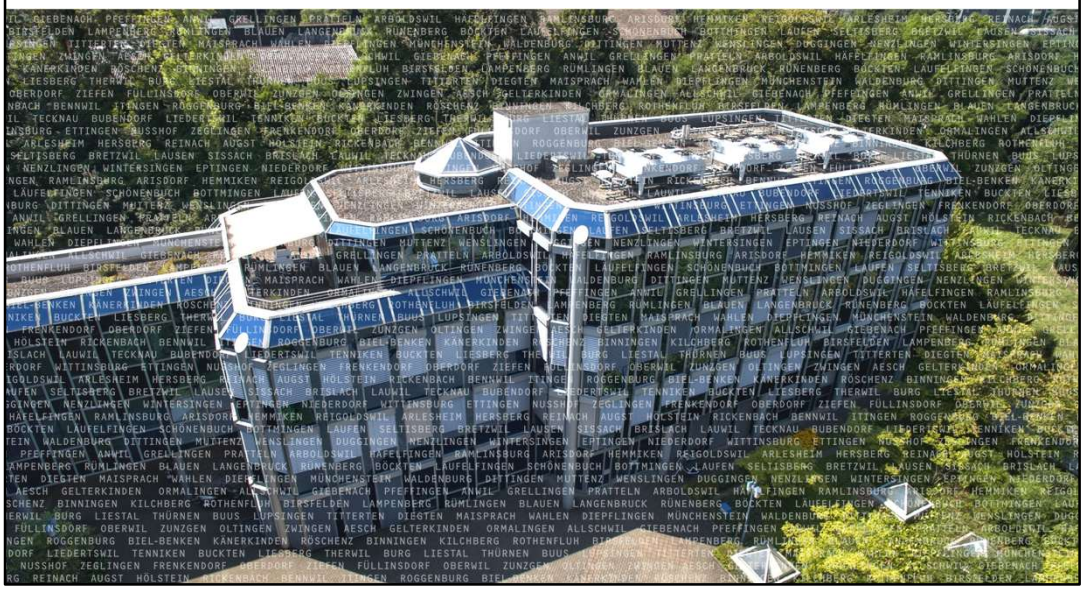
Pascal Reiniger
Kantonaler Informationssicherheitsbeauftragte (CISO) Kanton Basel-Landschaft
19.02.2026 – Schweizer Gemeindeverband / myni Gmeind

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

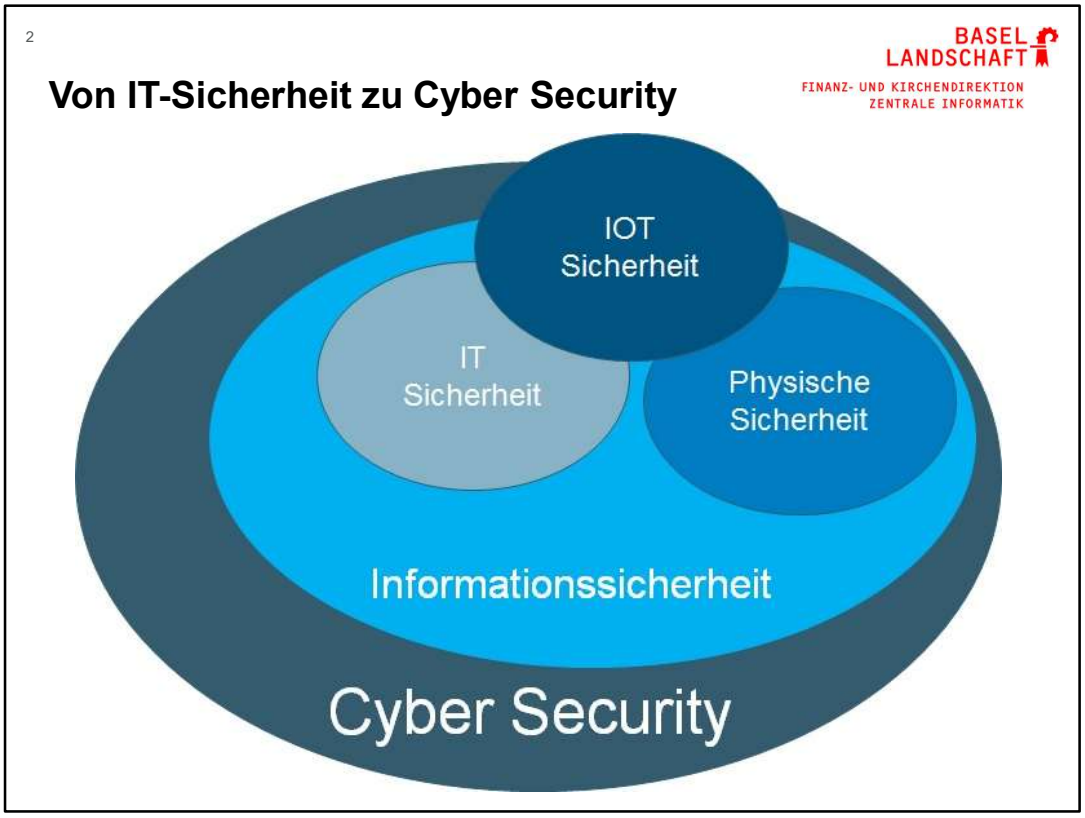
Cyber Security in der öffentlichen Verwaltung



Disclaimer:

In der vorliegenden Präsentation wurden viele Grafiken und Statistiken verwendet. Bei der Informationssicherheit und bei den Cyber-Risiken handelt es sich um kein objektiv messbares Feld. Vieles läuft im Verborgenen. Viele der Daten stammen von Forschungsteams (und Marketingabteilungen) von Anbietern von Cyber Security Services. Diese Daten können einen unterschiedlichen Fokus und abweichende Gewichtungen haben. Es wurde versucht, auf möglichst seriöse und aktuelle Datenquellen abzustützen. In der Tendenz zeigen diese Daten jedoch in die grundsätzlich richtige Richtung.

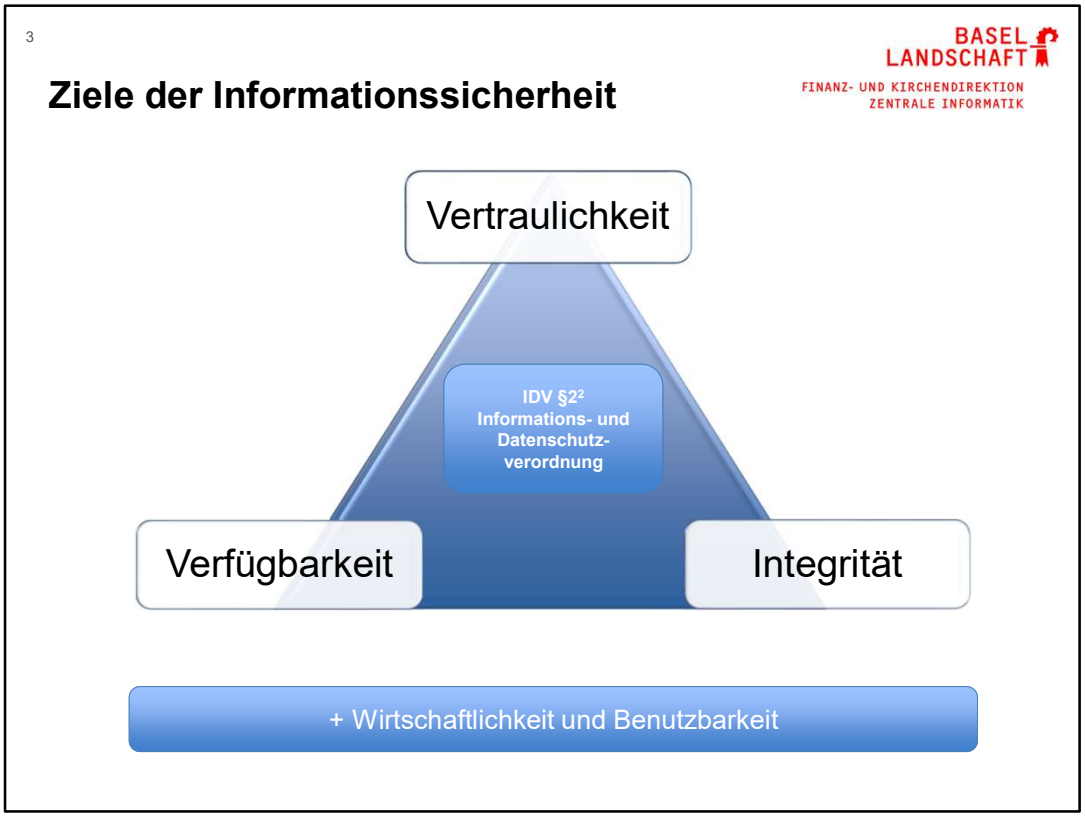
Die Covid-Pandemie hat einen erheblichen Einfluss auf die Vergleichbarkeit der Daten vor und nach 2020.



