer eingegebene) bevor sie angezeigt werden.
Bsp. Ersetzen von <>" durch < > ; " ; ' ; /

Zusätzlich sollen folgende Massnahmen getroffen werden:

- Cookie als HttpOnly-Cookie setzen
- Header-Felder setzen
Bsp. Content-Security-Policy: default-src: 'self'; script-src: 'self' static.domain.tld
Bsp. X-XSS-Protection: 1; mode=block

Code Injection: Was ist das? Vermischung von 'Code' und 'Daten'

Ausgeföhrter Code:

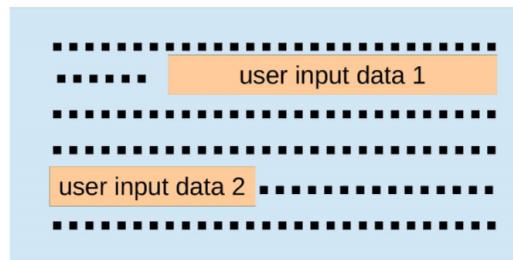
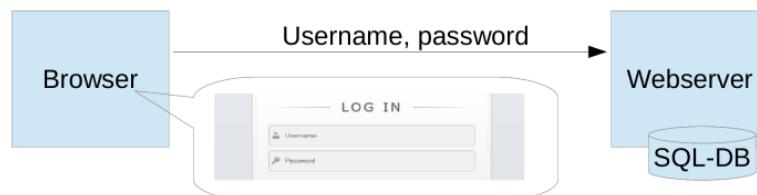


Abbildung 38: Code Injection



Auf Server-Seite ausgeführter Code:

```
$result = mysql_query(" select * from Users
    where(name='frank' OR 1=1); DROP TABLE Users; --
    and password='whatever');");
```

Abbildung 39: Beispiel Code Injection

Code Injection: Was kann man dagegen tun?

- ‘Prepared statements’ verwenden
Beispiel:

```
$statement = $db->prepare('SELECT * FROM Users WHERE(name=? password=?);';
$stmt->bind_param('ss', $user, $pass);
```
- Whitelisting der Inputs
- Sanitizing der Inputs
Bsp. Löschen von Zeichen wie ’;- oder Ersetzen durch ‘sichere’ Zeichen wie \\;\\"-
- Rechte des technischen Benutzers auf der DB einschränken
- Verwenden eines sicheren APIs

Layer 8

Die 7 Tierschichten des OSI-Models, wobei die 8. sich auf den Mensch bezieht.

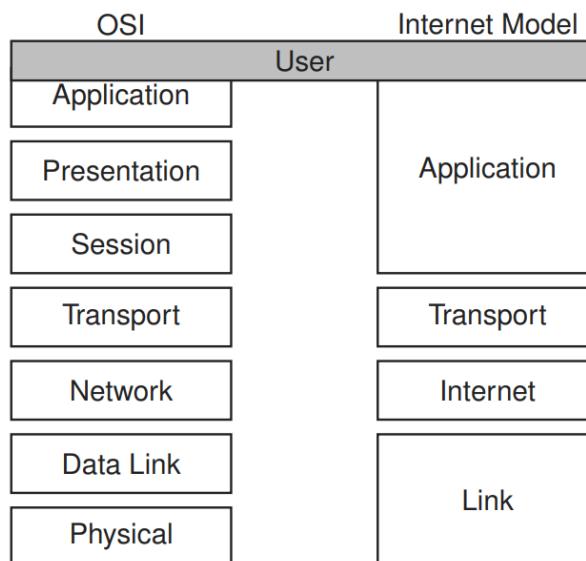


Abbildung 40: Layer 8, der User

Social Engineering: Was ist das? Zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.

Social Engineering: Was kann man dagegen tun?

- Benutzer schulen (‘awareness’)
- Für den Benutzer verständliche Abläufe Sicherstellen
- Benutzer nicht zum Umgehen von Sicherheitsmaßnahmen verleiten
- Fraud Detection-Maßnahmen
- Technische Maßnahmen welche den Angriff verhindern, z.B. Vereinzelungsanlage, nicht vorlesbare Codes etc.

Teil IV

Management (SW 07-09)

7 Standards & Frameworks, ISMS

Sie wissen, was ein ISMS ist und wie man damit umgeht

ISMS Ein *Information Security Management System (ISMS)* (auf Deutsch: Managementsystem für die Informationssicherheit) definiert Regeln, Methoden und Abläufe, um die IT-Sicherheit in einem Unternehmen zu gewährleisten, zu steuern, zu kontrollieren und zu optimieren.

Zweck

- Die (durch die IT verursachte) Risiken sollen identifizierbar und beherrschbar werden.
- Sicherheit erhalten, dass teure Informationen und Daten der Unternehmung angemessen geschützt sind.
- Rechtliche (Datenschutz- oder Berufsgesetz bei Ärzten / Anwälte) und auch Marktanforderung erfüllen (wenn morgen in den Medien publik wird, dass bei der UBS Bank gehackt und Millionen gestohlen wurde, dann würden die Kunden nicht länger ihr Vermögen bei der UBS deponieren).

Vorgehen

- Man sollte einen Prozess unterhalten, mit dem die Risiken der Informationssicherheit identifiziert und bewertet werden können. Dazu sollen Kontrollen bestimmt, eingeführt und stetig verbessert werden können.
- Davor muss zuerst der Schutzbedarf von Vermögenswerten bestimmt und Schutzmassnahmen eingeführt werden.

Sie kennen die wichtigsten Standards der Informationssicherheit

Standards

- ISO 27000: ISMS – Overview and vocabulary (Überblick / Index)
- ISO 27001: ISMS – Requirements (Anforderungskatalog)
- ISO 27002: Code of practice for information security controls (Analog: Kochbuch; darin steht drin, welche Massnahmen ich tätigen muss)
- ISO 27003: implementation guidance (wie ich die Anforderung umsetze)
- ISO 27004: Information security management – Measurement (Ziele müssen messbar sein, z.B. Jahresziele beim Mitarbeiter Gespräch; Ende Periode kann überprüft werden, ob die Ziele erreicht wurden)
- ISO 27005: Information security risk management (Risiko Bewältigung)

Überblick der Zusammenhänge

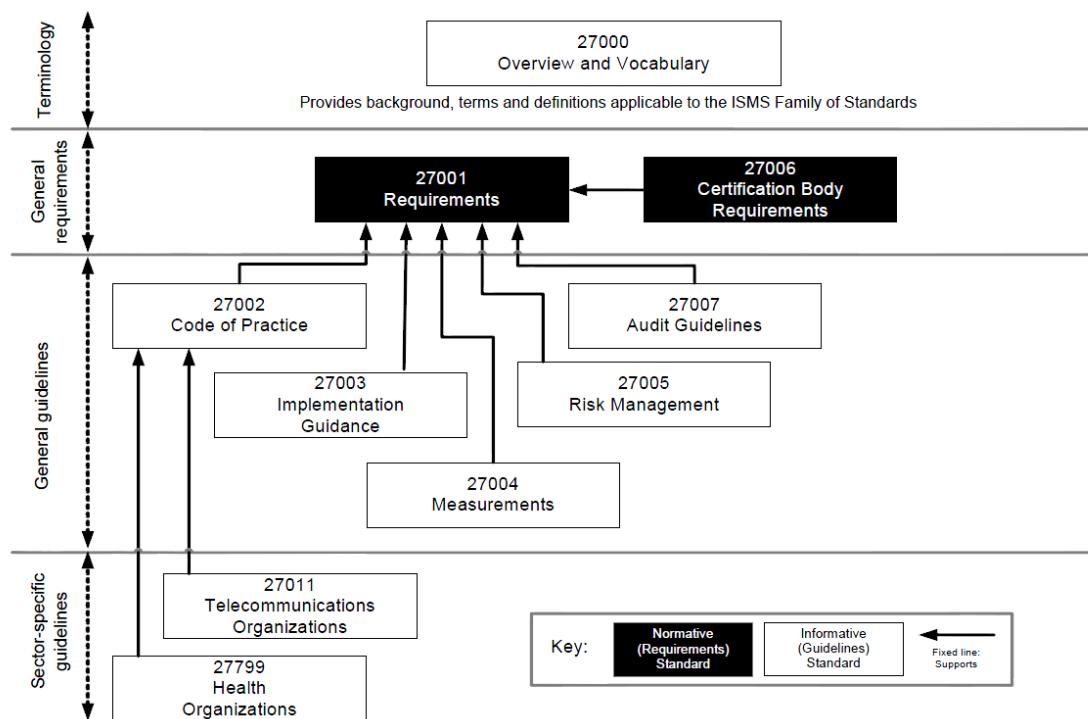


Abbildung 41: Zusammenhang der verschiedenen ISO Standards [3]

ISO 27000 - Overview and vocabulary

- Definiert Begriffe, welche in der ISO 27000 Standard-Reihe verwendet werden
- Definiert und erläutert kurz, was ein Information Security Management System (ISMS) ist
- Erklärt den dazu verwendeten Prozess-Ansatz „Plan - Do - Check - Act“ (PDCA)
- Gibt einen Überblick über die ISO 27000 Standard-Reihe

ISO 27001 - Requirements

- Definiert
 - Einführung
 - Betrieb
 - Überwachung
 - Wartung
 - Verbesserung
 eines dokumentierten ISMS's
- Wurde aus dem britischen Standard BS 7799-2:2002 entwickelt und als ISO-Norm im Jahr 2005 veröffentlicht
- Definiert den Sicherheitsprozess nach dem Prozess-Ansatz PDCA
 - Dieses Vorgehensmodell wird in ISO 27001:2013 nicht mehr explizit erwähnt, da es auch andere Ansätze gibt, um einen Sicherheitsprozess zu modellieren
- Definiert in Anhang A Ziele und Massnahmen zur Verbesserung der Informationssicherheit (die Ziele und Massnahmen sind aus ISO 27002 entlehnt)
- Eine Firma kann sich nach ISO 27001 zertifizieren lassen
- Freiheitsgrade beim Aufbau eines ISMS
 - „Scope“: Bereich, über den sich das ISMS erstreckt
 - * Ganze Firma
 - * Eine Abteilung
 - * Ein Standort
 - * Ein Teil der Infrastruktur: z.B. die DMZ
 - * etc.
 - Kontrollziele und Steuerungen (Controls aus ISO 27002), welche vom ISMS berücksichtigt werden („Statement of Applicability“, SOA)
- „Scope“ und „SOA“ definieren den Umfang einer Zertifizierung nach ISO 27001

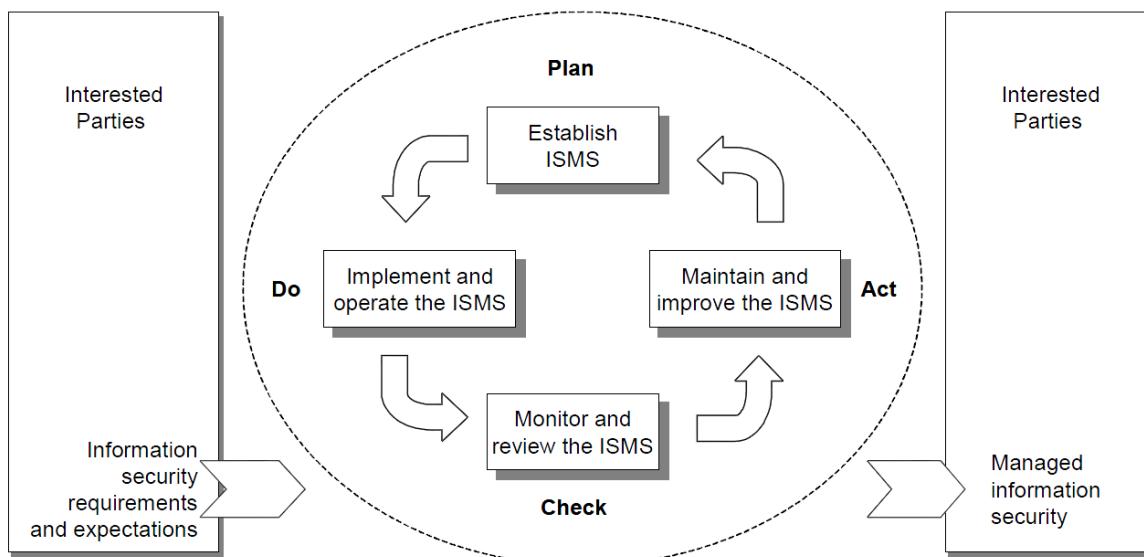


Abbildung 42: Prozess nach ISO 27001 [4]

Plan-Do-Check-Act nach ISO 27001

- **Planen (Erstellung des ISMS)**

Erstellung der jeweils für das Risikomanagement und zur Informationssicherheitsverbesserung relevanten ISMS-Richtlinien, Zielsetzungen, Prozesse und Prozeduren zur Erzielung von Ergebnissen gemäss den Gesamtrichtlinien und -zielsetzungen einer Organisation.

- **Machen (Einführung und Durchführung des ISMS)**

Einführung und Durchführung der ISMS-Richtlinien, -Steuerungsmassnahmen, -Prozessen, und -Prozeduren

- **Prüfen (Überprüfung und Revision des ISMS)**

Beurteilung und, wo massgebend, Messung des Prozesserfolgs gegenüber den ISMS-Richtlinien, -Zielsetzungen und praktischen Erfahrungen, sowie Berichterstattung über die Ergebnisse an das Management zwecks Revision

- **Handeln (Wartung und Verbesserung des ISMS)**

Ergreifung korrigiernder und vorbeugender Massnahmen, basierend auf den Ergebnissen des ISMS-Audits und der Management-Revision oder anderen relevannten Informationen zur Erzielung einer laufenden Verbesserung des ISMS

ISO 27002 - Code of practice for information security management

- Standardwerk zum Thema Informationssicherheit, kurz oft CoP genannt
- Definiert 114 Steuerungsmassnahmen¹² für den sicheren Umgang mit Informationen
- Zu jeder Massnahme sind Umsetzungsanleitungen angegeben, allerdings jeweils mit nur wenig Detailgrad
- Eine Zertifizierung nach ISO 27002 ist nicht möglich, da es keine harten Forderungen gibt (nur *sollte*-Formulierungen)
- Der Standard eignet sich sehr gut zur Umsetzung eines sog. Grundschutzes (Mindestanforderung im Sicherheitsbereich)
- Ursprung aus British Standard BS 7799-1:1999, wurde zu ISO 17799:2000; dann zu ISO 27002:2007 umbenannt, welches wortgleich mit ISO 17799:2005 war.
- Aktuell ISO 27002:2013
- Adressierte Themen
 - Organisatorische, physische und logische Sicherheit
 - Anwendungsentwicklung und -unterhalt
 - Notfallvorsorge
 - Einhaltung und Überprüfung der Sicherheit
 - etc.

¹²auch Massnahmen oder Prüfpunkte genannt

14 Domänen (Kapitel) von ISO 27002

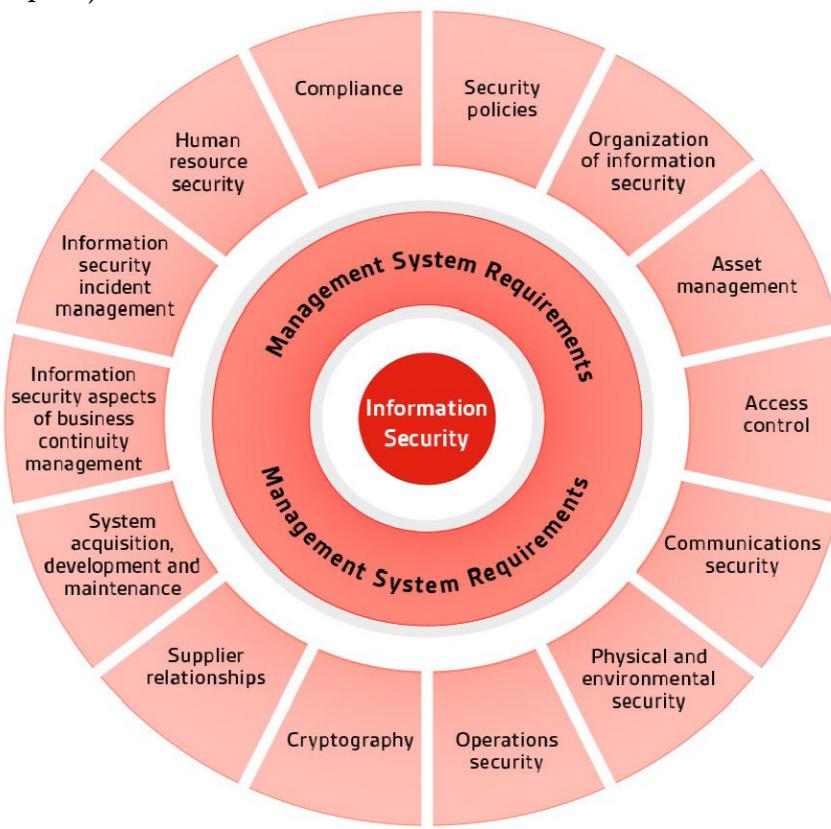


Abbildung 43: 14 Domänen (Kapitel)

ISO 27003 - ISMS implementation guidance

- Anleitung für die Entwicklung eines Implementierungsplans für eine ISMS nach ISO 27001
- Der Standard enthält nur Empfehlungen, jedoch keine Anforderungen
- Aufwand für den Aufbau eines ISMS in einer Firma mittlerer Grösse (ca. 250 Mitarbeitende)
 - 12-18 Monate
 - Mehrere hunderttausend Franken

ISO 27004 - Information security management - Measurement

- Anleitung für die Implementation eines Messsystems für die Beurteilung der Effektivität eines ISMS und der damit verbundenen Steuerungsmassnahmen gemäss ISO 27002
- Der Standard enthält Empfehlungen zu folgenden Aktivitäten:
 - Entwicklung von Messkriterien
 - Implementation eines Information Security Measurement Program (ISMP)
 - Analyse von Messresultaten und Reporting an die Stakeholders
 - Nutzung der Resultate, um das ISMS und die zugehörigen Massnahmen, sowie Kontrollen zu verbessern
 - Nutzung der Resultate, um das ISMP zu verbessern

ISO 27005 - Information security risk management

- Anleitung für ein Information Security Risk Management ohne Spezifikation einer Risiko Management Methode
- Beliebige Risiko Management Methoden können unter dem vorgegebenen Framework angewendet werden
- Der Standard basiert auf ISO 27001 und ISO 27002 und setzt deshalb für die Anwendung die Kenntnis dieser beiden Standards voraus
- Er spezifiziert den ganzen Risiko Management Prozess, beginnend mit der Risiko Analyse bis zum Plan für den Umgang mit den identifizierten Risiken

Sie finden sich in den Standards ISO 27001 und 27002 zurecht

Unterschiede Die Kontrollen in ISO 27002 haben dieselbe Bezeichnung wie in Anhang A von ISO 27001. In ISO 27002 wird Kontrolle 6.1.2 beispielsweise als „Aufgabentrennung“ bezeichnet, in ISO 27001 als „A.6.1.2 Aufgabentrennung.“ Der Unterschied liegt jedoch in der Detailgenauigkeit – im Durchschnitt erklärt ISO 27002 ein Steuerelement auf einer ganzen Seite.

Und zu guter Letzt ist der Unterschied, dass ISO 27002 keine Unterscheidung zwischen Kontrollen, die für eine bestimmte Organisation anwendbar sind und jenen, die das nicht sind, macht. ISO 27001 hingegen schreibt eine vorzunehmende Risikobewertung vor, um für jede Kontrolle zu ermitteln, ob es notwendig ist, die Risiken zu reduzieren und ist dies der Fall, in welchem Ausmass dies anzuwenden ist.

Es stellt sich die Frage: warum ist es so, dass diese zwei Normen getrennt existieren, warum wurden sie nicht zusammengeführt, um damit die positiven Seiten beider Normen hervorzu bringen? Die Antwort ist die Benutzerfreundlichkeit – eine einzelne Norm wäre zu komplex und zu gross für eine praktische Anwendung[5].

Sie verstehen die Grundzüge der BSI-Standards (BSI=Bundesamt für Sicherheit in der Informationstechnik, Deutschland)

BSI

- Unabhängige und neutrale Stelle für Fragen der Informationssicherheit in der INformationsgesellschaft
- Gründung 1991 per Gesetz als nationale Behörde für IT-Sicherheit
- Jahresbudget: ca. € 64 Mio.
- Mitarbeiter: >600
- Standort: Bonn
- Kunden: Bundesverwaltung, Wirtschaft, Wissenschaft, Bürger

BSI-Standards und IT-Grundschutz-Kataloge

- Die **BSI-Standards** beschreiben die Vorgehensweise nach IT-Grundschutz und enthalten Ausführungen zum Informationssicherheitsmanagement und zur Risikoanalyse
- Die **IT-Grundschutz-Kataloge** beinhalten die Baustein-, Massnahmen- und Gefährdungskataloge
 - Umfang:
 - * über 80 Bausteine
 - * über 1300 Massnahmen
 - * über 4000 Seiten



Abbildung 44: BSI-Standards und IT-Grundschutz-Kompendium [6]

BSI-Standard 200-1 - Managementsysteme für Informationssicherheit

- Zielgruppe: Management
- Definiert allgemeine Anforderungen an ein ISMS
- Kompatibel mit den entsprechenden Standards der ISO 27000 Reihe
- Berücksichtigt insbesondere Empfehlungen aus ISO 13335 und ISO 27002
(Siehe ISO 27002 - Code of practice for information security management, Seite 33)
- Didaktisch sehr gut aufbereitet (leicht verständlich)
- Enthält diverse Hinweise zur Zusammenarbeit Sicherheitsmanagement und Datenschutz

BSI-Standard 200-2 - IT-Grundschutz-Vorgehensweise

- Konkretisiert die Darstellung des ISMS nach BSI-Standard 200-1
- Beschreibt Aufbau und Betrieb eines ISMS in der Praxis
 - Aufgaben des IT-Sicherheitsmanagements
 - Aufbau von Organisationsstrukturen für die Informationssicherheit
- Gibt Anleitung
 - zur Erstellung eines Sicherheitskonzepts
 - zur Auswahl von angemessenen Sicherheitsmaßnahmen
 - zum Aufrechterhalten und Verbessern der Informationssicherheit

BSI-Standard 200-3 - Risikoanalyse auf Basis von IT-Grundschutz

- Die Standard-Sicherheitsmaßnahmen der IT-Grundschutzkataloge sind in der Regel ausreichend
- Es gibt allerdings auch Ausnahmen
 - Objekte mit besonders hohen Sicherheitsanforderungen
 - Objekte, welche in den IT-Grundschutzkatalogen nicht behandelt werden
 - Objekte, welche in Einsatzszenarien betrieben werden, die im Rahmen des IT-Grundschutz nicht vorgesehen sind
- In diesen Fällen muss eine Risikoanalyse auf der Basis von IT-Grundschutz durchgeführt werden

