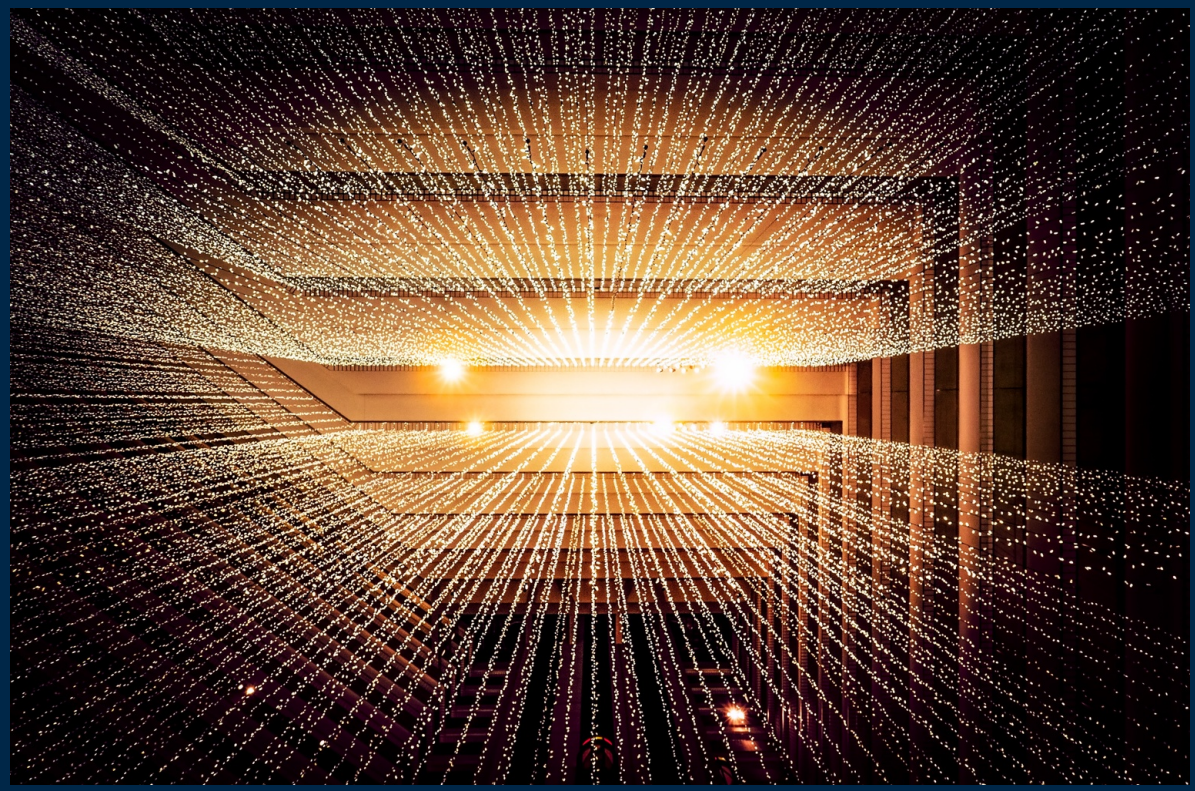
OneGov Cloud als resiliente Plattform für die Digitalisierung der Verwaltung

Resilienz (Psychologie)

«**Resilienz** (von lateinisch *resilire* ‚zurückspringen' ‚abprallen') auch Anpassungsfähigkeit, ist der Prozess, in dem Personen auf Probleme und Veränderungen mit Anpassung ihres Verhaltens reagieren.»

https://de.wikipedia.org/wiki/Resilienz_(Psychologie)



Cyberattacke auf die Gemeinde Rolle VD

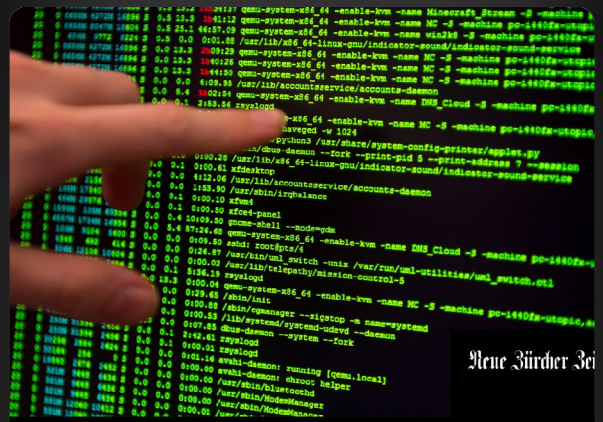
Tausende persönliche Daten im Darknet: Die Cyberattacke auf Rolle ist gravierender als von den Behörden kommuniziert.

- Ransomware-Attacke mit Lösegeldforderung
- Eskalation mit Publikation sensitiver Informationen über Bürger, Mitarbeiter und Unternehmen im Darknet
- AHV-Nummern, Adressen, Geburtstage, Zivilstandsangaben, Schulnoten etc.

NZZ vom 25. August 2021

Cyberattacke auf Rolle ist deutlich schlimmer als kommuniziert

www.nzz.ch



Cyberattacke von Rolle: Behördliches Versagen sollte Lehre sein

www.nzz.ch

Warum wird es immer schlimmer?

1. Oberfläche für Angriffe wird grösser: alles im Internet.
2. Volumen gespeicherter Daten steigt.
3. Der Angreifer scheint technisch im Vorteil und kann sich gut verstecken.

https://www.inspire.ethz.ch/en/research-for-the-industry/industry-4.0-digitisation-iot/internet-of-things/

Internet of Things (IoT)

www.inspire.ethz.ch

Wie läuft ein Cyber Angriff ab?

1. Initial compromise
2. Establish foothold
3. Escalate privileges
4. Internal reconnaissance
5. Move laterally
6. Maintain presence
7. Complete mission

https://en.wikipedia.org/wiki/Advanced_persistent_threat

The Cyber Kill Chain

Das Konzept des «Kill Chain» ist Angriffsmodell des Militärs und wurde von Lockheed Martin für die Informationssicherheit adaptiert.

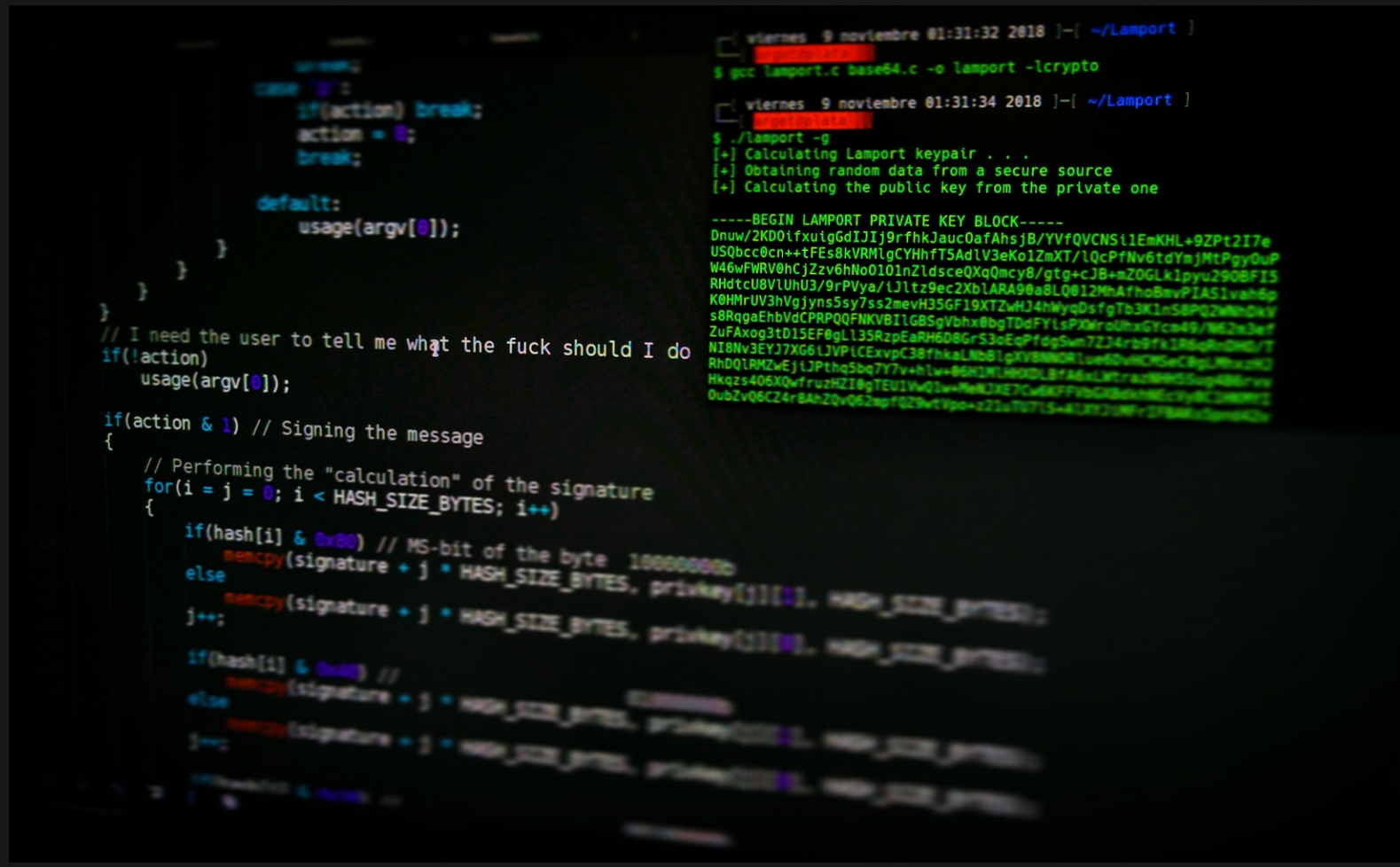
https://www.ondeso.com/wp-content/uploads/2021/04/cyber-kill-chain-freebie-ondeso.pdf

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

“Zero-day”

Die englische Ausdruck „**Zero-Day**“ bezieht sich auf die Tatsache, dass ein Hersteller oder Entwickler gerade erst von diesem Fehler erfahren hat und damit „Null Tage“ Zeit hat, ihn zu beheben.

Was kann ich tun, um mich gegen eine Zero-Day Sicherheitslücke zur schützen?



"Zero Days" kann man kaufen

The price range for 0day exploits is from $60,000 (Adobe Reader) up to $2,500,000 (Apple iOS) per one zero-day exploit.

https://www.wired.com/story/untold-history-americas-zero-day-market/

The Untold History of America's Zero-Day Market

www.wired.com

Der Faktor Mensch

90% aller Sicherheitsvorfälle sind auf menschliche Fehler zurückzuführen.

IBM Cyber Security Intelligence Index

https://www.ibm.com/security/data-breach/threat-intelligence?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US

Cyber Hygiene

1. Password Manager
2. Two-factor authentication
3. Software (Hardware) Updates
4. Data Backups
5. Awareness Training
6. ....
7. ...
8. Employ a Cyber Security Framework

Cyber-Hygiene ist wie Zähneputzen

www.security-insider.de

What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best...

digitalguardian.com

Organisatorische und technische Massnahmen

Zertifizierung ISO/IEC 27001:2013

1. Sensibilisierung der Mitarbeitenden
2. Organisatorische Massnahmen
3. Technische Vorkehrungen

swiss safety center

swiss safety center ISO/IEC 27001 certified system

Zertifikat

Die Zertifizierungsstelle von Swiss Safety Center AG
bescheinigt, dass die Firma

seantis gmbh
Pilatusstrasse 3
CH-6003 Luzern

seantis
data. web. applications.

für den Geltungsbereich

Entwicklung und Betrieb von digitalen Plattformen für die medizinische Forschung, die öffentliche Verwaltung sowie für die Aviatik

ein **Informationssicherheitsmanagementsystem (ISMS)**
erfolgreich anwendet nach

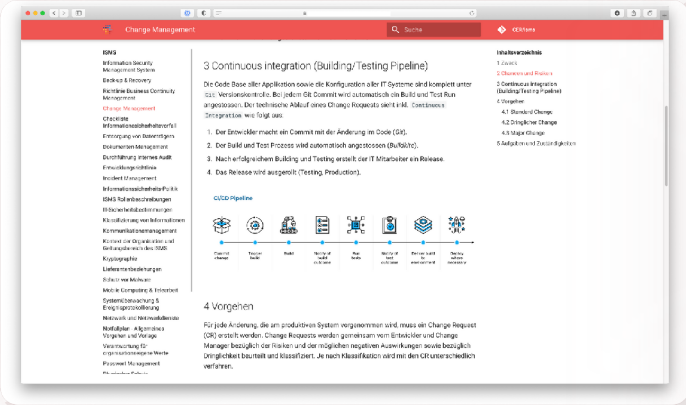
ISO/IEC 27001:2013

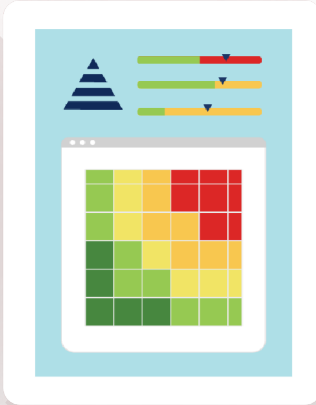
Erklärung zur Anwendbarkeit:	**29.03.2021**
Registriernummer:	**21-200-911**
Erstzertifizierung:	**13.04.2021**
Gültig ab:	**13.04.2021**
Gültig bis:	**12.04.2024**

Heinrich A. Bieler
Leiter der Zertifizierungsstelle

Wallisellen, 23.04.2021

Swiss Safety Center AG, Certifications
Richtistrasse 15, CH-8304 Wallisellen
Ein Unternehmen der SVTI-Gruppe, Mitglied des VdTÜV





Information Security Management System (ISMS)

- Systematische Risikoanalyse
- Strukturierte Dokumentation
- Kontinuierliche Verbesserung
- **Messbare Ziele**

Messbare Ziele ISMS

1. Die Services, welche wir für unsere Kunden entwicklen und betreiben, sind hochverfügbar.
2. Unser Webapplikationen sind sicher und werden regelmässig auf bekannte Sicherheitslücken geprüft.
3. Wir überwachen unsere Services und erkennen Fehler proaktiv.
4. Unser testgetriebener Entwicklungsansatz beinhaltet automatisierte und transparente Build- und Test-Prozeduren.
5. ...

https://seantis.ch/portrait/informationssicherheit-iso-27001/

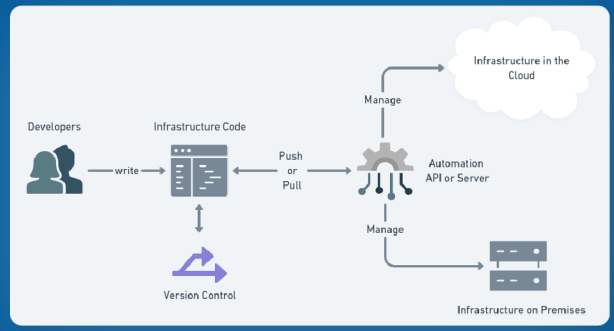
Resilienz und DevOps

«Infrastructure as Code» **Prinzipen**:

- Systeme können einfach reproduziert werden.
- Systeme sind wegwerfbar/ersetzbar (disposable).
- Systeme sind konsistent.
- Prozesse sind reproduzierbar.

DevOps Praktiken:

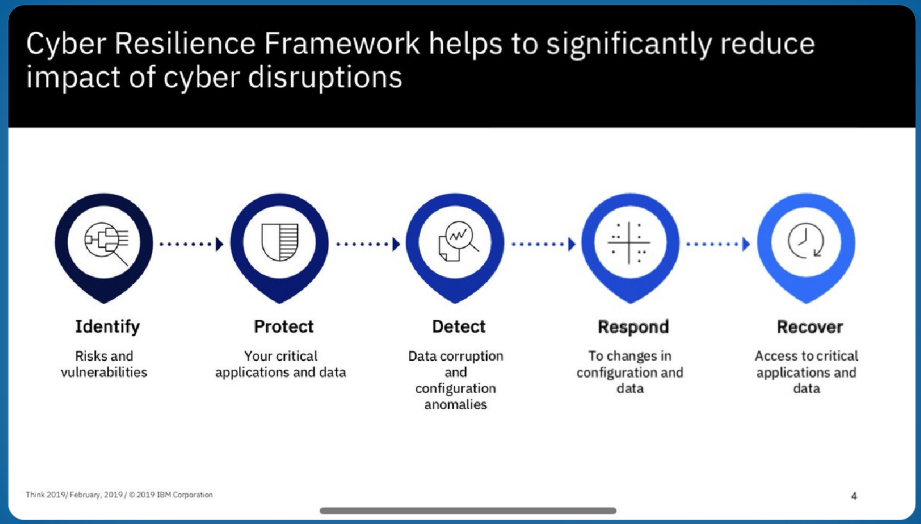
- Konfigurationen sind in Definitions-Dateien abgelegt.
- System und Prozesse sind selbst-dokumentiert
- Die gesamte Konfiguration ist unter Versionskontrolle.
- Kontinuierliche automatische Tests für Systeme und Prozesse.



Resilienz statt Resignation

«There are two types of companies: those who have been hacked, and those who don’t yet know they have been hacked.»

Dmitri Alperovitch, McAfee Vice President of Threat Research

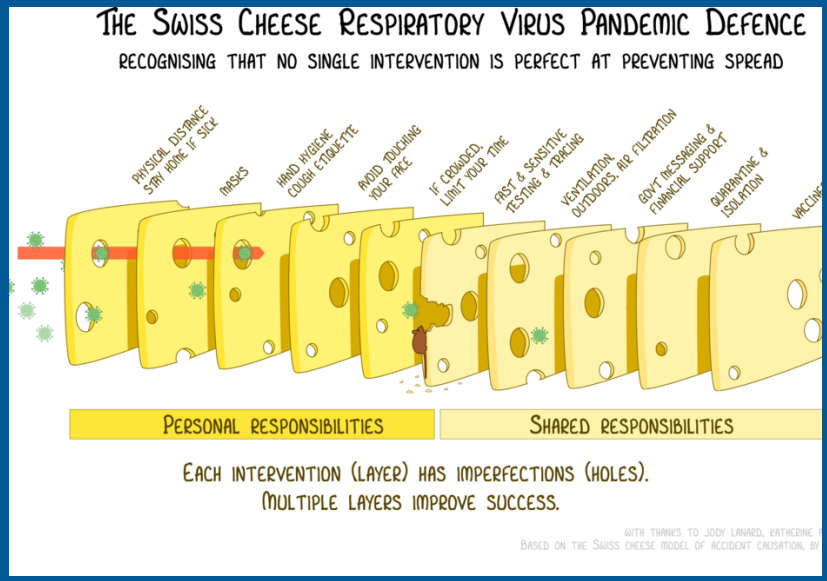


Resilienz dank «Swiss Cheese Model»

Der Schutz wird mit mehreren übereinander liegenden Schichten verbessert. Im Wissen, dass eine Abwehrschicht alleine nie zu 100% sicher sein kann. Der Unfall tritt nur ein, wenn der "Angriff" durch alle Schichten hindurchgeht.

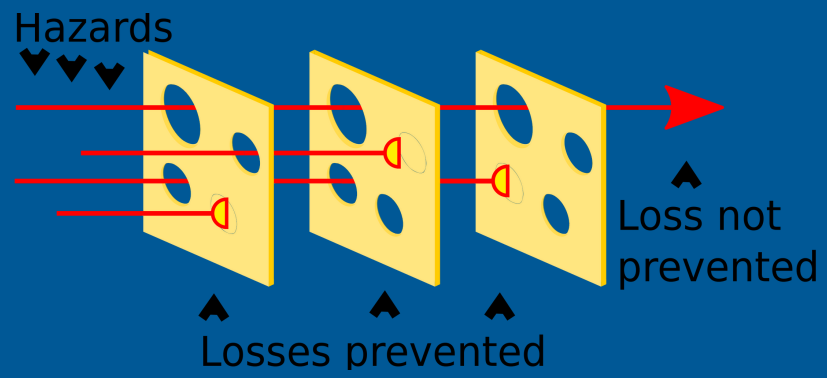
Die Löcher im Käse dürfen nicht übereinander liegen!

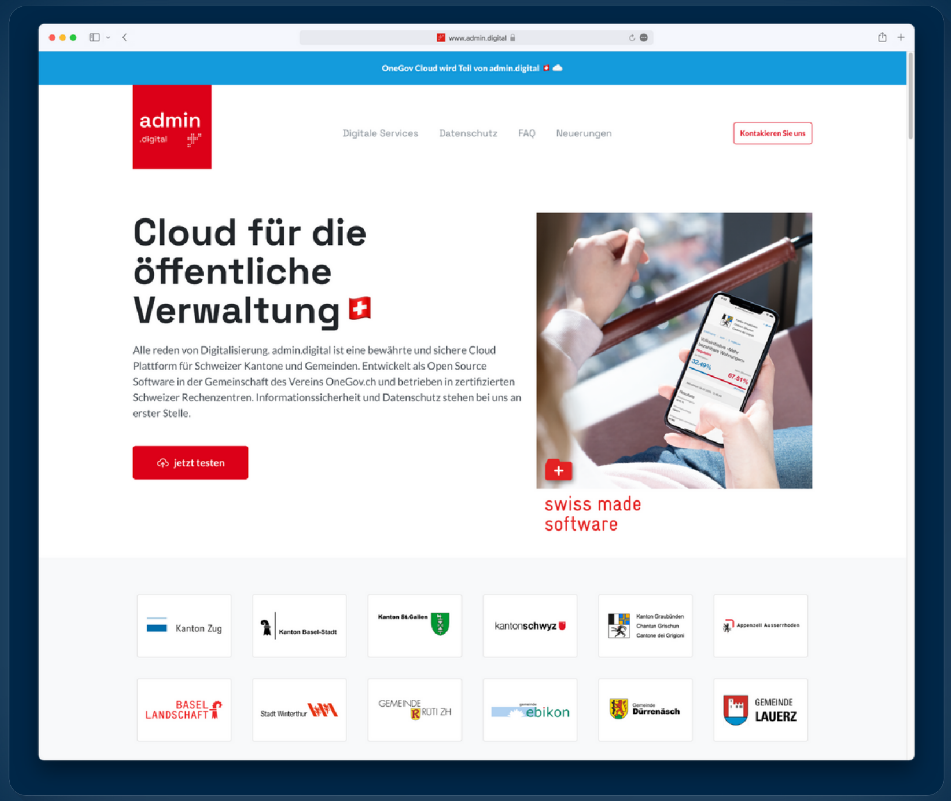
https://en.wikipedia.org/wiki/Swiss_cheese_model



Swiss cheese model - Wikipedia

en.wikipedia.org





🙏 Herzlichen Dank!

🙋 Fragen?

fabian.reinhard@seantis.ch
+41 79 703 94 14

http://www.seantis.ch
http://www.admin.digital