Informationssicherheit und Cyber Security umfassen **alle Aspekte der Sicherheit** in der Informations- und Kommunikationstechnik (**IKT**) inklusive **der Auswirkung** auf direkt und indirekt davon abhängige Anwendungen, Prozesse, Informationen und Gegenstände wie bspw. das Internet der Dinge = IoT (Internet of Things).

Cyber Risiko ist kein einzelnes spezifisches IT-Risiko, sondern eine Gruppe von Risiken mit unterschiedlicher Herkunft und Komplexität.
Bsp. **IoT-Risiken** (Internet of Things) durch Vernetzung von technischen Geräten wie TV, Drucker, Autos, Uhren etc. über Internet und interne Netzwerke.
Der Einsatz dieser Sensoren werden heute grösstenteils nicht geregelt. Oftmals werden sie als Bestandteil von technischen Anlagen einfach von den Lieferanten bezogen ohne Sicherheitskontrollen und einer Einbindung in die Sicherheitsarchitektur der Gesamtorganisation. Die Lieferanten sind zudem oft KMU ohne grosses IT-Knowhow und haben häufig Remote-Zugriff auf die technischen Anlagen. Sie sind somit der ideale Angriffsvektor, um das eigentliche Ziel anzugreifen.
Beispiel 2013 Target (USA): Hacking über einen Lieferanten für Klimasteuerungen. Schaden: 41 Mio. Kreditkarteninformationen von Kunden entwendet. Target bezahlt 18.5 Mio. USD in Vergleich.

>>> **Cyber Security ist eine ganzheitliche Betrachtung der Sicherheit.**



Das klassische Dreieck in der Informationssicherheit definiert die drei Schutzziele:

1. Verfügbarkeit: Informationen und die Systeme dazu müssen bei Bedarf vorhanden sein. Themen: Service Level Agreements SLA, Notfallkonzept, …

2. Vertraulichkeit: Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen. Der Schutz ist abhängig von der Klassifikation **öffentlich, intern, vertraulich, geheim/streng vertraulich.** Themen: Personendaten, Berechtigungen, Zutrittsschutz, anonymisierte Testdaten, clean desk policy, sichere Entsorgung, …

3. Integrität: Informationen müssen richtig und vollständig sein. Schutz vor ungewollter oder unabsichtlicher Veränderung und Inkonsistenzen. Themen: Backup + Restore, Inputvalidierung, Hash, Checksummen, …

Beim Datenschutz geht es um den Schutz von **Personen**daten! Das Schweizer Datenschutzgesetz (DSG) und der Datenschutzverordnung (VDSG) reglementiert den Umgang und den Schutz für private Personen und Firmen einerseits sowie für staatliche Behörden andererseits. Jeder Kanton erlässt eigene Datenschutzgesetze, v.a. für die Verwaltung des Kantons. Darin können diese Ziele erweitert oder verfeinert werden, bspw. Gemäss §8 des Informations- und Datenschutzgesetzes (IDG) von Basel-Stadt mit:

4. Zurechenbarkeit: Bearbeitungen von Informationen müssen Benutzern zugerechnet werden können (Themen: Dateneigner/innen, keine unpersönlichen Benutzerkonten etc.)

5. Nachvollziehbarkeit: Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein (wann, was, warum). Themen: Protokollierung, Mussfelder bei Buchungen, Visierung, Archivierungsfrist, …

4

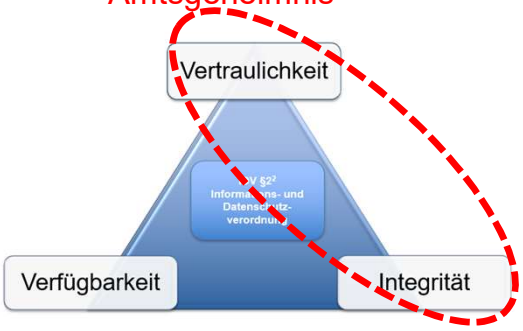
(Personen-)Datenschutz

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

Kriterien zur legitimen Datenbearbeitung:

a. Gesetzmässigkeit (!)
b. Verhältnismässigkeit
c. Zweckbindung
d. Transparenz
e. Richtigkeit
f. Informationssicherheit

Fokus Datenschutzbeauftragte:
- Personendaten
- besondere Personendaten (!)
- Amtsgeheimnis



«besonders schützenswerte» Personendaten:

besondere Gefahr einer Grundrechtsverletzung (Gesundheit, religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten, Sozialhilfe,…).
Persönlichkeitsprofil: Summe erlaubt eine Beurteilung wesentlicher Aspekte der Persönlichkeit.

a. Gesetzmässigkeit

Personendaten benötigen gesetzliche Grundlage (Gesetz oder Verordnung) und sind erforderlich zur Erfüllung einer gesetzlichen Aufgabe. «Besonders schützenswerte Personendaten» benötigen gesetzliche Grundlage (Gesetz. Verordnung reicht nicht) und sind zur Erfüllung einer gesetzlich klar umschriebenen Aufgabe zwingend notwendig.

b. Verhältnismässigkeit

Geeignetheit, d.h. Datenbearbeitung dient dem Bearbeitungszweck
Erforderlichkeit, d.h. Datenbearbeitung ist dem Bearbeitungszweck angepasst
Zumutbarkeit, d.h. vernünftiges Verhältnis zwischen dem Bearbeitungszweck und der Wirkung des Bearbeitens.

C. Zweckbindung

Datenbearbeitung darf nur zum selben Zweck stattfinden, der bei der Erhebung der Daten angegeben wurde. Zweckänderung muss in einem Gesetz vorgesehen sein.

d. Transparenz

betroffene Personen müssen erkennen können, dass Daten über sie bearbeitet werden.
Information über die Datenbearbeitung (rasch, umfassend und sachlich)

e. Richtigkeit

bearbeitete Daten müssen im Rahmen des Bearbeitungszwecks der Wahrheit entsprechen und vollständig sein.

f. Informationssicherheit

angemessene organisatorische und technische Massnahmen.
Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit (und je nach Kanton Zurechenbarkeit sowie Nachvollziehbarkeit).

Risiken werden oftmals als Funktion zwischen Eintrittswahrscheinlichkeit und potentiellem Schaden definiert. Für eine angemessene Beurteilung der effektiven Risikosituation muss man aber auch weitere Aspekte mit berücksichtigen:

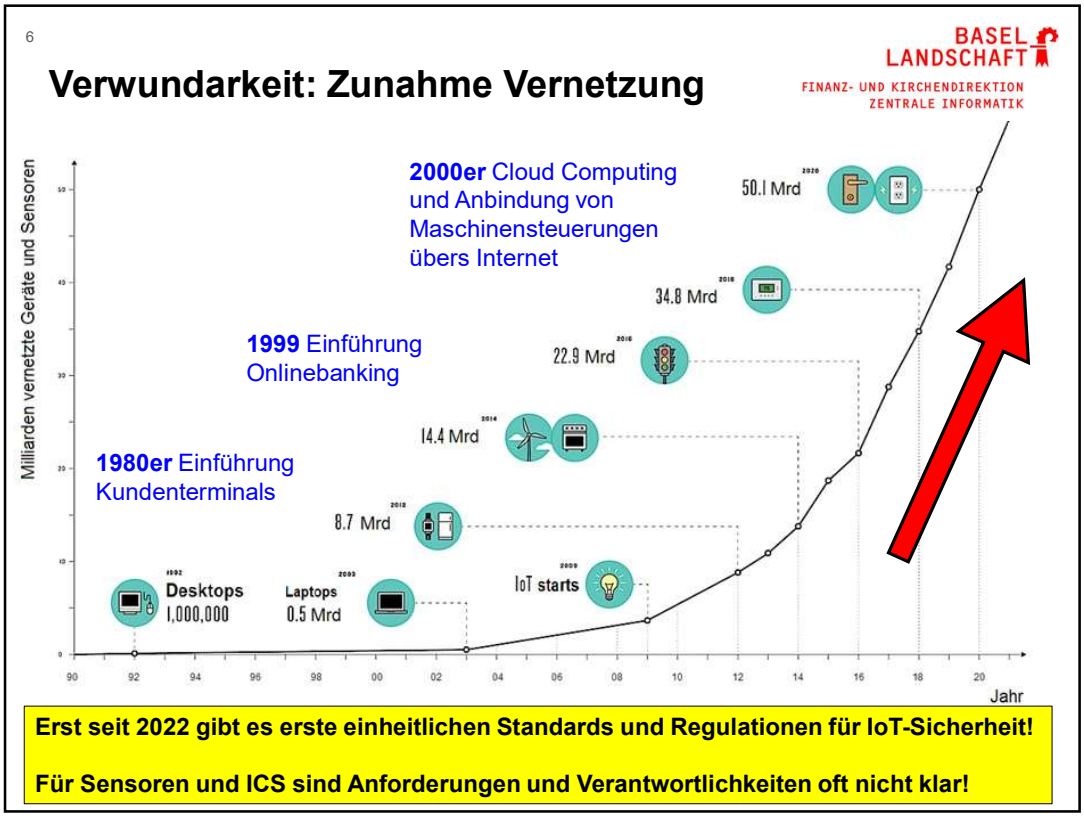
A) Welches sind die wirklich kritischen Werte, resp. Anlagen? Was muss besonders geschützt werden?