Risikoanalyse auf Basis von IT-Grundschutz

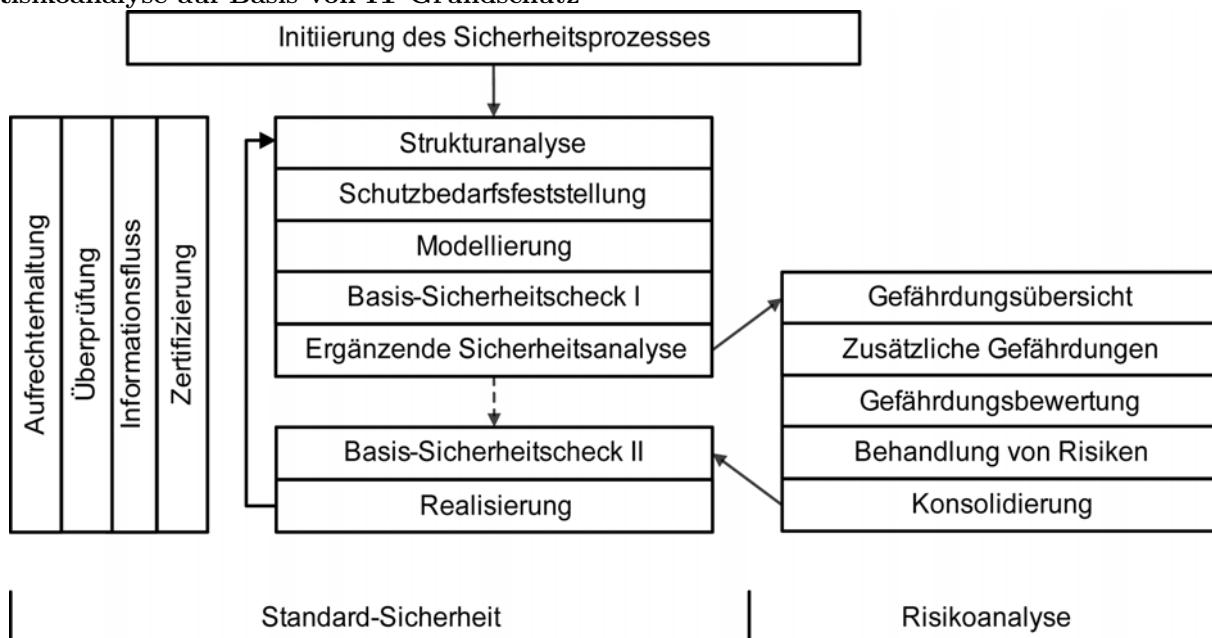


Abbildung 45: Standard-Sicherheit und Risikoanalyse

BSI-Standard 100-4 - Notfallmanagement

- Methodik zur Etablierung und Aufrechterhaltung eines unternehmensweiten, internen Notfallmanagements
- Führt zu einem eigenständigen Managementsystem für die Geschäftsfortführung und Notfallbewältigung
- Baut auf der IT-Grundschutzvorgehensweise auf (BSI-Standard 100-2)

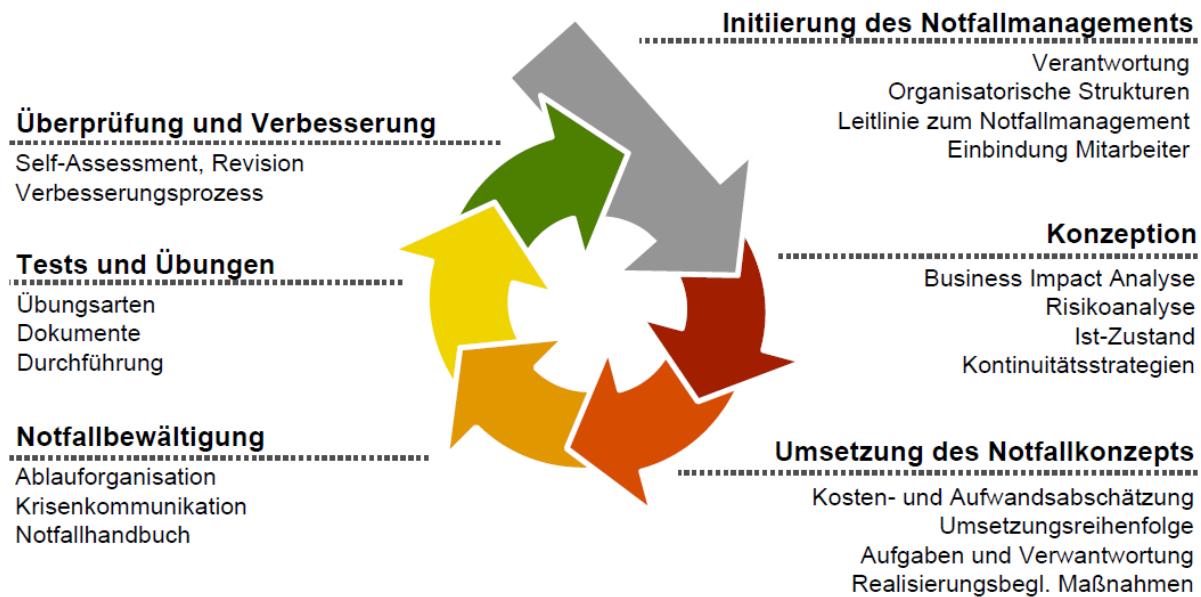


Abbildung 46: Iteration des Notfallmanagements nach BSI 100-4 [7]

Sie kennen die Struktur und Grundziele des NIST Cybersecurity Frameworks

NIST Cybersecurity Framework Das Cybersecurity Framework ist eine Reihe von Richtlinien für Privatunternehmen, die befolgt werden müssen, um bei den Funktionen Identify, Detect und Respond im Thema Cyberangriffe besser vorbereitet zu sein. Es enthält auch Richtlinien, wie man einen Angriff verhindern und sich von ihm erholen kann. Einfach ausgedrückt, ist das NIST Cybersecurity Framework eine Reihe von Best Practices, Standards und Empfehlungen, die einem Unternehmen helfen, seine Cybersicherheitsmaßnahmen zu verbessern. Das NIST Cybersecurity Framework versucht, den Mangel an Standards zu beheben, wenn es um Sicherheit geht. Derzeit gibt es grosse Unterschiede in der Art und Weise wie Unternehmen Technologien, Sprachen und Regeln zur Bekämpfung von Hackern, Datenpiraten und Ransomware einsetzen. Die verschiedenen Policies, Guidelines, Best Practices und Technologien, die in der Cybersicherheit verwendet werden, werfen ein weiteres Problem auf: Unternehmen sind nicht in der Lage, Informationen über Angriffe auszutauschen. Aber Vorsicht, das was die andere Firma dagegen getan hat, muss nicht unbedingt für das eigene Unternehmen funktionieren. Das NIST Cybersecurity Framework zielt darauf ab, all dies zu beseitigen. Mit einem einheitlichen Satz von Regeln, Richtlinien und Standards ist es einfacher, Informationen zwischen zwei Unternehmen auszutauschen und alle auf das gleiche Niveau zu bringen[8].

Cybersecurity Framework Components Das NIST Security Framework besteht aus drei Komponenten. Dem Kern (Core), den Umsetzungsebenen (Tiers) und dem Profil (Profile).

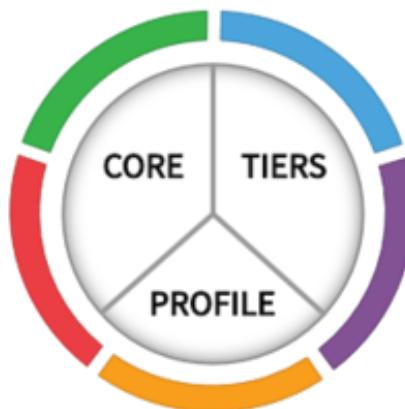


Abbildung 47: Die Komponenten des NIST Frameworks

Tiers und *Profile* haben wir nicht durchgenommen, weshalb dies nicht weiter beschrieben wird.

Core Der Framework-Kern definiert die Aktivitäten, die Sie durchführen müssen, um unterschiedliche Cybersicherheitsergebnisse zu erzielen. Diese wird in vier verschiedene Elemente unterteilt:

- Fünf **Funktionen** für grundlegende Cybersicherheitsaufgaben¹³
 - Identifizierung
 - Schutz
 - Erkennung
 - Reaktion
 - Wiederherstellung
 - Für jede der fünf Funktionen gibt es **Kategorien**, die eigentlich spezifische Herausforderungen oder Aufgaben sind, welche ausgeführt werden müssen (z.B. Betriebssystem- & Software-Updates, Antiviren- & Antimalwareprogramme)
 - **Unterkategorien** sind Aufgaben oder Herausforderungen, die mit der Kategorie verbunden sind (z.B. für Betriebssystem-Updates (Kategorie) müssen automatische Updates auf allen Maschinen aktiv sein)
 - **Informative Quellen** sind Dokumente & Handbücher, die spezifische Aufgaben für Benutzer detailliert beschreiben, wie die Dinge durchgeführt werden sollen (z.B. wie automatische Updates aktiviert werden)
- Tiers und *Profile* haben wir nicht durchgenommen, weshalb dies nicht weiter beschrieben wird.

Fünf Funktionen der Cybersicherheitsaufgaben



Abbildung 48: Fünf Frameworkfunktionen

- **Identifizierungsfunktion** hilft bei der Entwicklung eines organisatorischen Verständnisses für das Management des Cybersicherheitsrisikos für Systeme, Personen, Anlagen, Daten und Fähigkeiten
- **Schutzfunktion** unterstützt die Fähigkeit, die Auswirkungen potenzieller Cybersicherheitereignisse zu begrenzen oder einzudämmen, und setzt Rahmenbedingungen der Schutzmassnahmen für die Bereitstellung kritischer Dienste
- Die **Erkennungsfunktion** definiert die geeigneten Aktivitäten, um das Auftreten eines Cybersicherheitsereignisses rechtzeitig zu erkennen
- Die **Reaktionsfunktion** umfasst geeignete Aktivitäten, um Maßnahmen in Bezug auf einen erkannten Cybersicherheitsvorfall zu ergreifen und die Auswirkungen zu minimieren
- Die **Wiederherstellungsfunktion** identifiziert geeignete Aktivitäten zur Aufrechterhaltung von Ausfallsicherheitsplänen und zur Wiederherstellung von Diensten, die bei Cybersicherheitsvorfällen beeinträchtigt werden

¹³Siehe [Fünf Frameworkfunktionen](#), Seite 38

8 Risiko-Management und IT-Grundschutz

Sie kennen den Aufbau der IT-Grundschutz-Kataloge und deren Anwendungsweise

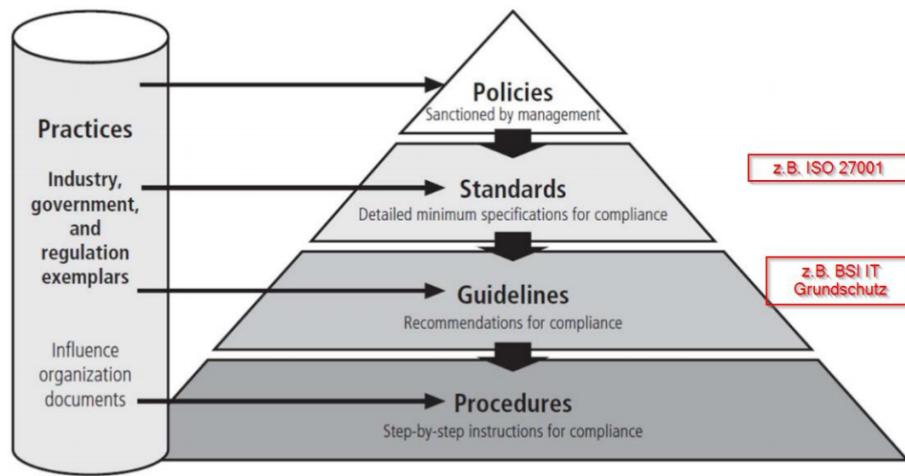


Abbildung 49: IT-Grundschutz-Aufbau

Vergleich ISO und BSI

- ISO 27001 ist eine Norm/Standard der 'High Level' beschreibt an was zu denken ist. (Organisation, Planung, Risikomanagement)
- Der BSI IT Grundschutz ist eine 'Low Level' Sammlung von Guidelines und Procedures zum erreichen von Sicherheitszielen.
- Der IT Grundschutz ist aufgeteilt in Gefahren / Anforderungen und Massnahmen, jeweils gegliedert in **Bausteine**

Warum ist der IT Grundschutz vollständig? Er spricht **sehr** viele IT Sicherheits-Themen in einem breiten Spektrum an.

Warum ist der IT Grundschutz nicht vollständig? Es ist fast unmöglich einen vollständigen Katalog mit allen aktuellen Gefahren und Massnahmen zu haben → aber ein gutes Nachschlagewerk

Was sind Bausteine? Bausteine sind unterteilt in Kategorien (z.B. Netzwerk) und Gefahren (Firewall Kompromittierung) und Massnahmen (Updates, Konfigurationen, ...)

Bausteine Hier noch ein Ausschnitt der Bausteine aus der Seite vom BSI.bund.de:

- > [ISMS: Sicherheitsmanagement](#)
- > [ORP: Organisation und Personal](#)
- > [CON: Konzeption und Vorgehensweise](#)
- > [OPS: Betrieb](#)
- > [DER: Detektion und Reaktion](#)
- > [APP: Anwendungen](#)
- > [SYS: IT-Systeme](#)
- > [IND: Industrielle IT](#)
- > [NET: Netze und Kommunikation](#)
- > [INF: Infrastruktur](#)

Abbildung 50: Bausteine IT Grundschutz Katalog

Definitionen des Begriffs 'Risiko'

- **Quelle Duden:**

Möglicher negativer Ausgang bei einer Unternehmung, mit dem Nachteile, Verlust, Schäden verbunden sind; mit einem Vorhaben, Unternehmen o. Ä. verbundenes Wagnis.

- **Quelle ISO 27000:2009**

Kombination aus der Wahrscheinlichkeit eines Ereignisses und dessen Auswirkungen.

- **Quelle: Hans-Peter Königs, IT-RisikoManagement mit System**

Risiko ist eine Bedrohung, deren Wirkung auf Ziele (SystemZiele) mit Wahrscheinlichkeit (Häufigkeit) und Konsequenz bewertet wird. Das Risiko betrachtet dabei die negative, unerwünschte und ungeplante Abweichung und deren Folgen von System-Zielen

Hinweis: Dem Risiko kann auch eine positive Abweichung, d.h. eine Chance, gegenüberstehen.

Risikomanagement-Stile

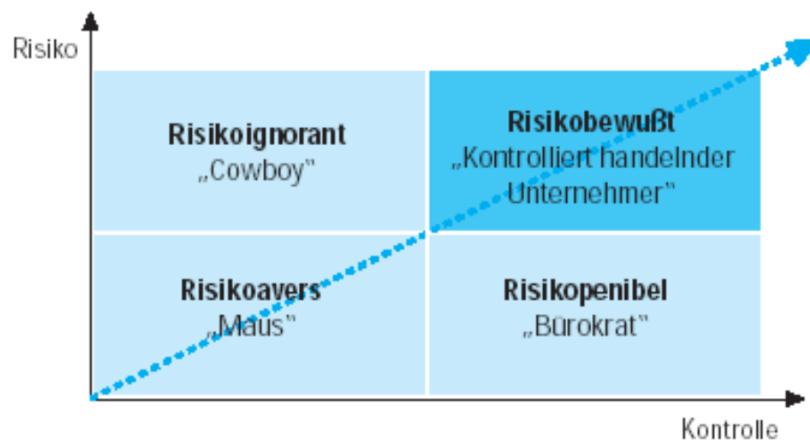


Abbildung 51: Verschiedene Stile von Risikomanagement

Unternehmensrisiken

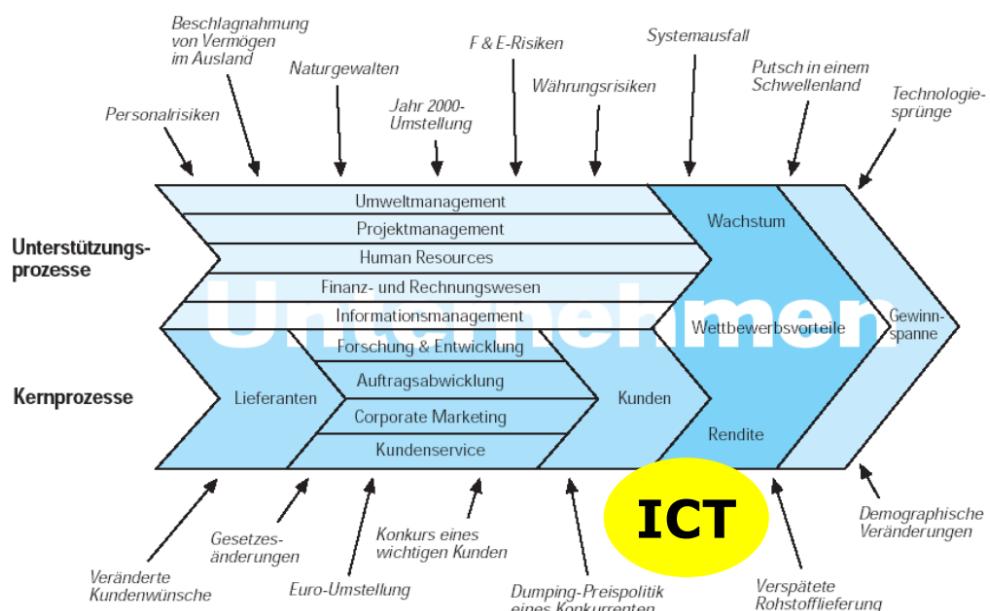


Abbildung 52: Risiken laut KPMG

Risiken im Bereich ICT

Organisatorische Risiken

- Nicht autorisierte Zugriffe auf Informationen und Applikationen
- Nicht prozessbezogener Einsatz von Applikationen
- Fehlende Fachkompetenz von Mitarbeitenden
- Mangelhafte Testverfahren
- Datendiebstahl

Anwendungs- und prozessbezogene Risiken

- Veraltete und nicht integrierte Softwarelösungen (Insellösungen)
- Fehlende strategische Neuorientierung

Infrastrukturelle Risiken

- IT-Infrastruktur kann den Ansprüchen (z. B. Leistungsfähigkeit) nicht gerecht werden
- Mangelhaftes Backupkonzept
- Fehlender Notfallplan
- Fehlender Wiederanlaufsplan (Business Continuity Management)
- Bauliche oder technische Standards werden nicht erfüllt (Schutz vor Zutritt, Feuer und Energieausfall)
- Mangelhafte Dokumentation der Systeme

Kostenbezogene Risiken

- Fehlende Kostentransparenz
- Mangelhafte Projektdefinition und -organisation mit daraus resultierenden Kostenüberschreitungen

Projektbezogene Risiken

- Run-away-Projekte (Zeit, Kosten und Termine laufen aus dem Ruder)
- Unprofessionelles Projekt-Management

OWASP TOP 10

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Fehler in Authentifizierung und Session-Mgmt.	→	A2:2017-Fehler in der Authentifizierung
A3 – Cross-Site Scripting (XSS)	↳	A3:2017-Verlust der Vertraulichkeit sensibler Daten
A4 – Unsichere direkte Objektreferenzen [mit A7]	↑	A4:2017-XML External Entities (XXE) [NEU]
A5 – Sicherheitsrelevante Fehlkonfiguration	↖ ↗	A5:2017-Fehler in der Zugriffskontrolle [vereint]
A6 – Verlust der Vertraulichkeit sensibler Daten	↗	A6:2017-Sicherheitsrelevante Fehlkonfiguration
A7 – Fehlerhafte Autorisierung auf Anw.-Ebene [mit A4]	↑	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Unsichere Deserialisierung [NEU, Community]
A9 – Nutzung von Komponenten mit bekannten Schwachstellen	→	A9:2017-Nutzung von Komponenten mit bekannten Schwachstellen
A10 – Ungeprüfte Um- und Weiterleitungen	☒	A10:2017-Unzureichendes Logging & Monitoring [NEU, Community]

Abbildung 53: OWASP TOP 10 IT Security Bedrohungen

Begriff: Operationelle Risiken Sämtliche betrieblichen Risiken, welche in einer Unternehmung Schäden verursachen können. Grosse Bedeutung haben operationelle Risiken im Bankwesen.

Das Risikoanalyse-Verfahren verstehen

Bestimmung / Messung von Risiken

Zugrunde liegende Größen:

- Eintretenshäufigkeit
- Schadensausmass

$$\text{Risiko} = \text{Eintretenshäufigkeit} * \text{Schadensausmass}$$

Quantitative vs. qualitative Risiko-Analyse

Quantitative Risikoanalyse

- Die an der Risikoanalyse beteiligten Größen sollen numerisch exakt berechnet werden.
- Der monetäre Wert von Assets muss genau bekannt sein.
- Die Eintrittshäufigkeit muss genau eingeschätzt werden (für Naturkatastrophen gibt es Tabellen, für andere Szenarien ist eine solche Schätzung oft sehr schwierig)

Qualitative Risikoanalyse

- Die an der Risikoanalyse beteiligten Größen werden anhand einer mehrstufigen Skala nur eingeschätzt, z.B. Schadensausmass '4' auf einer 5-stufigen Skala.

