Cybersicherheit für Betreiber, Nutzerinnen und Mieter – Anforderungen an smarte Bauwerke

Mittwoch | 21.01.2026
15.30 – 16.30 Uhr
Main Stage, Swissbau Lab

ergon smart people – smart software®

GIRA

sia
schweizerischer ingenieur- und architektenverein
société suisse des ingénieurs et des architectes
società svizzera degli ingegneri e degli architetti
swiss society of engineers and architects

SWISS BAU LAB

LEADING PARTNER

sia
schweizerischer ingenieur- und architektenverein
société suisse des ingénieurs et des architectes
società svizzera degli ingegneri e degli architetti
swiss society of engineers and architects

PATRONAT

Departement für Wirtschaft, Soziales und Umwelt des Kantons Basel-Stadt
Amt für Umwelt und Energie

INNOVATION PARTNER

BAU4X swiss construction management software
BAUEN DIGITAL SCHWEIZ buildingSMART Switzerland
bauer
brinno brilliant innovation
Catenda CDE FÜR DIE PROJEKTKOMMUNIKATION
COUNTDOWN 20 21 22 23 24 25 26 27 28 29 30
CONSTRUIX
DALUX
die Mobiliar
DIGITALL
ergon smart people – smart software
ERNE wir bauen vorwärts
n|w Fachhochschule Nordwestschweiz
GIRA Smart Home. Smart Building. Smart Life.
HSLU Hochschule Luzern spatial design
HSLU Hochschule Luzern
immoMedia MEDIEN FÜR IMMOBILIEN UND STANDORTE
IMPACT ACOUSTIC®
infoprodigital
iwb
keeValue.ch
PAPREC SCHWEIZ
PLOTJET PLANEN.DRUCKEN.BAUEN.
Regazzi
RHOMBERG
SCHNETZER PUSKAS INGENIEURE
SENN senn.com
SIEMENS
SWISSLUX
Swiss Safety VR
TS3 Timber Structures 3.0
uptown Basel
vanillaplan
Xella

ABLAUF DER VERANSTALTUNG

Dauer	Programmpunkt
7 min	**Gespräch Experten** Giovanni Crupi, Swiss Engineering STV | Peter Vonesch, SIA
10 min	**Von der Prävention bis zur Notfallplanung – Cybersicherheit nicht nur in der Gebäudetechnik** Bundesamt für Cybersicherheit BACS
10 min	**Secure by Design – was Bauherren über Software-Risiken wissen müssen** Ergon Informatik
10 min	**Vernetzt, aber oft ungeschützt – Cybersicherheit in Gebäuden** Gira
15 min	**Podium**

SWISS BAU LAB

GIOVANNI CRUPI

Zentralpräsident Swiss Engineering STV

SWISS ENGINEERING
STV UTS ATS

PETER VONESCH

Fachexperte Strategie, Risikomanagement, Cybersicherheit, Sensibilisierung SIA

sia
schweizerischer ingenieur- und architektenverein
société suisse des ingénieurs et des architectes
società svizzera degli ingegneri e degli architetti
swiss society of engineers and architects

CLÉLIA WARUNEE RUNTZ

Bundesamt für Cybersicherheit (BACS), Fachexpertin Sensibilisierung

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Cybersicherheit BACS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cybersicherheit im Bauwesen

Herzlich willkommen

21.01.2026

Clélia Warunee Runtz, Fachexpertin (BACS)

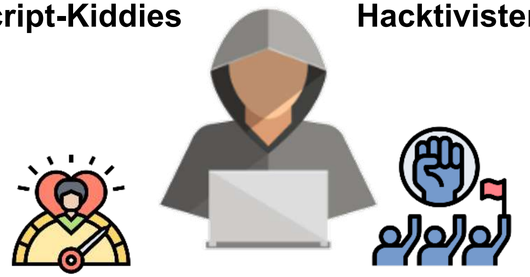
Cyberrisiken

Akteure

Angreifer

Script-Kiddies

Hacktivisten



Cyberkriminellen

Staat

Advanced Persistent Threat

Angriffstypen

Menschliches Versagen / technischer Fehler

Betrug

Phishing

Malware

DDoS

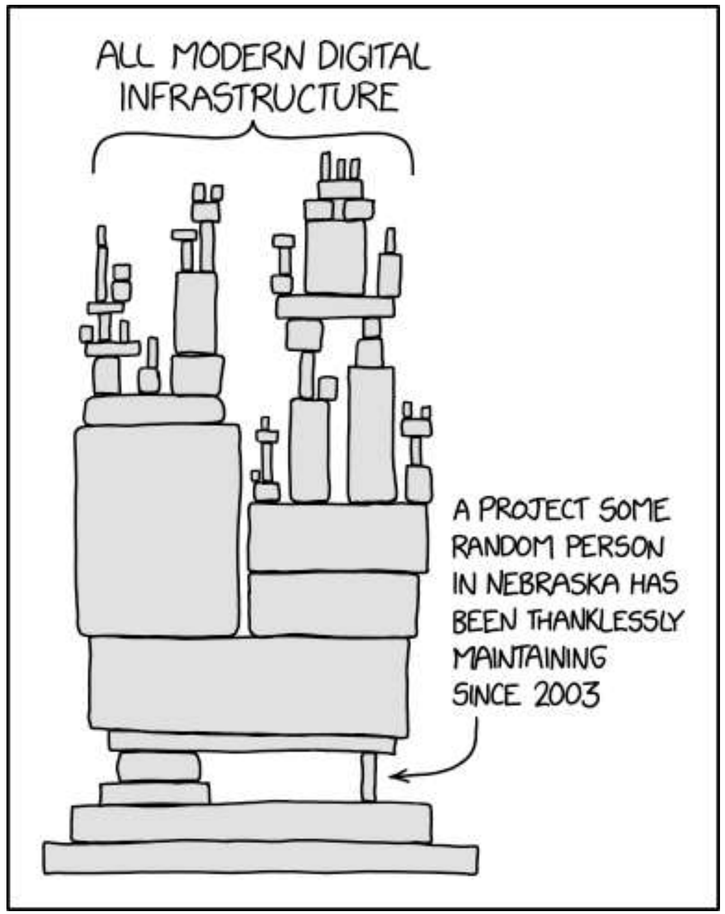
Ransomware

Beeinflussungsaktivitäten

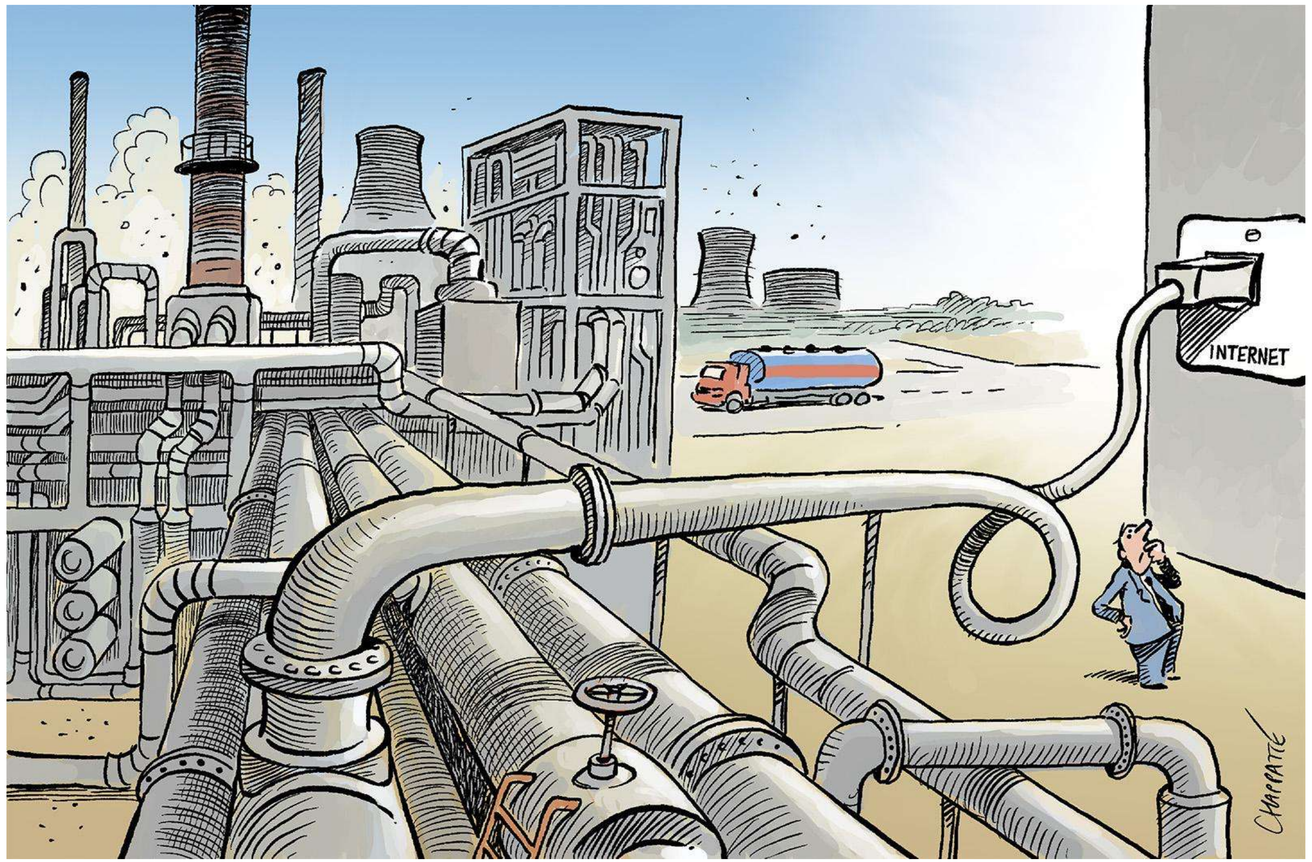
Sabotage

Spionage

Digitalisierung und Vernetzung



2347: Dependency - explain xkcd



Bedeutung der Cybersicherheit im Bauwesen/Gebäudetechnik

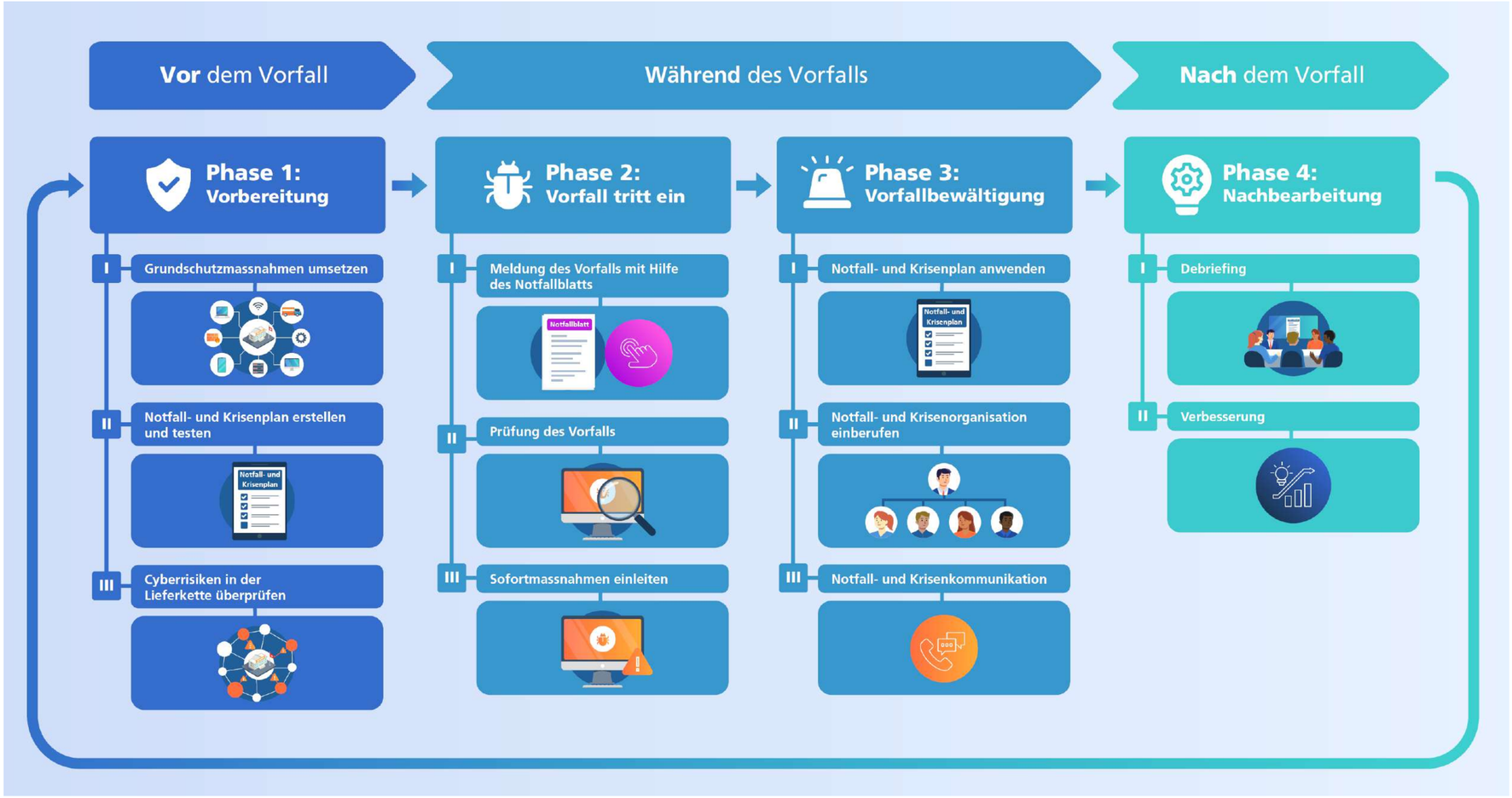
Cybersicherheit im Bauwesen

- Digitalisierung bewusst umsetzen (anhand zB. Security by Design). Langsame Digitalisierung reduziert zwar kurzfristig die Angriffsfläche, führt aber mittelfristig zu Technologieschulden