B) Wo bestehen Verwundbarkeiten, welche die Wahrscheinlichkeit erhöhen, dass ein Ereignis zu negativen Folgen führt?

C) Welche verschiedenen Szenarien von Bedrohungen inklusive der Kombinationen von Bedrohungen müssen berücksichtigt werden?

D) Welche unterschiedlichen Schäden können eintreten je nach dem Bedrohungsszenario und den Schwachstellen? Wo besteht je nach Kombination von Risikoszenario, Werte und Schaden der grösste Bedarf, um sich abzusichern?

Details auf den nachfolgenden Folien.

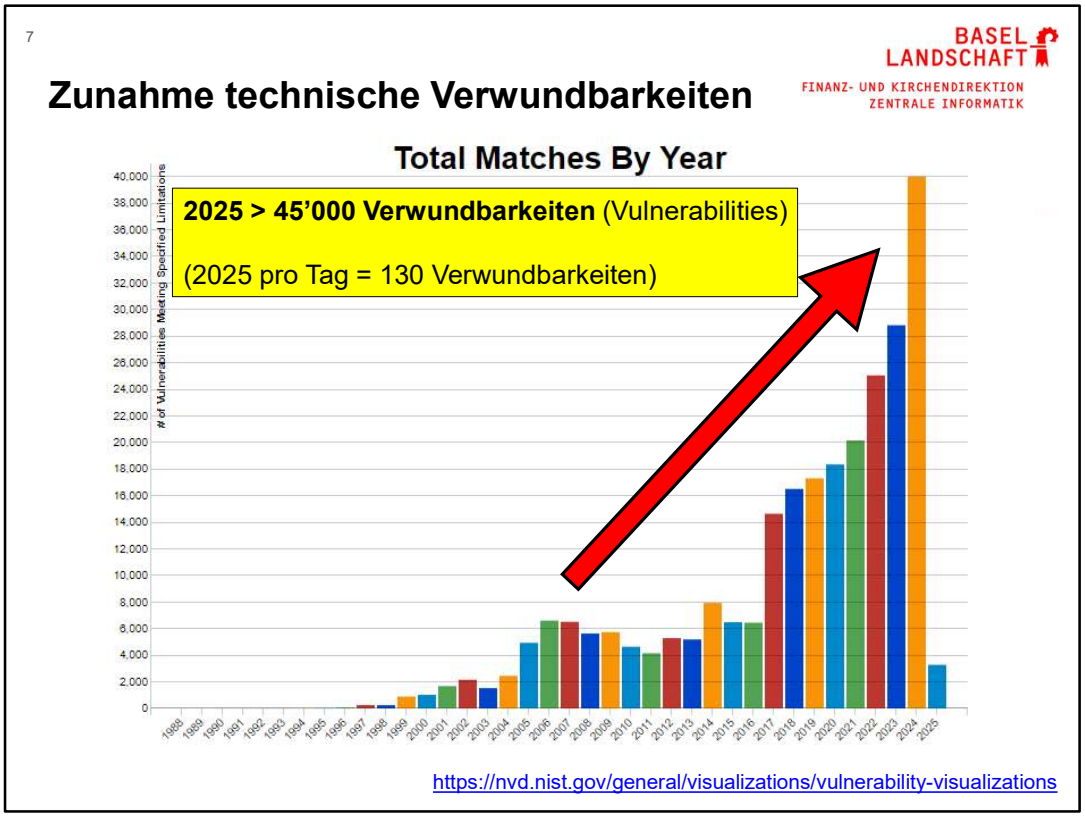


Je mehr Systeme verbunden sind, desto grösser werden die Abhängigkeiten. Damit steigt auch das Risiko, dass Systeme eingebunden werden, welche veraltet sind und ausfallen oder gehackt werden können. Nach dem Motto: „Never Change a winning team!“ oder „If it works, don‘t touch it!“ werden Systeme, die teilweise über Jahrzehnte nicht mehr aktualisiert wurden, auf einmal mit dem internen Netzwerk und direkt oder indirekt mit dem Internet verbunden, bspw. Produktionsmaschinen, Verkehrsampeln etc. Bei medizinischen Geräten war es bisher sogar so, dass diese nicht aktualisiert werden durften, um nicht die FDA-Zertifizierung zu verlieren (inkl. Sicherheits-Patches)!

Bei anderen Systeme erhalten Lieferanten Fernzugriff, um das System zu warten. Je nachdem, wie dieser Fernzugriff gemanagt wird, erhalten diese Externen damit potentiell Zugriff auf das gesamte interne Netzwerk. Solche Firmen sind das ideale Angriffsziel, um indirekt deren Kunden anzugreifen.

Das noch grössere Problem ist, dass viele technische Komponenten heute de facto IT-Systeme sind mit Sensoren, welche mit IT-Systemen kommunizieren zur Überwachung und Steuerung. Das betrifft Maschinen, Fahrzeuge, Videokameras etc. Ganz besonders kritisch ist das bei der Haustechnik mit einer Vielzahl an Steuerungssystemen für Türen, Licht, Klima, Brandmelder, Einbruchalarmanlagen etc.

Gerade bei öffentlichen Beschaffungen werden solche IT-Systeme meist nicht explizit berücksichtigt , sondern sind einfach Teil der Anlagen. Als absolutes Minimum müssen jedoch folgende Punkte geklärt und berücksichtigt werden:
- Festlegung der internen Verantwortlichkeiten zwischen IT, Technik und Fachbereich
- Klärung der Anforderungen für die Sicherheit und Schnittstellen zu anderen Systemen
- Prüfung der Sicherheitskonzepte und deren Umsetzung inkl. ausreichendes Testing!



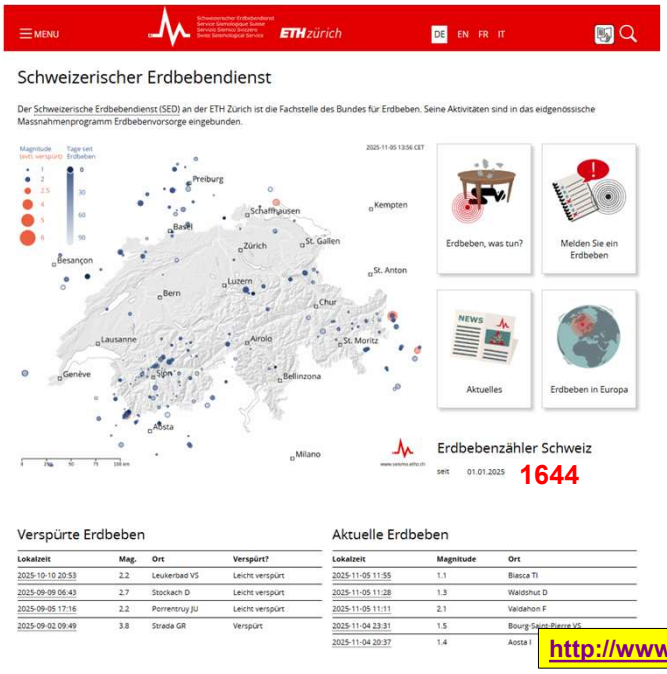
Verwundbarkeiten (Vulnerabilities) sind Schwachstellen des Herstellers oder bei den Anwendern, durch welche Fehler auftreten und/oder Hacker einbrechen können, z.B.
- Lieferant: Programmfehler, Unverträglichkeiten mit Hardware oder Software etc. Bspw. Crowdstrike im 2024.
- intern: fehlende Sicherheits-Updates, Fehlkonfiguration etc.

Je mehr Funktionalitäten, je schneller und agiler auf den Markt gebracht und je mehr vernetzt Systeme werden, desto mehr Verwundbarkeiten hat Software, d.h. mehr Möglichkeiten, wo Fehler und Probleme auftreten können und Sicherheitslücken, welche Hacker ausnützen können! Zum Beispiel neue Autos, welches voller Elektronik ist, die wiederum fehleranfällig sein könnte, verglichen mit alten Autos ohne Elektronik.

8

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

Bedrohung: Naturkatastrophen und IT



Verspürte Erdbeben

Lokalzeit	Mag.	Ort	Verspürt?
2025-10-10 20:53	2.2	Leukerbad VS	Leicht verspürt
2025-09-09 06:43	2.7	Stockach D	Leicht verspürt
2025-09-05 17:16	2.2	Porrentruy JU	Leicht verspürt
2025-09-02 09:49	3.8	Strada GR	Verspürt

Aktuelle Erdbeben

Lokalzeit	Magnitude	Ort
2025-11-05 11:55	1.1	Biasca TI
2025-11-05 11:28	1.3	Waldshut D
2025-11-05 11:11	2.1	Valdahon F
2025-11-04 23:31	1.5	Bourg-Saint-Pierre VS
2025-11-04 20:37	1.4	Aosta I

http://www.seismo.ethz.ch/de/home/

9

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

Bedrohung: Wer? Wieso?