Vorgehen bei der Risiko-Analyse

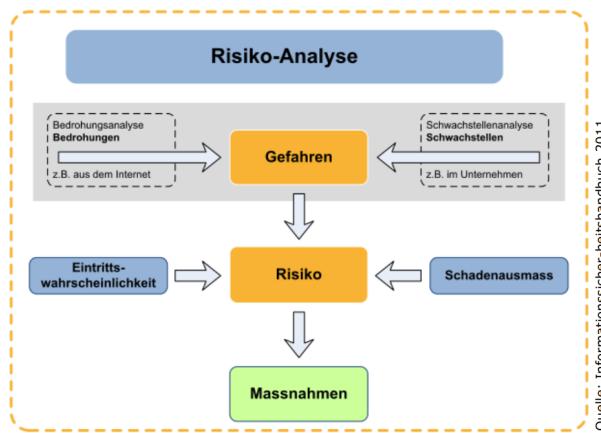


Abbildung 54: Vorgehen bei der Risiko-Analyse

Bedrohungen nach ISO 27005 (Annex C, 1/3) Citation kap. 8 s.16 [9]**Physical damage:**

- Fire
- Water damage
- Pollution
- Major accident
- Destruction of equipment or media
- Dust, corrosion, freezing

Natural events:

- Climatic phenomenon
- Seismic phenomenon
- Volcanic phenomenon
- Meteorological phenomenon
- Flood

Loss of essential services

- Failure of air-conditioning or water supply system
- Loss of power supply
- Failure of telecommunication equipment

Disturbance due to radiation

- Electromagnetic radiation
- Thermal radiation
- Electromagnetic pulses

Compromise of information:

- Interception of compromising interference signals
- Remote spying
- Eavesdropping
- Theft of media or documents
- Theft of equipment
- Retrieval of recycled or discarded media
- Disclosure
- Data from untrustworthy sources
- Tampering with hardware
- Tampering with software
- Position detection

Technical failures:

- Equipment failure
- Equipment malfunction
- Saturation of the information system
- Software malfunction
- Breach of info system maintainability

Unauthorised actions:

- Unauthorised use of equipment
- Fraudulent copying of software
- Use of counterfeit or copied software
- Corruption of data
- Illegal processing of data

Compromise of functions:

- Error in use
- Abuse of rights
- Forging of rights
- Denial of actions
- Breach of personnel availability

Human Threats:

- Hacking
- Social engineering
- System intrusion, break-ins
- Unauthorized system access
- Computer crime (e.g. cyber stalking)
- Fraudulent act (e.g. replay, impersonation, interception)
- Information bribery
- Spoofing
- Bomb / Terrorism
- Information warfare
- System attack (e.g. distributed denial of service)
- System penetration
- System tampering
- Defence advantage
- Political advantage
- Economic exploitation
- Information theft
- Intrusion on personal privacy
- Assault on an employee
- Blackmail
- Browsing of proprietary information
- Computer abuse
- Fraud and Theft
- Input of falsified, corrupted data
- Interception
- Malicious code (e.g. virus, logic bomb, Trojan horse)
- Sale of personal information
- System bugs
- System sabotage

Qualitative Risikoanalyse: Definition Schadensausmass

Es wird empfohlen, eine 3 bis 5-stufige Skala zu definieren, z.B.:

Schadensausmass:

- **Vernachlässigbar - Vernachlässigbare Auswirkungen**

- Dienstleistung nicht wesentlich gestört
- Sachschäden im Bereich von CHF 100.- bis 5'000.-*
- keine Verletzten
- kein Imageverlust

- **Marginal - Geringe Auswirkungen**

- Die Einhaltung gesetzlicher und vertraglicher Pflichten ist nicht gefährdet
- Die Dienstleistung sind nur geringfügig beeinträchtigt.
- Sachschäden im Bereich von CHF 5000.- bis 50'000.-*
- keine Verletzten
- kein Imageverlust

- **Kritisch - Grosse Auswirkungen**

- Die Einhaltung gesetzlicher und vertraglicher Pflichten ist gefährdet oder die Dienstleistungen sind beeinträchtigt.
- Sachschäden im Bereich von CHF 50'000.- bis 500'000.-*
- Keine Verletzten
- Imageverlust ist klein und von kurzer Dauer

- **Katastrophal - Sehr grosse Auswirkungen**

- Die Einhaltung gesetzlicher und vertraglicher Pflichten sind stark gefährdet oder die Dienstleistungen werden verunmöglich.
- Sachschäden im Bereich >CHF 500'000.-*
- einige Schwerverletzte
- grosser Imageschaden (Presse)

Eine einfache Risikoanalyse durchführen können

Definition Eintrittshäufigkeit nach Sicherheitshandbuch

Es wird empfohlen, eine 3 bis 5-stufige Skala zu definieren

- **Sehr selten**

- Möglich aber eher unwahrscheinlich
- z.B. 1-mal in 10 Jahren

- **Selten**

- Tritt selten ein, aber kann vorkommen
- z.B. alle 5 Jahre

- **Oft**

- Tritt gelegentlich ein
- z.B. jährlich

- **Sehr oft**

- Kommt öfters vor
- z.B. monatlich

Qualitative Risikoanalyse: Risikomatrix

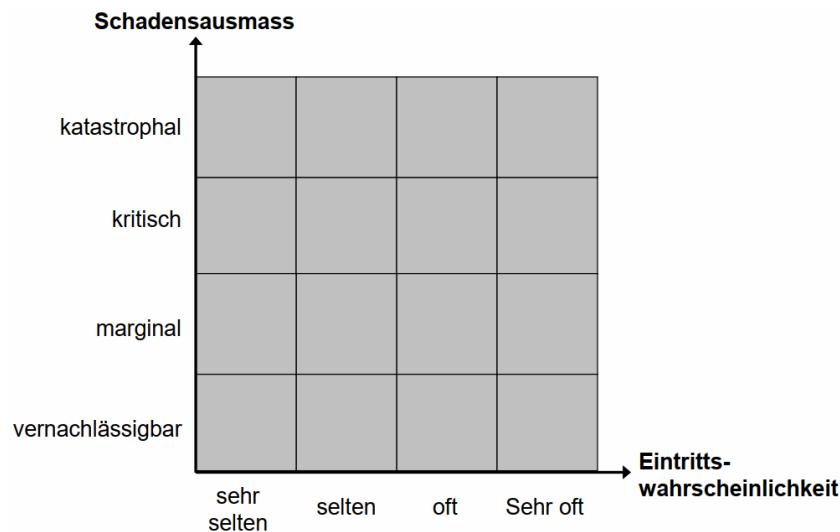


Abbildung 55: Risikomatrix

Risiko-Portfolio, Risiko-Landkarte (Risk-Map)

- Eine Menge von risiken, welche im Rahmen einer Risikoanalyse identifiziert worden ist, wird als **Risiko-Portfolio** bezeichnet.
- Risiko-Portfolios werden oft einzelnen Geschäftsfeldern zugeordnet (jedes Geschäftsfeld hat sein Portfolio)
- Werden die Einzelrisiken des Portfolios in einer Risikomatrix eingezeichnet, so spricht man von einer **Risiko-Landkarte (Risk-Map)**

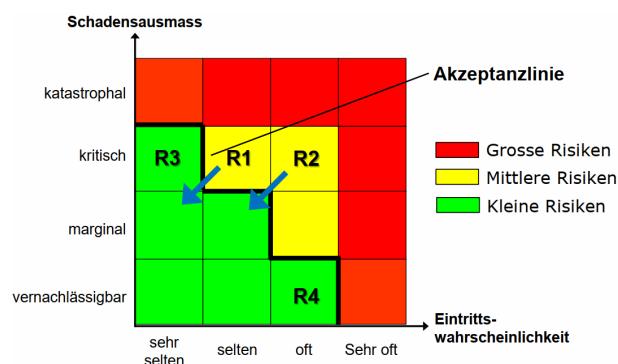


Abbildung 56: Risk-Map

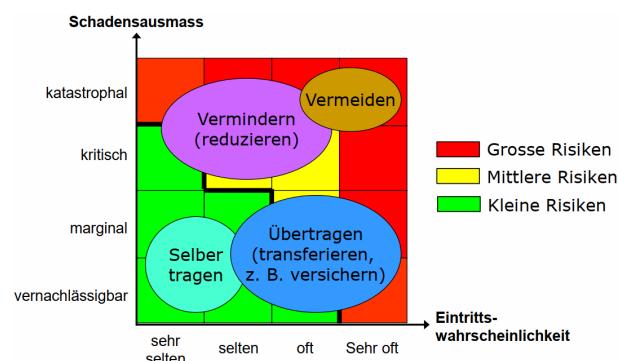


Abbildung 57: Risk-Map, Umgang mit Risiken

Umgang mit Risiken / Risikobewältigung

- Risiken vermeiden:**

Anpassen oder aufgeben von Geschäftsprozessen, sodass die Risiken nicht mehr vorhanden sind.

- Risiken vermindern (Mitigation):**

Mit geeigneten Sicherheitsmaßnahmen das Schadensausmass oder die Eintrittshäufigkeit reduzieren.

- Risiken übertragen (transferieren):**

Überwälzung finanzieller Schäden auf Versicherungen, Outsourcer oder Benutzer eines Service.

- Risiken tragen:**

Akzeptieren von Risiken (Restrisiken)

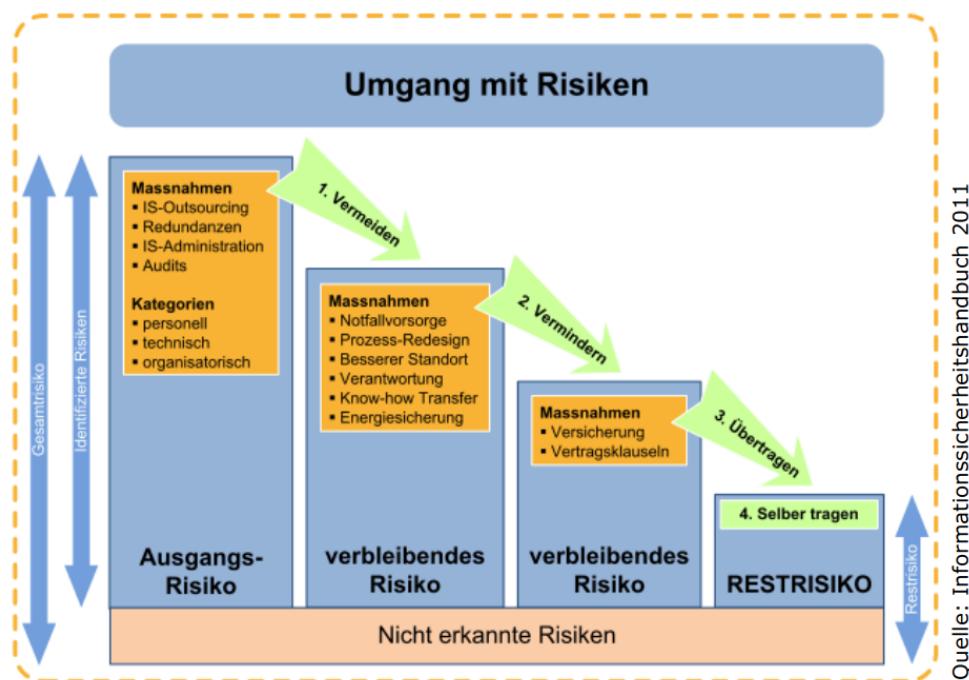


Abbildung 58: Umgang mit Risiken

Der Entscheid, wie mit Risiken umgegangen werden soll, muss dokumentiert und von der Geschäftsleitung genehmigt werden.

Das Gleiche gilt insbesondere auch für die verbleibenden Restrisiken.

Risiko-Katalog (Risk Register)														
Objekte	Bedrohung (Gefahr)			Schadenshöhe Einstufung			Eintritt 1 mal in		Bemerkungen zu den potentiellen Schäden	Bestehende Massnahmen Beschreibungen / Bemerkungen	Vorgeschlagene Massnahmen Beschreibungen / Bemerkungen			
	Bedrohung 1			System-Ziel 1			0,1 Jahr							
	Bedrohung 2			System-Ziel 2			1 Jahr							
Objekt 1	x	x	x	System-Ziel 3			10 Jahren	30 Jahren	> 30 Jahre					
Objekt 2	x	x	x							...				

Abbildung 59: Beispiel eines Risikokataloges

Auswahl von Massnahmen zur Risikoreduktion

- Welche Massnahmen haben die grösste Wirkung (Reduktion mehrerer Risiken)?
- Welche Massnahmen benötigen wenig Ressourcen?
- Welche Massnahmen können kurzfristig realisiert werden?
- Welche Massnahmen stossen auf breite Akzeptanz?

Wirtschaftlichkeit und den Faktor Mensch nie ausser Acht lassen!

Risiko-Management-Prozess

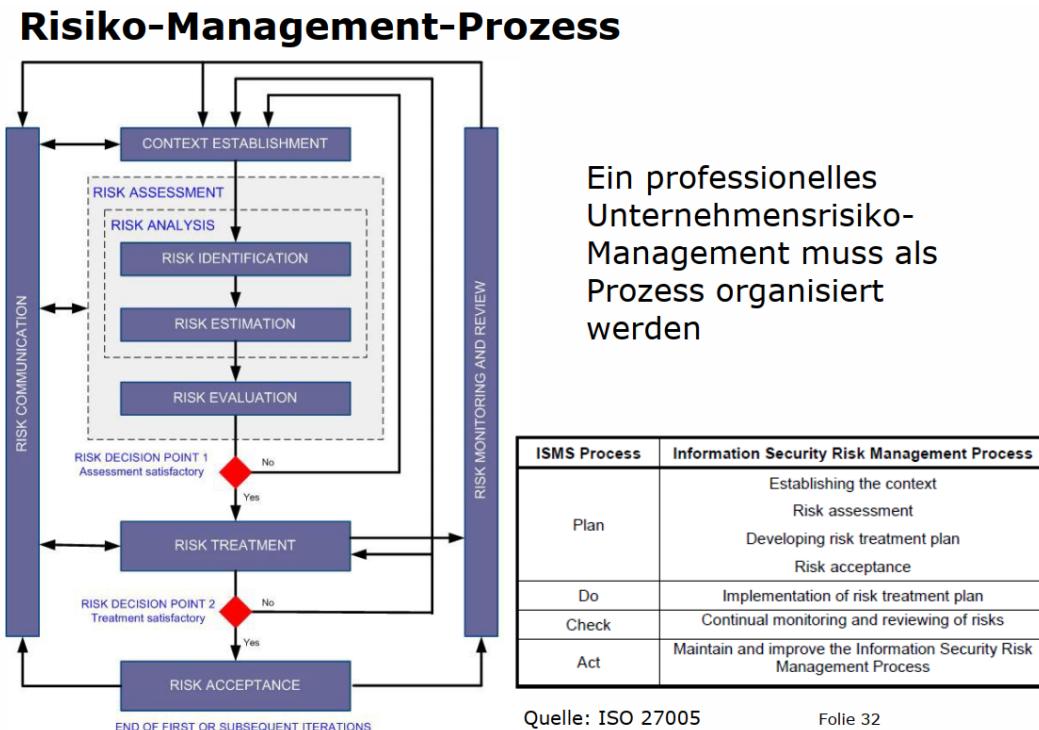


Abbildung 60: Organisation eines Risiko Managements

• Context Establishment

Gegenstand, Zweck, Absichten, Ziele, Fokus und relevante Einflüsse, Randbedingungen und Abgrenzungen aus externer und interner Sicht festlegen

- wichtige Ziele der Geschäfts- und Support-Prozesse
- „Risiko- und Sicherheitspolitik“ für wichtigste Kontext-Elemente
- für wen stehen Risiken zur Behandlung an und für wen/was wird das Risiko-Management durchgeführt (z.B. Anspruchsgruppen)?
- Gesetzliche, regulatorische und vertragliche Anforderungen
- Für das Risikomanagement massgebliche Führungs-Aspekte, organisatorische Festlegungen und Verantwortlichkeiten sowie Berichtserstattungs- und Eskalations-Wege
- Anzuwendender Risiko-Management-Ansatz
- Schnittstellen zum Corporate Risikomanagement (z.B. Op-Risk)
- Risiko-Arten und System-Ziele (z.B. Prozessrisiken, Verfügbarkeits- und Integritätsanforderungen)
- Impact Kriterien (Schadensmetrik)
- Bewertungskriterien und –massstäbe (z.B. Risiko-Matrix, Dringlichkeitsstufe)
- Akzeptanzkriterien (z.B. Akzeptanzlinie)
- Dokumentationsvorgaben

• Risk Identification

Objekte, Bedrohungen, Schwachstellen und bereits existierende Massnahmen erfassen

- Erfassung der Assets (Risiko-Objekte)
- vollständigen Erfassung der Gefahrenquellen und der Aufsuchen bereits existierender Massnahmen
- Identifikation der vorhandenen Vulnerabilities (Schwachstellen)
- Relevante Kausalketten (Ursachen/Wirkungen und Konsequenzen) zusammenstellen

• Risk Estimation

Häufigkeit und Schadensausmass einschätzen

– **Teil-Analysen:**

- Impact-Analyse (Analyse der potentiellen Schäden)
- Bedrohungs-Analyse (Analyse der relevanten Bedrohungen)
- Schwächen-Analyse (Analyse der relevanten Schwachstellen)
- Beliebige Kombination der Analysen 1 bis 3
- Qualitative oder quantitative Risiko-Analyse
- Semi-quantitative Analyse

• Risk Evaluation

Bewertung der identifizierten Risiken im definierten Kontext (Bsp. zeitl. Prioritäten für die Umsetzung von Massnahmen; Reduktion Häufigkeit oder Schadensausmass?; Abwägung Risiken/Chancen etc.)

- Bewertung im Kontext des Untersuchungs- und Behandlungs-Gegenstands (Vergleich mit den im Kontext definierten Kriterien, z.B. Risiko-Toleranz)
- Reduktion Häufigkeit oder Schadensausmass?
- Für Massnahmen relevante zusätzliche Anforderungen, z.B. vertragliche, gesetzliche, regulatorische Anforderungen, Standards, Qualitäts- und Leistungsanforderungen, Zeit- und Kostenbeschränkungen
- Risiken / Chancen abwägen hinsichtlich Optimum
- Risiko-Wahrnehmung der Umgebung und des Managements einbeziehen
- Risiken mit Attributen versehen: z.B. „wichtig“, „dringlich“ oder „beobachten“
- Entscheid über allenfalls notwendige Nachbesserung der Assessment-Ergebnisse

• Risk Treatment

Definition, Konzeption, Planung und Umsetzung von Massnahmen aufgrund der bei der Risk Evaluation definierten Anforderungen (Varianten: vermeiden, vermindern, transferieren, tragen)

- Berücksichtigung Anforderungen an Massnahmen
- Auswahl von Massnahmen mit Hilfe von ISO/IEC 27002
- Machbarkeit der Massnahmen
- Bewältigungs-Optionen-Wahl:
 - Risiken vermeiden, z.B. durch Aufgabe risikoreicher Aktivitäten
 - Risiken reduzieren, durch Reduktion entweder der Eintritts-Wahrscheinlichkeit oder des Schadensausmasses
 - Risiken transferieren, z.B. Überwälzung finanzieller Schäden auf Versicherungen
 - Risiken bewusst eingehen und tragen, z.B. Tragen des Restrisikos, welches im Rahmen der betrieblichen Reserven und eines allfälligen Goodwill-Verlusts verkraftbar ist
 - Abwägen Risiken mit Massnahmenkosten
 - Kosten-/Nutzen-Untersuchungen
 - Umsetzungsplan

• Risk Acceptance

Formaler Akzept des Risk Treatment Plans sowie der Restrisiko-Einschätzung durch das zuständige Management

- Bewältigungsplan (mit Verantwortlichkeiten und Terminen) sowie Restrisiko-Einschätzung müssen durch das zuständige Management formal akzeptiert sein
- Restrisiken, die nach der Bewältigung die Akzeptanz-Kriterien nicht erfüllen, müssen schriftlich begründet und durch das zuständige Management schriftlich zur Kenntnis genommen und akzeptiert werden.
- Massnahmen-Überwachung, -Überprüfung Erneute Risiko-Einschätzung und –Bewertung aufgrund veränderter Situation
- Wiederholung im Rahmen eines jährlichen Risikoberichts (z.B. synchron zum rollierenden Strategieprozess)

• Risk Communication

Information der direkt Beteiligten und der Betroffenen in jedem Teilprozess

- Kommunikation mit Beteiligten und Betroffenen (z.B. Anspruchsgruppen)
- angemessene Kommunikation unter Fachpersonen, Experten, Entscheidungsträgern und Anspruchsgruppen
- Berücksichtigung der Risiko-Wahrnehmung
- Stärkung des Risiko-Bewusstseins
- Einsatz „stark strukturierter“ Kommunikationsformen
- Kommunikations-Konzept für Risiko-Kommunikation im Normalbetrieb, für risikorelevante Ereignisse und in Notfallsituationen

- **Risk Monitoring and Review**

Prozess und Risiko-Situation bezüglich allfälliger Veränderungen überwachen

- Prozess und Risiko-Situation überwachen (z.B. Überwachung Änderungs-Prozesse, Entwicklungsprozesse und Betriebsprozesse)
- Überwachung mit Risiko-Indikatoren und mit Frühwarnsystem
- Registrierung von Veränderungen von Kontext und Risikosituation sowie Verbesserungs-Empfehlungen hinsichtlich Risikomanagement sowie aktueller und zukünftiger Risikosituation aufzeigen
- Überprüfung durch unabhängige Auditoren
- Verifikation anhand Reifegradmodell
- Risiko-Berichte
- Unabhängigkeit der Berichterstattung

Kriterien für die Prozesswiederholung:

- **Externer Trigger:**

Sich ändernde Umgebungsbedingungen; inakzeptable Restrisiken aufgrund ungenügend realisierter Massnahmen; neue regulatorische Anforderungen

- **Periodische Durchführung:**

Synchron mit anderen Management-Prozessen (z. B. Strategieprozess)

Verfahren für den Umgang mit Risiken

- Grundschutz (z.B. gemäss BSI)
 - Standardisierte Massnahmen
 - Generelle Risikobetrachtung
- Risikoanalyse
 - Spezifische Massnahmen
 - Detaillierte Risikobetrachtung
- Kombinierter Ansatz (zweistufiges Vorgehen, z.B. gemäss BSI)
 - Grundschutz bei Schutzbedarf klein und mittel
 - Risikoanalyse bei schutzbedarf hoch und sehr hoch

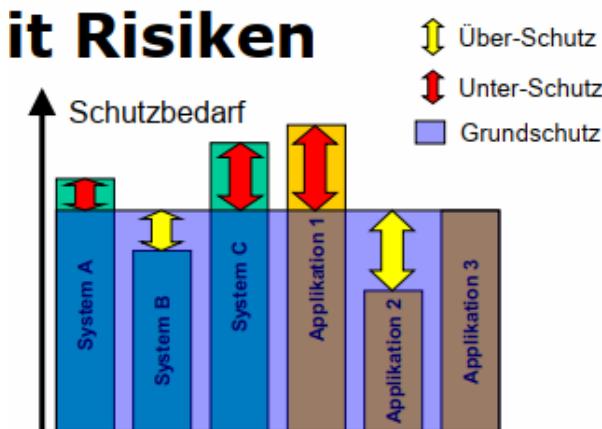


Abbildung 61: Schutzbedarf

Kombinierter Ansatz: Grundschatz und Risikoanalyse

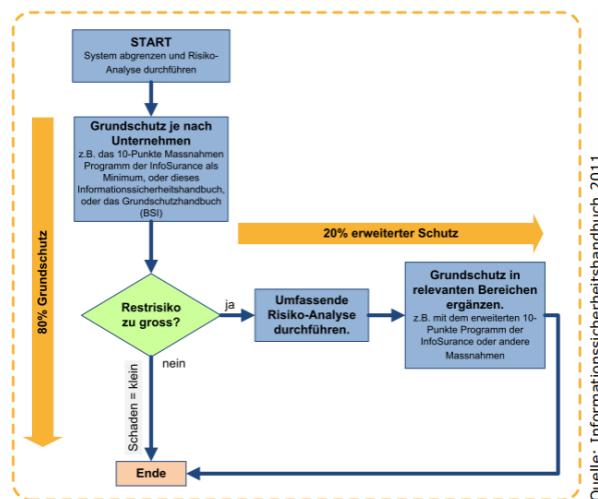


Abbildung 62: Kombinierter Ansatz

BSI-Standard 200-3: Risikoanalyse auf Basis von IT-Grundschatz

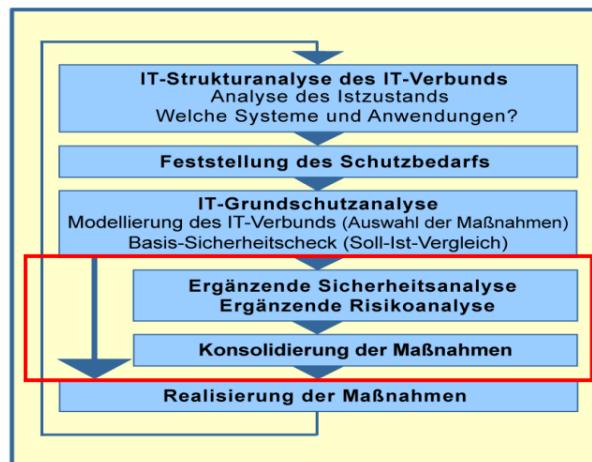


Abbildung 63: BSI-Standard 200-3

IT-Grundschatz-Kataloge

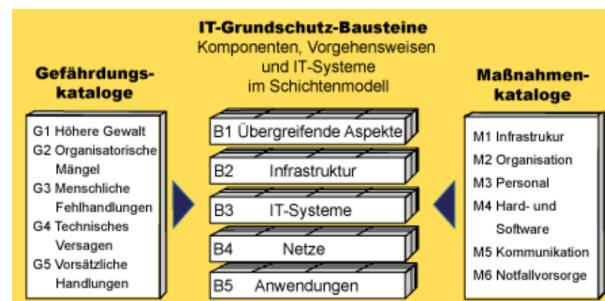


Abbildung 64: IT-Grundschatz-Kataloge

Die Unterschiede zum Grundschutzverfahren kennen

Bemerkungen zu den IT-Grundschutz-Katalogen

- Die Beschreibung der Gefährdungen dient lediglich der Sensibilisierung und der Begründung von Massnahmen und hat im Grundschutz-Vorgehen keine weitere Funktion!
- Das BSI macht keine Unterscheidung zwischen Gefahren und Schwachstellen!
- Die Inhalte haben Empfehlungscharakter und sind keine 'Gesetze'!
- Es gibt keine Garantie auf Vollständigkeit!
- IT-Grundschutz-Massnahmen müssen gegebenenfalls individuell angepasst und angewendet werden!