- Technische Massnahmen: Updates, Regelmässige offline Backups, Passwortmanagement und MfA, Firewalls…
- Organisatorische Massnahmen: klare Kommunikation, Governance, Sicherheitskultur, internationale Standards, Notfallkonzepte, Schulungen und Übungen…

Notfallkonzept

Infographic



Phase 1 – Vorbereitung

Phase 1 – Vorbereitung

A Akzeptierte Auswirkungen bei Ausfall IT-unterstützte Aufgaben

IT-unterstützte Aufgaben	Maximal tolerierbare Ausfallzeit	Nicht akzeptierbare Auswirkungen
- CAD-/BIM-Planung und Modellierung	4 h	Veränderung der Parameter durch Nichtberechtige
- Simulationen (Statik, Energie, Bauphysik)	8 h	Veränderung der Parameter durch Nichtberechtige
- Zugriff auf Digitale Genehmigungsprozesse	4 h	Abfluss von sensiblen Daten
- Projekt- und Terminplanung (Software)	1 Tag	Veränderung der Parameter durch Nichtberechtige
- Kollaborationstools für interdisziplinäre Teams	2 h	Teilnahme an Meetings durch Nichtberechtigte
- Kommunikation mit Baustellen	1 h	Manipulation vor Ort

Phase 2 – Vorfall tritt ein

Notfallblatt zum Melden von Cybervorfällen

Verhalten im Cybervorfall – so gehen Sie vor

1. Vorfall melden:
Rufen Sie umgehend die Haupt- oder Ersatznummer an.
Im Zweifel, besser melden.

IT-Notfallnummern

Hauptnummer | Ersatznummer

2. Vorfall schildern:
Was ist passiert? Wann ist es passiert?

3. Betroffene Systeme angeben:
Welche IT-Systeme sind betroffen?

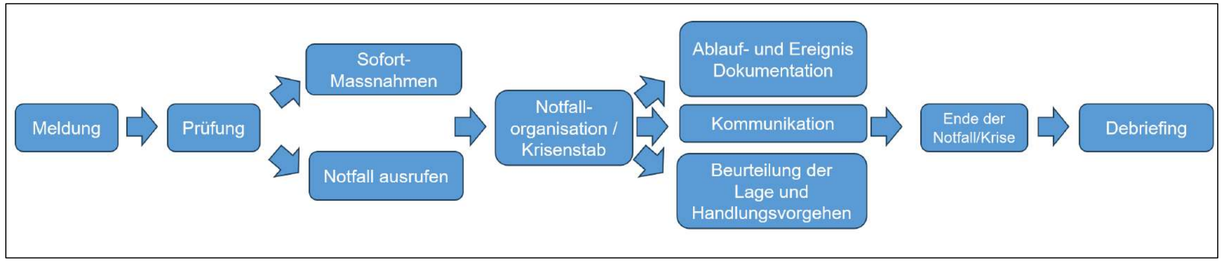
4. Standort nennen:
Wo befinden sich die betroffenen Systeme (Gebäude, Raum, Arbeitsplatz)?

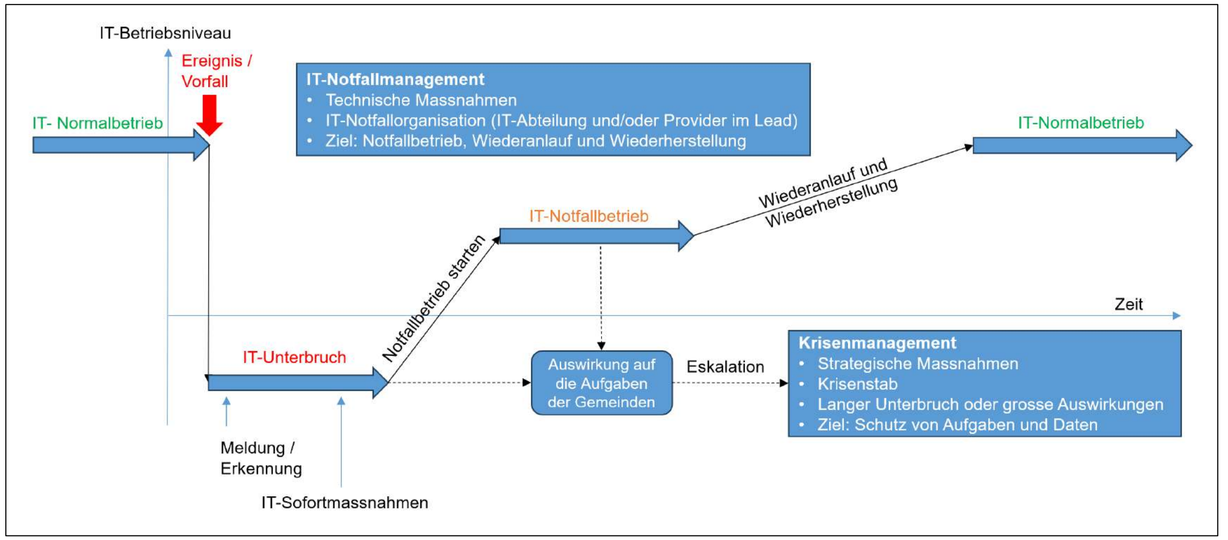
Verhaltenshinweise

- Arbeit am IT-System stoppen
- Vorfall dokumentieren
- Massnahmen erst nach Anweisung

Herausgeber: Bundesamt für Cybersicherheit (BACS)

Phase 3 – Vorfallbewältigung





Phase 3 – Vorfallbewältigung

D Priorisierung bei Wiederanlauf und Wiederherstellung im Planungsbüro (3.3.2)

Die folgende Tabelle enthält dieselben Aufgaben, wie in Tabelle A beschrieben, und ist mit zusätzlichen Informationen zu relevanten IT-Systemen und Sofortmassnahmen ergänzt.

Prio	IT-unterstützte Aufgaben	Nicht akzeptierbare Auswirkungen	Sofortmassnahmen und Notfallbetrieb
1	- Kollaborationstools für interdisziplinäre Teams	Teilnahme an Meetings durch Nichtberechtigte	Sitzungen vor Ort
1	- Kommunikation mit Baustellen	Falschmeldungen und Falschlieferungen	Mit Mobile-Phone und Kurier
2	- CAD-/BIM-Planung und Modellierung	Veränderung der Parameter durch Nichtberechtige	Sitzungen vor Ort
3	- Projekt- und Terminplanung (Software)	Veränderung der Parameter durch Nichtberechtige	Rekonstruktion Tageseinsatz durch PL / Sachbearbeiter
3	- Simulationen (Statik, Energie, Bauphysik)	Veränderung der Parameter durch Nichtberechtige	Rekonstruktion der Tagesänderungen für spätere Nachführung
4	- Zugriff auf Digitale Genehmigungsprozesse	Abfluss von sensiblen Daten	Rekonstruktion der Tagesänderungen

Phase 4 – Nachbearbeitung

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS
Bundesamt für Cybersicherheit BACS

Post Incident Review (PIR)

Best Practice

1 Einleitung

Nach der Wiederherstellung von Netzwerken und Systemen infolge eines Cybervorfalls ist es entscheidend, zeitnah – idealerweise innerhalb von zwei Wochen nach Abschluss des Vorfalls – eine **Post Incident Review (PIR)**[1] durchzuführen und zu dokumentieren.

Ziel dieses PIR ist eine systematische Analyse, wann und durch wen der Vorfall entdeckt wurde, welche Ursachen zugrunde lagen und ob sowie wie er hätte verhindert werden können. Ebenso wird bewertet, welche Massnahmen bei der Reaktion gut funktioniert haben, wie die Bedrohung eingedämmt und beseitigt wurde und wo Optimierungspotenzial besteht. Dies betrifft insbesondere den IT-Notfall- und Krisenplan und die Reaktionsstrategien.

Ein PIR bietet zudem die Gelegenheit zur offenen Diskussion, um gemeinsam Verbesserungen für zukünftige Vorfälle zu ermitteln. Die aus der Vorfallbewältigung gewonnenen Erkenntnisse fliessen direkt in die kontinuierliche Weiterentwicklung des IT-Notfall- und Krisenplans und die zugehörigen Prozesse ein. Das Ziel besteht darin, künftige Bedrohungen und Vorfälle effektiver zu erkennen und zu bewältigen.

2 Zusammenfassung des Vorfalls

Name des Vorfalls	*z. B. "Erster Grosser Ransomwarevorfall bei uns»*
Datum des Vorfalls	*01.01.2025*
Zeitpunkt des Vorfalls	*12:00*
Abschluss des Vorfalls	*31.01.2025*
Vorfallkategorie	Choisissez un élément.
Angriffsmethode	Choisissez un élément.
Beteiligtes Personal	*Die Namen der Personen, die an der Lösung des Vorfalls beteiligt waren, sowie ihre Rolle in Bezug auf den Vorfall, einschliesslich aller Dienstleister.*
Auswirkungen des Vorfalls	*Verfügbarkeit, Vertraulichkeit, Integrität*
Kurze Zusammenfassung	*Was ist passiert?*

[1] Auch bekannt als «After Action Review (AAR)» oder «Hot wash up».

3 Vorfallanalyse

Die Vorfallanalyse ist in die folgenden Kategorien[2] unterteilt:

- **Chronologie (IDENTIFY)** – Zusammenfassung des Vorfalls und des zeitlichen Ablaufs. Bietet allgemeine Verbesserungsmöglichkeiten.
- **Schutz (PROTECT)** – Identifiziert die zum Zeitpunkt des Vorfalls vorhandenen Schutzmassnahmen und deren Wirksamkeit. Legt fest, wie der Schutz der eigenen Netzwerke und Systeme verbessert werden kann.
- **Erkennung (DETECT)** – Legt fest, wie die Zeit bis zur Erkennung eines Vorfalls verkürzt werden kann. Behandelt, welche Erkennungsmechanismen vorhanden waren und wie diese verbessert werden können.
- **Reaktion (RESPOND)** – Identifiziert Verbesserungen für die Reaktion auf Vorfälle.
- **Wiederherstellung (RECOVER)** – Behandelt Verbesserungen für die Wiederherstellung nach Vorfällen (d. h. wie man schneller nach einem Vorfall wiederherstellen kann).

3.1 Chronologie (IDENTIFY)

Datum des Vorfalls	*01.01.2025*
Zeitpunkt des Vorfalls	*12:00*
Datum der Entdeckung des Vorfalls	*01.01.2025*
Zeitpunkt der Entdeckung des Vorfalls	*16:00*
Wann wurde der Vorfall bestätigt?	*01.01.2025 / 16:00*
Abschluss des Vorfalls	*31.01.2025*
Wer hat den Vorfall zuerst entdeckt und wie wurde er entdeckt?	*Wer wurde zuerst darauf aufmerksam gemacht? Wie kam es zu der Entdeckung und/oder Meldung? Wie hat der interne Meldeprozess funktioniert?*
Wurde der Vorfall extern gemeldet? Wenn ja, wann?	*Hat Ihre Organisation dies beispielsweise dem BACS oder dem DSB/EDÖB gemeldet?*
Wer hat bei der Lösung des Vorfalls geholfen? Wann haben sie Unterstützung geleistet?	*Listen Sie die Namen der Mitarbeitenden auf, die an der Lösung des Vorfalls beteiligt waren, sowie die Uhrzeit (und das Datum, wenn nicht alle am selben Tag beteiligt waren), zu der sie hinzukamen.*
Welche Massnahmen wurden zur Behebung des Vorfalls ergriffen? Wer hat welche Massnahmen entschieden? Wann wurden sie durchgeführt und welche Auswirkungen hatten sie?	*Dies lässt sich z. B. in einer Liste darstellen, zum Beispiel: Zeit > Aufgabe > Auswirkung*
Mögliche Verbesserungsmassnahmen	*Führen Sie alle Massnahmen auf, die in den Normalbetrieb oder den IT-Notfall- und Krisenplan aufgenommen werden können.*

[2] Diese Kategorien basieren auf dem NIST Cybersecurity Framework: Cybersecurity Framework | NIST

2/5

3.2 Schutz (PROTECT)

Welche Schutzmassnahmen waren vorhanden, um einen ähnlichen Vorfall zu verhindern?	*z. B. Antivirus, MFA, EDR/NDR, usw.*
Wie wirksam waren diese Schutzmassnahmen?	*Haben sie funktioniert? Warum? / Warum nicht? Wie könnten sie verbessert werden?*
Gibt es andere Schutzmassnahmen, die zum Schutz vor einem ähnlichen Vorfall als besser geeignet angesehen werden?	*Welche?*
Welche Geschäftsprozesse waren vorhanden, um Vorfälle dieser Art zu bewältigen?	*D. h. die Richtlinien und Verfahren Ihrer Organisation.*
Wie effektiv waren diese Geschäftsprozesse?	*Haben sie funktioniert? Warum? / Warum nicht? Wie könnten sie verbessert werden?*
Mögliche Verbesserungsmassnahmen	*Führen Sie alle Massnahmen auf, die in den Normalbetrieb oder den IT-Notfall- und Krisenplan aufgenommen werden können.*

3.3 Erkennung (DETECT)

Wie wurde der Vorfall entdeckt?	*Wie haben Sie erfahren, dass der Vorfall passiert ist?*
Welche Kontrollen gab es, um den Vorfall zu entdecken?	*Haben sie funktioniert? Warum? / Warum nicht? Wie könnten sie verbessert werden?*
Welche Geschäftsprozesse waren vorhanden, um Vorfälle dieser Art zu entdecken?	*D. h. die Richtlinien und Verfahren Ihrer Organisation.*
Wie effektiv waren diese Geschäftsprozesse?	*Haben sie funktioniert? Warum? / Warum nicht? Wie könnten sie verbessert werden?*
Gibt es Möglichkeiten, die «Zeit bis zur Erkennung» zu verkürzen?	*Wie könnte Ihr Unternehmen diese Zeit verkürzen?*
Gibt es Indikatoren, mit denen sich ähnliche Vorfälle in Zukunft erkennen lassen?	*Indicators of Compromise*
Sind zusätzliche Werkzeuge oder Ressourcen erforderlich, um ähnliche Vorfälle in Zukunft zu erkennen?	*Gibt es (aus Sicht der Erkennung) etwas, das dazu beitragen könnte, zukünftige Vorfälle zu mindern? Technologie? Personal mit spezifischen Fähigkeiten?*
Gibt es weitere Erkenntnisse und/oder Verbesserungsvorschläge?	*Welche Massnahmen haben gut funktioniert? Welche Massnahmen haben nicht so gut funktioniert? Was könnte im Nachhinein geändert werden?*
Mögliche Verbesserungsmassnahmen	*Führen Sie alle Massnahmen auf, die in den Normalbetrieb oder den IT-Notfall- und Krisenplan aufgenommen werden können.*

3.4 Reaktion (RESPOND)

Wie wurde der Vorfall gelöst?	*Was musste geschehen, damit das Problem gelöst werden konnte?*
Welche Verzögerungen und Hindernisse traten bei der Reaktion auf den Vorfall auf?	*Technisch, legal, kommunikativ, …*
Wurde bei der Reaktion auf den Vorfall ein IT-Notfall- und Krisenplan angewendet?	*Falls ja, hat es funktioniert? Warum? / Warum nicht? Wie könnte es verbessert werden?*
Wie gut funktionierten der interne Informationsaustausch und die Kommunikation?	*Was hat gut funktioniert? Was hat nicht gut funktioniert? Wie könnte es verbessert werden? Gab es Informationen, die früher benötigt wurden?*
Gab es während des Vorfalls Medienanfragen?	*Wenn ja, um welche Medien handelte es sich und wie hat Ihre Organisation darauf reagiert?*
Wurde die Betroffene Personen während des Vorfalls benachrichtigt?	*Warum? / Warum nicht? Wann? Wie?*
Waren geschulte Mitarbeitende verfügbar, um zu reagieren?	*Gibt es Wissens- und/oder Qualifikationslücken beim Personal? Welche sind das? Waren genügend Ressourcen verfügbar, um zu reagieren?*
Mögliche Verbesserungsmassnahmen	*Führen Sie alle Massnahmen auf, die in den Normalbetrieb oder den IT-Notfall- und Krisenplan aufgenommen werden können.*

3.5 Wiederherstellung (RECOVER)

Wie lange hat es gedauert, bis alle Systeme und Netzwerke wiederhergestellt waren?	*Stunden, Tage, Wochen?*
Wie könnte diese Zeit verkürzt werden?	*Wie könnte die Wiederherstellungszeit verkürzt werden?*
Gab es nach dem Vorfall Anfragen von Medienvertretern?	*Falls ja, von welchen Medien?*
Wurden Mitarbeitende und/oder Betroffene über den Vorfall informiert?	*Warum? / Warum nicht? Wie wurde die Benachrichtigung durchgeführt? War sie wirksam? Wie könnte sie verbessert werden?*
Gibt es weitere Erkenntnisse und/oder Verbesserungsvorschläge?	*Welche?*
Mögliche Verbesserungsmassnahmen	*Führen Sie alle Massnahmen auf, die in den Normalbetrieb oder den IT-Notfall- und Krisenplan aufgenommen werden können.*

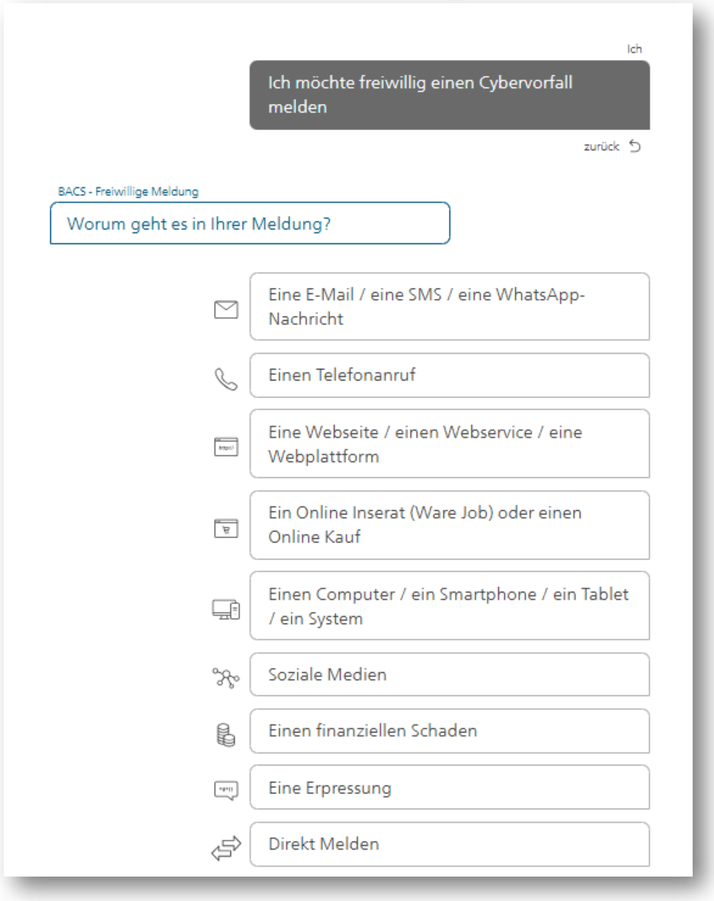
4 Lessons Learned und Massnahmen

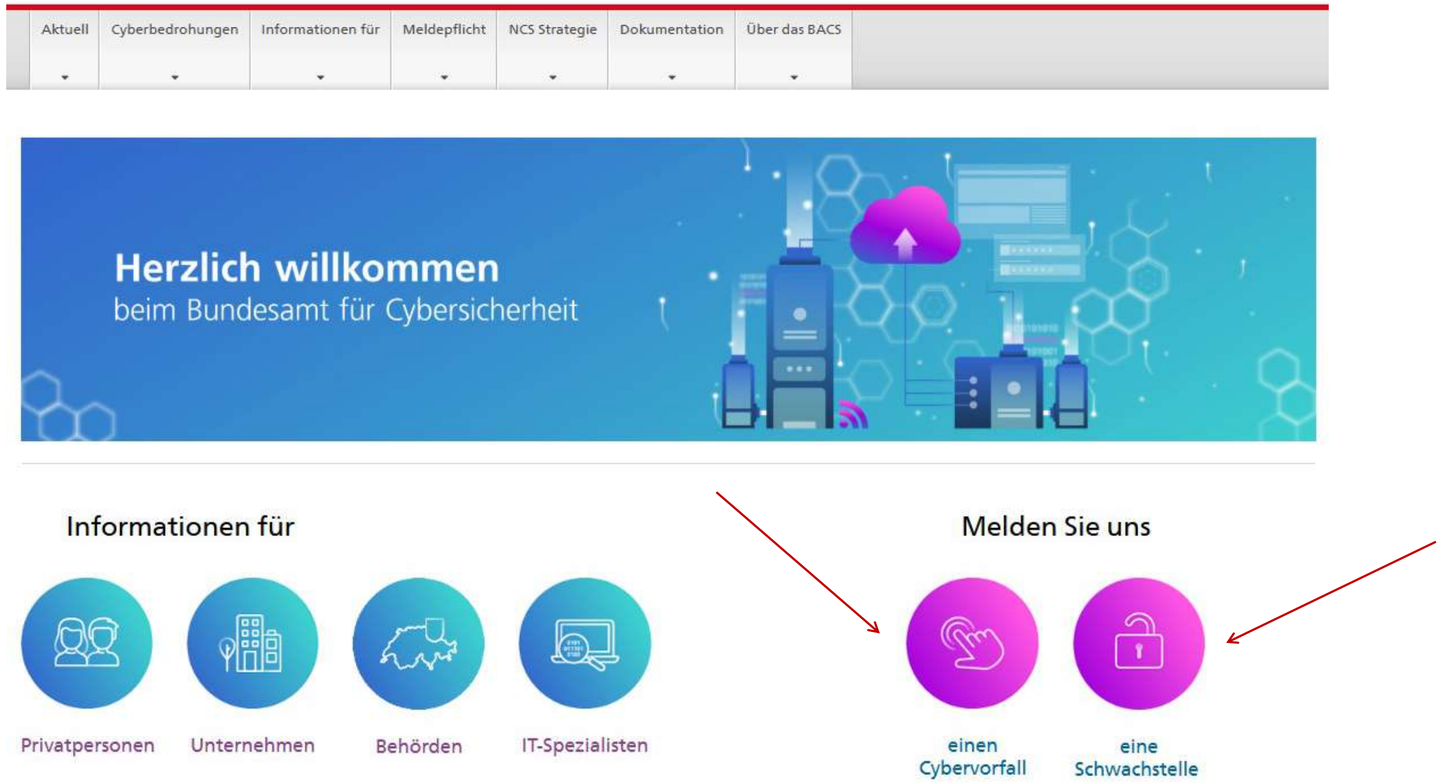
Zusammenfassung des Lessons Learned von Kapitel 3.1 bis 3.5

Massahmen	***Verantwortlichkeiten***	***Fristen***
Neue Konfigurations-Firewall	*Max Muster*	*28.02.2025*
Aktivierung MFA auf Systeme X	*Lilian Beispiel*	*28.02.2025*
…	…	…

Im Falle eines Angriffs

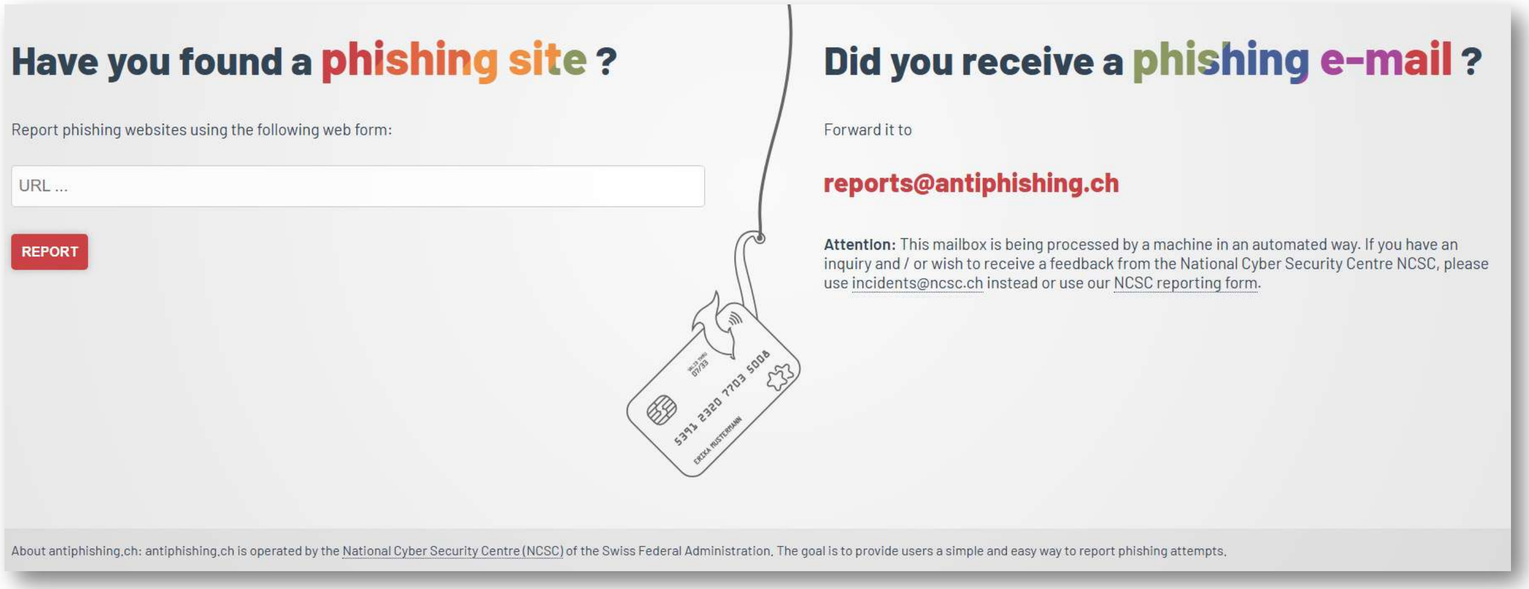
Konkrete Hilfestellungen und Meldemöglichkeiten





Weitere Hilfsmittel

Antiphishing.ch



Vielen Dank für Ihre Aufmerksamkeit

FABIAN STELLING

Senior Software Engineer & Security Consultant Ergon Informatik

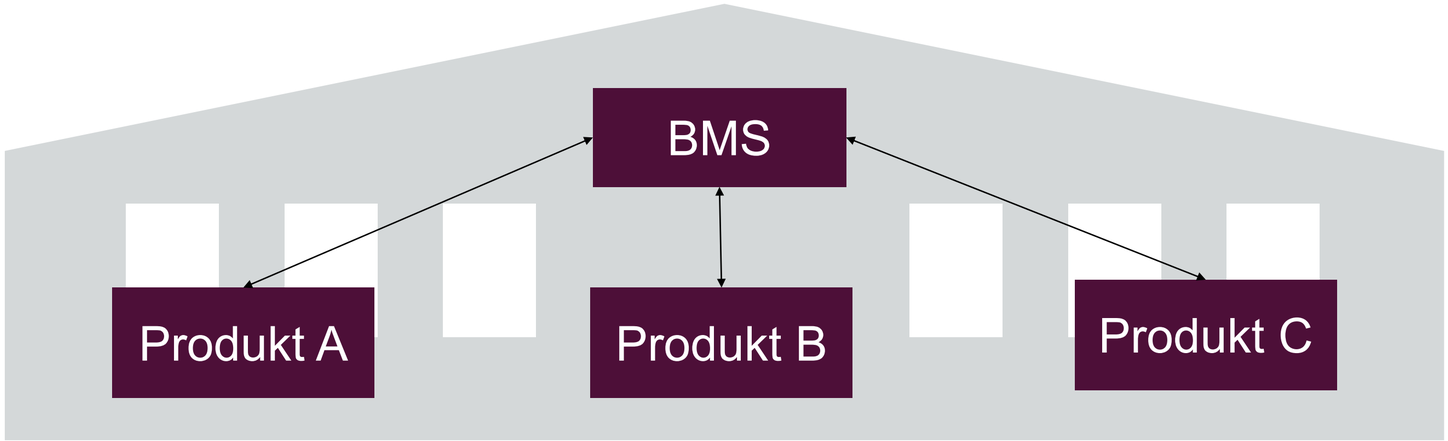
ergon

Secure by Design – was Bauherren über Software-Risiken wissen müssen

Swissbau, Januar 2026

ergon

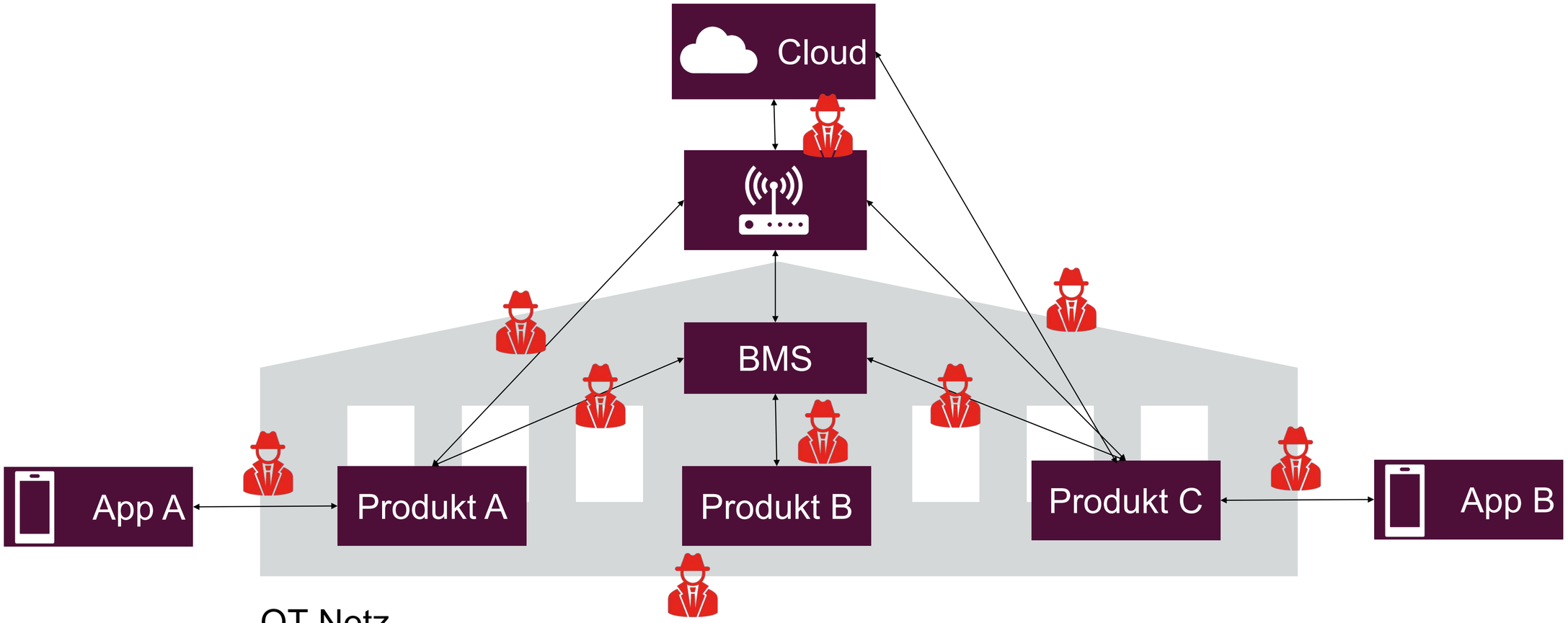
Gebäudetechnik vor 2010



OT-Netz

ergon

Gebäudetechnik heute



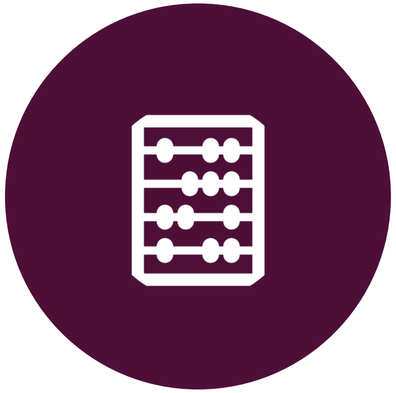
ergon

Security by Design

ergon

Zentrale Sicherheitsaspekte

Sichere Kommunikation
verschlüsselt
authentifiziert
manipulationssicher



Sichere (Default-)Konfiguration
Minimal
keine Default-Passwörter
Sicher vorkonfiguriert

Sichere Speicherung
Geschützt
Verschlüsselt
Getrennt

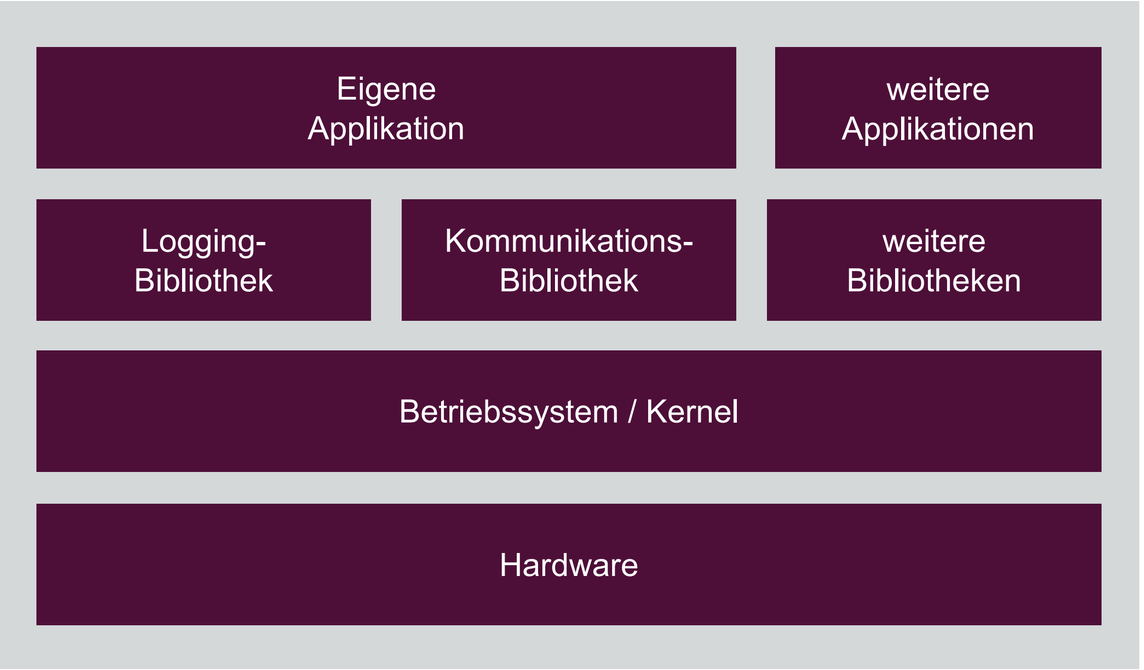
Sichere Updates
Signiert
Updatefähig
Langfristig

ergon

Jedes digitale Produkt wird unsicher – die Frage ist nur wann.

ergon

Aufbau von Software



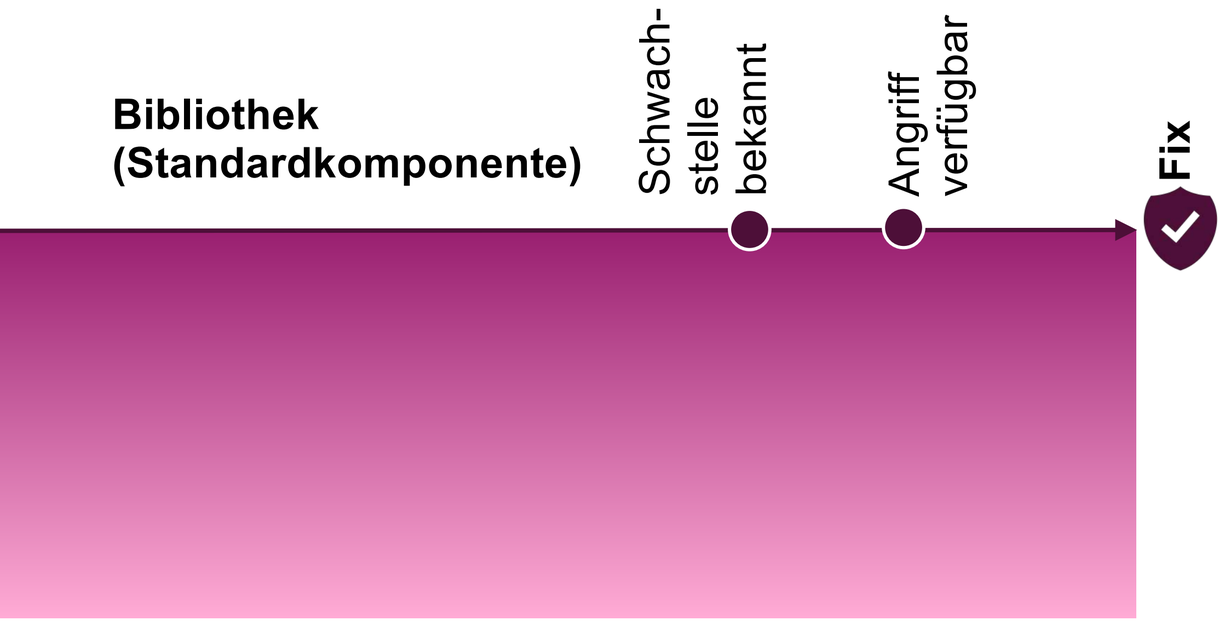
→ (Mehrheitlich) Eigenentwicklung

→ (Mehrheitlich) Standardkomponenten

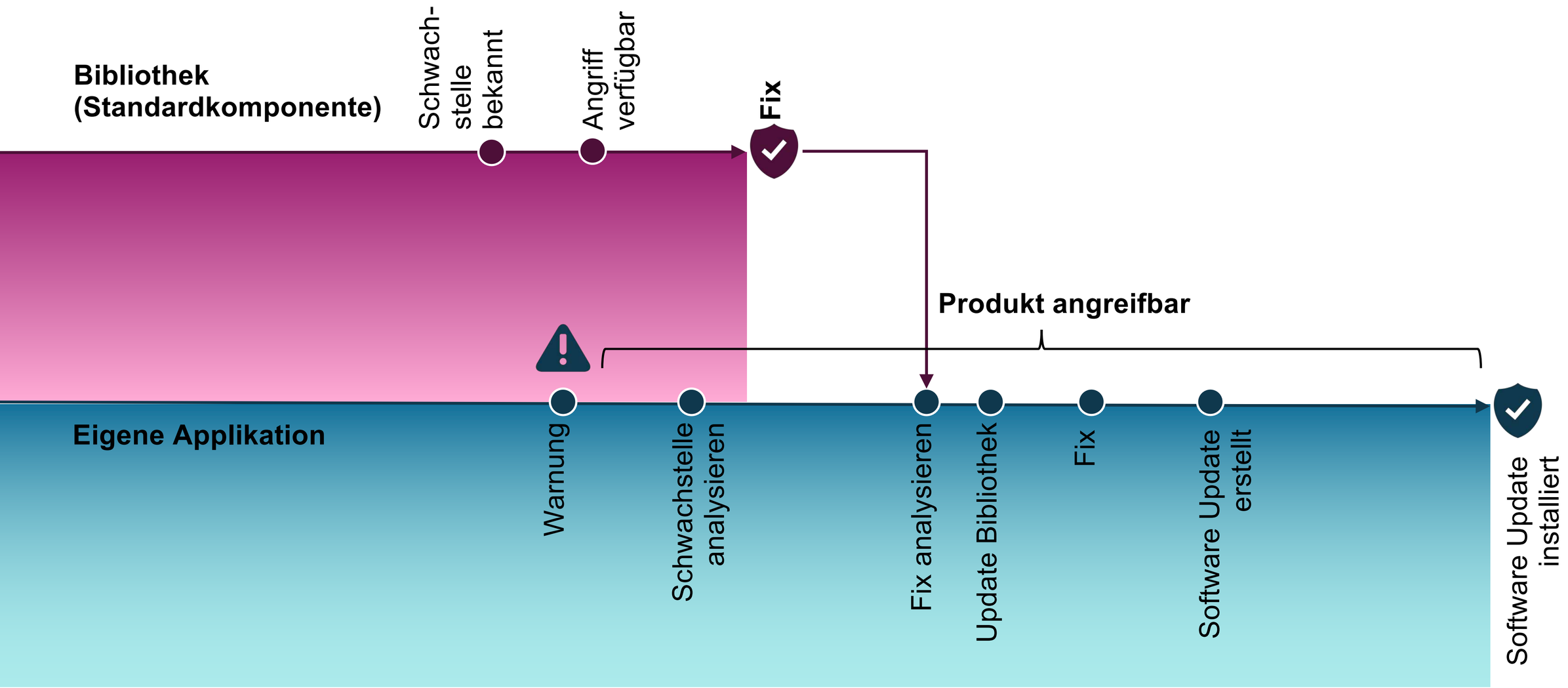
→ (Mehrheitlich) Standardkomponenten

→ (Mehrheitlich) Standardkomponenten

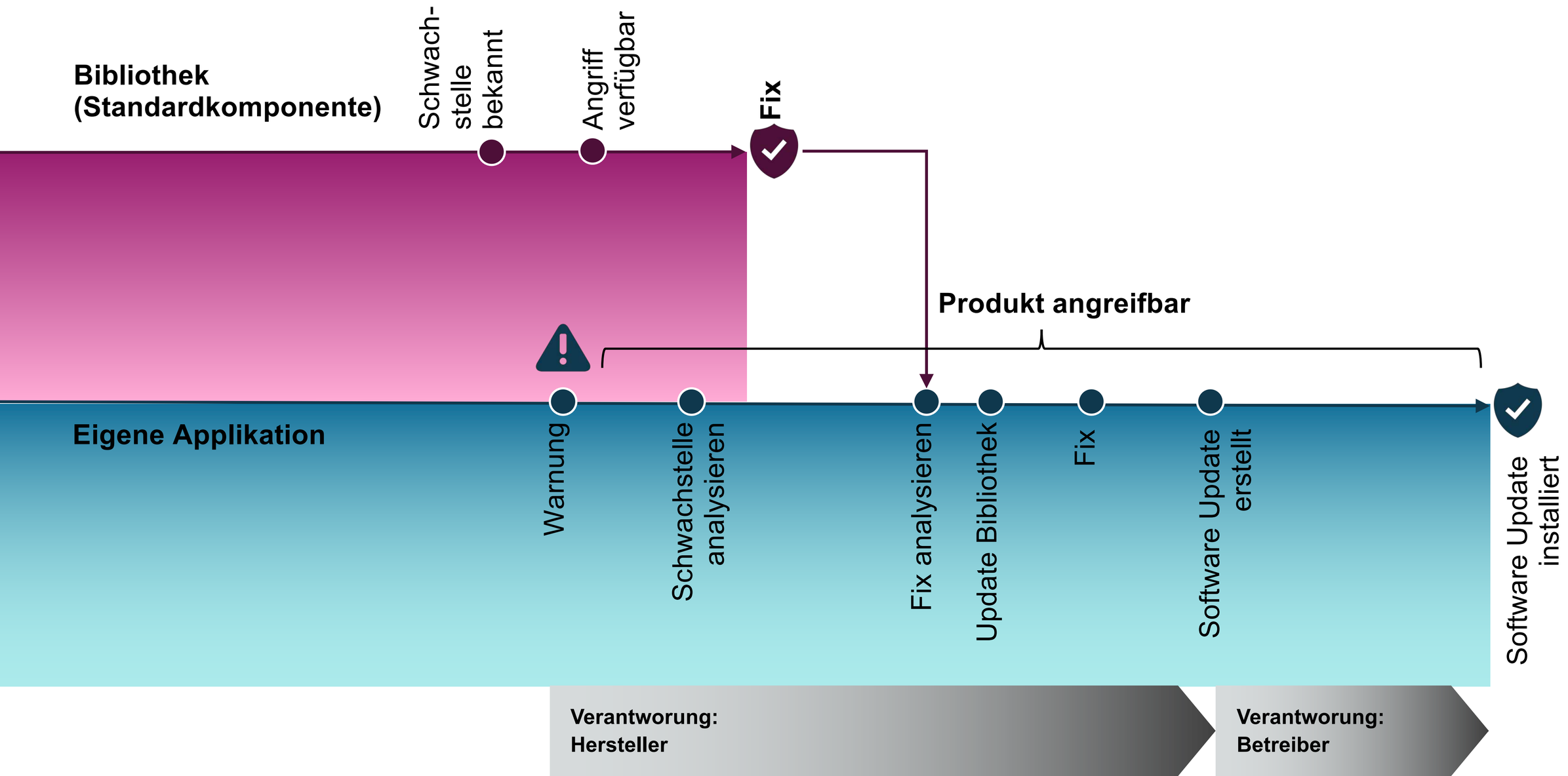
Was passiert bei Schwachstellen?



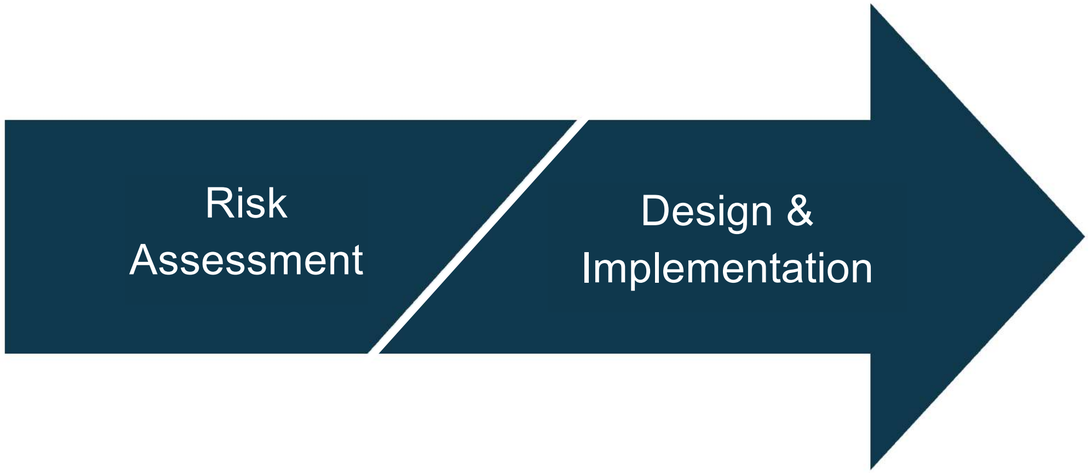
Was passiert bei Schwachstellen?

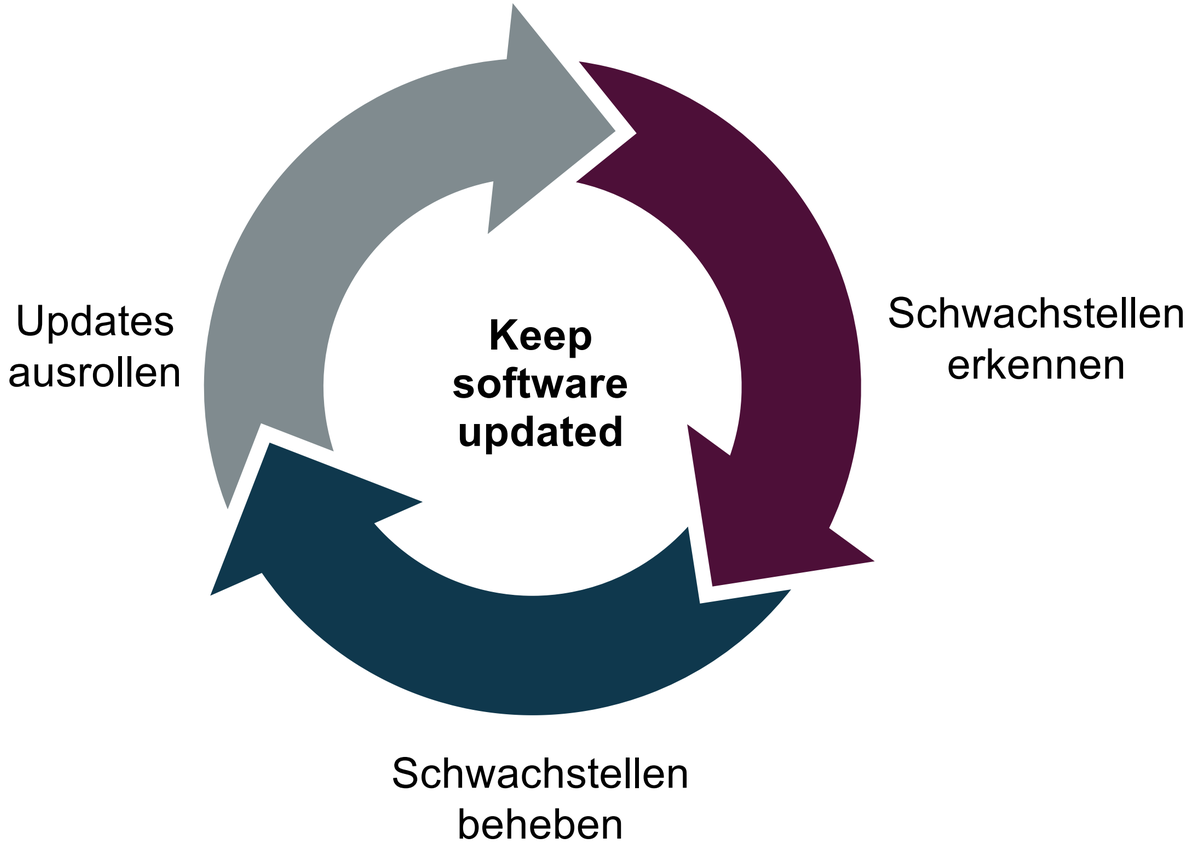


Was passiert bei Schwachstellen?



Fortlaufende Sicherheit





ergon

…On an EU-level, the situation is even worse with **a firmware-update delay of 930 days** (2.5 y)…

Frauenhofer Institute for Systems and Innovation Research ISI, December 2023

‘Never touch a running system’ ist der grösste Feind der IoT Sicherheit.

ergon

MARKUS BIEDERMANN

Country Manager Schweiz Gira

GIRA

GIRA

Smart Home.
Smart Building.
Smart Life.

Vernetzt, aber oft ungeschützt – wie Smart Buildings sicherer werden

SWISSBAU Themenanlass Cyber-Security

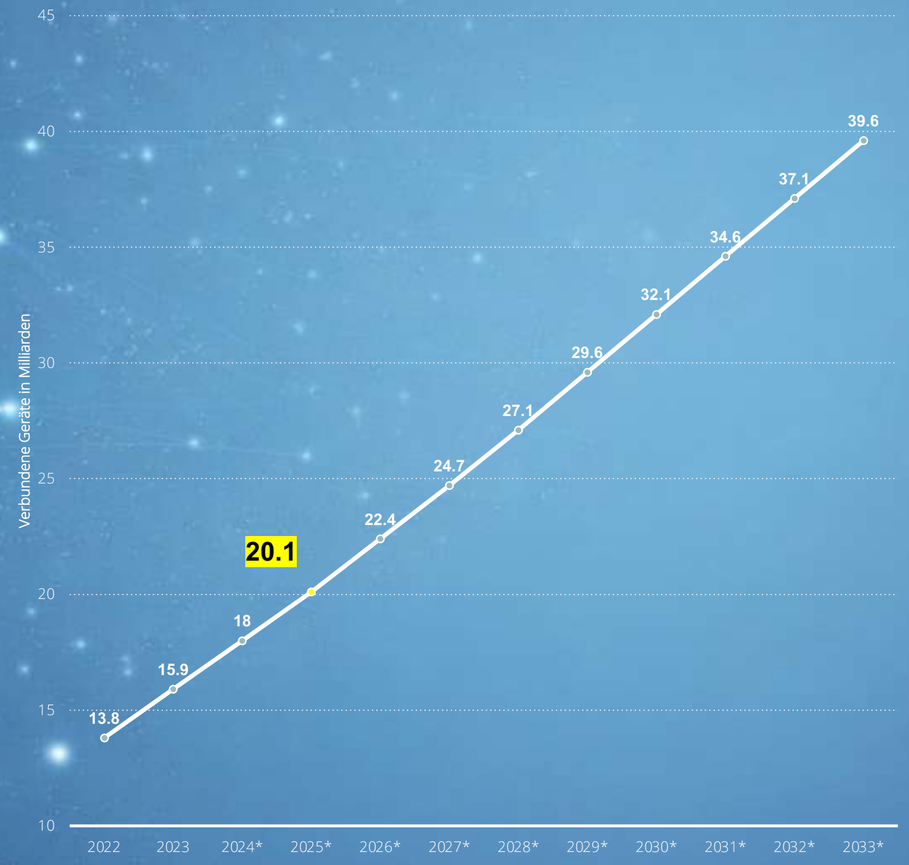
21.01.2026

Markus Biedermann

GIRA

20 Milliarden IoT-Geräte sind weltweit Online

Entwicklung der Anzahl der mit dem Internet der Dinge verbundenen Geräte weltweit bis 2033



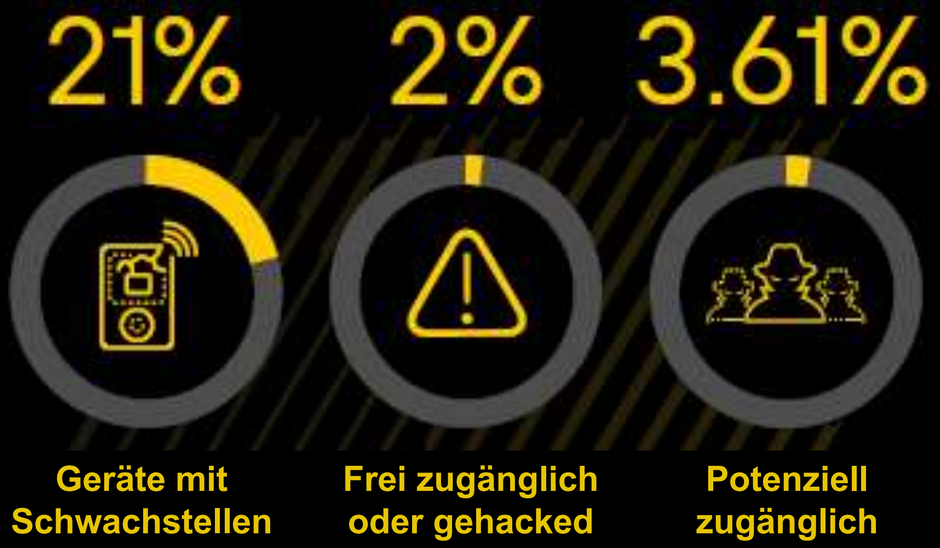
*Quelle: Statista Petroc Taylor, 27.11.2025, * = Prognose*

GIRA

Billige IoT-Geräte und Geräte ohne SW-Updates sind eine Sicherheitsbedrohung

Widespread vulnerabilities in IoT devices

Approximately 21% of all IoT devices have at least one known vulnerability. More critically, 2% of IoT devices are susceptible to Known and Exploited Vulnerabilities (KEV), meaning they're already being actively abused in the wild. Another 3.61% are affected by vulnerabilities with publicly available exploits (proof of concept [PoC] available), significantly lowering the technical barrier for attackers.



Quelle: Device Security Threat Report 2025, Paloalto Networks Strata,

GIRA

1.Input: Roboter-Staubsauger als Sicherheitsrisiko

Massive Sicherheitsmängel bei führenden Herstellern (Ecovacs, Dreame und Narwal) im Sept 2025

Kamera-Missbrauch
Bei Modellen wie dem Dreame X50 Ultra konnten Angreifer aus der Ferne die eingebaute Kamera aktivieren und das Live-Bild streamen, ohne dass der Nutzer dies bemerkte.

Mangelnde Authentifizierung
Bei Narwal (Freo Z Ultra) und Ecovacs (Deebot X8 Pro Omni) war es möglich, ohne korrekte Prüfung auf Fotos zuzugreifen, die der Roboter während der Reinigung zur Hinderniserkennung aufgenommen hatte.

Audio-Manipulation
In Experimenten konnten Forscher nicht nur auf die Kamera zugreifen, sondern den Roboter sogar „sprechen“ lassen oder bösartige Dateien in die Fotoalben der verknüpften Nutzer-Apps einschleusen.

GIRA

2.Input: Passwörter als Sicherheitsrisiko

Passwörter werden nie im Klartext gespeichert

Nur der Hash wert

Aus Passwort
"geheim"
wird der SHA1-Hash

906072001efddf3e11e6d2b5782f4777fe038739

GIRA

Zeitdauer um Hash-Wert eines Passwortes zu entschlüsseln

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

GIRA

WLAN ist daher oft nicht sicher

1. Hacker stören kurzzeitig Verbindung zum WLAN-Router
2. Gerät muss sich neu anmelden
3. Passwort-Hashwert wird ausgelesen
4. Passwort wird entschlüsselt

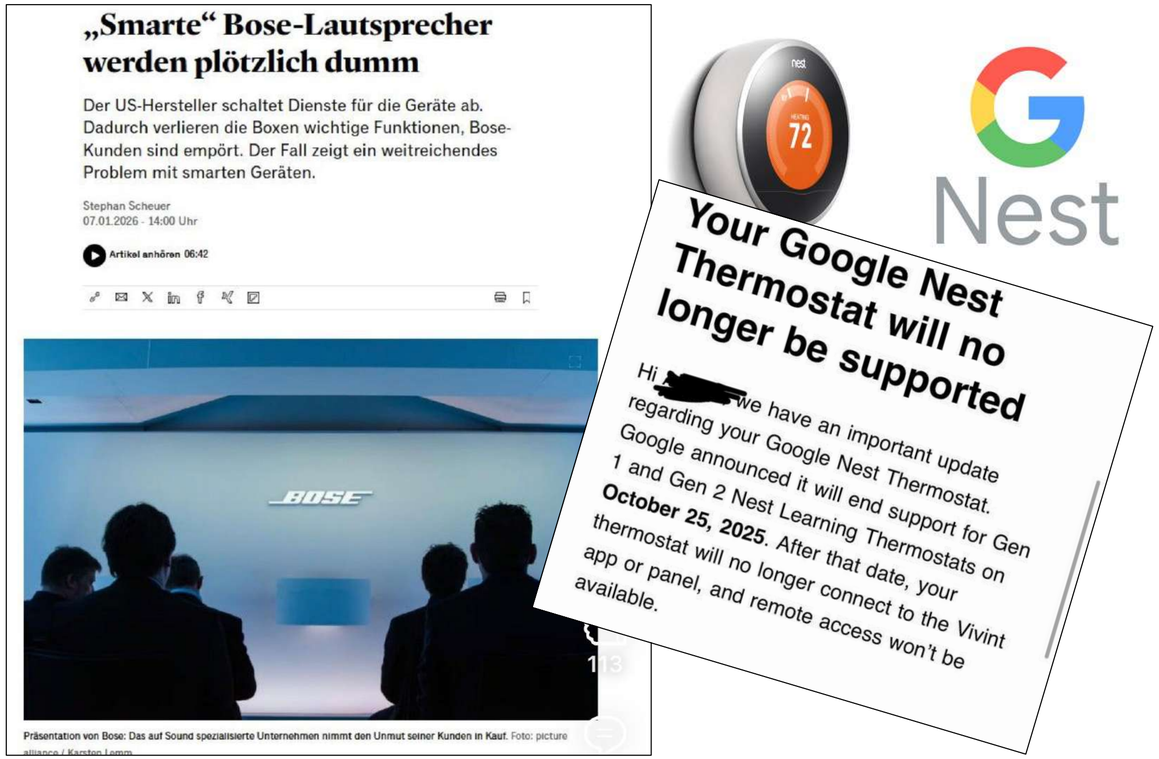
Zeit ist Geld → Passwörter immer mit
Gross- und Kleinbuchstaben, Zahlen, Sonderzeichen, min. 12 Zeichen

Kabelgebundenes LAN für OT/IoT bevorzugen

GIRA

3.Input: Updatefähigkeit sowie (zu) frühes Out-of-Date

Consumer Electronic oft nur für kurze Lebenszyklen ausgelegt



„Smarte“ Bose-Lautsprecher werden plötzlich dumm

Der US-Hersteller schaltet Dienste für die Geräte ab. Dadurch verlieren die Boxen wichtige Funktionen, Bose-Kunden sind empört. Der Fall zeigt ein weitreichendes Problem mit smarten Geräten.

Stephan Scheuer
07.01.2026 - 14:00 Uhr

Artikel anhören 06:42

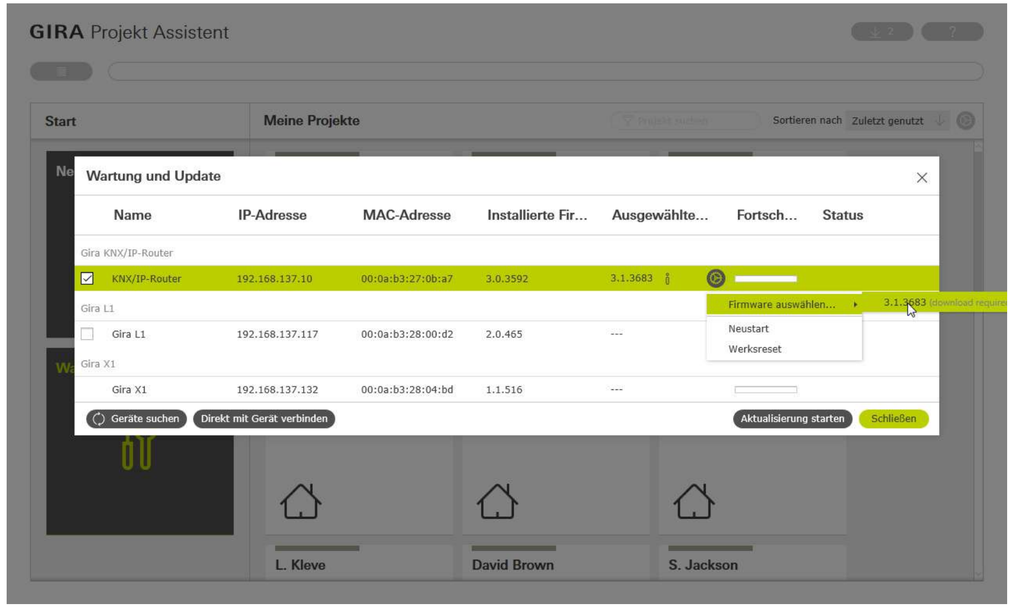
Präsentation von Bose: Das auf Sound spezialisierte Unternehmen nimmt den Unmut seiner Kunden in Kauf. Foto: picture alliance / Karsten Lemm

Nest

Your Google Nest Thermostat will no longer be supported

Hi [redacted], we have an important update regarding your Google Nest Thermostat. Google announced it will end support for Gen 1 and Gen 2 Nest Learning Thermostats on **October 25, 2025**. After that date, your thermostat will no longer connect to the Vivint app or panel, and remote access won't be available.

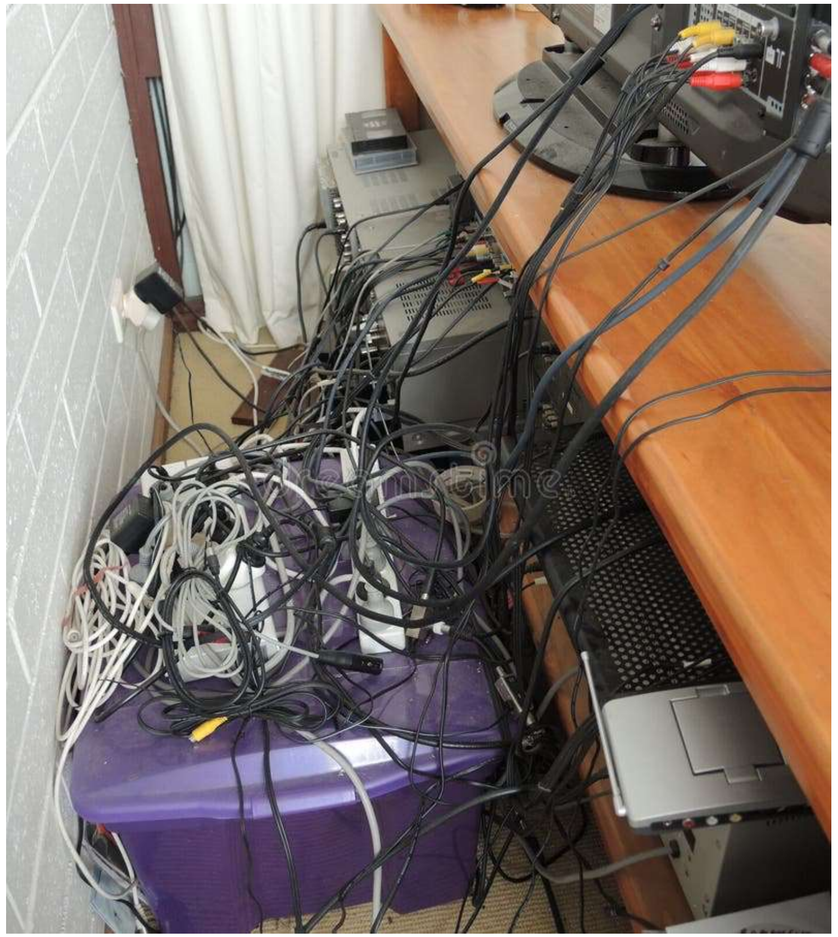
Updatefähigkeit und langlebiger Service kostet und wird im Profi-Bereich kaufentscheidend



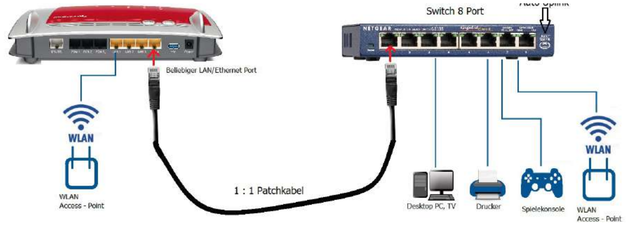
GIRA

4.Input: Infrastruktur im Gebäude und Wohnbau?

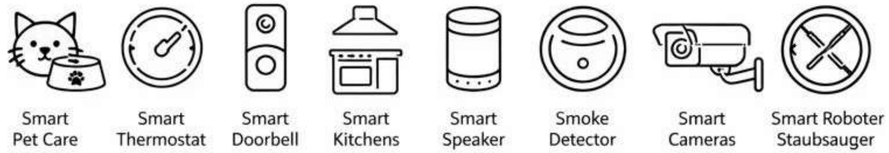
Wenig Sicherheitsbewusstsein, unzureichende Elektro- & Netzwerk-Installation



- Nutzende oft sich selbst überlassen
- Alles wird einfach am Provider-Router eingesteckt



- Geräte über Gateways oder direkt via WLAN in Internet!



- Nicht nur Wohnbau: Niedrigsichere Geräte wie Kaffeemaschinen teilen sich Netzwerke mit hochsensiblen Systemen wie Finanzservern

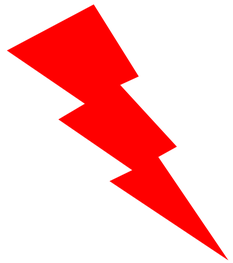
GIRA

5.Input Gebäudetechnik - Updates & Verschlüsselung

Problematik: Geräte sind für die Lebensdauer von 20+ Jahre ausgelegt

- Alte, unsichere Protokolle:
  Telnet, Modbus/TCP, BACnet
  sind oft unverschlüsselt

- Öffentlich zugängliche Leitungen oder
  Zugänglichkeit ausserhalb des Gebäudes
  z.B. unverschlüsseltes KNX statt KNX-Secure



- Nicht erkannte Sicherheitslücken in Firmware/Treiber
  z.B. oft in IP-Kameras, TCP-Stack "Ripple20„ , etc.
- Keine Update-Fähigkeit von Geräten
- Unklar wo und welche Geräte & Firmware im Einsatz sind
- keine Segmentierung, keine Isolierung gefährlicher Geräte

GIRA

6.Input: Datenschutz & Vertrauen

Wem vertrauen wir?

- Hersteller
  - Hardware
    - Software

- Dienstleister
  - Unternehmer
    - Anwender

GIRA

Take-Aways: Vertrauen, Kontrolle, routinierte Services

Grundsatz: Gerätefunktion muss (auch) ohne Internet-Verbindung möglich sein

1. Vollständiges Inventar vernetzter Geräte (Asset- & Lifecycle-Management)
2. Risikobewertung der Geräte/Systeme
3. Segmentierung welche IoT, Büro-IT und OT-Bereiche trennt
4. Technik-Netzwerk mit Subnetzen oder physische Trennung, ggf. Hardware wie Gira F1 KNX/SPIS-Bridge
5. Firewall & gesicherte Verbindung z.B. über VPN-Anwendung, Hardware wie z.B. Gira S1 VPN-Gateway
6. Verschlüsselung, Firmwareupdates, Zugangsschutz, Protokollfilter, Monitoring/Überwachung, UM/IAM

Legacy-Geräte/Systeme: Verwundbare Altsysteme «Kronjuwelen» erkennen und schützen

→ **Separate Ausschreibung und Budgetierung des OT-Netzwerkes bzw. OT-Security**
nicht nur UKV-Design sondern auch OT-Netzwerke, Security, IP-Konzept/-Ranges/-Subneting, Routing, etc

Orientierung:
- ✓ Empfehlung IKT-Sicherheit in der Gebäudeautomation von der KBOB → Link
- ✓ Sichere Gebäudeinformatik und KNX Secure von der KNX Association → Link
- ✓ Normenreihe ISA/IEC 62443

GIRA

Kommende Veranstaltungen

Forum Smart Home

electro suisse

25. Februar 2026 | Technopark ZH

13:15 **KEYNOTE**
Präsentiert by Gira Swiss AG (Gold Partner)
Sicherheit & Datenschutz: Infrastruktur für ein Smart Building
Gebäude vernetzen sich rasant: Heizungen, Ladesäulen, Kameras und andere IoT-Geräte kommunizieren über IP-Netzwerke und sind oft direkt online. Besonders im Wohnbau führt eine fehlende oder unzureichende Infrastruktur jedoch zu erheblichen Sicherheits- und Datenschutzrisiken. Der Vortrag zeigt, wie sich Angriffsflächen durch saubere Netzwerkarchitektur, Segmentierung, Verschlüsselung, sichere Standards wie KNX Secure und konsequente Updates reduzieren lassen – und wie diese Anforderungen bereits in Planung und Betrieb eines Smart Buildings integriert werden können.
Ernst Grassmann, Br@intop Schulungsinstitut

13:55 **Smart-Home-Daten: Goldgrube oder Datenschutzfalle?**
Moderne Smart Homes erfassen eine Vielzahl von Daten, darunter Temperaturverläufe, Bewegungsmuster, Sprachbefehle und Energiedaten. Diese Informationen ermöglichen Komfort, Effizienz und Sicherheit, bergen jedoch auch Risiken. Der Vortrag beleuchtet, welche Daten erhoben werden, wie sie genutzt werden können und wo Gefahren für die Privatsphäre und den Datenschutz entstehen. Abschliessend werden Tipps für den sicheren Umgang mit Daten gegeben.
Prof. Olivier Steiger, Hochschule Luzern –Technik & Architektur

14:15 **Datenräume – Daten sicher und souverän austauschen**
In modernen Gebäuden erfassen Geräte Daten für die eigentlichen Funktionen der Systeme und für Datenanalysen. Diese Daten könnten im Rahmen einer Zweitnutzung auch für Energiemanagement oder das Training von KI genutzt werden. Damit Kund:innen ihre Daten freigeben, braucht es Vertrauen. Datenräume bieten eine sichere Plattform für souveränen Datenaustausch. Das Referat zeigt Eigenschaften, Geschäftsmodelle und wie die

GIRA Akademie

IP-Netzwerk Seminar

für Elektrotechniker und Systemintegratoren

Dienstag - Donnerstag
21. - 23. April 2026

2er Arbeitsplätze an Managed Switches
Rahmenprogramm
Top-Referenten

Hotel Rheinsberg, Bad Säckigen
Direkt an Grenze, ZH 30min, BS 20min

Quellen / Weblinks

https://www.kbob.admin.ch/dam/de/sd-web/xnqPcdeyRemd/20250710_KBOB-Empfehlung%20IKT-Sicherheit%20in%20der%20Geb%C3%A4udeautomation_V1.0_Publikation_DE.pdf

https://www.knx.ch/wAssets/docs/publikationen/dt_KNX-Ratgeber_Sichere-Gebauedenetzwerke.pdf

https://www.paloaltonetworks.com/resources/infographics/device-security-threat-2025

https://www.zscaler.com/de/blogs/security-research/industry-attacks-surge-mobile-malware-spreads-threatlabz-2025-mobile-iot-ot

https://arxiv.org/abs/2508.02375

https://www.all-about-security.de/studie-2025-device-security-threat-report-vernetzte-geraete-stellen-massive-sicherheitsrisiken-dar/

https://www.comconsult.com/versteckte-gefahren-im-heimnetz/

https://www.forescout.com/blog/probe-into-chinese-connected-devices-in-us-networks/#:~:text=Over%20the%20past%20five%20years%2C,espionage%20or%20disrupt%20critical%20infrastructure

Anhang

Ausgewählte Lösungen & Geräte

Gira Smart Home, Smart Building

Familienunternehmen

Hightech-Fabrik und Firmen-Campus in der Nähe Düsseldorf

Deutscher Marktführer für hochwertige Elektrotechnik

Starke Marke & Design für stilvollen Wohnbau

Schalter & Steckdosen

Smart Home, Elektronik Türsprechsysteme

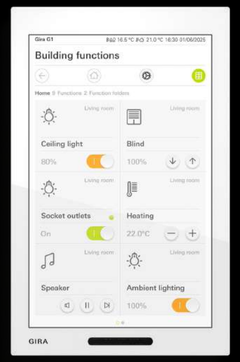
HomeServer, X1-Server KNX-Komponenten

Attraktive Lösung für smarte MFHs

GIRA

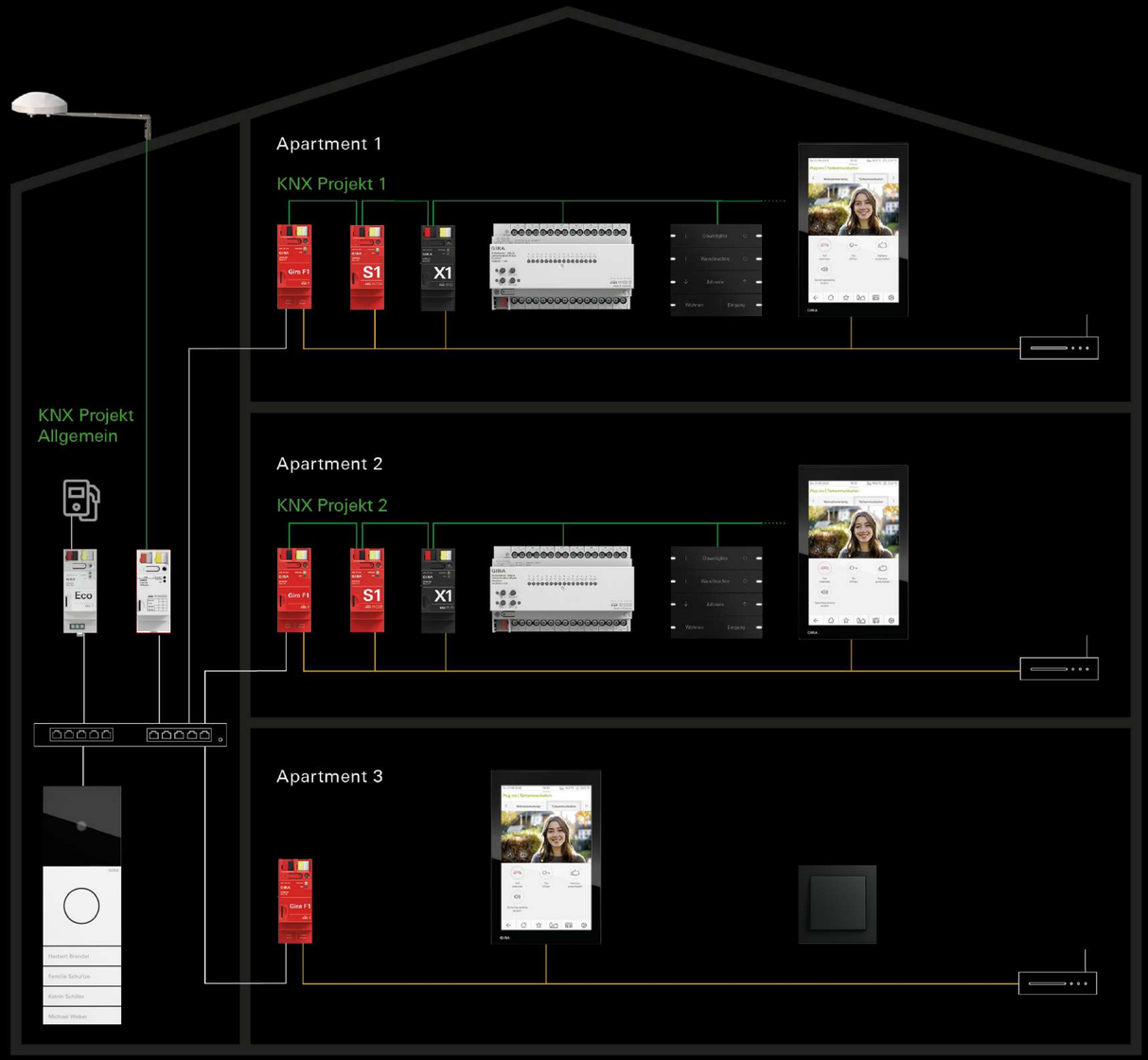
G1 Touch-Display

Türkommunikation, Licht, Jalousie, Temperatur, Musik Szenarien, etc.



Aussensprechstelle System 106

Ruftasten oder Ruftastendisplay inkl. Code-Schloss, HD-Kamera mit Infrarot-Nachtsicht, Heizung, 126° Erfassungswinkel, Wasserfeste-Membrane, Active Noise Cancelling



IP-Türsprechsystem und KNX-Gebäudeautomation bis 1000 Wohnungen

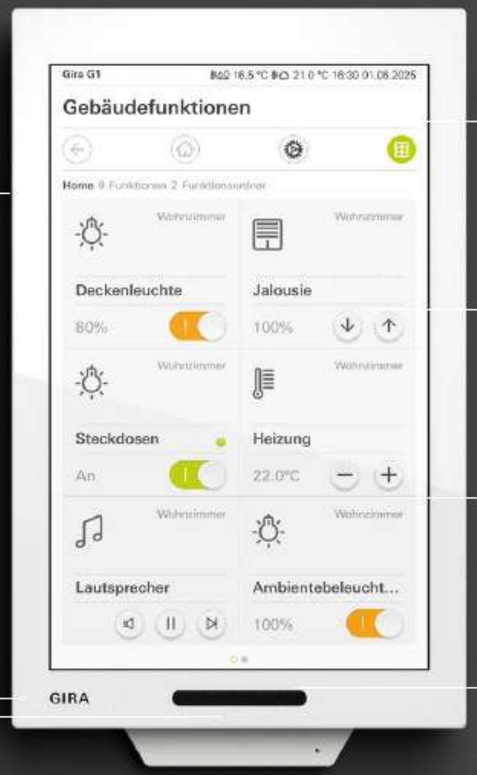
Sichere Verschlüsselung & Segmentierung (Privat, Public) u.a. mit Gira F1

Bewährtes Gira Design in hochwertiger Qualität

Einfachste Planung, Inbetriebnahme und Betrieb mit Verwaltung der Nutzer und mobiler Weiterleitung

Gebäudenetzwerk
Privates Netzwerk
KNX TP

Schneller. Größer. Stärker. Der neue Gira G1.



Lautsprecher für die Türkommunikation im Gehäuse integriert

Brillantes, hochauflösendes 7-Zoll-Touchdisplay

Display ist aus allen Betrachtungswinkeln sehr gut lesbar

Bruchsicheres Glas

8-farbige LED synchronisiert zu den Farben des Gira Tastsensor 4

Integrierte Mikrofone für beste Sprachqualität

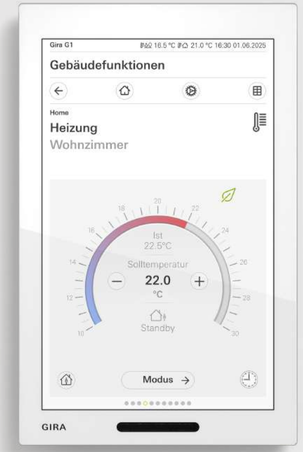
Helligkeits- und Näherungssensor für automatische Displayanpassung

Temperatur- und Feuchtigkeitsfühler (optional) zur Messung von Temperatur und Luftfeuchte in einem Raum

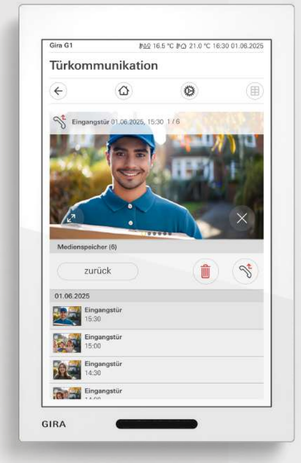
Weiß Schwarz

GIRA

KNX Gebäudeautomation und Türkommunikation



Mit X1-Miniserver Client zur Anbindung an KNX-Gebäudeautomation



Als Wohnungsstation für das Türkommunikationssystem

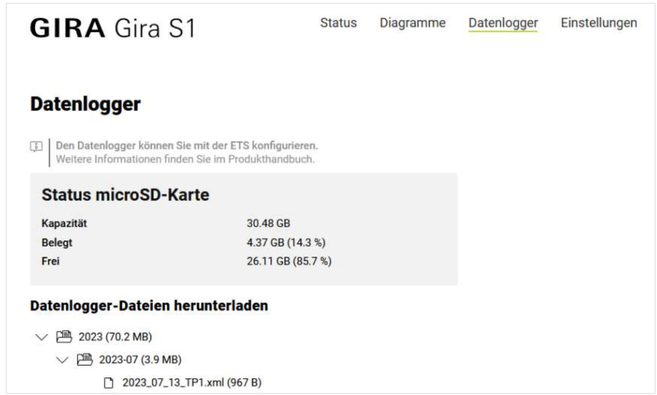
HomeServer Client mit neuen Funktionen

S1 VPN-Schnittstelle

GIRA

- Sicherer Fernzugriff, Fernwartung und Ferndiagnose von KNX- & Netzwerk-Geräten
- Sichere VPN-Verschlüsselung
- Einfache Inbetriebnahme ohne spezielle Netzwerk- & Router-Kenntnisse
- Anschlüsse: 2xRJ45-Switch, KNX-TP, 24VDC

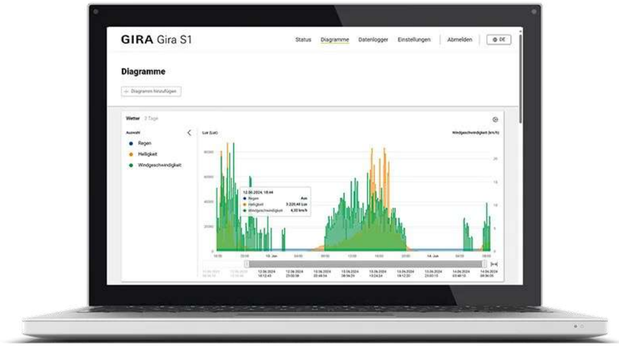
KNX-Busmonitoring



Ausgezeichneter Datenschutz und IP-Sicherheit

VDE 10/2024 Smart Home Informationssicherheit geprüft S1 Gateway

Diagramme, Zeitgeber, Benachrichtigungen

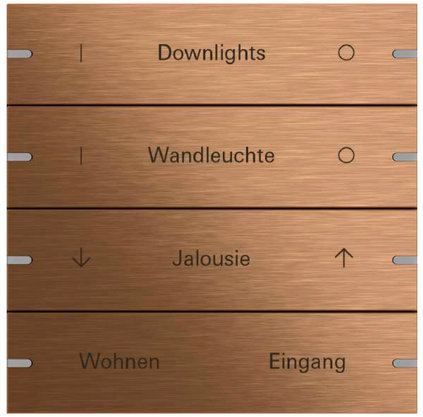


Zugriffsverwaltung für Endkunden

Smart Home Geräte

GIRA

Tastsensoren KNX Secure



- Verschiedene Designs und Grössen in Kunststoff und Echtmaterialien
- Glas, Bronze, Edelstahl, Alu
- Angenehme taktile Tasten
- Umfassende Funktionen
- Hochwertige Beschriftung
- Integrierter Temperatur- & Feuchtigkeit-Sensor

Steuergräte KNX Secure

X1 Mini-Server

- Visualisierungen, Automatisierungen und Steuerungen mit grafischen Logik-Bausteinen zur Inbetriebnahme
- Intuitive Darstellung über Gira Smart Phone App
- Schaltuhren, Anwesenheitssimulation,
- Szenen und Sequenzen etc.
- Anbindung von Drittanbieter wie Tado, Sonos, Philips Hue, Google

F1 KNX/SIPS-Bridge

- Koppelung von zwei autarken KNX-Anlagen und/oder IP-Netzwerken
- Einsatz bei Eigentumswohnungen mit separaten ETS-Projekten, Mietflächen, Shopping-Center oder um mehrere Gebäude zu verbinden
- Verbinden von zentralen KNX-Gruppen-Adressen (Treppenhaus, Wetterstation, Energiewerte, etc)
- SIP/S-Funktionalität für Trennung der IP-Netzwerke (Public/Privat)

PODIUM

Giovanni Crupi
Zentralpräsident Swiss Engineering STV

Urs Wiederkehr
Berater FB "Digitalisierung IT» SIA

Peter Vonesch
Fachexperte Strategie, Risikomanagement, Cybersicherheit, Sensibilisierung SIA

Clélia Warunee Runtz
Bundesamt für Cybersicherheit (BACS), Fachexpertin Sensibilisierung

.

Fabian Stelling
Senior Software Engineer & Security Consultant, Ergon Informatik

Markus Biedermann
Country Manager Schweiz Gira

VERANSTALTUNG ALS EVENTREPORT VERFÜGBAR

Video-Podcast und Präsentationen ab morgen auf swissbau.ch/eventreports

Cybersicherheit für Betreiber, Nutzerinnen und Mieter – Anforderungen an smarte Bauwerke

Mittwoch | 21.01.2026
15.30 – 16.30 Uhr
Main Stage, Swissbau Lab

ergon smart people – smart software®

GIRA

sia
schweizerischer ingenieur- und architektenverein
société suisse des ingénieurs et des architectes
società svizzera degli ingegneri e degli architetti
swiss society of engineers and architects