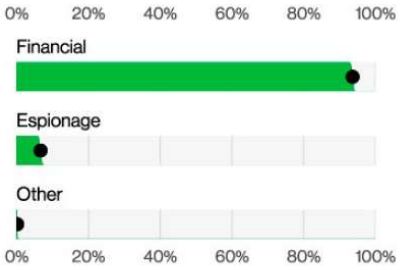


Figure 12. Threat actor motives in breaches (n=5,632)

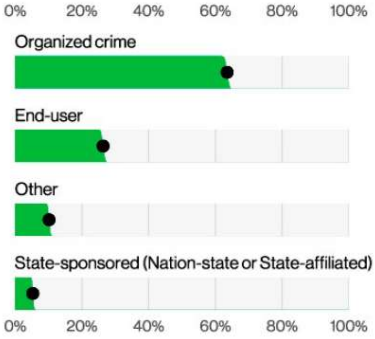
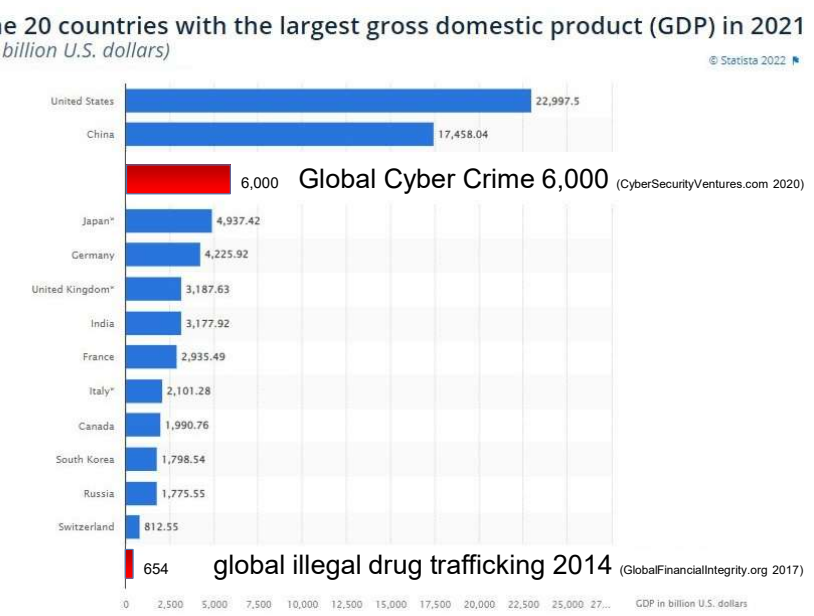


Figure 13. Threat actor varieties in breaches (n=7,921)

Gemäss Verizon Data Breach Report 2024 (DBR) erfolgt Hacking zu 95% aus finanziellen Motiven und zu über 60% durch das organisierte Verbrechen.

10



World GDP 84,705 billion U.S. dollars (data.worldbank.org 2022)

11

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

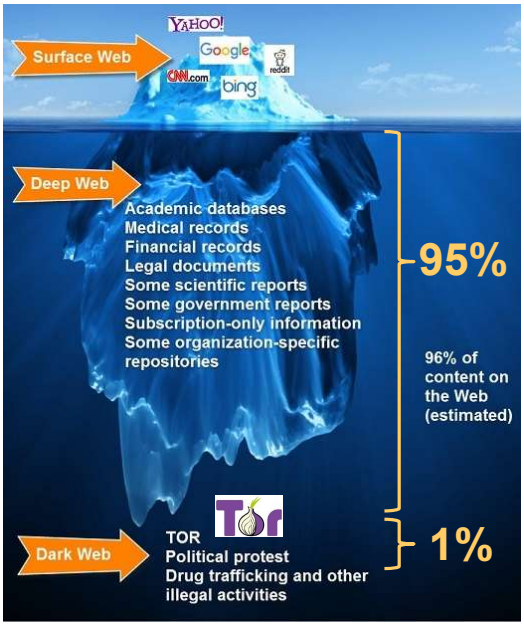
Bedrohung: Hacking as a Service (Darkweb)

Das organisierte Verbrechen ist im Cyber Crime angekommen.

Auch ohne technisches Wissen kann man Cyberangriffe in Auftrag geben inkl. AGBs, Hotline etc. «HaaS» analog zu SaaS (Cloud = SW as a Service oder Plattform as a Service).

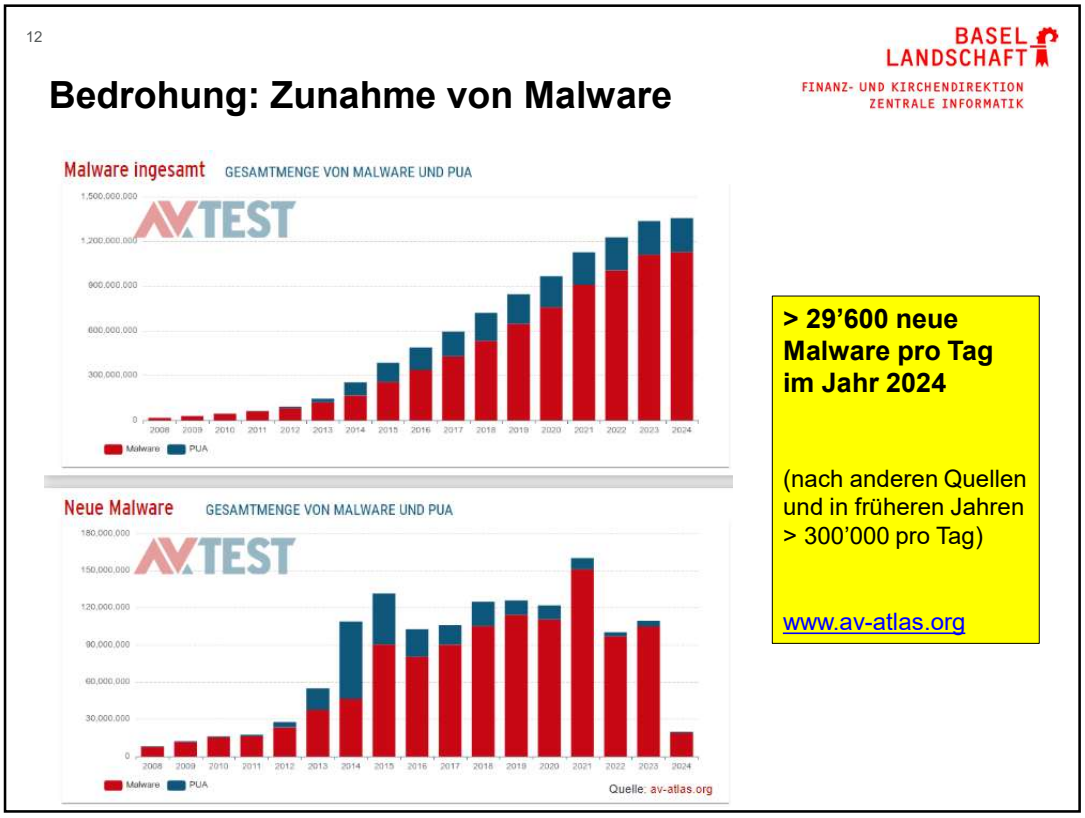
z.B. DDoS

Es gibt berechtigte Gründe fürs Darknet (bspw. Menschenrechts-aktivisten), aber nach einer Studie enthalten **57% der Webseiten im Darknet** illegales Material (Drogen, Waffen, Malware etc.). Viele davon mit kommerziellen Strukturen.



Der Begriff „Cyberattacken“ umfasst viele **unterschiedliche Angriffsmethoden** mit jeweils einer Vielzahl unterschiedlicher Technologien. So gibt es beispielsweise alleine 29 verschiedene Arten von Angriffen über USB-Ports. (Hier ist eine Liste von 29 verschiedenen Arten von USB-Angriffen – ZAM)

Im Darknet besteht längst ein Markt für kundenspezifische Cyberattacken (Crime-as-a-service) wo man vom Einsteiger bis zum Experten komplexe Hacking-Werkzeuge und illegale Services einkaufen kann, z.B.:
- Kreditkarten mit PIN
- Viren
- DDOS
- Hacking-Services



Wenn es um Malware geht, ist Ransomware eine der am schnellsten wachsenden Bedrohungen der jüngeren Geschichte. Nach Angaben des Antivirensoftware-Anbieters Emsisoft beläuft sich die liberale Schätzung für die Kosten im Zusammenhang mit Ransomware-Hacks allein für 2019 auf 7,5 Milliarden.
(Quelle: https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector/)