Sie verstehen die Idee, die Ziele und die Konzepte des IT-Grundschutz-Vorgehens

IT-Grundschutz Wirkungsprinzip Gilt generell, unabhängig vom angewandten Standard, also nicht nur für den BSI IT-Grundschutz!

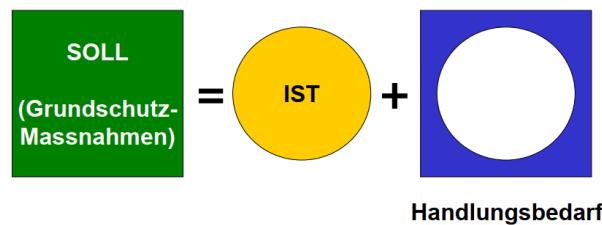


Abbildung 65: IT-Grundschutz Wirkprinzip

Grundregeln beim Vorgehen nach IT-Grundschutz

- Die Initiative für IT-Sicherheit geht vom Management aus
- Die Verantwortung für IT-Sicherheit liegt beim Management
- Nur wenn sich das Management um Informationssicherheit bemüht, wird die Aufgabe auch wahrgenommen

Erstellung eines IT-Sicherheitskonzepts Der blau hinterlegte Bereich beschreibt diejenigen Schritte, welche notwendig sind, um einen IT-Grundschutz zu etablieren. Als Resultat des erstellten IT-Grundschutzes liegt ein Sicherheitskonzept vor.

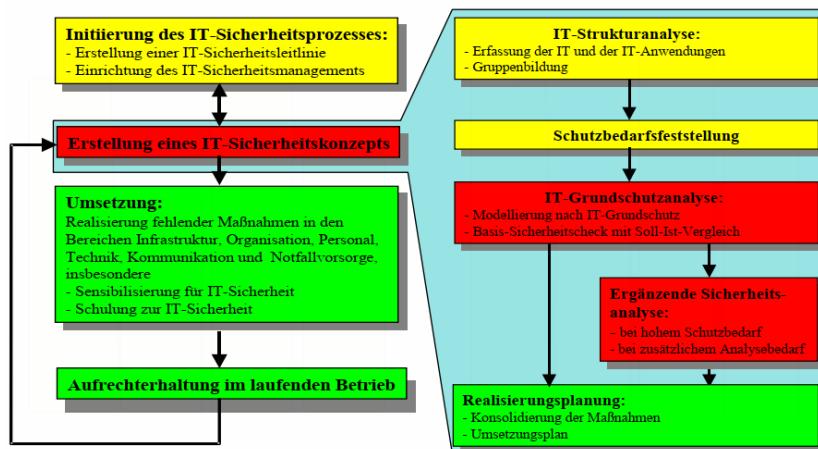


Abbildung 66: IT Sicherheitskonzept

IT-Grundschutz - Pro Argumente

- Standardbasierend
- Vollständigkeit der **Massnahmenpakete**
- Keine detaillierte Risikoanalyse notwendig
- Gleichmässiger, umfassender Schutz auf allen Objekten
- Einfach und schnell anwendbar
- Definierte Basis für weitergehende Schutzmaßnahmen (ergänzende Sicherheitsanalyse)

Achtung beim IT-Grundschutz!!

- Ungenügender Schutz bei erhöhten Risiken oder besonderem Schutzbedarf
- Mögliche Einschränkung der Funktionalität durch Überschutz
- Begründung von Massnahmen schwierig
- Je nach Detaillierungsgrad, Anspruch an Aktualität und Vollständigkeit des Massnahmenkataloges aufwändig
- Vorteile des Grundschutzvorgehens nicht durch administrativen ‘Overkill’ zunichte machen

Kreuzreferenztabellen

ISF 08 - Risiko-Analyse und BSI-Grundschutz

Legende für Spalte „Zyklus“:
 PK: Planung und Konzeption
 BE: Beschaffung
 UM: Umsetzung
 BT: Betrieb
 AU: Aussonderung
 NV: Notfallvorsorge

Kreuzreferenztabellen

B 3.106 Server unter Windows 2000

B 3.106	Zyklus	Siegel	G 1.2	G 2.7	G 2.18	G 3.9	G 3.48	G 4.10	G 4.23	G 4.35	G 5.7	G 5.23	G 5.52	G 5.71	G 5.79	G 5.83	G 5.84	G 5.85
M 2.227	PK	A		X		X	X						X			X		X
M 2.228	PK	A		X		X							X					X
M 2.232	PK	C		X						X				X			X	X
M 2.233	PK	B				X	X			X	X	X	X	X		X	X	X
M 4.48	UM	A		X											X			
M 4.56	BT	C		X	X									X				
M 4.75	UM	A											X		X			
M 4.136	UM	A	X	X		X		X	X	X	X	X	X	X	X	X	X	X
M 4.137	UM	A		X		X	X	X	X	X	X	X	X	X		X	X	X
M 4.139	UM	A		X		X	X	X	X	X	X	X	X	X		X		X
M 4.140	UM	A		X			X		X	X			X	X				X
M 4.141	UM	A		X			X			X	X		X					X
M 4.142	UM	B		X			X		X	X			X					X
M 4.143	UM	B		X			X		X	X			X					X
M 4.144	UM	B		X									X	X		X	X	X

Abbildung 67: Kreuzreferenztabellen

Kreuzreferenztabellen: Tabellen, welche angeben, welchen Gefährdungen mit welchen Massnahmen begegnet werden kann (bezogen auf einen bestimmten Baustein)

- Die Massnahmen werden priorisiert (sog. Siegelstufe)
 - **A:** Essenzielle Massnahme, vorrangig umzusetzen
 - **B:** Besonders wichtige Massnahme, zügig umsetzen
 - **C:** Wichtige Massnahme, verzögerte Umsetzung zulässig
 - **Z:** Ergänzende Massnahme, Umsetzung nicht zwingend notwendig
- Wichtig:
 - Anzahl ‘X’ ist kein Mass für die Wichtigkeit einer Massnahme
 - Nur die wichtigsten Gefährdungen sind aufgeführt

Sie können die Teilschritte zum Aufbau eines Sicherheitskonzeptes nach IT-Grundschutz durchführen, kombinierte Risikoanalyse

IT-Strukturanalyse

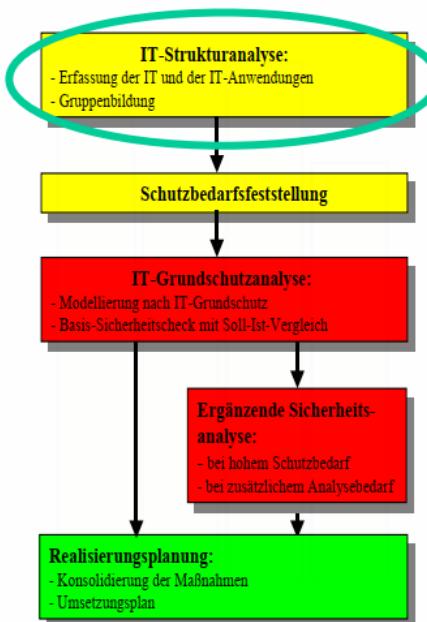


Abbildung 68: IT-Strukturanalyse

IT-Strukturanalyse - Erhebung Netzwerkplan

- Netzwerkplan — aktualisieren
 - Netzwerkpläne sind meist nicht auf dem aktuellsten Stand
 - Entsprechende Informationen beschaffen bei IT-Verantwortlichen, Administratoren resp. Netz- und Systemmanagement
- Netzwerkplan auserten
 - Welche IT-Systeme gibt es? (Clients, Server, Netzwerk-Komponenten etc.)
 - Welche Verbindungen zw. diesen Systemen?
 - Welche Verbindungen nach aussen (Einwahl, Internet, VPN etc.)

IT-Strukturanalyse - Komplexitätsreduktion

- Gleichartige Komponenten zu Gruppen zusammenfassen
- Mögliche Gruppierungskriterien
 - Systeme von gleichem Typ
 - Systeme mit gleicher oder nahezu gleicher Konfiguration
 - Systeme mit gleicher oder nahezu gleicher Netzwerkanbindung
 - Systeme mit gleichen administrativen und infrastrukturellen Rahmenbedingungen
 - Systeme, welche für gleiche Aufgaben genutzt werden
 - Systeme, welche den gleichen Schutzbedarf aufweisen
- Die bei der Komplexitätsreduktion entstandenen Gruppen werden fortan wie einzelne Objekte behandelt
- Wichtig: Keine Komponenten mit zu unterschiedlichem Schutzbedarf zusammen fassen, Beispiele:
 - Clients der Geschäftsleitung nicht in Gruppe der ‘normalen’ Clients integrieren
 - Dito für Clients von Entwicklungsabteilung, Personalabteilung, Buchhaltung und IT-Administration
 - Sie alle haben einen erhöhten Schutzbedarf

Beispiel für das Resultat einer Komplexitätsreduktion (Gruppen gleichartiger Komponenten)

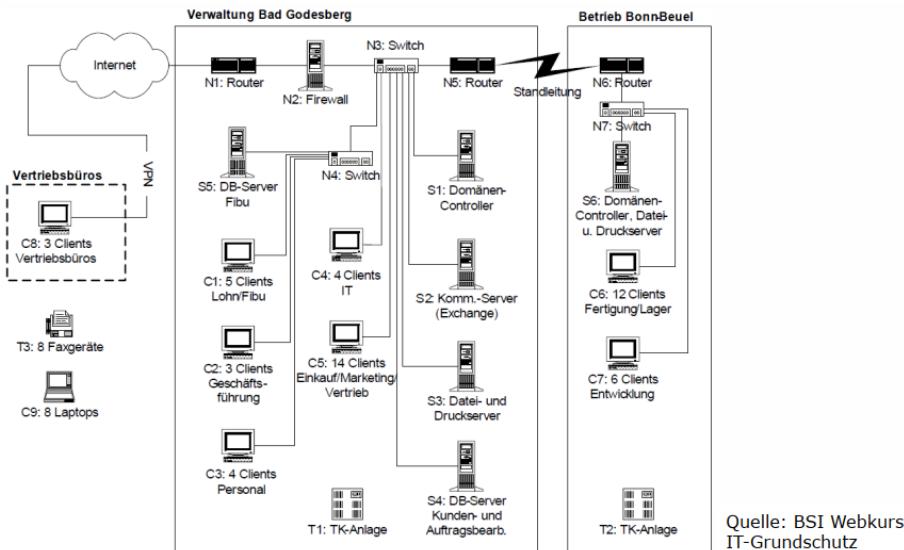


Abbildung 69: Komplexitätsreduktion

Nr.	Beschreibung	Plattform	Standort	Anzahl	Status	Benutzer/Administrator
S1	Domänen-Controller	Windows Server 2003	BG, R. 1.02 (Serverraum)	1	in Betrieb	alle IT-Benutzer/IT-Administration
S4	DB-Server Kunden- und Auftragsbearbeitung	Windows Server 2003	BG, R. 1.02 (Serverraum)	1	in Betrieb	Marketing und Vertrieb, Fertigung, Lager/IT-Administration
C5	Clients Kunden- und Auftragsbearbeitung	Windows Vista	BG, R. 2.03 – 2.09	14	in Betrieb	Einkauf, Marketing und Vertrieb/IT-Administration
C7	Clients in Entwicklungsabteilung	Windows Vista	Beuel, R. 2.14 – 2.20	6	in Betrieb	Entwicklung/IT-Administration
C8	Clients in Vertriebsbüros	Windows Vista	Vertriebsbüros (Berlin, Hamburg, München)	3	in Betrieb	Mitarbeiter in Vertriebsbüros/IT-Administration
N4	Switch für Personalabteilung	Switch	BG, R. 1.02 (Serverraum)	1	in Betrieb	alle IT-Benutzer/IT-Administration
N5	Router zur Anbindung des Standorts Beuel	Router	BG, R. 1.02 (Serverraum)	1	in Betrieb	alle Mitarbeiter in BG/IT-Administration
T1	Telefonanlage BG	ISDN-TK-Anlage	BG, R. 1.01	1	in Betrieb	alle Mitarbeiter in BG/IT-Administration

Abbildung 70: Erhebung IT-Systeme

IT-Strukturanalyse –Erhebung IT-Systeme

IT-Strukturanalyse - Zuordnung von Systemen und Anwendungen

- Der Schutzbedarf eines IT-Systems hängt vom Schutzbedarf der Anwendungen ab, welche es unterstützt
- IT-Systeme (Server, Clients) und Anwendungen werden einander deshalb zugeordnet

Nr.	Beschreibung	Personenbezogene Daten	C2	C5	C6	C8	C9	S1	S3	S4	S6
A4	Auftrags- und Kundenverwaltung	X		X	X	X	X			X	
A5	Benutzeroauthentisierung	X						X			X
A9	Druckservice BG								X		
A10	Druckservice Beuel										X
A13	Application Gateway										

A = Anwendung, S = Server, C = Client

Quelle: BSI Webkurs IT-Grundschutz

Abbildung 71: Zuordnung in Gruppen

- Für den Schutzbedarf eines Systems ist diejenige Anwendung mit den höchsten Sicherheitsanforderungen (bezüglich Vertraulichkeit, Integrität und Verfügbarkeit) relevant
- Es gilt das sog. Maximumprinzip (vgl. zugehörige Folien)

Schutzbedarfsfeststellung

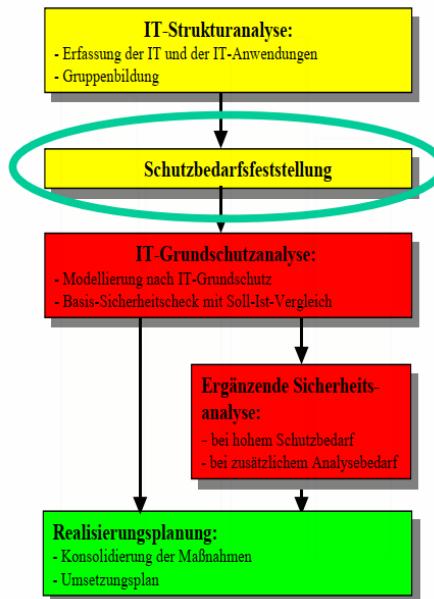


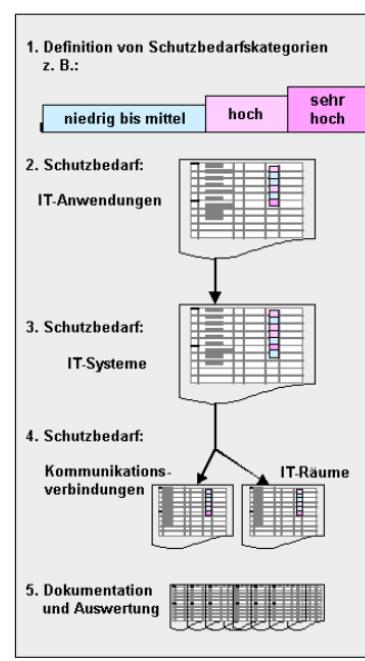
Abbildung 72: Schutzbedarfsfeststellung

Schutzbedarfsfeststellung - Ziel

- Bestimmung des Schutzbedarfs des betrachteten Informationsverbunds
- Zu beantwortende Fragen:
 - Wie viel Schutz benötigen die identifizierten Objekte?
 - Wie kommt man zu einer begründeten und nachvollziehbaren Einschätzung des Schutzbedarfs?
 - Welche Objekte haben einen erhöhten Schutzbedarf?

Schutzbedarfsfeststellung – Vorgehen

- Definition der Schutzbedarfskategorien entsprechend der Besonderheiten der Organisation (sog. Individualisierung)
- Schutzbedarfsfeststellung
 - von IT-Anwendungen und Daten
 - davon abgeleitet von IT-Systemen
 - davon abgeleitet von Kommunikationsverbindungen und IT-Räumen
- Dokumentation und Interpretation der Ergebnisse



Quelle: BSI Webkurs IT-Grundschatz

Abbildung 73: Vorgehen bei Schutzbedarf

Schutzbedarfsfeststellung – Schutzbedarfskategorien Die IT-Grundschutz-Vorgehensweise empfiehlt drei Schutzbedarfskategorien anhand der maximalen Schäden und Folgeschäden bei Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit:

- **Normal / Niedrig bis mittel**
Begrenzte und überschaubare Schäden
- **Hoch**
Beträchtliche Schäden möglich
- **Sehr hoch**
Existentiell bedrohliche, katastrophale Schäden möglich

Schutzbedarfsfeststellung – Individualisierung der Kategorien

- Die Definition der Auswirkungen von Schadensereignissen einer bestimmten Kategorie muss die individuellen Eigenschaften resp. Besonderheiten der Organisation berücksichtigen
- Folgende typischen Schadszenarien können der Definition zu Grunde gelegt werden
 - Verstoss gegen Gesetze/Vorschriften/Verträge
 - Beeinträchtigung des informationellen Selbstbestimmungsrechts
 - Beeinträchtigung der persönlichen Unversehrtheit
 - Beeinträchtigung der Aufgabenerfüllung
 - Negative Aussenwirkung (Imageschäden)
 - Finanzielle Auswirkungen

Schutzbedarfsfeststellung – Abhängigkeiten / Vererbung von Schutzbedarf

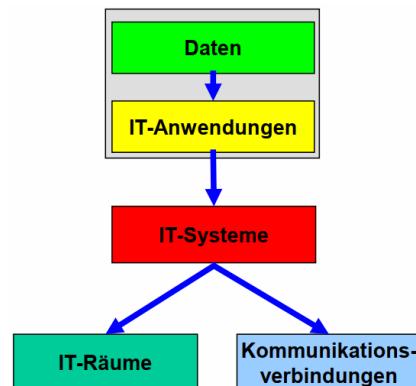


Abbildung 74: Vererbung Schutzbedarf

Schutzbedarfsfeststellung – Maximumprinzip

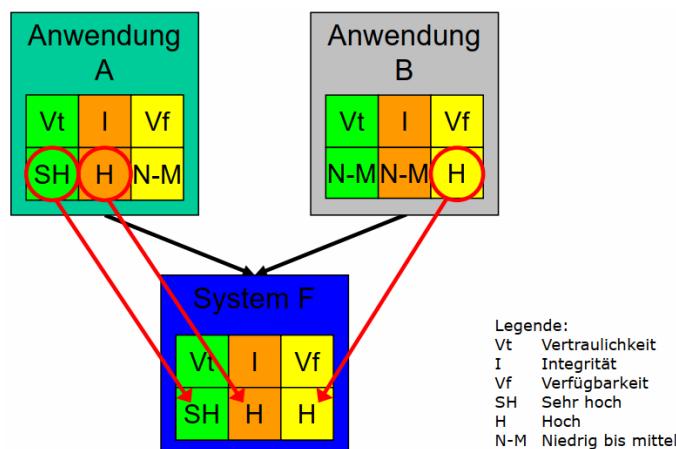


Abbildung 75: Schutzbedarf - Maximumprinzip

Schutzbedarf feststellung – Regeln

- **Maximumprinzip**

Höchster Schutzbedarf der Anwendungen, welche ein System nutzen, gilt für das System

- **Kumulationseffekt**

System hat höheren Schutzbedarf als die zugeordneten Anwendungen (höherer Schaden aufgrund von gleichzeitigem Ausfall von mehreren Anwendungen)

- **Verteilungseffekt**

System hat niedrigeren Schutzbedarf als die zugeordnete Anwendung (Anwendung ist auf mehrere Systeme verteilt; auf dem betrachteten System laufen nur weniger wichtige Teile davon)

Schutzbedarf feststellung – Schutzbedarf von IT-Anwendungen

- Für alle IT-Anwendungen muss der Schutzbedarf für die drei Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität bestimmt werden
- Grundlage: Schutzbedarf der verarbeiteten Daten
- Hilfsmittel: Die definierten Schadenszenarien
- Die Szenarien müssen dabei aus der Sicht der Nutzer der IT-Anwendungen betrachtet werden
⇒ ‘Was wäre, wenn...’-Fragen stellen
- Die evaluierten Schutzbedarfskategorien müssen begründet und dokumentiert werden (auch für die GL verständlich!)

Schutzbedarf feststellung – Schutzbedarf von IT-Anwendungen

Schutzbedarf feststellung			
Nr.	Bezeichnung	Schutzbedarf	Begründung
A1	Personaldatenverarbeitung	Vertraulichkeit: hoch	Personaldaten sind besonders schutzbedürftige Daten, deren Missbrauch die Betroffenen erheblich beeinträchtigen kann.
		Integrität: normal	Fehler werden rasch erkannt und können entweder aus der Datensicherung eingespielt oder durch Eingabe korrigiert werden.
		Verfügbarkeit: normal	Ausfälle bis zu einer Woche können mit manuellen Verfahren überbrückt werden.
A5	Benutzerauthentisierung	Vertraulichkeit: normal	Die Passwörter sind verschlüsselt gespeichert und damit praktisch nicht zugänglich.
		Integrität: hoch	Der hohe Schutzbedarf ergibt sich daraus, dass sich alle Mitarbeiter hierüber identifizieren.
		Verfügbarkeit: hoch	Bei Ausfall dieser Anwendung ist keine Identifizierung und damit keine Ausführung von IT-Verfahren möglich. Ein Ausfall ist allenfalls bis zu 24 Stunden tolerabel.
A12	Internet-Zugang	Vertraulichkeit: normal	Es werden keine vertraulichen Daten verarbeitet.
		Integrität: normal	Fehlerhafte Daten können in der Regel leicht erkannt werden.
		Verfügbarkeit: hoch	Die Recherche im Internet ist für einige Abteilungen wichtig (insbesondere die Einkaufsabteilung). Ein Ausfall ist höchstens 24 Stunden hinnehmbar.

Abbildung 76: Schutzbedarf IT-Anwendungen

Schutzbedarf feststellung – Schutzbedarf von IT-Systemen

IT-System		Schutzbedarf feststellung	
Nr.	Bezeichnung	Schutzbedarf	Begründung
S1	Domänen-Controller	Vertraulichkeit: normal	Maximumprinzip gemäß Anwendung A5 (Benutzerauthentisierung)
		Integrität: hoch	Maximumprinzip gemäß Anwendung A5 (Benutzerauthentisierung)
		Verfügbarkeit: normal	Gemäß Anwendung A5 (Benutzerauthentisierung) wäre der Schutzbedarf hoch. Er wurde als normal festgelegt, weil die Benutzer aus Bad Godesberg sich auch über den Domänen-Controller S6 in Beuel anmelden können. Ein Ausfall bis zu drei Tagen ist hinnehmbar (Verteilungseffekt).
S2	Kommunikationsserver	Vertraulichkeit: hoch	Maximumprinzip gemäß Anwendung A7 (E-Mail)
		Integrität: hoch	Maximumprinzip gemäß Anwendung A7 (E-Mail)
		Verfügbarkeit: hoch	Maximumprinzip gemäß Anwendung A7 (E-Mail)
S5	DB-Server Finanzbuchhaltung	Vertraulichkeit: hoch	Maximumprinzip, da hohe Vertraulichkeit bei Anwendungen A1 (Personaldatenverarbeitung) und A3 (Finanzbuchhaltung)
		Integrität: hoch	Maximumprinzip von Anwendung A3 (Finanzbuchhaltung)
		Verfügbarkeit: normal	Ausfälle können mittels manueller Verfahren überbrückt werden.

Abbildung 77: Schutzbedarf IT-System

Schutzbedarf feststellung – IT-Räume

- Vererbung und Maximumprinzip berücksichtigen: Schutzbedarf bemisst sich am Schutzbedarf der ITSysteme und der Informationen, welche im IT-Raum gelagert und verarbeitet werden
- Evtl. müssen Kummulationseffekte berücksichtigt werden: Höherer Schutzbedarf als für die einzelnen Objekte im Raum, z. B. bei gespiegelten (redundanten) Servern mit normalen Verfügbarkeitsanforderungen (Erklärung?)
 - Antwort: Zwei redundante Server im gleichen Raum erhöhen den Schutzbedarf des Raums, da beim Ausfall des Raums das redundante System als Ganzes nicht mehr verfügbar ist.

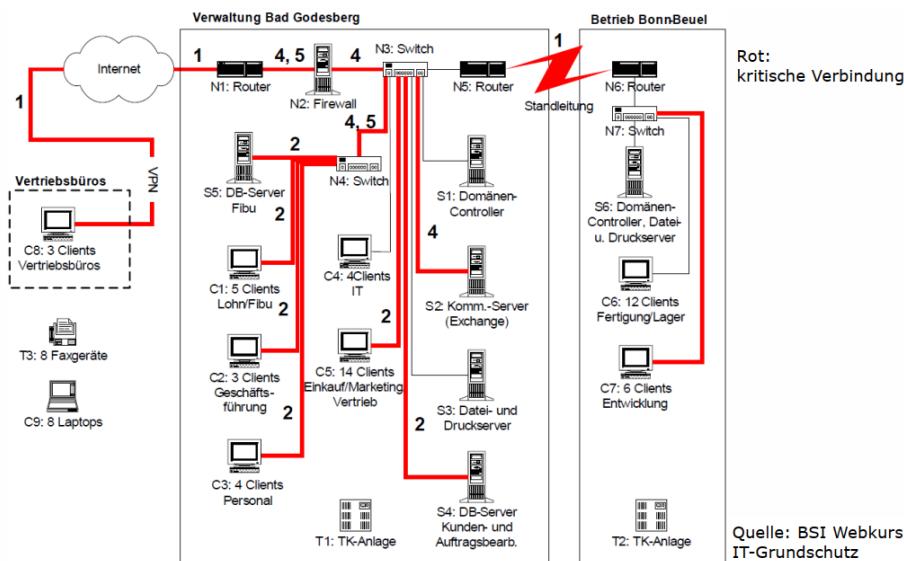
Raum			Schutzbedarf			
Bezeichnung	Art	Lokation	IT-Systeme	Vertraulichkeit	Integrität	Verfügbarkeit
BG, R. 1.01	Technikraum	Verwaltungsgebäude	TK-Anlage T1	normal	normal	hoch
BG, R. 1.02	Serverraum	Verwaltungsgebäude	S1 bis S5 N1 bis N5	hoch	hoch	hoch
Beuel, R. 2.01	Serverraum	Produktionshalle	S6, N6, N7	normal	normal	normal
Beuel, R. 2.10 – 2.13	Büroräume	Produktionshalle	C6, einige mit Faxgeräten	hoch	normal	normal

Quelle: BSI Webkurs IT-Grundschutz

Abbildung 78: Schutzbedarf IT-Räume

Schutzbedarf feststellung – Kommunikationsverbindungen

- Folgende Verbindungen sind als kritisch einzustufen
 - Verbindungen in ein öffentliches Netz (Internet, Telefonnetz etc.) oder über öffentlichen Grund
 - Verbindungen, über die besonders schützenswerte Informationen übertragen werden
 - Verbindungen, über die vertrauliche Informationen nicht übertragen werden dürfen
- Der Schutzbedarf der übertragenen Informationen leitet sich vom Schutzbedarf der miteinander verbundenen IT-Systeme ab



IT-Grundschutzzanalyse – Modellierung nach IT-Grundschutz

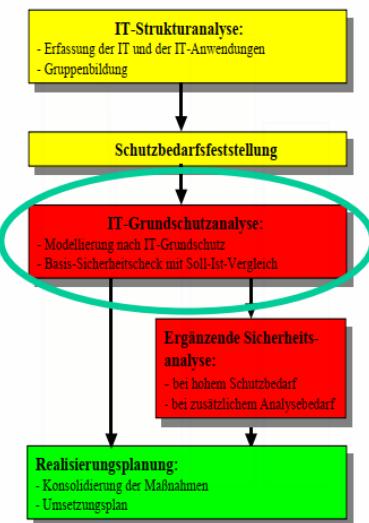
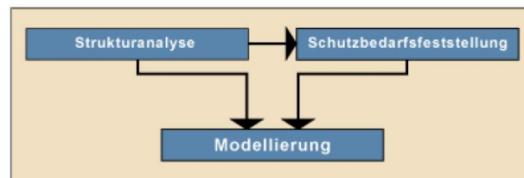


Abbildung 80: IT-Grundschutzzanalyse

- Nachbilden des erhobenen IT-Verbunds mit Hilfe der vorgegebenen IT-GrundschutzzBausteine
- Ergebnis: **IT-Grundschutzz-Modell**



Quelle: BSI Webkurs IT-Grundschutz

Abbildung 81: IT-Grundschutzz-Modell

- Die Modellierung erfolgt entsprechend dem Schichtenmodell der IT-GrundschutzzBausteine (Total 85 Bausteine)
- Schichtweise werden diejenigen Bausteine ausgewählt, welche für die Sicherheit des IT-Verbunds notwendig sind
- Ausgewählte Bausteine werden dem jeweiligen Zielobjekt (IT-Systeme, Räume etc.) zugeordnet
- Bei Bedarf können Bausteine im Rahmen der Modellierung modifiziert werden (z. B. Ergänzung um zusätzliche Massnahmen oder Konkretisierung von technischen Details)

Wichtig: Abschliessende Prüfung auf Vollständigkeit durchführen

- Alle übergreifenden Aspekte berücksichtigt?
- Alle Gebäude, Räume, Schutzschränke inkl. Verkabelung im Hinblick auf infrastrukturelle Sicherheit berücksichtigt?
- Alle IT-Systeme einbezogen?
- Alle netzwerktechnischen Sicherheitsaspekte berücksichtigt?
- Alle Anwendungen berücksichtigt?
- Alle Objekte ohne unmittelbar passenden Baustein durch andere Bausteine angemessen modelliert?

Baustein	Zielobjekt	Hinweise
B.1.4 Datensicherungskonzept	Gesamte Organisation	Gilt einheitlich für alle Betriebsteile.
B.2.1 Gebäude	Verwaltungsgebäude	Der Baustein muss auf beide Gebäude getrennt angewendet werden.
B.2.1 Gebäude	Produktionshalle	
B.2.4 Serverraum	Serverraum BG, R. 1.02	Der Baustein muss auf beide Serverräume getrennt angewendet werden.
B.2.4 Serverraum	Serverraum Beuel, R. 2.05	
B.3.203 Laptop	C9	Die Laptops in den Vertriebsbüros, in Bad Godesberg und in Beuel werden von den Vertriebsmitarbeitern benutzt und sind in einer Gruppe zusammengefasst.
B.5.7 Datenbanken	A3 Finanzbuchhaltung	Die Datenbanksysteme unterscheiden sich bezüglich ihrer Server, ihrer Benutzer und ihres Schutzbefehls. Der Baustein ist daher getrennt auf beide Anwendungen anzuwenden.
B.5.7 Datenbanken	A4 Auftrags- und Kundenverwaltung	

Quelle: BSI Webkurs IT-Grundschutz

Abbildung 82: IT-Grundschutz Modellierung

IT-Grundschutzzanalyse – Basis-Sicherheitscheck Der Basis-Sicherheitscheck soll folgende Fragen beantworten:

- Sind meine Informationen hinreichend geschützt?
- Was bleibt noch zu tun?

Vorgehen:

- Bereits umgesetzte Massnahmen mit den Empfehlungen der IT-Grundschutz-Kataloge vergleichen

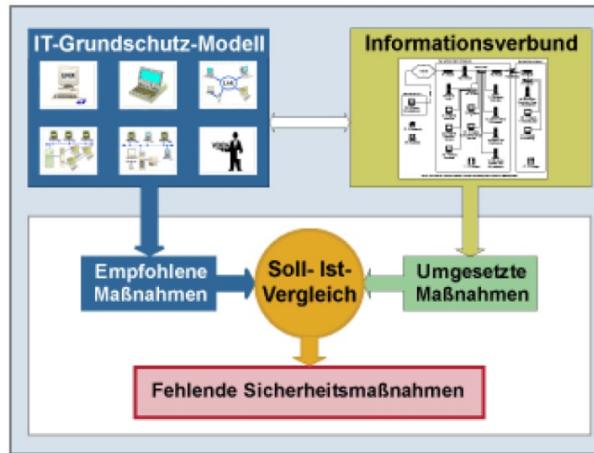


Abbildung 83: Fehlende Sicherheitsmassnahmen beim Basis-Grundschutz müssen ergänzt werden

Vorgehen im Detail:

- Organisatorische Vorarbeiten leisten
- Soll-Ist-Vergleich durchführen
- Ergebnisse dokumentieren

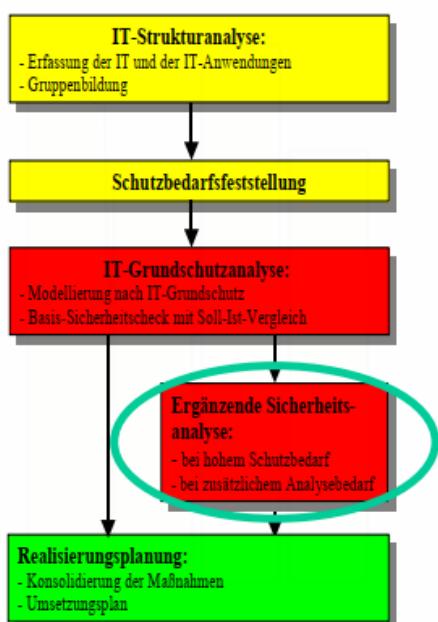
Organisatorische Vorarbeiten:

- Vorhandene Dokumente sichten
- Bezug externer Stellen klären/organisieren (Provider, Outsourcing-Partner etc.)
- Ermittlung der Interviewpartner (entsprechend Schichtenmodell)
 - Übergeordnete Aspekte: Personalabteilung, konzeptionell Verantwortliche etc.
 - Infrastruktur: Haustechnik, evtl. Externe
 - IT-Systeme / Netze: System- / Netzadministratoren
 - IT-Anwendungen: Anwendungsverantwortliche
- Termine planen

Soll-Ist-Vergleich:

- Erheben des Umsetzungsstatus der einzelnen Massnahmen mithilfe der Interviews
- Mögliche Umsetzungsstati
 - **Entbehrlich:**
benötigt immer eine Begründung!
 - **Ja:**
Massnahme vollständig umgesetzt
 - **Teilweise:**
Einzelne Aspekte nicht umgesetzt
 - **Nein:**
Massnahme überwiegend nicht umgesetzt
- Wichtig
 - Interviews dienen auch der Sensibilisierung
 - Aussagen verifizieren, Stichproben durchführen

Ergänzende Sicherheitsanalyse



Sie ist durchzuführen, wenn für einzelne Zielobjekte

- die Schutzbedarfskategorie 'hoch' oder 'sehr hoch' in mindestens einem der drei Grundwerte vorliegt,
- kein geeigneter Baustein im BausteinKatalog zu finden ist oder
- Objekte in untypischer Weise oder Einsatzumgebung betrieben werden

Abbildung 84: Ergänzende Sicherheitsanalyse

Ergänzende Sicherheitsanalyse - Ergebnis

- Ergebnis der ergänzenden Sicherheitsanalyse
 - Grundschutzmassnahmen – allenfalls der Siegelstufe 'zusätzlich' – genügen oder
 - Es sind weitergehende Untersuchungen, z. B. eine klassische Risikoanalyse, notwendig

Ergänzende Sicherheitsanalyse – Vorgehensweisen für weitere Untersuchungen

- Klassische Risikoanalyse
 - relevante Bedrohungen oder Schwachstellen ermitteln
 - Eintrittshäufigkeiten und Schadenshöhen schätzen
- Penetrationstest
 - Verhalten eines Angreifers simulieren
 - Blackbox- und Whitebox-Ansatz unterscheiden
- Differenz-Sicherheitsanalyse
 - Feststellen, welche der Sicherheitsmaßnahmen über die Grundschutzmaßnahmen hinausgehend realisiert sind
 - Vergleich durchführen, ob die ergriffenen Massnahmen den 'Best Practices' entsprechen, die sich in der Praxis für hochschutzbedürftige IT-Bereiche etabliert haben

Realisierungsplanung

- Ergebnisse sichten (fehlende Sicherheitsmaßnahmen zusammenstellen)
- Massnahmen konsolidieren (überfl. M. streichen, verbleibende konkretisieren >Massnahmenliste)
- Aufwand schätzen (finanziell, personell / einmalig, wiederkehrend)
- Umsetzungsreihenfolge festlegen (zuerst diejenigen, welche Voraussetzung für andere sind)
- Verantwortliche und Termine bestimmen (für Realisierung und Überwachung von jeder Maßnahme)
- Begleitende Massnahmen festlegen (*Sensibilisierung und Schulung*)
- Ergebnis: Realisierungsplan

Zielobjekt: BG R. 1.02 Serverraum Baustein: B 2.4 Serverraum				
Maßnahme (erforderlich ab Siegelstufe)	Umsetzung bis	Verantwortlich	Budget	Bemerkungen
M 1.3 (A) Angepasste Aufteilung der Stromkreise	38. KW	Umsetzung: M. Wachsam Kontrolle: P. Muster	a) 0,- € b) 0,3 PT c) 0,- € d) 0 PT/Jahr	Die Elektro-Installation wird von der Haustechnik geprüft. Eine mindestens jährliche Überprüfung wird festgelegt.
M 1.7 (A) Handfeuerlöscher	38. KW	Umsetzung: M. Wachsam Kontrolle: P. Muster	a) 0,- € b) 0,3 PT c) 0,- € d) 0 PT/Jahr	Alle Mitarbeiter mit Zugangsberechtigung zum Serverraum sollen in die Handhabung der vorhandenen CO2-Löscher eingewiesen werden.
Z1: Einbau von Wasser ableitenden Blechen und Installation eines Wassermelders mit Sirene	39. KW	Umsetzung: M. Wachsam Kontrolle: P. Muster	a) 500,- € b) 1 PT c) 0,- € d) 0 PT/Jahr	Diese Maßnahme ersetzt Maßnahme M 1.24.

Legende: Z = Zusatzmaßnahme, PT = Personenzahl, KW = Kalenderwoche
 a) Einmalige Investitionskosten b) Einmaliger Personalaufwand
 c) Wiederkehrende Kosten d) Wiederkehrender Personalaufwand

Quelle: BSI Webkurs
IT-Grundschutz

Abbildung 85: Beispiel eines Realisierungsplans

Beispiel eines Realisierungsplans

Zusammenfassung

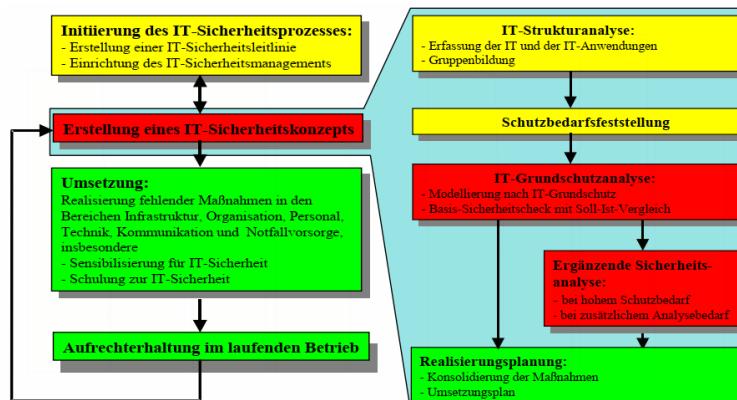


Abbildung 86: IT-Strukturanalyse Zusammenfassung

9 Awareness

Sie verstehen die Wichtigkeit der „Awareness“

Bedeutung In Verbindung mit der IT: Sich bewusst sein, wie Wertvoll Informationen sind und welches Ausmass es haben kann, wenn diese an Unbefugte gelangen. Wie z.B. Passwörter für den Fernzugriff auf die wichtigsten Servern.

Ziel Awareness hat zum Ziel, den Faktor Mensch gebührend in einer holistischen¹⁴ Sicht der Informations-sicherheit zu würdigen, weil die anderen beiden Säulen - Technik und Prozess-Aspekte - keine ausreichende Sicherheit bieten. Wichtig für die Nachhaltigkeit ist daher eine grundsätzliche Schulung der Mitarbeitenden mit regelmässigen **Kampagnen**, begleitet von **flankierenden Massnahmen**, essentiell.

Sie kennen verschiedene Prozesse und Vorgehensweisen für die Initiierung, Durchführung und Erfolgsprüfung einer Awareness-Kampagne und können diese anwenden

Prozess Der Awareness-Prozess im ISO 27002 beschreibt den Prozess in etwa wie folgt:

- Alle Mitarbeitenden und Lieferanten des Unternehmens sollten im Zusammenhang mit der von ihnen ausgeführten Tätigkeiten, bewusstseinsbildende Ausbildungen und Trainings ausführen, sowie regelmässige Updates von Bestimmungen und Verfahren erhalten.
- Das Ziel eines Awareness-Programms ist es, das Bewusstsein von Mitarbeitenden und Lieferanten auf sicherheitsrelevante Bestimmungen und Verfahren einzuhalten, um Firmeninformationen zu schützen.
- Das Unternehmen soll bewusstseinsbildende Aktivitäten Planen, wie Kampagnen (z.B. Information Security Day), Broschüren oder Newsletter erstellen
- Die Aktivitäten des Awareness-Programms sollten in regelmässigen Abständen stattfinden.
- Das Awareness-Programm sollte auch regelmässig erneuert werden, um von erlebten Vorfällen im Bereich der Informationssicherheit zu lernen

Prozess der Verhaltensänderung

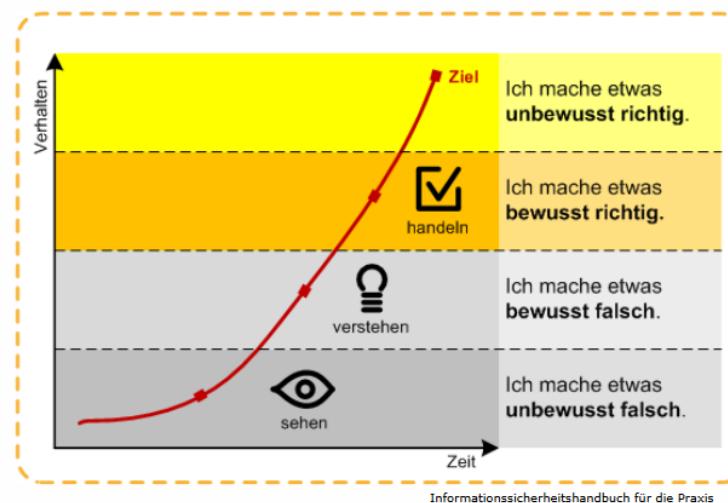


Abbildung 87: Prozess der Verhaltensänderung

Awareness und deren Bedeutung im Unternehmen

- Awareness muss vom obersten Management unterstützt werden!
- Awareness stufengerecht schulen
 - Benutzer/Anwender
 - IT-Mitarbeiter
 - Management
- Schon „kleine“ Massnahmen können die Informationssicherheit wesentlich erhöhen. „Weniger ist mehr“.

¹⁴ganzheitlich

Zeitlicher Ablauf eines Awareness-Programms

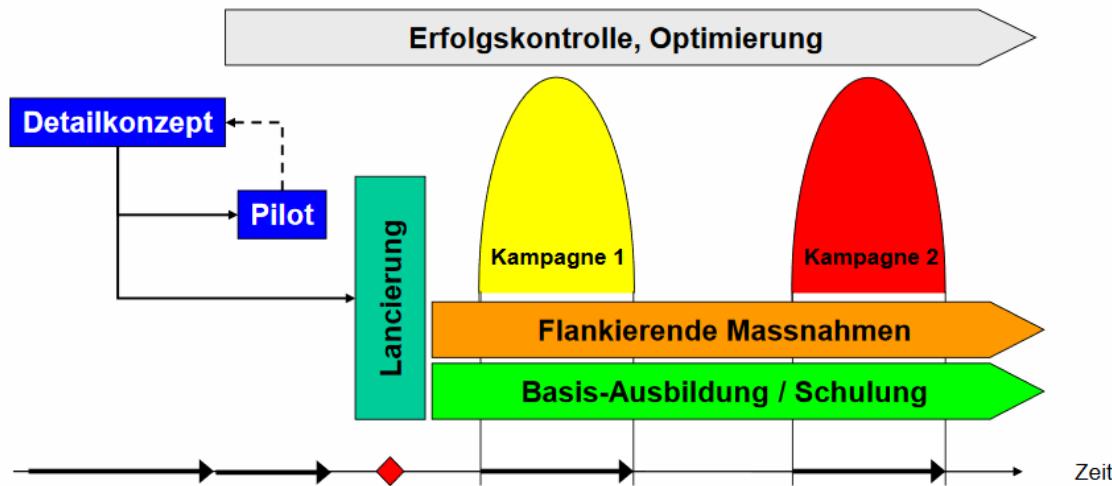


Abbildung 88: Basisausbildung, Kampagnen und flankierende Massnahmen

Umsetzung wie folgt: Basisausbildung, Kampagnen und flankierende Massnahmen

Umgang mit Verstößen

- Verletzungen der Vorschriften in der IT-Security können zu grossen Schäden führen
- Sanktionen sind zu definieren und anzuwenden (Unterstützung des Managements notwendig)
- „Thema geht alle an“, Verstöße melden
- Kein Kavaliersdelikt
- Auswertung von Aufzeichnungen

Sie kennen die relevanten Erfolgsfaktoren der Mitarbeiter-Sensibilisierung und -Schulung und können diese in einer Kampagne umsetzen

Mitarbeiter müssen über ihre Verantwortung aufgeklärt und entsprechend geschult werden. Mittels wiederkehrenden Kampagnen kann die Sensibilität für Informationssicherheit gesteigert, bzw. aufrechterhalten werden. Ein Awareness-Programm sollte wie Informationssicherheits Policies gepflegt und etabliert werden.

Erfolgreiche Awareness-Kampagnen zeichnen sich durch eine systematische Planung und Durchführung funktions- und stufengerechter Aktivitäten und Massnahmen aus. Diese sollen immer mit dem Ziel, eine nachhaltige Verhaltensänderung zu bewirken wiederkehrend konzipiert und umgesetzt werden. Aktivitäten und Massnahmen sollen in jeweils kleineren Umfang durchgeführt werden (weniger ist mehr).

Teil V

Access Control (SW 10)

10 Access Control

Sie kennen verschiedene Arten der Authentisierung, wissen wie diese technisch ablaufen und was deren Vor- und Nachteile sind

Methoden der Authentisierung

- Etwas, das ich weiss (**Wissen**)
 - Passwort
 - Pin
 - Sicherheits- / Geheimfragen
- Etwas, das ich habe (**Besitz**)
 - Physikalischer Schlüssel
 - Magnetstreifenkarte
 - Hardware-Token¹⁵
- Etwas, das ich bin (**Eigenschaft** / körperliches Merkmal)
 - Foto
 - Fingerabdruck
 - Iris
- Etwas, das ich kann (**Fähigkeit**)
 - Unterschrift
 - Stimmenerkennung (Sprechen)

Wissen

Vorteil

- man benötigt keine zusätzlichen Hilfsmittel

Nachteil

- kann vergessen oder (v)erraten werden (Passwort, Geheimfragen)

Besitz

Vorteil

- kann benutzerindividuelle Daten speichern
- kann sich selbst schützen und aktiv verändern (SedurID, Smartcard)

Nachteil

- Verwaltung des Besitzes ist unsicher und muss mitgeführt werden
- kann verloren gehen (Schlüssel, Karte, HW-Token)

Eigenschaft / körperliches Merkmal

Vorteil

- kann nicht verloren werden
- kann nicht an Dritte weitergegeben werden

Nachteil

- benötigt zur Erkennung spezielle Vorrichtung (Technik)
- fälschliche Akzeptanz/Zurückweisung möglich

Fähigkeit

Vorteil

- ziemlich einmalig, schwierig zu kopieren

Nachteil

- kann von Nachahmern imitiert werden
- kann Probleme beim Datenschutz aufwerfen

¹⁵z.B. Kartenleser für E-Banking

Sie wissen wie verschiedene Authentisierungstoken technisch funktionieren, was deren Vor- und Nachteile sind und wie sie beim Login oder bei der Transaktionsbestätigung im e-Banking eingesetzt werden

Token Bei einem Token, resp. Security-Token, handelt es sich um eine Hardwarekomponente zur Authentisierung von Usern, welche neben weiteren Sicherheitsmerkmalen wie PIN oder Passwort zur Anwendung kommt.

Vergleich verschiedener Authentisierungsmethoden

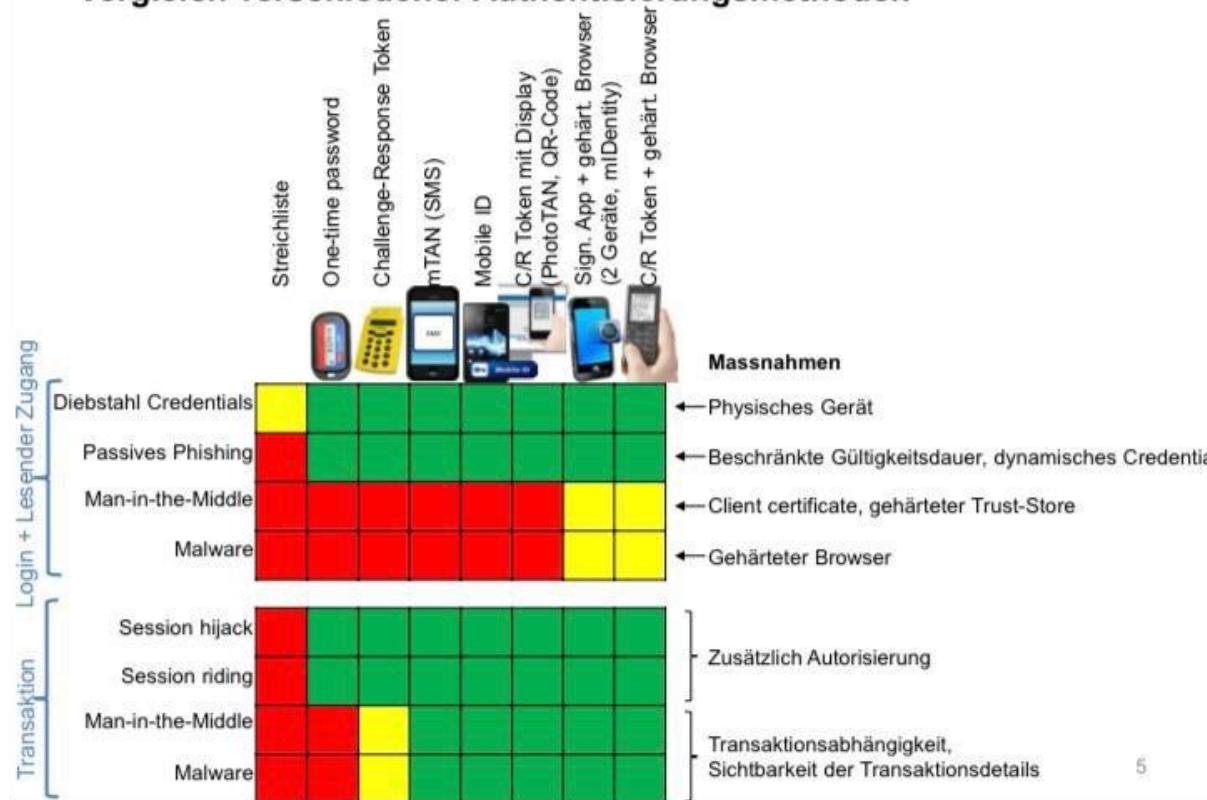


Abbildung 89: Verschiedene Varianten von Token und Authentisierungsmethoden

Vorteil

- Mehr Sicherheit
- Wenn Token verloren geht: für Unbefugte ohne OTP¹⁶ unmöglich zu verwenden

Nachteil

- Etwas zeitaufwändiger als nur ein Passwort
- Braucht Komponenten um zu funktionieren

¹⁶Siehe One-time pad, Seite 11

Sie wissen was Authentisierung, Autorisierung ist, warum diese wichtig sind und wie Angriffe darauf ablaufen

Begriffe Bei der Zugriffskontrolle unterscheidet man drei Begriffe:

Authentisierung Die Authentisierung ist ein **Nachweis einer Person**, dass sie tatsächlich die Person ist, die sie vorgibt zu sein.

- geheime Information, dass nur ihr bekannt ist (Passwort)
- Identifizierungsgegenstand (z.B. Identitätskarte)
- sie ist selbst das Identifizierungsobjekt (z.B. Fingerabdruck)

Authentifizierung Die Authentifizierung ist die **Prüfung der behaupteten Authentisierung**. Die Authentifizierung wird von einem **Prüfer** durchgeführt. Der Prüfer überprüft die Echtheit der Authentisierung.

Autorisierung Die Autorisierung räumt Rechte für die Nutzung von speziellen Diensten und Leistungen ein.

Auf die IT übertragen Beispiel für ein Editor auf einer Wordpress Seite

- Authentisieren: Logindaten eingeben
- Authentifizieren: Server überprüft die Logindaten
- Autorisierung: als Editor hat man mehr Rechte als ein registrierter Benutzer, der z.B. nur Kommentare schreiben darf. Man darf eigene Blogbeiträge schreiben, bearbeiten und löschen. Nicht jedoch von Co-Autoren, dies darf nur der Administrator. Weiter hat der Editor Zugang zu einer Verwaltungsseite mit seinen Blogbeiträgen. Etc.

Fehlerhafte Authentisierung

- Unzureichend gegen Brute-Force geschütztes Login
- Keine Verhinderung von schwachen Passwörtern
- Keine 2-Faktor Authentisierung
- Unsicherer Passwort recovery/reset Prozess
- Passwörter werden Klartext oder mit schwachen Hashfunktionen gehasht

Gegenmassnahmen

- Anzahl Loginversuche limitieren
- Passwortpolicy, welche unsichere Passwörter verhindert
- Multi-Faktor Authentisierung
- Sicherstellen, dass alle Loginmöglichkeiten dieselbe Sicherheitsanforderungen erfüllen
- Logininformationen sicher speichern

Teil VI

Multi-Party-Computation (SW 11)

11 Cryptographic Protocols

Sie kennen einfache Beispiele von verteilten sicheren Berechnungen und verstehen wie die entsprechenden Protokolle ablaufen

Beispiel Eine Rechnung wird an alle Teilnehmenden aufgeteilt und jede Partei weiss nur ihren Teil (Polynom). Werte des eigenen Polynoms werden an die anderen Teilnehmer verteilt, ein Wert wird selbst behalten. Um das Resultat zu erhalten, müssen alle zusammen ihre Werte zusammenrechnen, diese Werte sind dann die Punkte auf dem Graph des Resultats. Wenn mindestens die Hälfte der Teilnehmenden fair spielen, ist es nicht möglich, das Resultat oder die Teile der anderen Parteien herauszufinden. Das System kann umgangen werden, wenn jemand eine nichterlaubte Rechnung macht oder die letzte Person, die ihr Resultat teilt, ihre Antwort so anpasst, dass das resultierende Polynom ihre gewünschte Antwort ergibt.

12 Secret Sharing

- Absicherung eines Geheimnisses gegen Verrat durch einzelne
 - Einzelpersonen haben nur Teilinformationen
 - Geheimnis kann aus Teilinformation rekonstruiert werden
- Schutz der Gruppe gegen Blockade durch einzelne
 - Geheimnis kann von Teilgruppe rekonstruiert werden
- Sicherheitsschwelle abhängig von Bedeutung des Geheimnisses

Sie kennen Arten von Sicherheit von verteilten sicheren Berechnungen und wie diese angegriffen werden können

Beispiel Verwendung des linearen Secret-Sharing-Protokolls, um sicher zu bestimmen, wie viele Personen in die Badi gehen wollen.

- Alice wählt drei shares a_a, a_b, a_c , sodass $a_a + a_b + a_c = a \bmod 3$, wobei a Alice's Input ist.
- Alice sendet a_a an Alice, a_b an Bob und a_c an Charlie über den paarweisen geheimen Kommunikationskanal.
- Auf gleiche Art und Weise sharen Bob und Charlie ihre Inputs zwischen den drei Spielern.
- Jeder Spieler addiert seine Shares modulo 3, i.e., Alice berechnet $r_a = a_a + b_a + c_a \bmod 3$ und analog für Bob und Charlie.
- Die Spieler senden ihre Resultate an alle anderen Spieler.
- Jeder Spieler berechnet $r = r_a + r_b + r_c \bmod 3$.

Das Protokoll ist sicher gegen $n - 1$ passive Gegner. Eine obere Grenze an die Summe m wird dabei als bekannt vorausgesetzt (in diesem Beispiel 3). Nach Anpassen des Modulus können Alice, Bob und Charlie dieses Protokoll z.B. auch dafür verwenden, sicher ihren Notendurschnitt berechnen.

Shamir's Secret Sharing erlaubt das Aufteilen eines Secrets s über T Personen, wobei $n \leq T$ Personen für das Öffnen des Schlüssels benötigt werden. Dazu wird das Secret in einer Funktion $(n - 1)$ -ten Grades mit folgenden Aufbau versteckt:

$$f(x) = s + a_1 * x + a_2 * x^2 + a_3 * x^3 + \dots + x_{n-1} * x^{n-1}$$

a_i wird in diesem Fall zufällig gewählt und ist allen bekannt, während s geheim bleibt. Der Wert von s lässt sich durch Rekonstruktion der Funktion $f(x)$ anhand von n Punkten herausfinden und mittels $s = f(x=0)$ berechnen.

(Bei einer Funktion n -ten Grades werden zur Bestimmung der Funktion $n + 1$ Punkte benötigt um diese eindeutig zu bestimmen).

In einem weiteren Schritt werden die Shares p mithilfe von $x \geq 1$ berechnet (das Secret sollte geheim bleiben) und verteilt:

$$\begin{aligned} p_1 &= f(x=1) \\ p_2 &= f(x=2) \\ p_3 &= f(x=3) \\ p_i &= f(x=i) \\ p_T &= f(x=T) \end{aligned}$$

In einem letzten Schritt müssen wieder mindestens n Shares zusammenkommen, um die Funktion anhand von ihren Werten zu berechnen und damit das Secret s zu erlangen.

Dieses Protokoll ist gegen $n - 1$ Gegner sicher.

Sie wissen welche Eigenschaften elektronisches Geld ausmachen und kennen die technischen Grundlagen von Bitcoin

1. Dezentralisiert & keine Zentralbehörde In den traditionellen Fiat-Währungen kontrollieren die Zentralbehörden und Banken das Finanzsystem. Mit Bitcoin und anderen Kryptowährungen können diese Transaktionen jedoch über ein verteiltes und offenes Netzwerk, das niemandem gehört, verarbeitet und validiert werden. Im Gegensatz zu zentralisierten Banksystemen sind die meisten Kryptowährungen dezentral auf verteilten Netzwerken mit weltweit verteilten Computern, auch Knoten genannt, installiert. Transaktionen werden von den Netzwerkknoten durch Kryptographie verifiziert und in einem öffentlichen, verteilten Ledger, einer sogenannten Blockchain, aufgezeichnet. Die Transaktion wird über das Peer-to-Peer-Netzwerk verbreitet und von jedem Knoten repliziert, wobei ein grosser Prozentsatz der Knoten innerhalb weniger Sekunden erreicht wird.

2. Anonym / Pseudoanonym Da es keine Notwendigkeit für eine zentrale Behörde gibt, müssen sich die Benutzer bei Transaktionen mit Kryptocurrency nicht identifizieren. Bei einer Transaktionsanforderung wird die Transaktion vom dezentralen Netzwerk geprüft und verifiziert und entsprechend in der Blockkette erfasst. Kryptowährungen, wie Bitcoin, verwenden einen privaten Schlüssel und ein System mit öffentlichem Schlüssel, um diese Transaktionen zu authentifizieren. Das bedeutet, dass die Benutzer anonyme digitale Identitäten und digitale Brieftaschen erstellen können, um auf dem dezentralen System Transaktionen zu tätigen, und dennoch in der Lage sind, ihre Transaktionen sicher zu authentifizieren.

3. Irreversibel & Unveränderlich (kann nicht rückgängig gemacht werden) Kryptocurrency-Transaktionen sind irreversibel und unveränderlich. Die irreversiblen und unveränderlichen Eigenschaften von Cryptocurrency bedeuten, dass es für niemanden außer dem Besitzer des jeweiligen privaten Schlüssels möglich ist, seine digitalen Vermögenswerte zu verschieben, und dass Transaktionen nicht mehr geändert werden können, sobald sie in der Blockkette aufgezeichnet sind. Es ist zwar nicht unmöglich, die Transaktion zu ändern, aber die sichere Kryptographie macht eine Änderung sehr schwierig, da die meisten Knoten in der Blockkette geändert werden müssen. Um betrügerische Transaktionen (die nicht rückgängig gemacht werden können) zu verhindern, werden alle Transaktionen transparent auf der Blockkette aufgezeichnet und der Öffentlichkeit zugänglich gemacht.

4. Begrenztes Angebot & Knappheit Fiat-Währungen (z.B. Dollar, Euro) haben einen unbegrenzten Vorrat, da die Zentralbanken beliebig viele Fiat-Währungen ausgeben können. Die Zentralbanken manipulieren im Rahmen ihrer Wirtschaftspolitik häufig den Wert der Währungen der Länder. Die meisten Länder manipulieren ihre Währung oft so, dass sie über einen bestimmten Zeitraum inflationär sind. Der inflationäre Charakter von Fiat-Währungen würde einen Wertverlust der Währung im Laufe der Zeit bedeuten. Daher könnten die Inhaber von Fiat-Währungen die Kosten des Wertverlusts tragen und auch mit der Unsicherheit der Währungsmanipulation konfrontiert sein. Auf der anderen Seite haben die meisten Kryptowährungen einen begrenzten und vorher festgelegten Vorrat an der Kryptowährung, die bei ihrer Erstellung in den zugrunde liegenden Algorithmus kodiert wird. Zum Beispiel hat Bitcoin einen maximalen Vorrat von 21 Millionen, und wenn diese Grenze erreicht ist, kann keine neue Bitcoin mehr abgebaut werden. Cryptocurrency erzeugt absichtlich eine Knappheit, um Währungsmanipulationen und den Wertverlust im Laufe der Zeit zu verhindern.

Das macht es so besonders

Effizient Die Verwendung einer Peer-to-Peer-Datenbank bedeutet, dass es keine zentrale Behörde oder Zwischenhändler von Drittanbietern braucht, um Transaktionen zu bearbeiten und zu validieren. Die Benutzer können über das dezentrale System direkt miteinander kryptoelektronische Währungen abwickeln und austauschen, wobei jede Transaktion auf der Blockkette verifiziert werden kann. So kann jeder, der über das Internet verfügt, auf Knopfdruck weltweit Wertsachen austauschen. Zudem sind die Kosten für Transaktionen mit Kryptowährungen deutlich geringer als bei interkontinentalen Überweisungen.

Sicher Da die Transaktion auf einem verteilten Ledger aufgezeichnet wird, bedeutet dies außerdem, dass es keinen einzigen Punkt gibt, an dem eine Schwachstelle oder ein Ausfall auftreten kann. Jeder im Netzwerk hat eine Kopie des Ledgers, so dass kein zentrales System benötigt wird, da jede Transaktion gegen dieses Ledger verifiziert werden kann. Das dezentralisierte Ledger wird als Blockkette bezeichnet. Dies macht Transaktionen weniger anfällig für Hacking, Fehler und Systemausfälle (im Vergleich zu einem einzelnen und zentralen System), da die Informationen dezentral in einem verteilten Netzwerk gespeichert werden. Daher macht die Blockchain-Technologie, die Krypto-Währungen unterstützt, Transaktionen sicherer.

Vertrauenslos Cryptocurrency ermöglicht, wie Bitcoin, ein ‘vertrauenswürdiges’ System von Transaktionen. Das dezentrale Netzwerk bedeutet, dass niemand einem anderen vertrauen muss, damit das Netzwerk funktioniert. Die Blockkette kann jede Transaktion zwischen den Benutzern validieren. Wenn ein Benutzer eine Kryptowährungstransaktion sendet, empfangen alle Knoten diese und überprüfen, ob die digitalen Signaturen gültig sind, bevor sie in die Blockkette aufgenommen werden. Wenn die Signaturen ungültig sind, verwerfen die Knoten die Transaktion. Der Proof-of-Work-Algorithmus gibt auch einzelnen Knoten im Netzwerk einen Anreiz, diese Peer-to-Peer-Transaktionen zu validieren.

Wertsteigerung & Deflationierung Die meisten Kryptowährungen haben einen begrenzten Vorrat in ihrem Protokoll kodiert, wodurch ein System der Knappheit entsteht. Zum Beispiel hat Bitcoin ein maximales Angebot von 21 Millionen und sobald das Angebotslimit erreicht ist, wird keine neue Bitcoin mehr hinzugefügt. Dies macht die vorhandene Bitcoin, die im Umlauf ist, attraktiver und wertvoller als Vermögenswert.

Wenn die Nachfrage nach Bitcoin wächst, bleibt das Angebot gleich, was dazu führt, dass der Wert von Bitcoin im Laufe der Zeit steigt und es somit deflationär wird. Benutzer von Kryptowährung müssen sich keine Sorgen über die Wertminderung ihrer Vermögenswerte machen (im Gegensatz zu Fiat-Währungen).

13 Zero-Knowledge-Proof

Sie wissen was Zero-Knowledge-Proofs sind und wie diese ablaufen

Zero-Knowledge-Proof Das Zero-Knowledge-Proof ist eine Technik etwas zu beweisen, ohne den eigentlichen Inhalt preiszugeben.

Beispiel Paula („Proofer“) möchte Victor („Verifier“) überzeugen, dass sie die Lösung eines Sudokus kennt, ohne die Lösung im Klartext preiszugeben. Wie geht man vor?

1. Paula löst das Sudoku
2. wählt eine Permutation
3. permutiert alle Zahlen der Lösung
4. verdeckt die Lösung
5. Victor wählt aus:
 - 1 Zeile
 - 1 Spalte
 - 1 kleines Quadrat, oder
 - alle Start-Zahlen
6. Victor akzeptiert, falls er Paula nicht beim Schummeln erwischt
 - Wenn Paula eine Lösung hat, akzeptiert Victor immer
 - Wenn Paula keine Lösung hat, kann sie mit einer Wahrscheinlichkeit von $\frac{27}{28} \approx 96\%$ trotzdem durchkommen
 - ⇒ Wiederholen mit **neuer Permutation** bis Victor überzeugt ist, dass Paula die richtige Lösung hat
 - z.B. bei 150 Wiederholungen liegt die Wahrscheinlichkeit, dass Paula mit Schummeln durchkommt bei $(\frac{27}{28})^{150} < 0.5\%^{17}$
 - Victor lernt somit nichts über den Inhalt der Lösung, nur dass eine Lösung existiert und Paula sie kennt

Teil VII

Quantum (SW 12)

14 Quantum Computing and Quantum Cryptography

Sie wissen was ein Quantencomputer ist und was ihn von einem „klassischen“ Computer unterscheidet

Unterschied Ein Quantencomputer arbeitet mit Zuständen in Atomen. Ein C-Atom hat eine Grösse von unter 0.2nm, der Abstand zwischen Transistoren in einer CPU hingegen 10nm. Weiter arbeitet es mit Qubits (Quantencomputer-Bits). Anstelle von normalen Bits, kann man gewisse Probleme mit Qubits effizienter lösen als mit einem klassischen Computer.

Sie verstehen welchen Einfluss die Existenz eines Quantencomputers auf die Kryptographie hat

Differenz Quantencomputer sind gut in umkehren der vermeintlich sicheren Operationen. D.h. brute-forcing von symmetrischen Algorithmen wird einfacher.

¹⁷9 Zeilen + 9 Spalten + 9 Quadrate + Start-Zahlen

Sie verstehen wie Quantenschlüsselaustausch funktionert

Quantenschlüsselaustausch mit BB84-Protokoll Photonen werden mittels einen polarisierten Filter gefiltert. Der Filter lässt das Photon durch, wenn das Photon parallel (gerade) zum Filter steht. Gefiltert wird das Photon, falls es orthogonal (quer) zum Filter steht. Steht das Photon jedoch 45° zum Filter, besteht eine je eine 50%-ige Chance, dass das Photon entweder parallel oder orthogonal zum Filter polarisiert wird. Dabei ist das Resultat, wie das Photon polarisiert wird, gemäss Quantenmechanik zufällig.

1. Alice sendet n Photonen an Bob. Für jedes Photon wählt sie
 - eine zufällige Filterbasis (vertikal[], diagonal \diagup, \diagdown) oder horizontal [—]). Dabei muss sie achten, alle 4 Basispositionen mit gleicher Wahrscheinlichkeit auszuwählen.
 - den Wert der Polarisierung (0 oder 1). Dabei wird vorgängig definiert, dass zwei Polarisierungen eine 0 bekommen (z.B. — und \diagup), die anderen zwei 1 (| und \diagdown).
2. Bob misst jedes der Photonen in einer seinerseits zufällig gewählten Basis und erhält das Resultat, ob er ein Photon erhalten hat oder nicht (0 oder 1)
3. Um aus den erhaltenen Werten einen Schlüssel zu erzeugen, vergleichen Alice und Bob die gewählten Basen (Vertikal- und Horizontalbasis +, Diagonalbasis \times) über einen **authentifizierten Kanal**. Werte mit unterschieden Basen werden verworfen.
4. Von den Messungen mit gleicher Basis wählen sie die ersten paar Bits zur Kontrolle der Übereinstimmung, die restlichen werden zu einem Schlüssel generiert

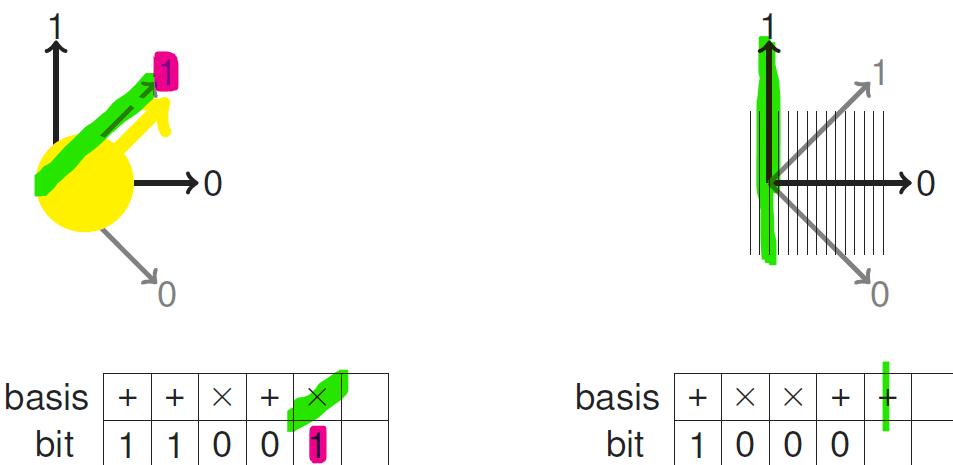


Abbildung 90: Alice sendet Bob ein diagonal [\diagup] polarisiertes Photon mit Wert 1

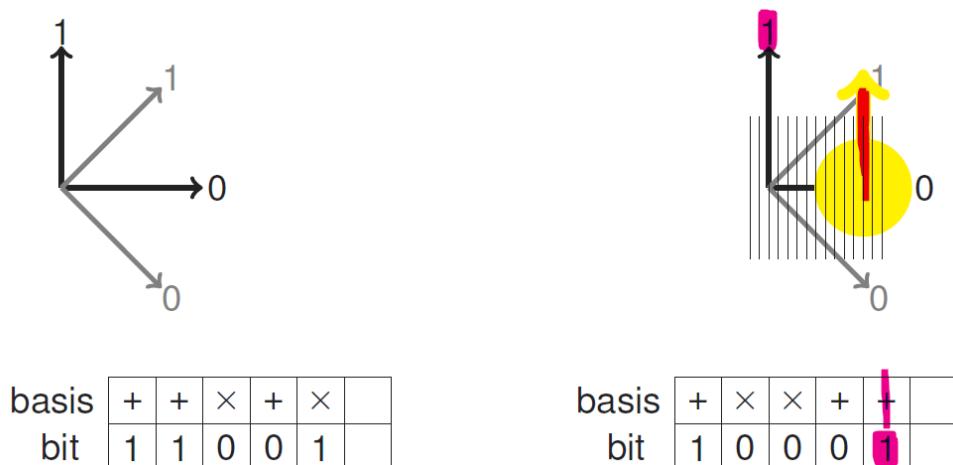
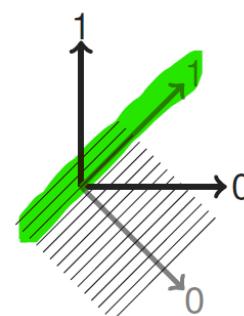
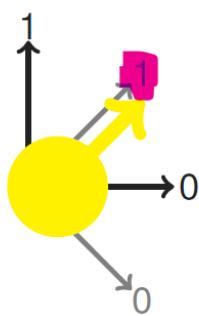


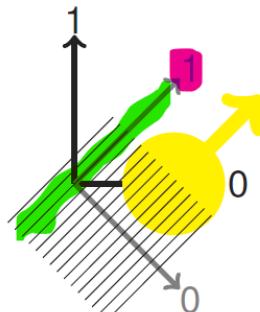
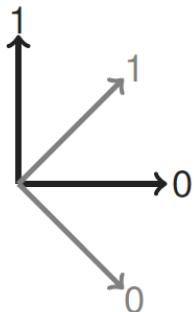
Abbildung 91: Bob empfängt Photon, zufälliger senkrechter Polfilter [] aber nicht dieselbe Richtung, nur Wert ist derselbe, da diagonales Photon zufällig in senkrechte Richtung gepolt wurde



basis	+	+	\times	+	\times	\times
bit	1	1	0	0	1	1

basis	+	\times	\times	+	+	\times
bit	1	0	0	0	1	

Abbildung 92: Alice sendet weiteres polarisiertes Photon, gleich wie vorheriges



basis	+	+	\times	+	\times	\times
bit	1	1	0	0	1	1

basis	+	\times	\times	+	+	\times
bit	1	0	0	0	1	1

Abbildung 93: Bob hat identische Polarisierung verwendet

basis	+	\pm	\times	+	\times	\times
bit	1	1	0	0	1	1
useful	✓	✗	✓	✓	✗	✓

basis	+	\times	\times	+	\pm	\times
bit	1	0	0	0	1	1
useful	✓	✗	✓	✓	✗	✓

Abbildung 94: Polarisierung und Bits werden überprüft

Teil VIII

WAF, Federations (SW 13)

15 Firewalls

Sie wissen was die Aufgaben einer Firewall sind

Aufgaben einer Firewall Filtern der ein- (WAF) und ausgehenden (HTTP Proxy) Kommunikation nach

- **Service control:** Z.B. Protokoll, Portnummer, IP-Adresse
- **Direction control:** Wer hat die Verbindung aufgebaut bzw. den Service initiiert?
- **User control:** Welcher Benutzer versucht einen bestimmten Service auszuführen?
- **Behaviour control:** Wie wird ein Service verwendet? Z.B. Spam-Filter

Sie verstehen die Funktionsweise einer WAF und wie sie eine Webanwendung vor Angriffen schützen kann

WAF Funktionalitäten einer Web Application Firewall

- Terminierung der SSL-Verbindung
- Protokoll-Einschränkungen (Port, HTTP/HTTPS)
- Load Balancing
- DoS-Verhinderung
- Session-Management (Cookie-Store, Timeouts)
- Filter gegen SQL-, HTML-, Code-Injection, XSS
- URL-Verschlüsselung
- Fehlerseiten umschreiben
- Request- und Response-Header setzen, entfernen, blockieren
- CSRF-Token einfügen
- ‘Dynamic Value Endorsement’
- Logging und Monitoring

Muss eine WAF Zugriff auf den ‘private key’ des Server-Zertifikats für eingehende SSL-Verbindungen haben? Warum?

Diskutieren Sie gegen welche Angriffe URL-encryption’ schützt.

Was ist URL-encryption? Dynamisch verschlüsselte URLs (kombiniert mit kryptographisch geschützten HTML-Formularen) verhindern, dass jemand illegale Anfragen oder böswillige Benutzerdaten an den Anwendungsserver zu senden. Absolut keine internen Informationen über die Webanwendung werden potenziellen Angreifern offengelegt. Angreifer können die Details der Anfrage oder die URL-Parameter nicht sehen, weil sie verschlüsselt sind.

⇒ Dynamic white-listing with URL encryption = positive security model

- Die Webanwendung definiert die erlaubten Anfragen.
- Nur erlaubte URLs werden an den Applikationsserver weitergeleitet, alles andere wird blockiert.
- Nur ein positives Sicherheitsmodell kann unbekannte Angriffe und Zero-Day-Exploits¹⁸ verhindern.

Diskutieren Sie, welche Funktionalitäten einer WAF gegen Cross-Site Scripting (XSS) schützen. Sie können eine Firewall verwenden, um Angriffe auf Ihre Website virtuell zu patchen. Diese Methode fängt Angriffe wie XSS, RCE¹⁹ oder SQLi ab, bevor böswillige Anfragen Ihre Website überhaupt erreichen.

¹⁸Cyber Attacke findet am gleichen Tag statt, an welchem Schwachstelle entdeckt wurde

¹⁹Remote Code Execution; Ausführen von externen Code via Internet

16 Federations

Sie verstehen wie Authentisierung mit Identity Federation abläuft, was die Voraussetzungen dafür sind und was die Vor- und Nachteile von Federations sind

Föderierte Identität Unter einer föderierten Identität versteht man die Vernetzung einer elektronischen Identität und Eigenschaften von einer Person, welche von unabhängigen Systemen für das Identifikationsmanagement genutzt werden kann. Von der föderierten Identität macht die *single sign-on (SSO)* gebrauch. Mit nur einer Authentisierungsinformation oder einem Token wird über mehrere IT-Systeme oder gar Organisationen, einem Benutzer der Zugriff gewährt. Die Rechteverteilung²⁰ für einzelne Dienste obliegt jedoch der Hoheit einzelner Systeme.

Funktionsweise der föderierten Identität Nehmen wir als Beispiel SWITCH.ch als die *Authentication and Authorization Infrastructure (AAI)* Schweizer Hochschulen und Universitäten und mit SAML²¹ arbeitet. Teilnehmer dieser „Föderation“ (Hochschulen und Universitäten) schaffen einen *Circle of Trust*, indem sie sich auf technische Standards und organisatorische Regeln einigen. Durch die Immatrikulation an der HSLU wird einem ein Benutzername und Passwort zugewiesen. Die HSLU hat also auf SWITCH automatisch eine eduID mit meinen Angaben erstellt, da SWITCH das **Identitätmanagement** als Dienst anbietet. Auf andere Organisationen muss dies so nicht zutreffen, z.B. Google-Account, wo man selber ein Account erstellt. Angenommen, man möchte sich jetzt auf <https://elearning.hslu.ch> anmelden und wählt den SWITCHaaai-Login.



Abbildung 95: SWITCHaaai-Login

Man wird auf den *Discovery Service - Where Are You From* von SWITCH umgeleitet.

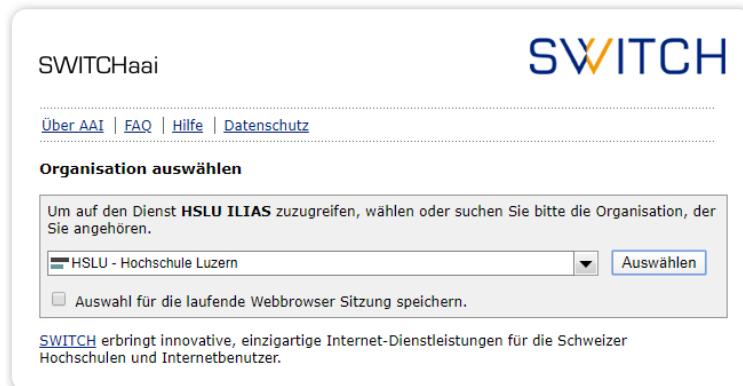


Abbildung 96: Auswahl zu welcher Organisation ich angehöre

²⁰Siehe Autorisierung, Seite 67

²¹Siehe Security Assertion Markup Language (SAML), Seite 78

The screenshot shows a login interface for 'HOCHSCHULE LUZERN'. At the top right, the university's name is displayed: 'Lucerne University of Applied Sciences and Arts'. The logo consists of the word 'HOCHSCHULE' in a large, bold, dark blue font above the word 'LUZERN' in a slightly smaller, bold, dark blue font. Below the logo, there is a sub-header 'SWITCHaaI'. The main form area contains fields for 'Benutzername' (Username) and 'Kennwort' (Password). There are also two checkboxes: one checked ('Nicht angemeldet bleiben') and one unchecked ('Persönlich freigegebene Informationen an diesen Dienst widerrufen'). A 'Anmelden' (Login) button is located at the bottom right of the form. Below the form, text indicates the user is logging into 'HSLU ILIAS' and provides a service description: 'HSLU e-learning produktiv System'.

Abbildung 97: Authentisierung mit meinen Logindaten

Das föderale System ist transparent und überprüfbar. Als User hat man die volle Kontrolle darüber, welche persönlichen Informationen vom IT-System oder Organisation eingesehen werden dürfen und/oder welche Berechtigungen zwischen den Beteiligten ausgetauscht werden dürfen.

The screenshot shows a page titled 'Informationen die an den Dienst übertragen werden' (Information transferred to the service). It lists several pieces of information with their corresponding values: Zugehörigkeit (member@student.hslu.ch), E-Mail (victor.fernandez@stud.hslu.ch), Vorname (Victor), Nachname (Fernández), and Heimorganisation (hslu.ch). Below this, a note states: 'Wenn Sie fortfahren werden diese Informationen an den Dienst übermittelt. Sind Sie damit einverstanden, dass diese Informationen zukünftig automatisch an diesen Dienst übermittelt werden?'. A section titled 'Legen Sie eine Einwilligungsdauer fest:' (Set a consent duration) contains two radio button options: 'Bei der nächsten Anmeldung erneut fragen' (Ask again at next login) and 'Bei Änderung meiner Informationen erneut fragen.' (Ask again when my information changes). Underneath, a note says: 'Ich bin damit einverstanden, dass diese Informationen zukünftig automatisch an diesen Dienst übermittelt werden.' At the bottom, there are 'Ablehnen' (Decline) and 'Akzeptieren' (Accept) buttons.

Abbildung 98: Transparenz der Daten und deren Nutzung

Doch das ist jetzt nicht alles. Die föderierte Identität gewährt mit die Authentisierung innerhalb des *Circle of Trusts* der Föderation. Zum beweisen, kann man sich nun auf einem anderen Portal anmelden, welches zur selben Föderation gehört, z.B. das von der Universität Bern unter <https://ilias.unibe.ch>.



Abbildung 99: Beispiel des Circle of Trust



Abbildung 100: Anmeldung auf ILIAS von Universität Bern

Sie sind dabei folgenden Dienst aufzurufen:
UniBE, ILIAS Server von unibe.ch

Durch den Dienst gegebene Beschreibung:
ILIAS-Server der UniBE

Informationen die an den Dienst übertragen werden	
Zugehörigkeit	student member
E-Mail	victor.fernandez@stud.hslu.ch
Vorname	Victor
Nachname	Fernández
Helmorganisation	hslu.ch

Wenn Sie fortfahren werden diese Informationen an den Dienst übermittelt. Sind Sie damit einverstanden, dass diese Informationen zukünftig automatisch an diesen Dienst übermittelt werden?

Legen Sie eine Einwilligungsdauer fest:

Bei der nächsten Anmeldung erneut fragen

- Ich stimme der einmaligen Übertragung meiner Informationen zu.

Bei Änderung meiner Informationen erneut fragen.

- Ich bin damit einverstanden, dass diese Informationen zukünftig automatisch an diesen Dienst übermittelt werden.

Diese Einstellung kann jederzeit bei der Anmeldung wiederrufen werden.

Abbildung 101: Auch hier Transparenz der Daten

Erfolgreiche Anmeldung in einer anderen, von der HSLU völlig unabhängigen Organisation, wenn doch nur mit rudimentären Rechten als einfacher Benutzer. Beispielsweise können freigegebene Portfolios angeschaut werden.

ILIAS Universität Bern

PERSÖNLICHER SCHREIBTISCH ▾ MAGAZIN ▾

Persönliche Daten und Profil
Einstellungen
Abmelden

FREIGEGEBENE RESSOURCEN

Benutzername/Nome	Titel der Ressource	Freigabe ab dem	Typ der Ressource	Freigegeben für	
		DD.MM.YYYY	Portfolio	-- Beliebig --	
<input type="button" value="Suche"/>	<input type="button" value="Suche zurücksetzen"/>				
(1 - 24 von 24)					
Nachname	Vorname	Benutzername	Freigabedatum ↓	Titel der Ressource	Freigegeben für
[redacted]	[redacted]	[redacted]	16. Okt 2019, 10:34	Neuropathologie: Zum Weiterlesen	Alle registrierten Benutzer
[redacted]	[redacted]	[redacted]	02. Okt 2019, 23:07	ZMK - Literatur	Alle registrierten Benutzer
[redacted]	[redacted]	[redacted]	12. Sep 2019, 14:17	[redacted]	Alle registrierten Benutzer
[redacted]	[redacted]	[redacted]	23. Mai 2019, 15:44	UniBe - DCB - Furrer - GB400	Internet/WWW mit Passwort
[redacted]	[redacted]	[redacted]	22. Mai 2019, 14:01	TestNMR	Internet/WWW mit Passwort
[redacted]	[redacted]	[redacted]	26. Sep 2017, 17:26	[redacted]	Alle registrierten Benutzer
[redacted]	[redacted]	[redacted]	22. Sep 2017, 16:42	ILIAS-Support	Internet/WWW
[redacted]	[redacted]	[redacted]	12. Okt 2016, 17:56	Links zu Astronomie Themen	Alle registrierten Benutzer
[redacted]	[redacted]	[redacted]	06. Okt 2015, 11:02	Zusammenfassungen	Alle registrierten Benutzer
[redacted]	[redacted]	[redacted]	13. Aug 2015, 06:05	Mein Profil	Alle registrierten Benutzer

Abbildung 102: Erfolgreich angemeldet

Security Assertion Markup Language (SAML) Die SAML ist ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen. Sie stellt Funktionen bereit, um sicherheitsbezogene Informationen zu beschreiben und zu übertragen.[1]

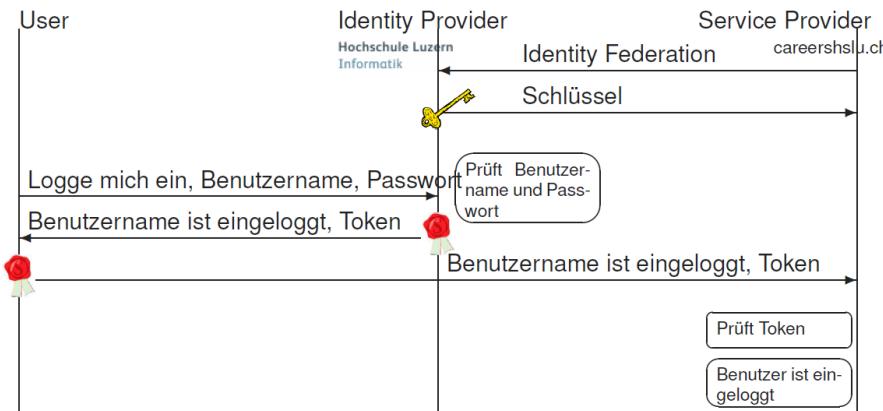


Abbildung 103: Funktionsweise der Authentifizierung und Autorisierung mittels SAML

- Single Sign-On
 - ein Benutzer ist nach der Anmeldung an einer Webanwendung automatisch auch zur Benutzung weiterer Anwendungen authentifiziert
- Verteilte Transaktionen
 - mehrere Benutzer arbeiten gemeinsam an einer Transaktion und teilen sich die Sicherheitsinformationen
- Autorisierungsdienste
 - die Kommunikation mit einem Dienst läuft über eine Zwischenstation, die die Berechtigung überprüft

OAuth Open Authorization ist der Name zweier verschiedener offener Protokolle, die eine standardisierte, sichere API-Autorisierung²² für Desktop-, Web- und Mobile-Anwendungen erlauben. Ein User kann mit Hilfe dieses Protokolls einer Anwendung den Zugriff auf seine Daten erlauben (Autorisierung), die von einem anderen Dienst bereitgestellt werden, ohne geheime Details seiner Zugangsberechtigung (Authentifizierung) dem Client preiszugeben. Der User kann so Dritten gestatten, in seinem Namen einen Dienst zu benutzen. Typischerweise wird dabei die Übermittlung von Passwörtern an Dritte vermieden.[1]

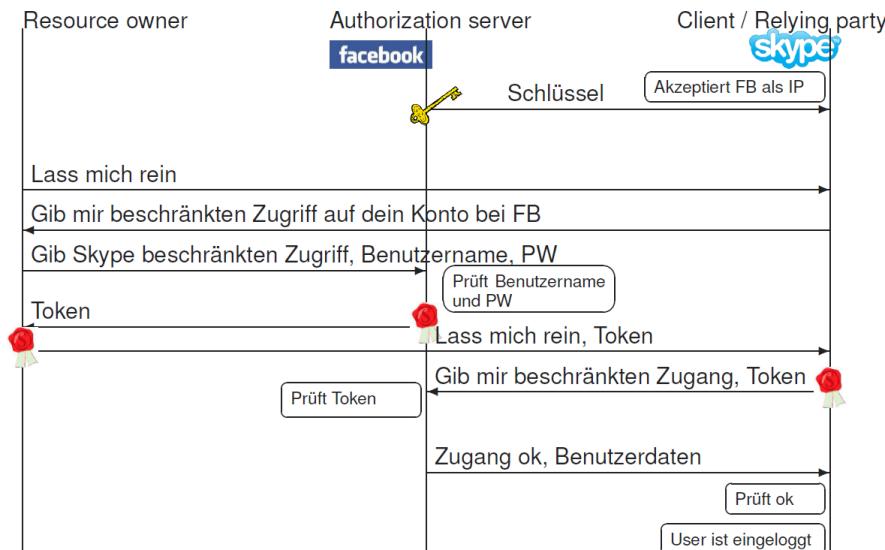


Abbildung 104: Autorisierung auf einen Dienst mittels OAuth

²²Application Programming Interface - Eine Programmschnittstelle, welche die Anbindung an das System zur Verfügung stellt.

OpenID OpenID ist ein dezentrales Authentifizierungssystem für webbasierte Dienste. Es erlaubt einem Benutzer, der sich bei seinem OpenID-Provider einmal mit Benutzernamen und Kennwort angemeldet hat, sich mithilfe der OpenID (einer URL, in diesem Kontext auch Identifier genannt) ohne Benutzernamen und Passwort bei allen das System unterstützenden Websites – den *Relying Parties* – anzumelden, wendet also das Single-Sign-on-Prinzip an.[1]

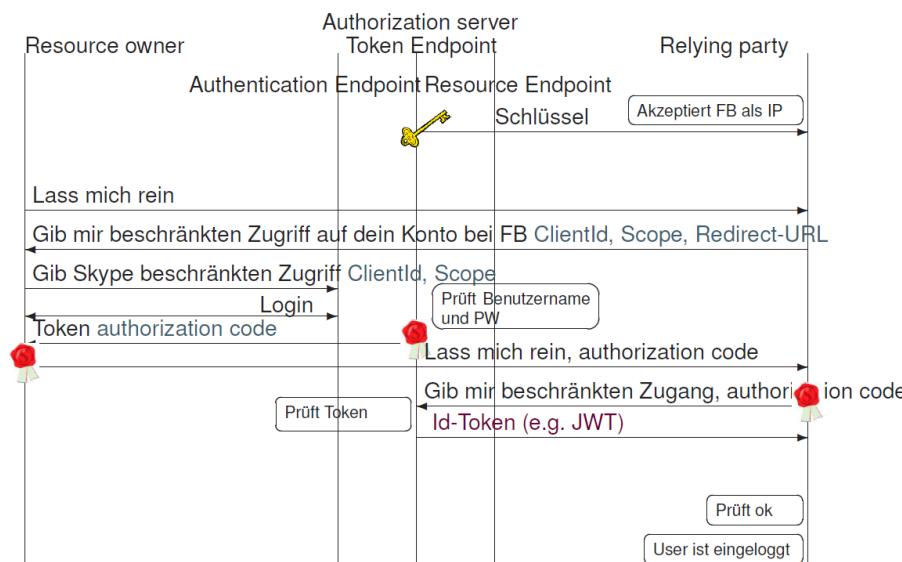


Abbildung 105: Authentisierung mit OpenID Connect

JSON Web Token (JWT) Das JWT ermöglicht den Austausch von verifizierbaren Claims. Es wird typischerweise verwendet, um in einem System mit einem Drittanbieter die Identität eines Benutzers zwischen einem Identity-Provider und einem Service-Provider auszutauschen. Des Weiteren eignet sich JWT zur Implementierung einer Stateless Session, denn da alle für die Authentifikation benötigten Informationen in dem Token übertragen werden, muss die Sitzung nicht auf dem Server gespeichert werden.[1]

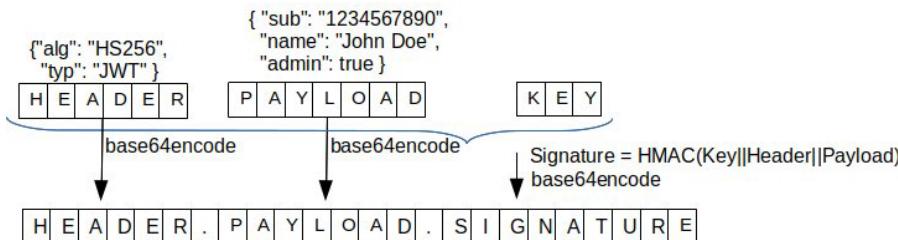


Abbildung 106: Aufbau eines JWTs

Vor- und Nachteile von Identity Federations

Chancen

- Vereinfachtes ID-Management für den User (stärkere Passörter möglich)
- Vereinfachtes Authentisierungsverfahren für Service Provider
- Komfort durch SSO

Risiken

- Sicherheitsmängel beim Identity-Provider geben Zugang zum Service-Provider
- Missbrauch von verwaisten Zugängen
- Unerwünschtes Verhalten des Identity-Providers
- Problem der Verkettung: mit einem erfolgreichen Angriff erlangt der Angreifer Zugang zu diversen Diensten

Teil IX

Talks (SW 14)

17 Malware

Sie verstehen, welche Arten von Malware es gibt, welche Massnahmen gegen Malware sinnvoll sind und wie diese wirken

Welche Arten von Malware es gibt:

- **Viren:** Malware, die sich verbreitet und versteckt, indem sie andere Programme „verseucht“.
- **Dropper:** Malware, die andere Malware nachlädt.
- **Würmer:** Malware, die sich selbst ohne Zutun des Benutzers verbreitet.
- **Trojaner:** Malware, die sich verdeckt hält und spioniert, ggf. andere Funktionen nachlädt.
- **Ransomware:** Malware, die das Opfer erpresst meistens indem sie Daten verschlüsselt.

Aktuelle Arten von Malware:

- **Emotet:** Ursprünglich Banking-Trojaner, Ziel deutschsprachiger Raum und mittlerweile Vehikel für andere Malware (Dropper).
- **Trickbot:** Banking-Trojaner, stiehlt Login-Daten, Kartennummern, TANs usw.
- **Ryuk:** Ransomware, verschlüsselt Daten und erpresst Opfer

Verbreitungsweg: Interne Weiterverbreitung, Infektion.

Massnahmen gegen Malware: Sollten verhältnismässig ausgewählt werden, konsequent durchgesetzt und verifiziert.

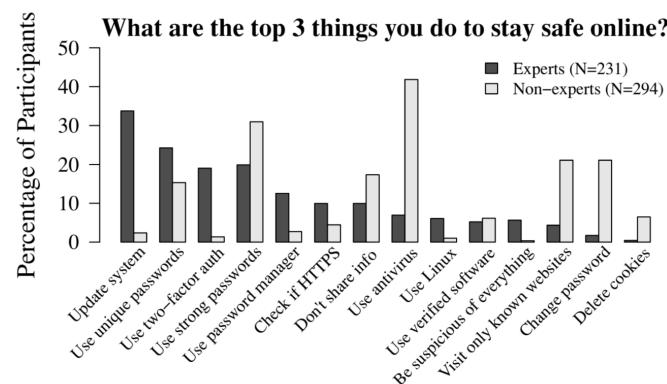


Abbildung 107: Experts vs Non-Experts

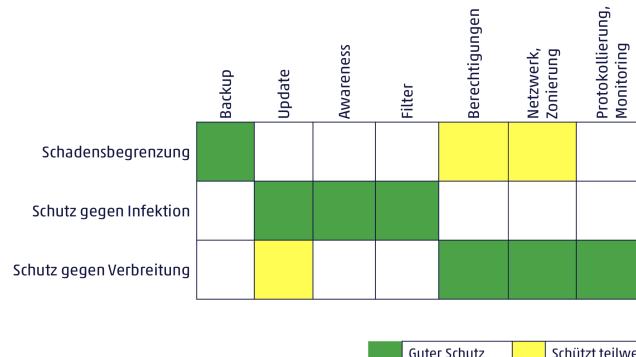


Abbildung 108: Positionierung Massnahmen

Schadensbegrenzung

- **Backup:** Verfügbarkeit der Daten und Systeme im Fall von technischen Problemen (Ausfall eines Servers, von Festplatten). Grundregel: Eine Sicherheitskopie ist nur dann ein Backup, wenn es wiederhergestellt werden kann. Für Malware zusätzlich Unveränderbarkeit der Daten und Systeme (Erpressung ist wirkungslos, wenn das Opfer eine intakte Kopie hat). Grundregel: Eine Sicherheitskopie ist nur nützlich, wenn sie vom Angreifer nicht verändert werden kann.

Schutz gegen Infektion

- **Update-Management:** Viele Programme verarbeiten Daten unbekannten Ursprungs (Anhänge von E-Mails (Kunden, Geschäftspartner), Downloads aus dem Internet). Für Malware müssen diese Programme immer aktuell gehalten werden: Betriebssystem, Browser, E-Mail, Messenger, Office-Suite, PDF-Reader, Tools generell.
- **Awareness-Schulung:** Sensibilisierung der Mitarbeiter. Für Malware ist eine hohe Sensibilisierung notwendig, Phishing-Angriffe können vom internen Netzwerk kommen.
- **Filtern:** Filtern beim E-Mail (Filter auf Malware und Phishing), Internet-Zugang (Filter auf Malware und Phishing), File-Server(Scan auf Schadcode) und eine restriktive Zugriffsberechtigungen auf Files. Für Malware zusätzliche eine aktive Auswertung von Protokolldaten und Webisolation.

Schutz gegen Verbreitung

- **Berechtigungen:** Mitarbeiter haben Zugriff (lesend und schreibend) auf Daten, die sie nicht benötigen, haben administrative Berechtigung an ihrem Arbeitsgerät oder Administratoren benutzen ihr Arbeitskennwort auch zur Systemverwaltung (Active Directory). Massnahmen fordern dazu, dass eine rigorose Einschränkung der Zugriffsberechtigungen durchgeführt wird sowie keine administrativen Berechtigungen für Benutzer. Jedoch starke Einschränkungen behindern die Arbeit.
- **Netzwerk, Zonierung:** Flache Strukturen oder einfache Zonierung (Perimeter-Schutz). Bei Malware behindert eine Zonierung Ausbreitung und Interaktion zwischen Clients. Server-zu-Server-Kommunikation einschränken und eine dediziertes Management-Netz. Sowie eine Abtrennung der Backup-Systeme.
- **Protokollierung und Monitoring:** Nachvollzug von Benutzer-Aktivitäten und System-Verhalten. Beim Malware eine Analyse im Rahmen des Incident-Managements (Nachforschungen).

Wie diese Massnahmen wirken:

Behebung

- **Sofortmassnahmen (Schadensbegrenzung):** Alle Systeme im betroffenen Segment (Netzwerkzone, Active-Directory-Domain) ausschalten/trennen, alternative Arbeitsumgebung aufbauen oder aktivieren.
- **Mittelfristige Massnahmen (Schadenbeheben):** Einsatz einer Task-Force (Notfallorganisation), Information an Kunden und Partner, Forensische Untersuchung der Infektion, Aufbau einer intakten Umgebung, Wiederherstellung der Daten (ab Backup), Nacharbeiten.
- **Längerfristige Massnahmen (zukünftige Schäden verhindern)**

Prüfung der Massnahmen:

- Warum braucht es eine Prüfung?
- Die Massnahmen sind im regulären Betrieb nicht sichtbar (z.B. Zonierung)
 - Aufweichung der Massnahmen, da diese hinderlich sind
 - Prüfungen gegen Standards reichen nicht (zu wenig spezifisch)

18 WAF

Sie verstehen wo Machine-Learning in einer WAF eingesetzt werden kann und was einen Machine-Learning-Ansatz vom „herkömmlichen“ Einsatz einer WAF unterscheidet

Wo Machine-Learning in einer WAF eingesetzt wird: Detection of new/unknown attacks in productive traffic. From catching requests (not useful) to catching sessions (useful). Am Anfang wurde die Attack-/Safe payloads angeschaut, die jedoch unnutzlich (does not adequately address real problem (robustness)) sind im vergleich zum requests und sessions.

Attack/Safe payload approach: Mittels supervised learning die existerende Lösung verbessern. Die Data wird angeschaut anstatt die requests/sessions. Good Strings beeinhalten ca. 1k human input strings und 10k technische strings (HTTP Headers...). Bad Strings beeinhalten ca. 500k attack payloads. Die approach war gemäss die Boosting Trees Model die die solche features haben: quote-count, quote-parity, keyword-count, SQL-comment-count, length, shrinkageAbsolute, unicodeCount, controlCount, punctuationRatio. Es ist zwar genau jedoch wird die echte Problem damit nicht gelöst, nämlich die robustness problem.

Requirement	Current solution (without machine learning)
Very low false positive rate	Context escape detection (start of attack payload) Tokenizing input string Validate tokens (syntax but no semantic)
	We do not block: 1 or 1 is not a valid injection
Low false negative rate	- Backtracking parser differences (symbol interpretation, operator orders) - Approach independent: fuzzing, bug bounty program, automated verification of collected attack payloads
Maintainability	- DSL to generate regular expressions - Interpretable rules (for developers) - no blackbox
Fast execution (milliseconds)	- Regex optimizers

Abbildung 109: Requirement and current solutions

Catching Requests (bisherige WAF):

- **Attacks:** injection attacks, CSRF
- **Decision:** good or bad (binary)
- **Property correlation:** not possible
- **Action:** block

Catching Sessions (ML Ansatz):

- **Attacks:** infected client, forceful browsing, vulnerability scanning, session stealing, DoS
- **Decision:** how bad and what kind of session is it?
- **Property correlation:** timestamp, IP/geolocation, path, status code, content-type, TLS session id
- **Action:** CAPTCHA, re-authentication, block, inform system/human, log-only

Sie kennen Beispiele von Angriffen, welche mittels Machine-Learning auf einer WAF erkannt werden konnten

Client controlled by command and control server: Phases of 404 Status Code, No js/css/images etc. (content type), explore a certain page and then continue. This is an IP attempting to make contact to unknown C&C-Server, with contents unique to unknown C&C-Command protocols.

Infected Clients: Normal content type distribution, multiple passes over unsuspecting URLs but from 8 (less or more) different IPs in parallel. IP infected or NATing for computer infected by Gozi botnet.

Vulnerability Scanner: Huge Session which is incredibly fast with suspicious URLs.

Internal Monitoring Tool: No js/css/images etc. (content type) and a lot of requests and no manual user. URLs known as well as IP therefore a desired bot.

Index

- 3-Way Handshake, 26
- Access Control, 65
- Aktive vs. Passive Angriffe, 24
- AnwendungsLayer, 24
- Argon2, 12
- ARP-Spoofing, 26
- Authentifizierung, 67
- Authentisierung, 20, 65, 67
- Authentizität, 6
- Autorisierung, 67
- Awareness, 63
- Awareness-Prozess, 63
- BB84-Protokoll, 71
- bcrypt, 12
- Bedrohungen, 3
- Bedrohungen auf OSI-Layern, 24
- Berechenmässige Sicherheit, 7
- BSI Standards, 35
 - BSI 100-4, 36
 - BSI 200-1, 36
 - BSI 200-2, 36
 - BSI 200-3, 36, 50
 - Vergleich zu ISO, 39
- Bug, 24
- Caesar cipher, 8
- Chosen plaintext attack, 8
- Ciphertext only attack, 8
- Code Injection, 24, 29
- Cookies, 22
- Cross Site Scripting (XSS), 24, 28
- CSRF, 24
 - Cross-Site Request Forgery, 24
- Datenschutz, 6
- Datensicherheit, 6
- DDoS, 3
- Diffie-Hellman, 14, 15
- Domänen, 34
- DoS, 24, 27
- DRDoS, 27
- Eintrittshäufigkeit, 44
- ElGamal, 14, 15
- Ergänzende Sicherheitsanalyse, 61
- Federations, 74
- Fehler vs. Bugs, 24
- Flaw, 24
- Gefährdungen, 3
- Grundschutz, 33
 - Bausteine, 39
 - IT Grundschutz, 39
 - IT-Grundschutz, 50, 51
 - Kataloge, 51
 - Teilschritte, 53
- Grundziele Informationssicherheit, 5
- Hash-Algorithmen, 12
- Hashfunktion, 11
- HTTP, 21
 - Requests, 21
 - Response-Codes, 21
 - Response-Header, 23
- Hybridverschlüsselung, 17
- Identität, 6
- Informationssicherheit, 3
- Informationstheoretische Sicherheit, 7
- Integrale Sicherheit, 6
- Integrität, 5
- ISMP, 34
- ISMS, 31
- ISO Standards, 31
 - ISO 13335, 36
 - ISO 27000, 32
 - ISO 27001, 32
 - ISO 27002, 33, 36, 63
 - ISO 27003, 34
 - ISO 27004, 34
 - ISO 27005, 34, 43
 - Vergleich zu BSI, 39
- IT-Grundschutz, 51
- IT-Grundschutzanalyse, 59
- IT-Sicherheitskonzept, 51
- JWT, 79
- Kerckhoff's Prinzip, 8
- Klassische symmetrische Verschlüsselungsverfahren, 8
- Known plaintext attack, 8
- Kombinierter Ansatz, 50
- Kreuzreferenztabellen, 52
- Layer 8, 24, 30
- Link-Layer, 24
- Malware, 80
- Maximumprinzip, 56
- Mitigation (Verminderung), 46
- NIST Cybersecurity Framework, 37
 - Components, 37
 - Core, 38
- OAuth, 78
- One-time pad, 11
- OpenID, 79
- Operationelle Risiken, 41
- OSI-Modell, 25
- OWASP Top 10, 41
- Password Based Key Derivation Functions, 12
- Passwort, 12
- PBKDF2, 12

- PDCA
 - Plan-Do-Check-Act, 32, 33
- Private Key Kryptographie, 7
- Public Key Encryption, 14
- Quantencomputer, 70
- Quantenschlüsselaustausch, 71
- Quantitative vs. qualitative Risikoanalyse, 42
- Random, 16
- Response-Codes, 21
- Response-Header, 23
- Restrisiken, 46
- Risiken im ICT Bereich, 41
- Risiken im Unternehmen, 40
- Risiken nach ISO 27005, 43
- Risiko, 6
 - Risiko Berechnung, 42
 - Risiko-Katalog, 46
 - Risiko-Management, 39
 - Risiko-Management-Prozess, 47
 - Context Establishment, 47
 - Risk Acceptance, 48
 - Risk Communication, 48
 - Risk Estimation, 48
 - Risk Monitoring and Review, 49
 - Risk Treatment, 48
 - Rist Evaluation, 48
 - Ristk Identification, 47
 - Risiko-Portfolio, 45
 - Risikobewältigung, 46
 - Risikodefinition, 40
 - Risikomanagement - Stile, 40
 - Risikomatrix, 45
 - Risk Register, 46
 - Risk-Map, 45
 - RSA, 14
- SAML, 78
- Schadensaussmass, 44
- Schlüsselaustauschprotokoll, 15
- Schutzbedarf feststellung, 55
- Schutzziele, 5
- scrypt, 12
- Secret Key, 7
- Secret Sharing, 68
 - Shamir's Secret Sharing, 68
- Sensitive Daten, 24, 28
- Session, 22
- Session Fixation, 23
- Sichere Zufallszahlen, 16
- Signatur, 16
- SOA
 - Statement of Applicability, 32
- Social Engineering, 24
- Social Enginering, 30
- Spoofing, 24
- SSL/TLS, 24, 28
- Steganographie, 7
- Strukturanalyse, 53
- Symmetrische Kryptographie, 7
- TCP Verbindungsauflaufbau, 26
- Threat, 24
- Threat vs. Threat Agent, 24
- Transport-Layer, 24
- Trust, 18
- URL-Encryption, 73
- Verbindlichkeit, 5
- Vertraulichkeit, 5
- Vigenère cipher, 10
- XSRF
 - siehe CSRF, 83
- XSS
 - siehe Cross Site Scripting (XSS), 24, 28
- Zahlengenerator, 16
- Zero-Knowledge-Proof, 70
- Zertifikat, 20
- Zugangskontrolle, 5
- Zugriffskontrolle, 5
- Zutrittskontrolle, 5

Abbildungsverzeichnis

1	Wissenspyramide[1]	3
2	Zeitpunkt der Entdeckung eines Grundziel-Verlustes	6
3	Alice verschlüsselt, Bob entschlüsselt mit dem gemeinsamen Schlüssel	7
4	Nur Geheimtext	8
5	Klartext-Geheimtext-Paare	8
6	Klartexte und Geheimtexte	8
7	Caesar cipher mit Verschiebung um 3 Stellen	9
8	Frequenzanalyse unchiffriert	9
9	Frequenz um 10 Stellen verschoben	10
10	Vigenère cipher	10
11	Funktionsweise des OTP	11
12	Einfaches Beispiel einer Hashfunktion	11
13	Funktionsweise eines Keyed-Hash Message Authentication Codes	13
14	Alice verschlüsselt mittels Bob's Public Key asymmetrisch	14
15	Identischer Geheimschlüssel wird erzeugt[1]	15
16	Signatur im Detail	16
17	Alice verschickt eine signierte Nachricht an Bob	17
18	Hybridverschlüsselung einer Nachricht	18
19	Eve als man in the middle	18
20	Alice vertraut Bob durch direkte Überprüfung	18
21	Alice vertraut Dave indirekt durch Vertrauensnetz	19
22	Hierarchical Trust durch Certificate Authorities	19
23	TLS Cipher im Detail	20
24	SSL / TLS	20
25	HTTP zustandslos	21
26	HTTP Zustand per Request (hidden field)	22
27	Einsatz eines Cookies	22
28	Cross-Site Request Forgery	24
29	OSI-Layers	25
30	OSI vs. Internet Reference Model	25
31	TCP-Encapsulation	25
32	ARP Spoofing	26
33	3-Way Handshake	26
34	SYN Flood	27
35	DRDoS	27
36	SSL/TLS	28
37	XSS	29
38	Code Injection	29
39	Beispiel Code Injection	29
40	Layer 8, der User	30
41	Zusammenhang der verschiedenen ISO Standards [3]	32
42	Prozess nach ISO 27001 [4]	33
43	14 Domänen (Kapitel)	34
44	BSI-Standards und IT-Grundschutz-Kompendium [6]	35
45	Standard-Sicherheit und Risikoanalyse	36
46	Iteration des Notfallmanagements nach BSI 100-4 [7]	37
47	Die Komponenten des NIST Frameworks	37
48	Fünf Frameworkfunktionen	38
49	IT-Grundschutz-Aufbau	39
50	Bausteine IT Grundschutz Katalog	39
51	Verschiedene Stile von Risikomanagement	40
52	Risiken laut KPMG	40
53	OWASP TOP 10 IT Security Bedrohungen	41
54	Vorgehen bei der Risiko-Analyse	42
55	Risikomatrix	45
56	Risk-Map	45
57	Risk-Map, Umgang mit Risiken	45
58	Umgang mit Risiken	46

59	Beispiel eines Risikokataloges	46
60	Organisation eines Risiko Managements	47
61	Schutzbedarf	49
62	Kombinierter Ansatz	50
63	BSI-Standard 200-3	50
64	IT-Grundschutz-Kataloge	50
65	IT-Grundschutz Wirkprinzip	51
66	IT Sicherheitskonzept	51
67	Kreuzreferenztabellen	52
68	IT-Strukturanalyse	53
69	Komplexitätsreduktion	54
70	Erhebung IT-Systeme	54
71	Zuordnung in Gruppen	54
72	Schutzbedarfsfeststellung	55
73	Vorgehen bei Schutzbedarf	55
74	Vererbung Schutzbedarf	56
75	Schutzbedarf - Maximumprinzip	56
76	Schutzbedarf IT-Anwendungen	57
77	Schutzbedarf IT-System	57
78	Schutzbedarf IT-Räume	58
79	Schutzbedarf Kommunikationsverbindungen	58
80	IT-Grundschutzanalyse	59
81	IT-Grundschutz-Modell	59
82	IT-Grundschutz Modellierung	60
83	Fehlende Sicherheitsmassnahmen beim Basis-Grundschutz müssen ergänzt werden	60
84	Ergänzende Sicherheitsanalyse	61
85	Beispiel eines Realisierungsplans	62
86	IT-Strukturanalyse Zusammenfassung	62
87	Prozess der Verhaltensänderung	63
88	Basisausbildung, Kampagnen und flankierende Massnahmen	64
89	Verschiedene Varianten von Token und Authentisierungsmethoden	66
90	Alice sendet Bob ein diagonal \checkmark polarisiertes Photon mit Wert 1	71
91	Bob empfängt Photon, zufälliger senkrechter Polfilter \square aber nicht dieselbe Richtung, nur Wert ist derselbe, da diagonales Photon zufällig in senkrechte Richtung gepolt wurde	71
92	Alice sendet weiteres polarisiertes Photon, gleich wie vorheriges	72
93	Bob hat identische Polarisierung verwendet	72
94	Polarisierung und Bits werden überprüft	72
95	SWITCHaaI-Login	74
96	Auswahl zu welcher Organisation ich angehöre	74
97	Authentisierung mit meinen Logindaten	75
98	Transparenz der Daten und deren Nutzung	75
99	Beispiel des Circle of Trust	76
100	Anmeldung auf ILIAS von Universität Bern	76
101	Auch hier Transparenz der Daten	77
102	Erfolgreich angemeldet	77
103	Funktionsweise der Authentifizierung und Autorisierung mittels SAML	78
104	Autorisierung auf einen Dienst mittels OAuth	78
105	Authentisierung mit OpenID Connect	79
106	Aufbau eines JWTs	79
107	Experts vs Non-Experts	80
108	Positionierung Massnahmen	80
109	Requirement and current solutions	82

Quellen

- [1] Wikipedia. URL: <http://de.wikipedia.org>.
- [2] Renato Renner. "Security of quantum key distribution". In: *Security of quantum key distribution*. Gesellschaft für Informatik, 2006. ISBN: 978-3-88579-330-4. URL: <http://dl.gi.de/handle/20.500.12116/4519> (visited on 12/22/2019).
- [3] ISO. *ISO Standard 27000*. Tech. rep. Genf: Internationale Organisation für Normung, 2018. URL: <https://www.iso.org/standard/73906.html>.
- [4] ISO. *ISO Standard 27001*. Tech. rep. Genf: Internationale Organisation für Normung, 2015. URL: <https://www.iso.org/standard/54534.html>.
- [5] Dejan Kosutic. *ISO 27001 im Vergleich zu ISO 27002*. URL: <https://advisera.com/27001academy/de/knowledgebase/iso-27001-im-vergleich-zu-iso-27002/> (visited on 12/30/2019).
- [6] Ronny Frankenstein and Manuel Atug. *BSI stellt modernisierten Grundschatz vor — iX — Heise Magazine*. URL: <https://www.heise.de/select/ix/2017/12/1512149671074410> (visited on 12/30/2019).
- [7] Isabelle Münch. "IT-Grundschatz –Informationssicherheit ohne Risiken und Nebenwirkungen". In: *IT-Grundschatz –Informationssicherheit ohne Risiken und Nebenwirkungen*. 2009.
- [8] Chris Brook. *What is the NIST Cybersecurity Framework?* Dec. 2018. URL: <https://digitalguardian.com/blog/what-nist-cybersecurity-framework> (visited on 12/30/2019).
- [9] ISO. *ISO Standard 27005*. Tech. rep. Genf: Internationale Organisation für Normung, 2018. URL: <https://www.iso.org/standard/75281.html>.