13

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

Cyber-Angriffe verändern sich fortlaufend

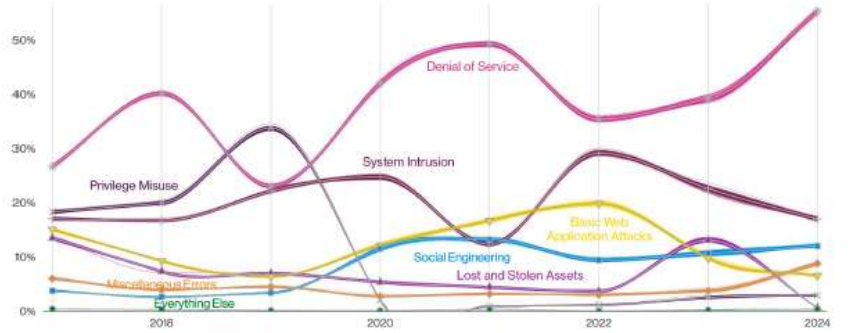


Figure 26. Patterns over time in incidents

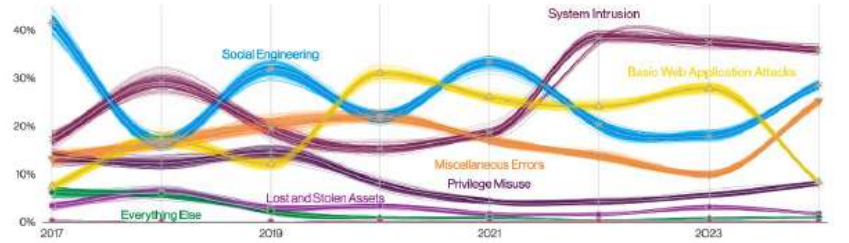


Figure 27. Patterns over time in breaches

14

Hacks

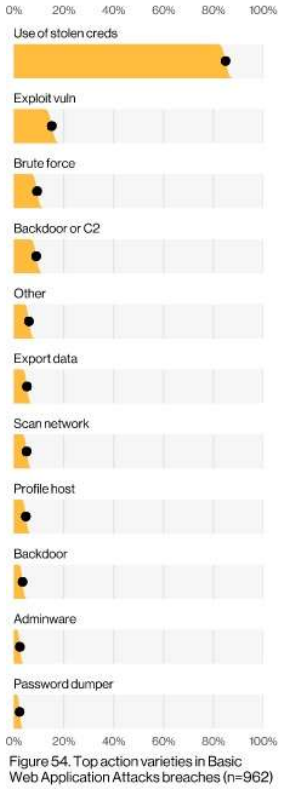


Figure 54. Top action varieties in Basic Web Application Attacks breaches (n=962)

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

Phase 1: Eindringen und Festsetzen

Phase 2: Ausspionieren und erlangen von Administratorenrechte. Damit können Hacker sich dann quer durchs Netzwerk bewegen und in Systeme eindringen.

Schützen Sie ihre Passworte (Credentials) vor allem Personen und Administratoren mit weitreichenden Berechtigungen!

Seien Sie misstrauisch, schützen Sie ihre Passworte, halten Sie sich an Vorgaben und geben Sie Passworte nicht weiter!

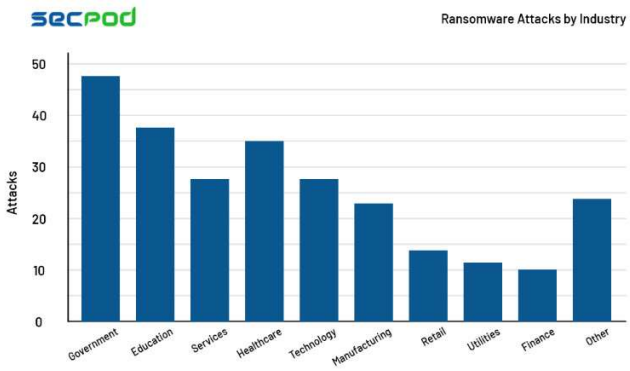
Wo immer möglich **2-Faktor-Authentifizierung!** Vor allem privates Email, Google, Facebook!!

Abbild links: Aktionen bei erfolgreichem Hacking .
Quelle: Verizon Data Breach Report 2022

15

Schaden: Häufigste Angriffsziele

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK



Trellix Cyber Threat Report Q1 2023

Die öffentlichen Verwaltungen und ihre Daten sind ein primäres Angriffsziel. Dabei geht es vor allem darum, die Daten zu Geld zu machen oder die Opfer zu erpressen. Andere Motive wie Spionage oder Sabotage dürfen aber nicht vernachlässigt werden.

Angriffe auf KMU werden immer häufiger verwendet als Sprungbrett um das eigentliche Opfer via Fernzugriff-Anbindungen anzugreifen.

Mindestanforderungen für die externe Datenbearbeitung und für technische Systemanbindungen sollten definiert, vertraglich festgelegt und eingefordert werden, falls möglich mit Sicherheitsaudits. Von den internationalen Standards sind Mindestanforderungen zu erwarten (ISO27001/27002, ITIL, NIST Cyber Security Framework). Darauf warten kann man aber nicht!

16

2016 Neues IT-Sicherheits-Paradigma

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK


Süddeutsche Zeitung
SZ.de Zeitung Magazin
Wirtschaft Panorama Sport München Bayern Kultur Wissen Digital Ch
04. März 2016 11:51 Internet
Paradigmenwechsel bei IT-Sicherheit: Das Ende der Brandmauer


SECURITYWEEK NETWORK: Information Security News | Infosec Island | Suits and Spooks
SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS
Subscribe (Free) | CISO Forum
June 2, 2016 Half Moon Bay, CA
Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture
From Prevention to Detection: A Paradigm Shift in Enterprise Network Security

Man muss davon ausgehen, bereits gehackt zu sein!

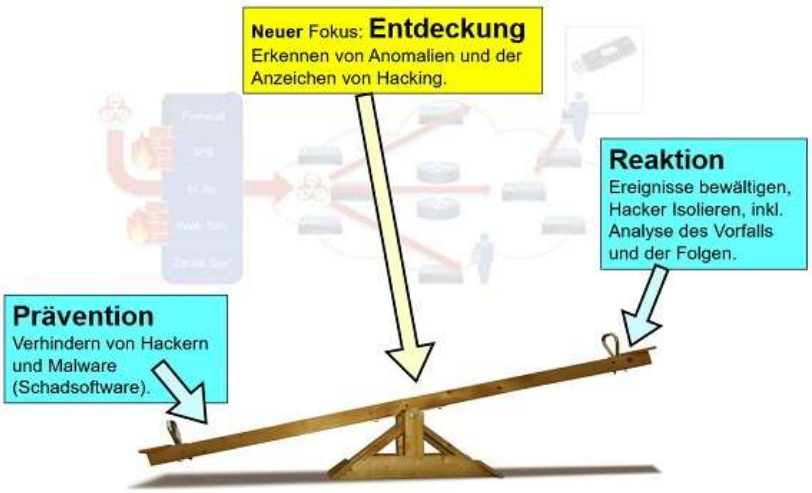
… man muss sich aber auch um die anderen IKT-Risiken vorbereiten!

Die Informationssicherheit muss sich auf den «real deal» vorbereiten, anstatt sich die Risiken mit der Wahrscheinlichkeiten schön zu rechnen!

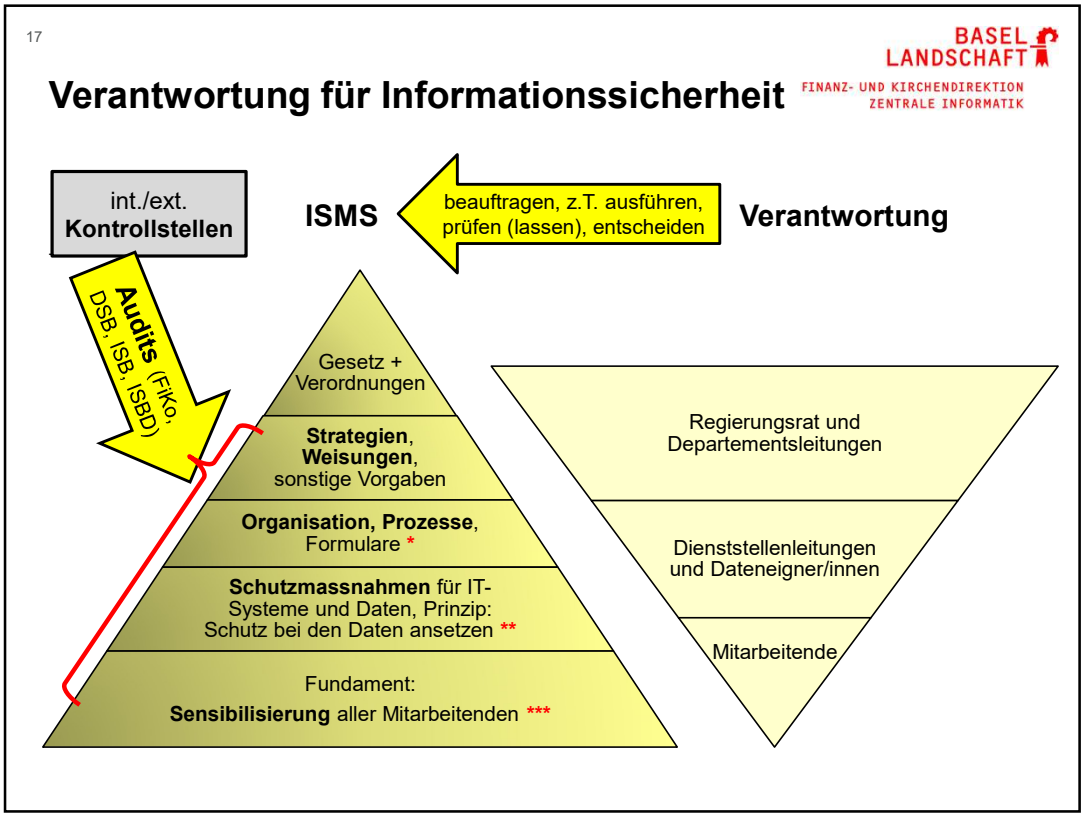
Die Gefahr von modernen langanhaltenden Cyberattacken, sogenannten **APT**'s (Advanced Persistent Threats) ist nachhaltig gestiegen. APT's erfolgen mittels Kombinationen unterschiedlicher Techniken und Vorgehensmuster wie gezieltes Social Engineering gegen Einzelpersonen (=Spearfishing), moderne Malware, das Ausnützen neuer Schwachstellen und Hintertüren im Internet der Dinge (**IoT**) etc.

Die Zunahme von…
+ Vernetzung und Digitalisierung
+ Verwundbarkeiten
+ Bedrohungen/Angriffsvektoren
+ Komplexität der Angriffe
+ Kryptowärungen

= Paradigmawechsel 2016:



Fazit: Es gibt zwei Arten von Organisationen:
1. die welche gehackt wurden,
2. die welche es noch nicht wissen!



* Prozesse sind abzusichern mit auf Risiken ausgerichtete Kontrollen. Die Prozesse sind zu dokumentieren und zu schulen. Das schützt Mitarbeitende vor:
1. aus Unwissenheit begangene Fehler
2. Social Engineering Angriffe um mittels Druck Mitarbeitende dazu zu bringen, Prozesse nicht einzuhalten. Auch ein CEO oder CFO muss Prozesse einhalten für rasche Geldüberweisungen!

>>> Keine Bestrafung von Mitarbeitenden, die auch gegenüber dem Top-Management auf die Einhaltung der vorgeschrieben Prozesse und Formulare beharren (CEO-Fraud)!

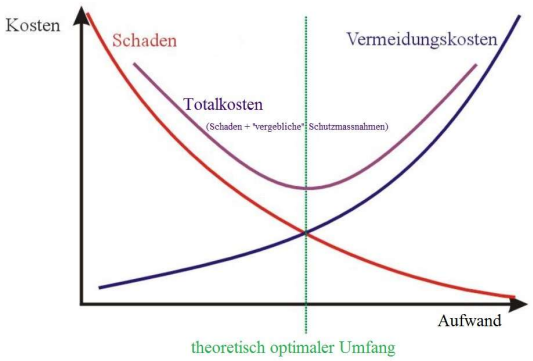
** Wo möglich sind in den Systemen Kontrollen präventiv und automatisiert einzubauen, bspw. Berechtigungseinschränkungen, Funktionstrennungen, Buchungsperiode sperren in SAP etc.

*** Das Fundament der Informationssicherheit ist die Sensibilisierung (Awareness) der Mitarbeitenden. Diese müssen die Vorgaben kennen (oder zumindest wissen, wo etwas nachgeschaut werden kann). Sie sensibilisiert werden, wie die Prozesse abzuwickeln sind, welche Informationen zu welcher Klassifizierung gehören und wie diese zu schützen sind. Sie müssen ein Gefühl dafür entwickeln welche Risiken bestehen und wie man Gefahren erkennt, bspw. Phishing.

18

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

Sicherheit = Risikoreduktion kostet ! ! !



Grundsatz: Massnahmen sollten nicht mehr kosten, als das verhinderte Risiko!

Problem 1 Kalkulierbarkeit: Risiken (Wahrscheinlichkeiten, potentieller Schaden etc.) lassen sich nicht genau berechnen aber gut „schönrechnen“, bspw. Erdbeben!

Problem 2 Moral-Hazard (Fehlanreize, unmoralisches Verhalten, Nachfolgerproblem)

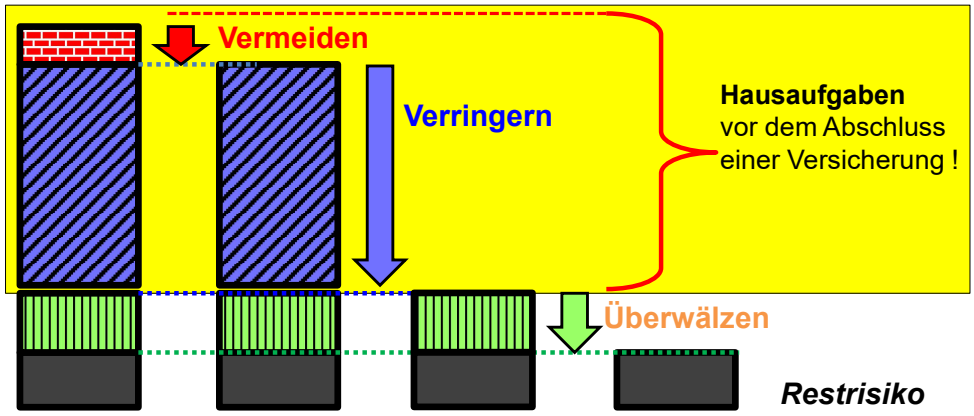
Lösung: Beim Schaden ansetzen, Annahmen offenlegen und Benchmarks verwenden!

19

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

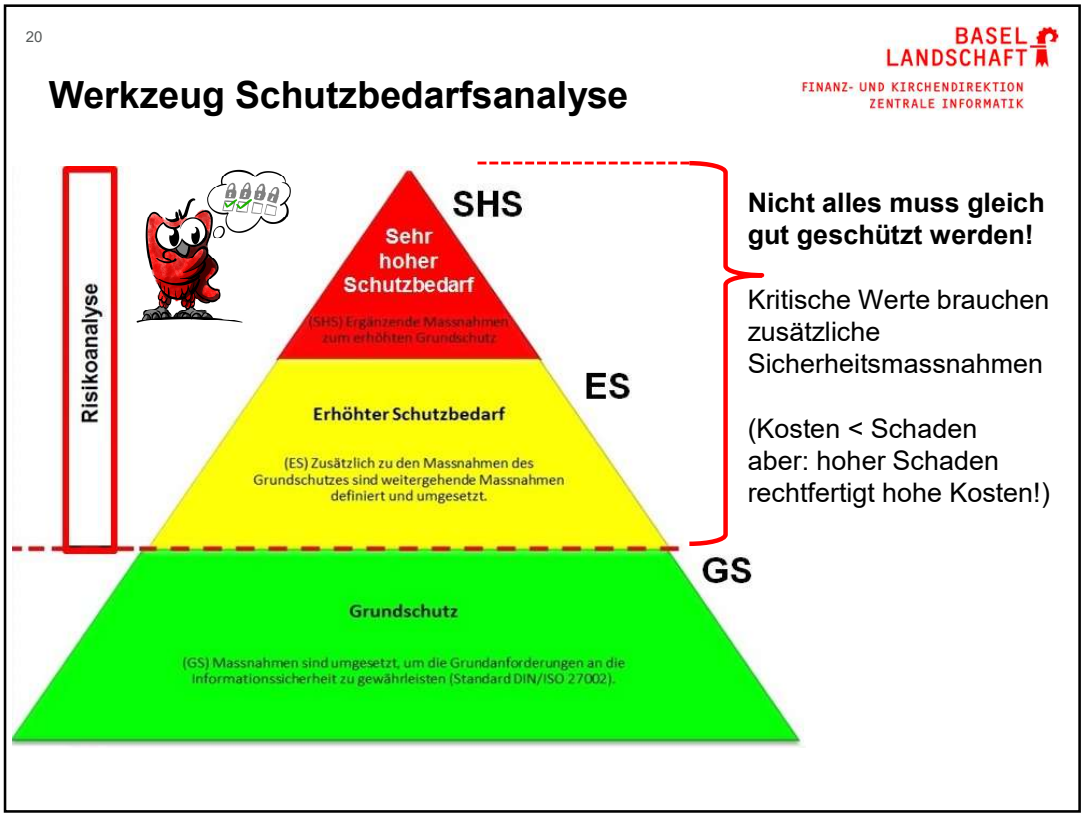
Richtiger Umgang mit Risiken

Bruttorisiko



Vor Abschluss einer Cyber-Versicherung müssen die Risiken genau analysiert und soweit möglich vermindert werden! (Versicherung nur inkl. Notfall-Support!)

Das Management bleibt immer für alle Risiken verantwortlich unabhängig von der Technologie.



Mittels der **Schutzbedarfsanalyse** werden für alle IKT-Systeme, -Anwendungen, Services und -Projekte das benötigte Sicherheitsniveau ermittelt. Davon hängt ab, welche Sicherheitsmassnahmen zusätzlich zu den obligatorischen Massnahmen des Grundschutzes zu implementieren sind. Zur Klassifizierung der Systeme und deren Daten wird ein standardisierter Kriterienkatalog benötigt, z.B.:

GS	ES	SHS
Öffentliche und interne Information	**Vertrauliche Information**	**Geheime Information**
Keine Personendaten und Personendaten	**Besondere Personendaten**	
Betriebszeiten nach Standard SLA	Spezialanforderungen	**7 x 24 x 365**
Max. Ausfall > 1 Arbeitstag	**Ausfall max. 8 Std**	**Ausfall bis max. 4 Std**
Bis 2 Ausfälle / Quartal	**Spez. Servicevertrag**	**Keine Ausfälle**
Keine Notfall-Relevanz	**IT-Notfallrelevanz**	

Bsp.1: Krankendaten = besondere Personendaten nach IDG = ES erhöhter Schutzbedarf beim Schutzziel Vertraulichkeit.

Bsp.2: Regierungsgeschäfte = vertrauliche Daten = «nur» ES erhöhter Schutzbedarf (auch wenn «geheim» drauf steht.) beim Schutzziel Vertraulichkeit

Bsp.3: Blaulichtorganisationen = Verfügbarkeitsanspruch 7 x 24 x 365 ohne Ausfall = sehr hoher Schutzbedarf in der Verfügbarkeit

Das Datenschutzgesetz, resp. die Verordnung schreiben zwingend vor, dass IKT-Systeme und deren Daten mit angemessenen organisatorischen und technischen Massnahmen geschützt werden müssen. Was dabei genau «angemessen» bedeutet, wird nicht definiert. Das ändert sich aufgrund der technischen Entwicklung auch fortlaufend. Daher muss jede Organisation für sich definieren, welche organisatorischen und technischen Massnahmen genau angemessen sind.

Angemessen heisst, dass…:

1. Standardisierte Prozesse werden regelmässig und systematisch angewendet.

2. Die Massnahmen sind auf den Schutzbedarf der Systeme und deren Daten ausgerichtet >>> Schutzbedarfsanalyse

3. Die Massnahmen sind auf die Risiken ausgerichtet >>> Risikoanalyse

4. Mittels Sicherheitsweisungen und Prozessvorgaben wird ein Minimum an Massnahmen definiert, welche umgesetzt werden müssen. Dies kann je nachdem unterschiedlich sein je nach der Einstufung des Schutzbedarfs und der Risikosituation.

5. Zur Identifizierung der konkreten technischen Umsetzung und zum Vorgehen bei Unsicherheiten sind Prozesse und Standards zu definieren, wonach man sich richten soll.

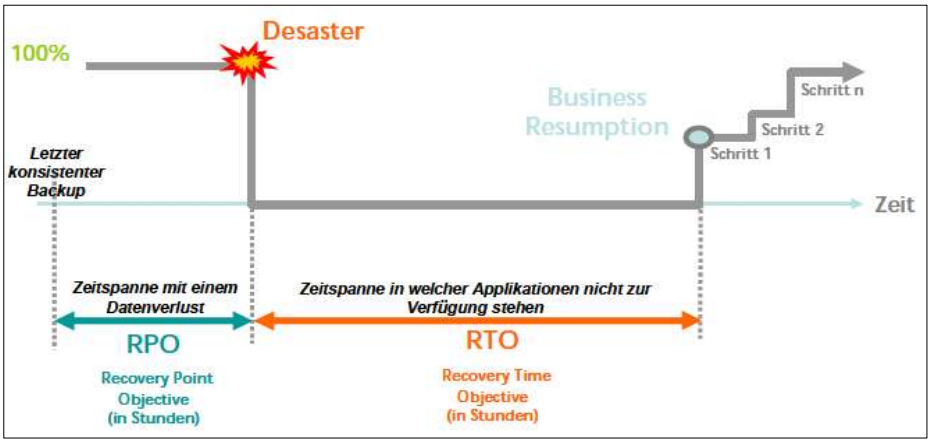
6. Compliance-Lücken sind Schwachstellen und müssen festgehalten und mittels

kompensierenden Massnahmen adressiert werden.

22

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

BCM-Notfallvorkehrungen



BCM (Business Continuity Management) zur Aufrechterhaltung der Leistungserbringung und schnellst möglicher Rückkehr zum Normalzustand.

Ausgangspunkt beim BCM sind die Anforderungen der Geschäftsbereiche. Sie bestimmen, wie wichtig und zeitkritisch die Verfügbarkeit und die Integrität der Geschäftsleistungen sind. Davon abhängig müssen Vorgaben zum Schutz und für die Wiederherstellung der Prozesse, der Systeme und der Daten gemacht werden.

Die IT-Notfallplanung ist ausgerichtet auf die Anforderungen der Geschäftsbereiche an die Informatik gemäss BCM.

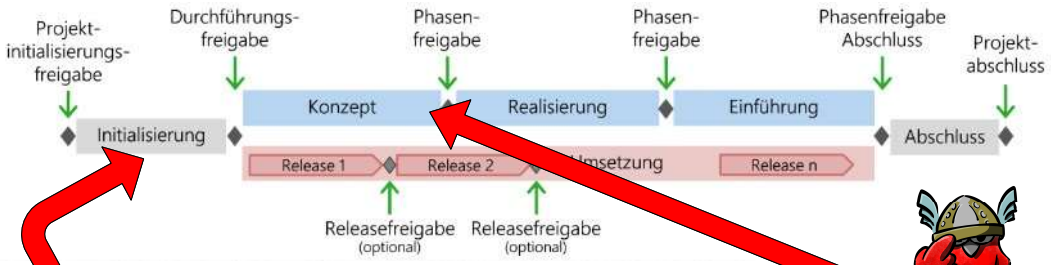
RPO (Recovery Point Objective): Maximaler Datenverlust (inkl. Systemeinstellungen) seit letzten Backup. (SLA: Umfang, Häufigkeit und Speicherort)

RTO (Recovery Time Objective): Maximale Ausfallzeit bis zur Wiederaufnahme mit beschränkter Systemunterstützung. (SLA: Priorisierung Geschäftsprozesse, Notfallprozesse und –Tests etc.)

23

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

IS und Datenschutz in Projekten



Rechtsgrundlageanalyse
+ SCHUBAN (Schutzbedarfsanalyse zur Datenklassifizierung)
+ Checkliste DSFA* / Vorabkonsultation Datenbearbeitung
= **Erstkontakt** Aufsichtsstelle Datenschutz (ASD)

+ ISDS** (inkl. Schutzmassnahmen, Restrisiken, Berechtigungskonzept etc.)
+ Risikoanalyse
= Datenschutzprüfung ASD

* DSAFA = Datenschutzfolgenabschätzung, ** ISDS = Informationssicherheit + Datenschutzkonzept

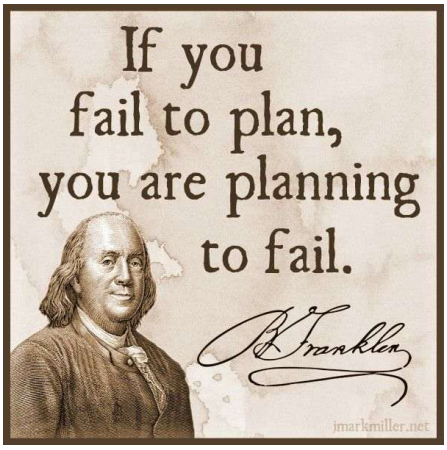
Vorlagen: 1. lhttp://kww.infoblits.bl.ch/informationen/informationssicherheit/dokumente-der-informationssicherheit.html
2. https://projektportal.bl.ch/sites/hermes/SitePages/HERMES-Vorlagen%20und%20Beispiel-Dokumente.aspx

24

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

Fragen?

Vielen Dank für Ihre Aufmerksamkeit!!



Pascal Reiniger
Kantonaler Informationssicherheitsbeauftragter (KIT-SIBE / CISO)
Finanz- und Kirchendirektion Basel-Landschaft
Rheinstrasse 33b
pascal.reiniger@bl.ch

25

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

WEF Global Risk Report Januar 2026

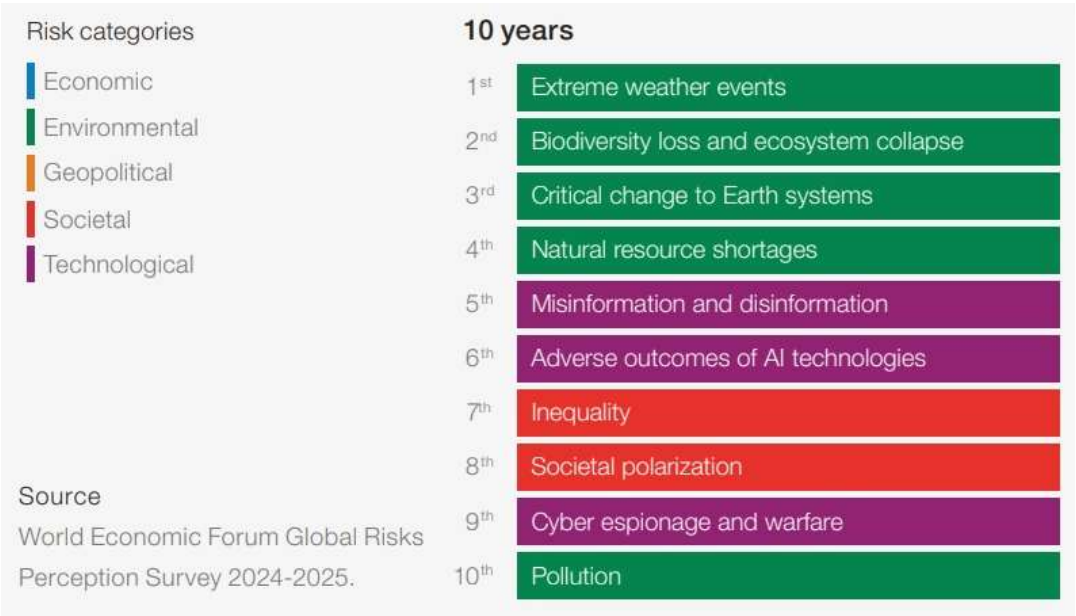
Global risks ranked by severity, short term (2 years) and long term (10 years)

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period."

Short term (2 years)	Long term (10 years)
1. Geoeconomic confrontation	1. Extreme weather events
2. Misinformation and disinformation	2. Biodiversity loss and ecosystem collapse
3. Societal polarization	3. Critical change to Earth systems
4. Extreme weather events	4. Misinformation and disinformation
5. State-based armed conflict	5. Adverse outcomes of AI technologies
6. Cyber insecurity	6. Natural resource shortages
7. Inequality	7. Inequality
8. Erosion of human rights and/or of civic freedoms	8. Cyber insecurity
9. Pollution	9. Societal polarization
10. Involuntary migration or displacement	10. Pollution

Source
World Economic Forum Global Risks Perception Survey 2025-2026

Risk categories: Economic, Environmental, Geopolitical, Societal, Technological



26

Übung: Wie die Organisation absichern?

1. **Verwundbarkeits- und Update-Management (Patching)**
   > Sicherheitslücken entdecken + stopfen! (siehe in Youtube: „Rob Joice, NSA TAO Enigma“ https://www.youtube.com/watch?v=bDJb8WOJYdA&t=2s (Enigma 2016 NSA TAO Rob Joyce)
2. **Schutzbedarf festlegen und Klassifizieren**
   > Kritische Daten, Systeme Leistungen identifizieren.
   > Was muss prioritär geschützt werden – egal von der Form (digital, Papier etc.)
3. **Vorgaben, Organisation und Prozesse festlegen/anpassen**
   inkl. Sicherheitsstrategie und –Weisungen inkl. Schulung
   > Orientierung an etablierten Standards oder Empfehlungen.
   > Sensibilisieren: Die beste Sicherheit nützt nichts, wenn sie nicht bekannt sind oder ignoriert werden.
4. **Risiko Management und Notfallplan** (Org., Prozesse, Tests)
   > Inklusive Anforderungen Business (Business Impact Analyse BIA) und Wiederherstellungsübungen.
   > Revisionsweisheit: Was nicht dokumentiert und getestet ist, gibt es nicht! (d.h. funktioniert sicher nicht!)
5. **Technik: Firewall, Malwareschutz, starke Passworte etc.**
   > Moderne Sicherheitskomponenten auf einander abgestimmt.
   > Bestehende Systeme (Software, Hardware) sicher konfigurieren (= härten, siehe Punkt 1)
6. **Partnerschaften mit etablierten Experten eingehen**
   > Aufbau ISMS und Monitoring
   > Verfügbarkeiten (SLA), Change Management und Dokumentation klären!
   > Bei Outsourcing «Right-to-Audit» und Rückführung vertraglich regeln (u.a. Recht an den Daten)

Voraussetzungen für Cyber-Versicherung

1. **Vorgaben und Konzepte festlegen**: Sicherheitsstrategie, ISMS-Konzept, Weisungen etc.
2. **Geschäftsprozesse**: definieren, dokumentieren (ISO 9001 QM, IKS etc.), verantwortliche Stellen zuordnen und schulen.
3. **Risiko Management**: Schutzbedarf und Risiken inkl. Business Impact Analyse (BIA) erfassen und fortlaufend beurteilen.
4. **Schutzmassnahmen zur Risikoreduktion** (Business Continuity Management (BCM)) definieren, in Prozesse einbauen, dokumentieren, umsetzen, Verantwortungen zuteilen und sensibilisieren/schulen.
5. **Audits:** Regelmässige Audits und Tests inkl. Notfallprozeduren zur Wiederherstellung durchführen und ins Risiko Management einspielen. Verbleibende offene Risiken bewirtschaften.

27

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

Orientierung an Standards z.B.:

ISO 27001 / 27002 (bspw. für Informationssicherheits-Managementsystem ISMS)
https://www.iso.org/isoiec-27001-information-security.html

NCSC Nationales Cyber Security Center (BACS): https://www.ncsc.admin.ch/

SVS Sicherheitsverbund Schweiz (**Gratis-eLearning**): https://elearningcyber.ch/de

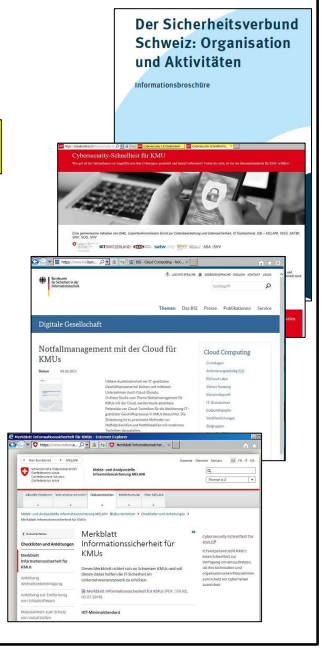
BSI (DE Bundesamt für Sicherheit in der Informationstech. bspw. für Sicherheitsmassnahmen) https://www.bsi.bund.de/

NIST (US National Institute for Standards and Technology, v.a. für Organisation):
https://www.nist.gov/cyberframework

CIS (Center for Internet Security, bspw. für System-Härtung):
https://www.cisecurity.org/

CH Bund IKT-Minimalstandard:
https://www.bwl.admin.ch/de/ikt-minimalstandards

SVS (Sicherheitsverbund Schweiz) Nationale Cyberstrategie (NCS):
https://www.ncsc.admin.ch/ncsc/de/home/strategie/cyberstrategie-ncs.html



28

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

Mögliche Schnellchecks

Gehackte Benutzer / Passworte:
https://haveibeenpwned.com/

Sicherheit Webseite:
https://observatory.mozilla.org/

Sicherheit Links und Doklumente:
https://www.virustotal.com/ (Achtung: Kein Hochladen vertraulicher Informationen!)

Domains (DNS-Server, IP-Adressen) und Scan der offenen Firewall-Ports:
https://censys.io/
https://dnsdumpster.com (Eingabe ohne „www.“ bspw. „bs.ch“)
(https://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports)

Phishing-Domains:
https://dnstwister.report/

Zufriedenheit der Mitarbeitenden:
https://www.kununu.com/

Generelle Checkliste:
https://ictswitzerland.ch/themen/cyber-security/check/online-check/

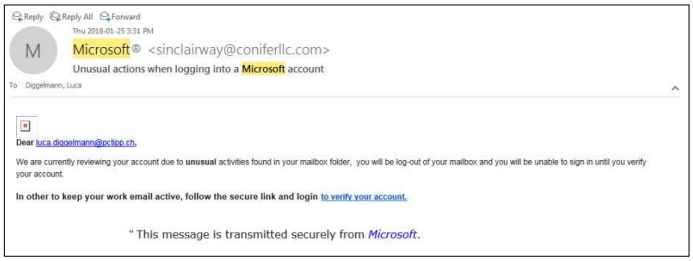
29

Social Engineering / Phishing erkennen

BASEL LANDSCHAFT
FINANZ- UND KIRCHENDIREKTION
ZENTRALE INFORMATIK

- Nachdenken, ob Email oder Info auf Webseite **Sinn macht** (bspw. Preise)?!
- Es wird **Druck** aufgebaut (physisch, zeitlich).
- Anrede, Grussformel, Rechtschreibung und/oder Grammatik stimmt nicht.
- Name und Adresse des Absenders überprüfen.
- Abbrechen und bei offizieller Webseite oder Tel. Nr. zurückrufen!
- Vorsicht vor Links, falschen URL / Webseiten und Eingaben!
- **Links und URL und Anhänge prüfen**, bspw. mit www.virustotal.com
- Keine https-Verbindung
- Zertifikat falsch
- Vorsicht bei **Waterhole**!
  (gehackte oder falsche Webseiten von Restaurants oder Anbietern)

https://www.ebas.ch/phishing-test/



Phishing wird immer professioneller. Ein grosser Teil basiert jedoch auf der grossen Masse und Empfängern und Zufallstreffer, bspw. Wahrscheinlichkeit, dass die Empfänger Kunden sind von UBS, Credit Suisse, Post oder Amazon und gerade etwas erwarten.

Auf Kleinigkeiten achten. Oft sind Dinge anders, aber kaum sichtbar, bspw. www.SWlSSCOM.ch mit einem kleinen «L» anstatt ein grosses «i».

Ein weiteres Merkmal sind ungewöhnliche Versandzeiten von E-Mails oder solche, die zu Zeiten eintreffen, wo die Aufmerksamkeit gering und das Mailvolumen hoch ist.: