Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

Cyberresilienz und Notfallplanung für die Gemeinden



30. Oktober 2026

Andreas Grünert, Leiter Technologie & Security Engineering - BACS

Kilian Cuche, Fachexperte Sensibilisierung Cybersicherheit - BACS



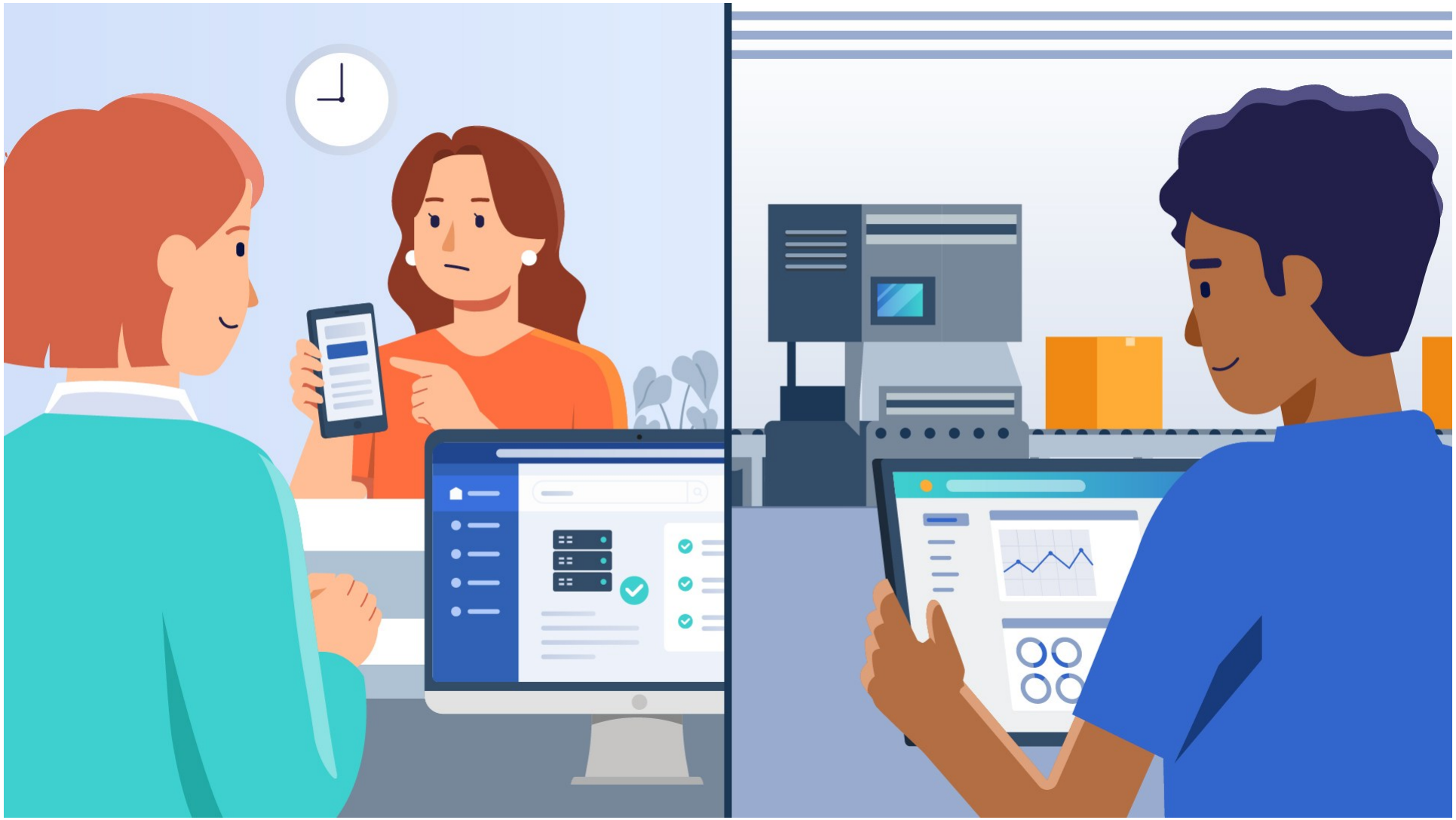
Cybersicherheit und Cyberresilienz

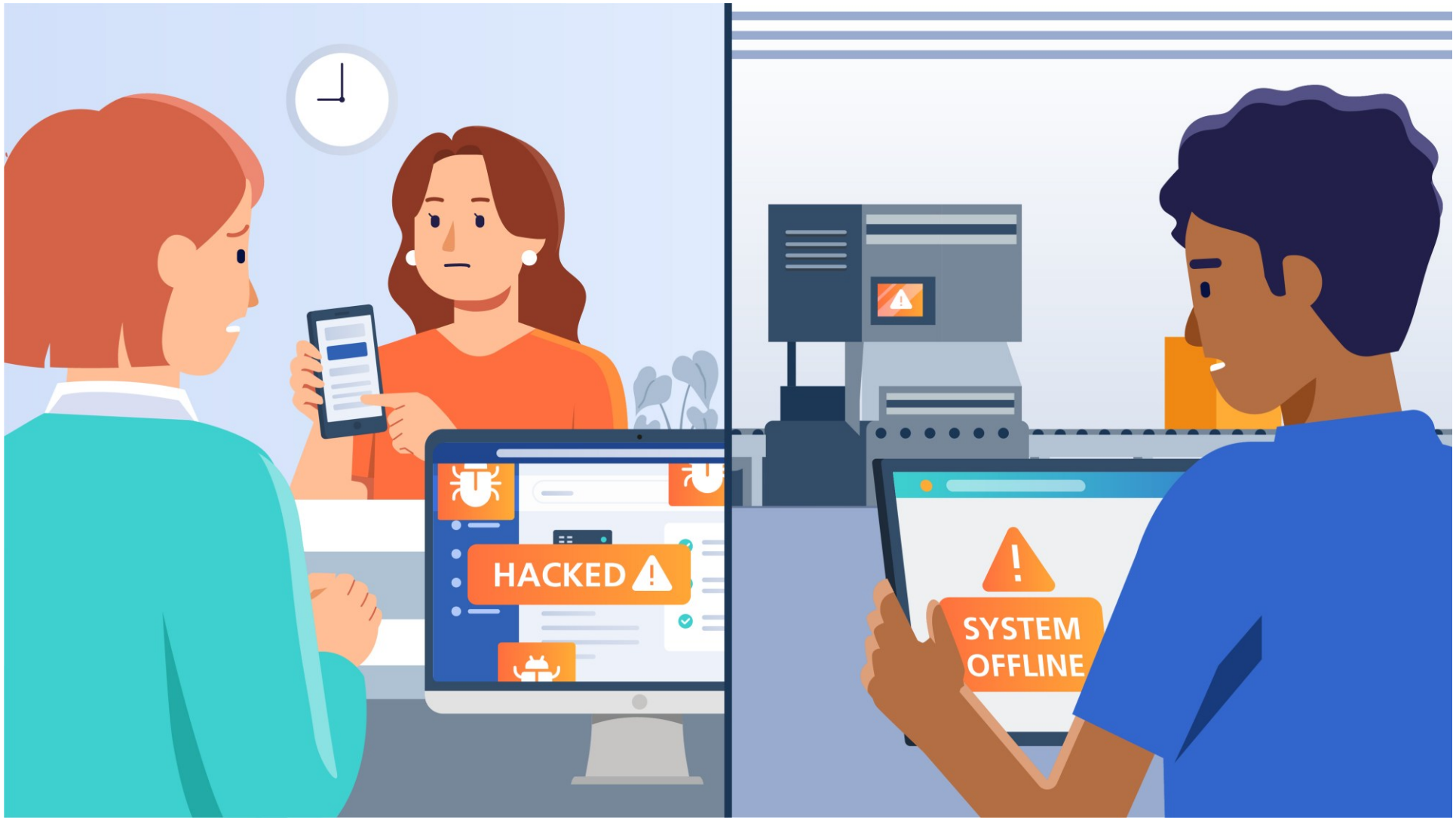
Ausgangslage

- ✓ Cyberangriffe nehmen zu
- ✓ Angriffe haben Auswirkungen auf geschäftskritische Prozesse (Produktion, Dienstleistung, …)
- ✓ Cyberangriffe sind **kaum vorhersehbar**
- ✓ Vernetzung verstärkt die Bedrohung



Was ist Cyberresilienz? Ein Beispiel




HACKED
SYSTEM
OFFLINE


ZUGRIFF
VERWEIGERT
PRODUKTION
GESTOPPT

Was ist Cyberresilienz?

Das Beispiel zeigt:

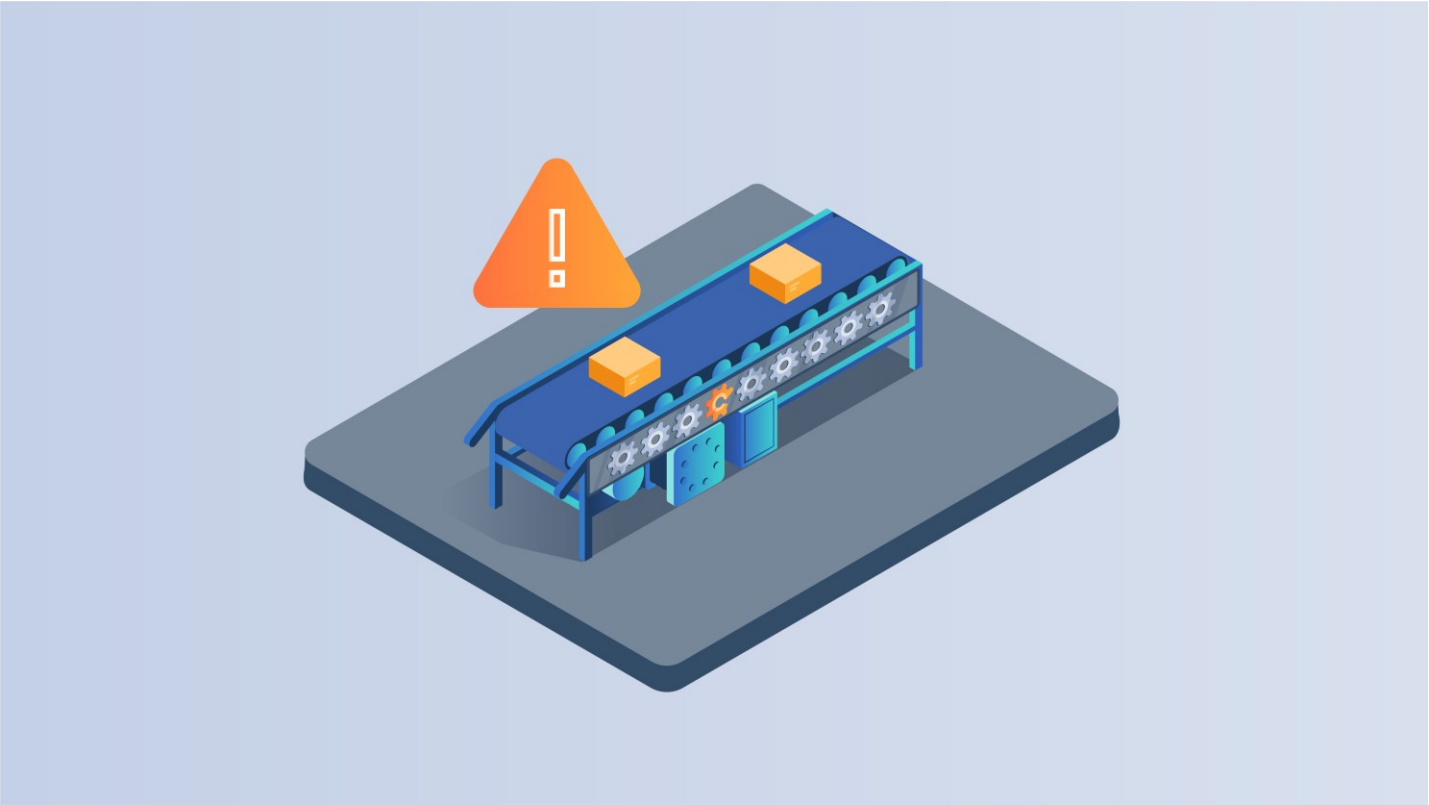
Entscheidend ist nicht nur, wie gut eine Organisation vor Cyberbedrohungen geschützt ist, sondern auch, wie gut sie ihre geschäftskritischen Prozesse trotz solcher Ereignisse aufrechterhalten oder rasch wiederherstellen kann.

Diese Fähigkeit wird als Cyberresilienz bezeichnet.



Wann ist eine Organisation Cyberresilient? Voraussetzungen

Voraussetzung für Cyberresilienz



Die geschäftskritischen Prozesse sind bekannt…

Voraussetzung für Cyberresilienz

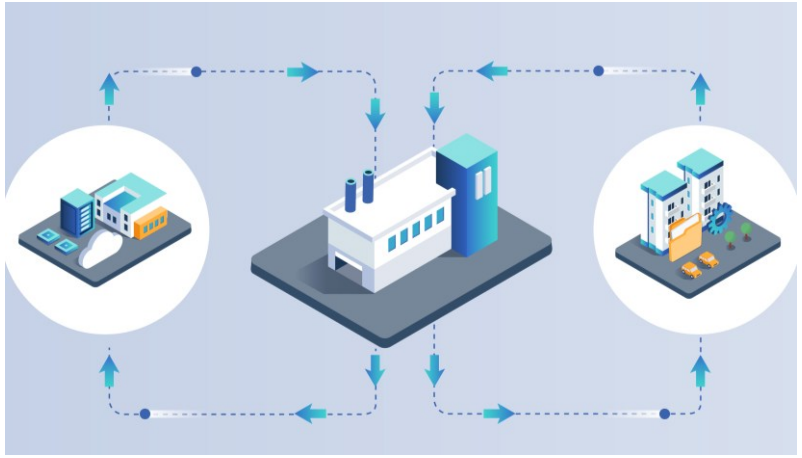
… sowie die Abhängigkeiten von IT-Systemen, …



…Steuerungssystemen, …



Lieferanten, Dienstleistern, …



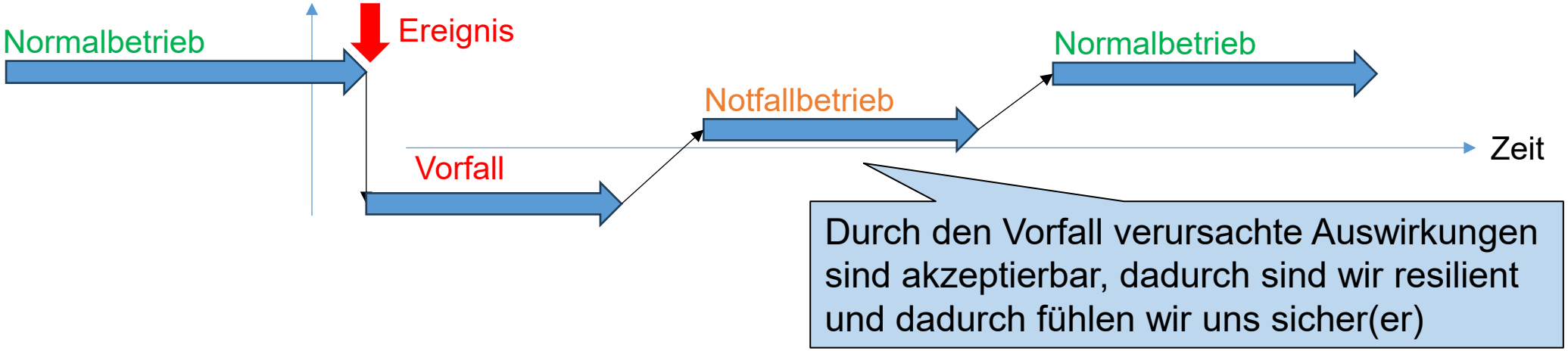
und weiteren Partnern.



Wann ist eine Organisation cyberresilient?

Wir sind resilient, wenn wir akzeptierbare Auswirkungen erleiden können.
Wir müssen also:

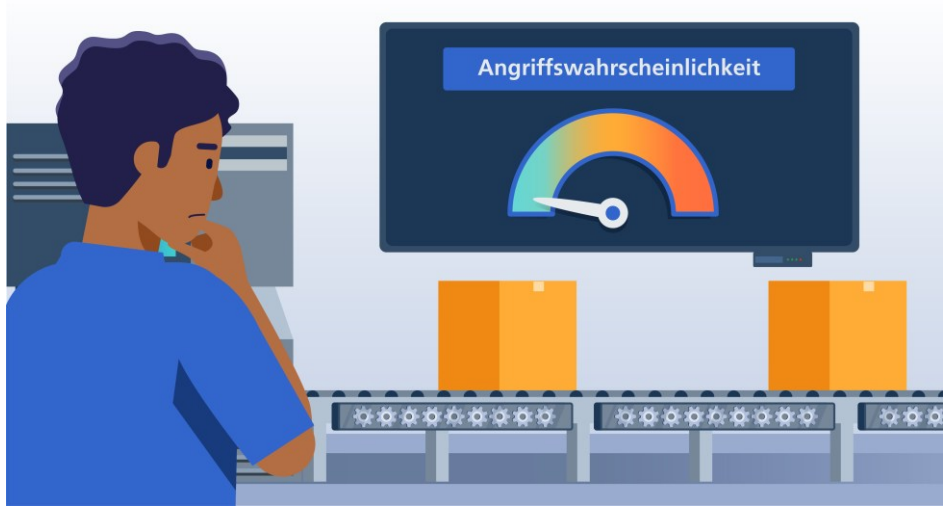
- wissen, was nicht akzeptierbar ist für unsere Organisation,
- präventive Massnahmen ergreifen, um Vorfälle zu verhindern,
- Vorfälle erkennen und bereit sein zu reagieren, wenn es zu einem Vorfall kommt



Ein Perspektivenwechsel ist notwendig

Statt zu fragen, wie wahrscheinlich ein Angriff ist, lautet die zentrale Frage:

„Welchen Ausfall und welche Auswirkungen auf unsere geschäftskritischen Prozesse können wir uns leisten?“







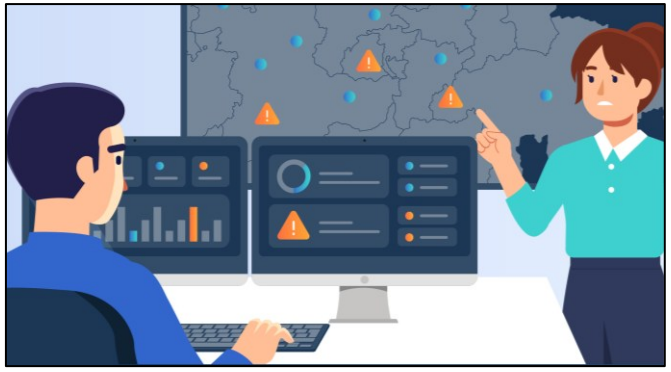
Cybersicherheit als Grundlage der Cyberresilienz

Vier Entscheidende Aspekte

Angriffe präventiv verhindern



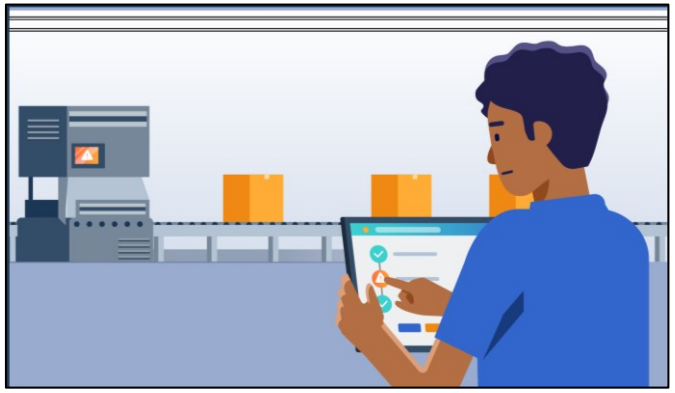
Ereignisse und Angriffe erkennen



Auswirkungen begrenzen



Systeme Rasch wiederherstellen

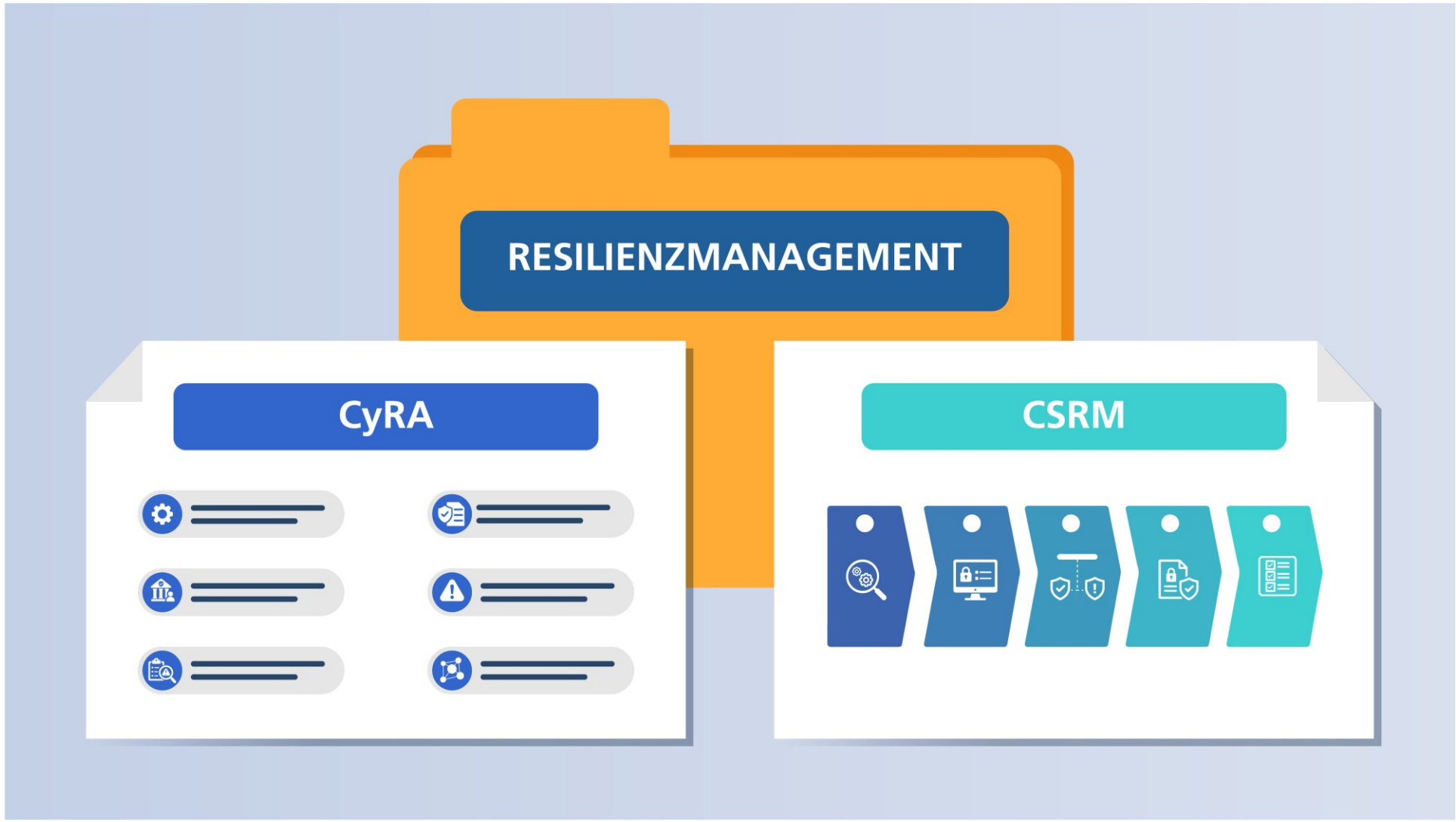


Cybersicherheit und Cyberresilienz

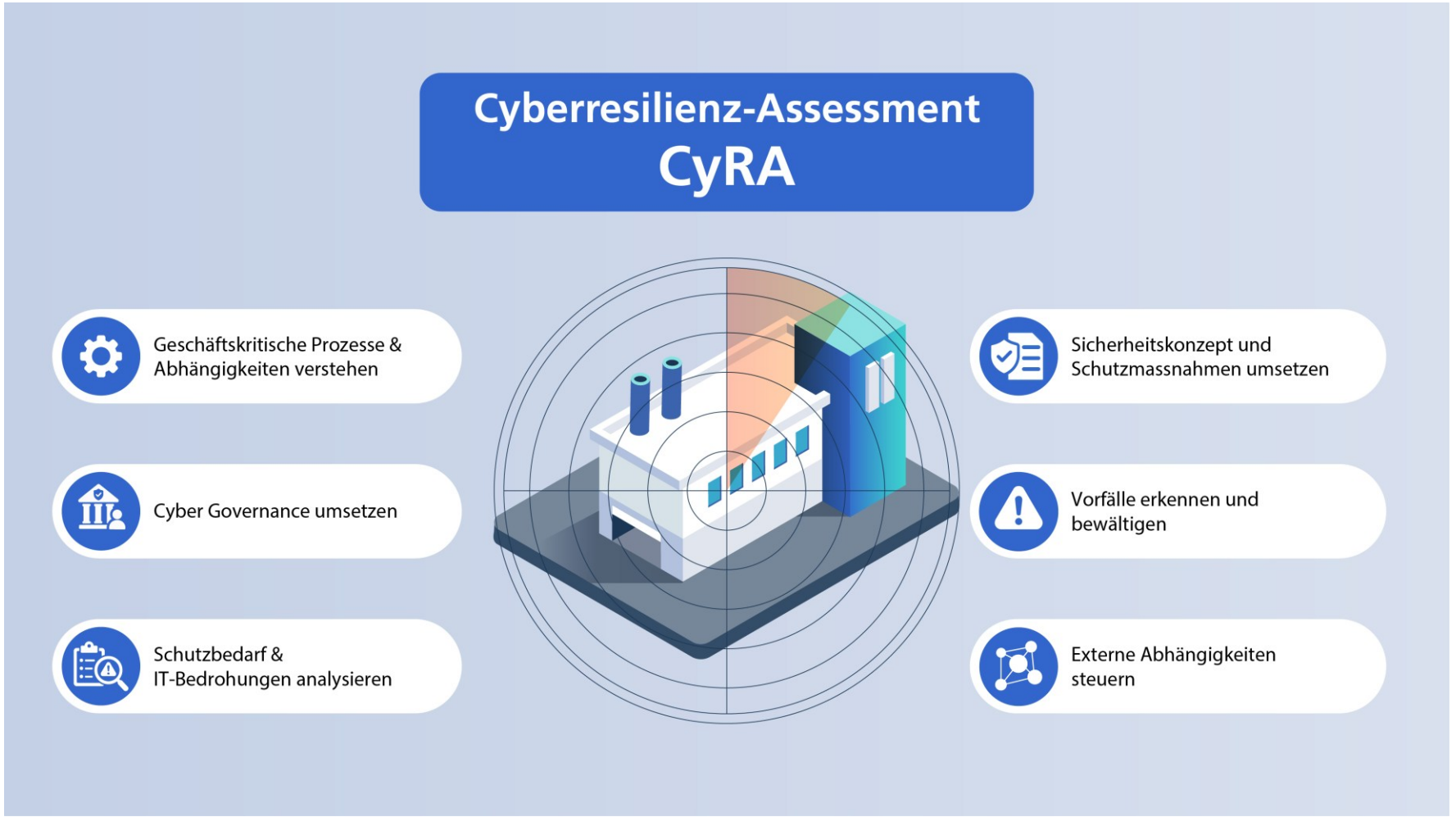
- ✓ Cyberresilienz baut auf der Cybersicherheit auf, geht jedoch darüber hinaus.
- ✓ Sie umfasst neben präventiven Schutzmassnahmen auch die Fähigkeit, Vorfälle frühzeitig zu erkennen, ihre Auswirkungen zu begrenzen und angemessen darauf zu reagieren.
- ✓ Das wichtigste Element dabei ist die Erkennung und die Fähigkeit zu reagieren. Die meisten Massnahmen zielen heute jedoch auf die Verhinderung von Angriffen ab.



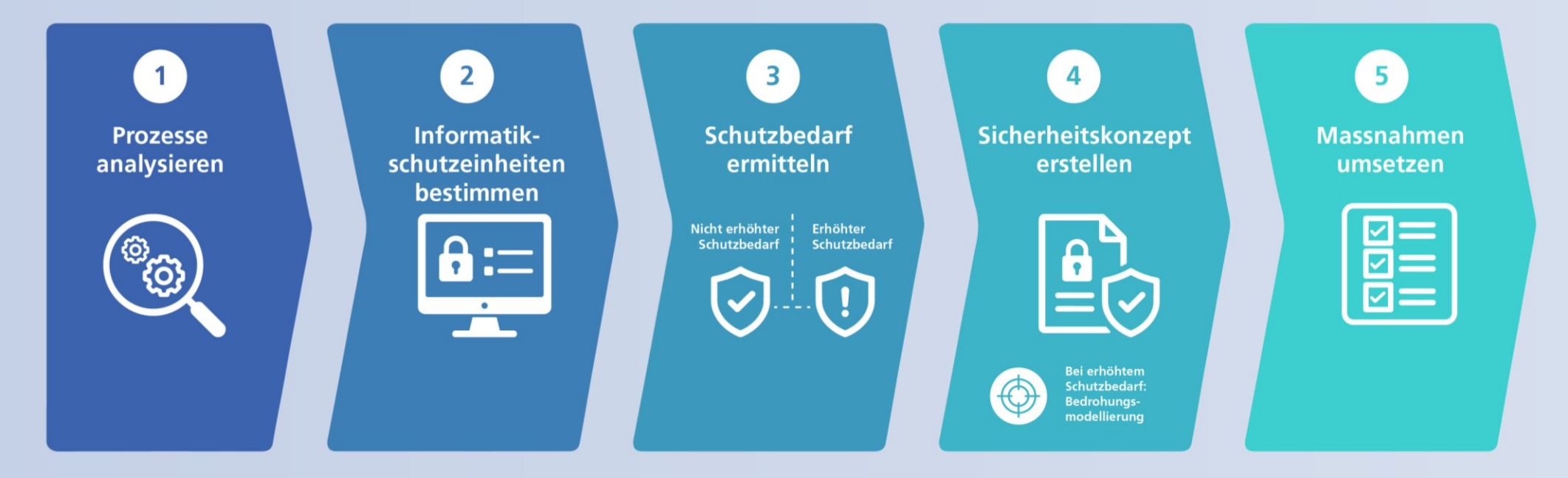
Resilienzmanagement – Methoden und Hilfsmittel von BACS


RESILIENZMANAGEMENT
CyRA
CSRM

Cyberresilienz-Assessment (CyRA)



Cybersicherheits- und Resilienzmethode



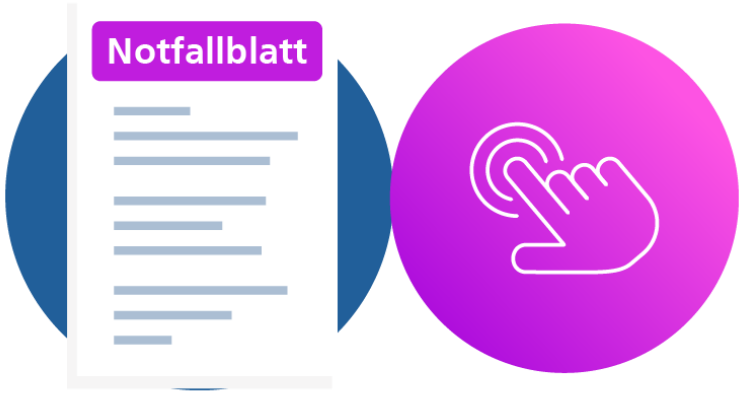


Notfallkonzept für Gemeinden

ncsc.admin.ch/notfallkonzept

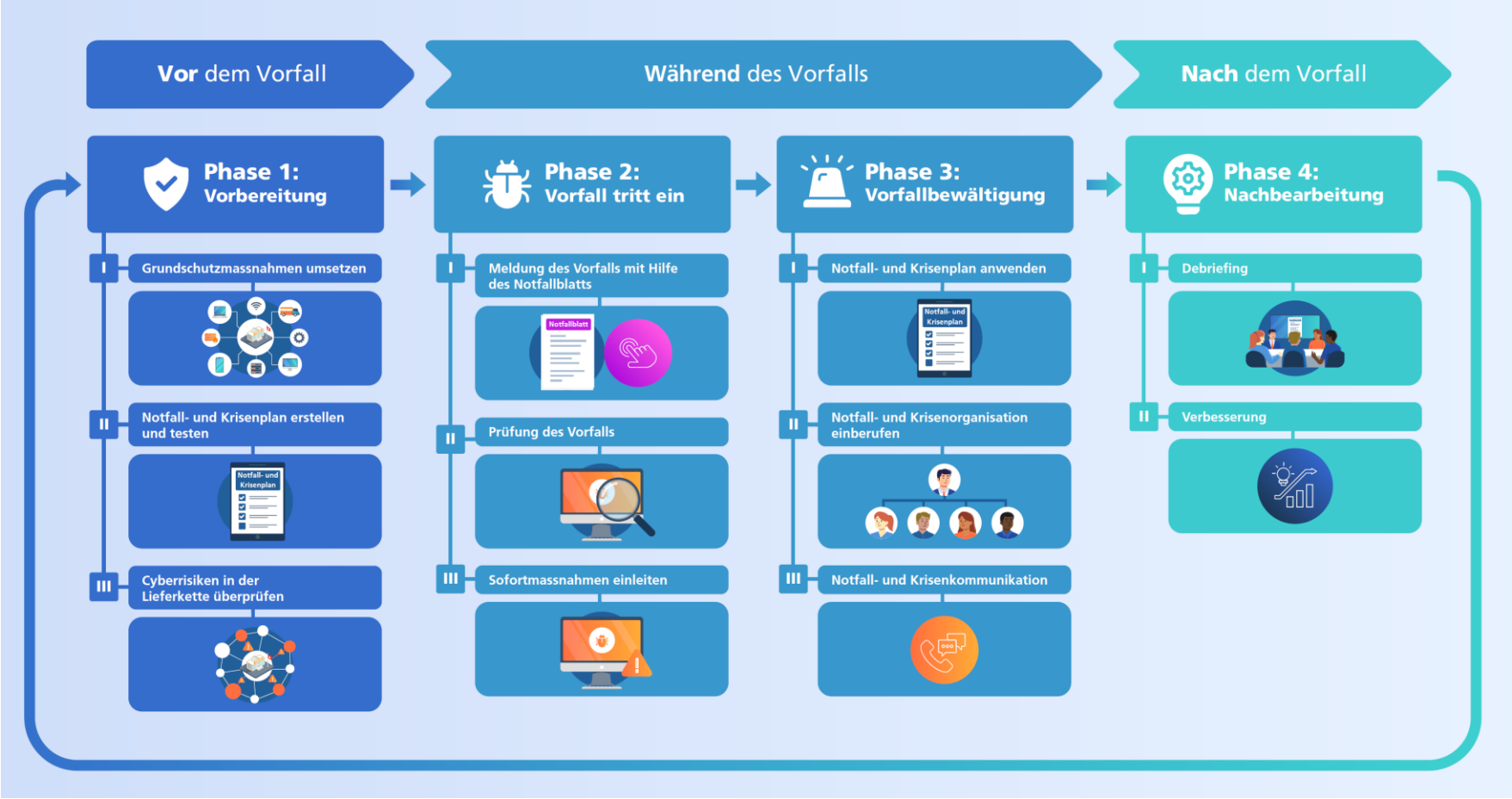
Hilfsmittel – Templates







Infografik


Vor dem Vorfall
Während des Vorfalls
Nach dem Vorfall
Phase 1: Vorbereitung
Phase 2: Vorfall tritt ein
Phase 3: Vorfallbewältigung
Phase 4: Nachbearbeitung
I Grundschutzmassnahmen umsetzen
II Notfall- und Krisenplan erstellen und testen
III Cyberrisiken in der Lieferkette überprüfen
I Meldung des Vorfalls mit Hilfe des Notfallblatts
II Prüfung des Vorfalls
III Sofortmassnahmen einleiten
I Notfall- und Krisenplan anwenden
II Notfall- und Krisenorganisation einberufen
III Notfall- und Krisenkommunikation
I Debriefing
II Verbesserung

Phase 1 – Vorbereitung



Grundschutzmassnahmen umsetzen

Cyberrisiken in der Lieferkette überprüfen

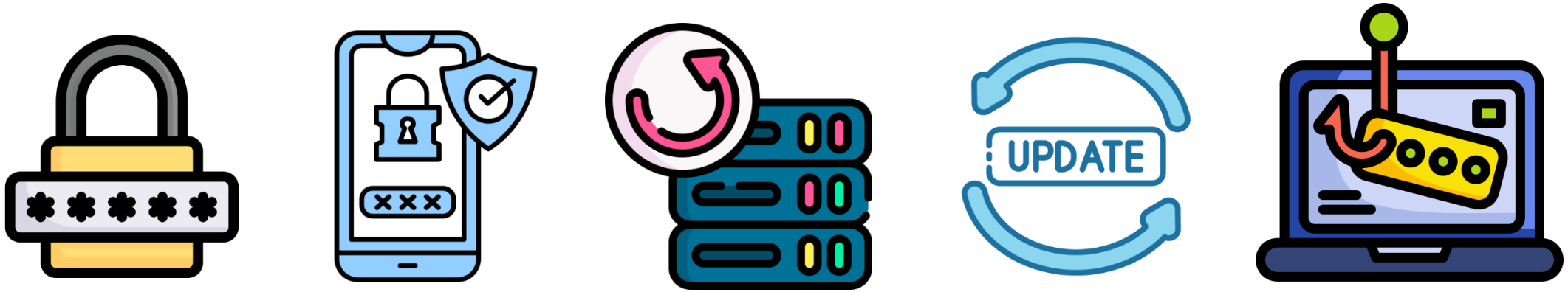




Notfall- und Krisenplan erstellen und testen

Grundschutzsmassnahmen

- Empfehlungen IKT-Minimalstandards
- Cybersicherheits- und Resilienzmethode (CSRM)
  -> Webinare im November (19.11 DE / 26.11 FR)



Quelle: Icons8 & Flaticon

Cybersicherheit in der Lieferkette



https://www.ncsc.admin.ch/supply-chain-de

Phase 1 – Vorbereitung

IT-unterstützte Aufgaben	Maximal tolerierbare Ausfallzeit	Nicht akzeptierbare Auswirkungen
[AUFGABE]	[ZEIT]	[AUSWIRKUNGEN]
Trinkwasserversorgung	*1 Stunde*	*Beeinflussung der Wasser Qualität*
Elektrizitätsversorgung	*1 Stunde*	*-*
Wärmeversorgung	*1 Stunde*	*-*
Finanzwesen / Cash-Management	*1 Tag*	*Abfluss von sensiblen Daten*
Einwohnerdienste	*1 Tag*	*Abfluss von sensiblen Daten*
Sozialdienste	*1 Tag*	*Abfluss von sensiblen Daten*
E-Government	*2 Tag*	*Abfluss von sensiblen Daten*

Tabelle 1: Liste der IT-unterstützenden Aufgaben der Gemeinde.

Interne Kontaktperson (inkl. Stellvertreter/-in), die bei einem IT-Vorfall oder bei Unsicherheiten hinsichtlich einer möglichen Kompromittierung der Informatik zu benachrichtigen sind:

Priorität	Person	Funktion	Erreichbarkeit
[PRIO]	[VORNAME, NAME]	[FUNKTION]	[KONTAKTDATEN]
1	*Max Muster*	*Verantwortliche/r Notfallmanagement (IT Single Point of Contact - SPOC) (darf extern sein)*	*1: +41 7X XXX XX XX* *2: +41 2X XXX XX XX* *3: Messaging-Apps*
2	*Lilian Beispiel (Stv)*	*Gemeindepräsident/-in und Leiter/-in Krisenstab*	*1: +41 7X XXX XX XX* *2: +41 2X XXX XX XX* *3: Messaging-Apps*
3	*Admin Muster*	*Gemeindeschreiber/-in*	*1: +41 7X XXX XX XX* *2: +41 2X XXX XX XX* *3: Messaging-Apps*

Tabelle 2: Liste der Kontaktpersonen der Gemeinde bei einen IT-Vorfall.

3.3.1. Dateninventar

Die folgende Tabelle beinhaltet die wichtigen Daten der Gemeinde, sinnvoll gruppiert und den Aufgaben zugeordnet. Weiter soll ersichtlich sein, wo diese gespeichert und für eine Wiederherstellung gesichert werden.

Daten	Verwendet bei folgenden Aufgaben	Standort der Daten	Backup-Häufigkeit	Backup-Standort
[DATENTYP]	[AUFGABEN]	[STANDORT]	[HÄUFIGKEIT]	[STANDORT]
Einwohnerdaten	*Einwohnerdienste*	*On-Prem Server*	*Täglich*	*Offline HD*
Buchhaltungsdaten	*Finanzwesen*	*…*	*Täglich*	*…*
Kommunikationsdaten	*…*	*Extern: MS Azure*	*[Monatlich]*	*…*
Arbeitsdaten	*…*	*…*	*[Wöchentlich]*	*…*

Tabelle 3: Dateninventar der Gemeinde

Notfall- und Krisenplan erstellen und testen

Phase 1 – Vorbereitung

3.3.2. Priorisierung bei Wiederanlauf und Wiederherstellung

Die folgende Tabelle enthält dieselben Aufgaben, wie in Kapitel 1 beschrieben, und ist mit zusätzlichen Informationen zu relevanten IT-Systemen und Sofortmassnahmen ergänzt.

Priorität	IT-unterstützte Aufgaben	Nicht tolerierbare Auswirkungen	Unterstützende IT-Systeme im Normalbetrieb	Sofortmassnahmen und Notfallbetrieb
[PRIO]	[AUFGABEN]	[ZEIT/ AUSWIRKUNG]	[IT-SYSTEME]	[MASSNAHMEN]
1	*Trinkwasserversorgung*	*Ausfall 1 Stunde Beeinflussung der Wasserqualität*	*OT-System remote gesteuert*	*OT-System vor Ort oder manuell gemäss BCM-Prozeduren X*
2	*Elektrizitätsversorgung*	*Ausfall 1 Stunde*	*[…]*	*[…]*
3	*Finanzwesen / Cash-Management*	*Ausfall 1 Tag Abfluss sensibler Daten*	*Arbeitstplatzsystem, M365, SAP (S4Hana), Abacus, Crésus, WinBiz, …*	*Ordner mit Papier XYZ im Schrank BCM-Prozeduren Y*
4	*Einwohnerdienste*	*Ausfall 1 Tag Abfluss von sensiblen Daten*	*Arbeitstplatzsystem, M365, FabaSoft, WWSoft, BDI, …*	*Ordner mit Papier XYZ im Schrank [BCM-Prozeduren Z]*

Tabelle 4: Priorisierung bei Wiederanlauf und Wiederherstellung sowie die damit verbundenen IT-Systeme und Massnahmen für den Notfallbetrieb.

3.3.3. Kritische IT-Abhängigkeiten der Gemeinde

Die folgende Tabelle zeigt die IT-Abhängigkeiten zwischen der Gemeinde und externen Partnern (z. B. Partnerorganisationen, interkommunale Organisationen, IT-Dienstleister). Dies ist insbesondere bei ausgelagerten oder extern betreuten IT-Leistungen wichtig, damit bei einem Notfall die relevanten Partner schnell kontaktiert werden können.

Partner	Aufgaben	Leistungen	Kontakt
[UNTERNEHMEN]	[AUFGABEN]	[LEISTUNGEN]	[KONTAKTDATEN]
Muster Informatik AG (IT-Dienstleister)	*Finanzwesen / Cash-Management Einwohnerdienste*	*Bereitstellung des ERP, Bereitstellung der Cloud-Infrastruktur*	*+41 7X XXX XX XX Notfallstrasse 110 7687 Helferswil*
Ramseier GmbH	*Trinkwasserversorgung*	*Bereitstellung der Fernsteuerungsysteme*	*+41 7X XXX XX XX Notfallstrasse 110 7687 Helferswil*

Tabelle 5: Liste der kritischen IT-Abhängigkeiten der Gemeinde und der externen Partner.

Notfall- und Krisenplan erstellen und testen

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)



4.2. Notfallerkennung / Triage

Der IT-Verantwortliche muss eine erste Einschätzung machen:

- Wer und welche IT-Systeme und Daten sind betroffen?
- Handelt es sich eher um einen IT-Unfall oder um einen IT-Angriff?

Ein IT-Notfall wird erkannt, wenn:

- Mindestens eine der Gemeindeaufgaben nicht mehr wahrgenommen werden kann aufgrund eines IT-Vorfalls oder nicht akzeptierbare Auswirkungen aufgetreten sind (siehe Kapitel 1);
- Es kann bereits abgeschätzt werden, ob die Wiederherstellung länger dauern wird als die maximale definierte zulässige Zeit, die Wiederherstellungszeit nicht eingeschätzt werden kann, oder nicht akzeptierbare Auswirkungen bereits absehbar sind.

Ein IT-Notfall wird zur Krise, wenn:

- Vitale Aufgaben nicht mehr wahrgenommen werden können und die Auswirkungen weit über die IT hinaus gehen.



4.3. IT-Sofortmassnahmen

Folgende Sofortmassnahmen sind je nach Ausgangslage sowie betroffene IT-Systeme und Daten von [im Kapitel 1 definierte IT-SPOC]] sofort umzusetzen:

- Im Falle eines Angriffs (z. B. mit Schadsoftware) die infizierten Systeme umgehend vom Netz trennen;
- Die Internetverbindungen unterbrechen (Web, E-Mail sowie Fernzugriff und VPN von Standort zu Standort), um eine Weiterverbreitung zu verhindern;
- Die Backups überprüfen und sofort schützen. Backups sollten so schnell wie möglich physisch vom infizierten Netzwerk getrennt werden («offline genommen werden»);
- [Weitere definierte, kontext- und systemabhängige IT-Sofortmassnahmen].

Phase 3 – Vorfallbewältigung

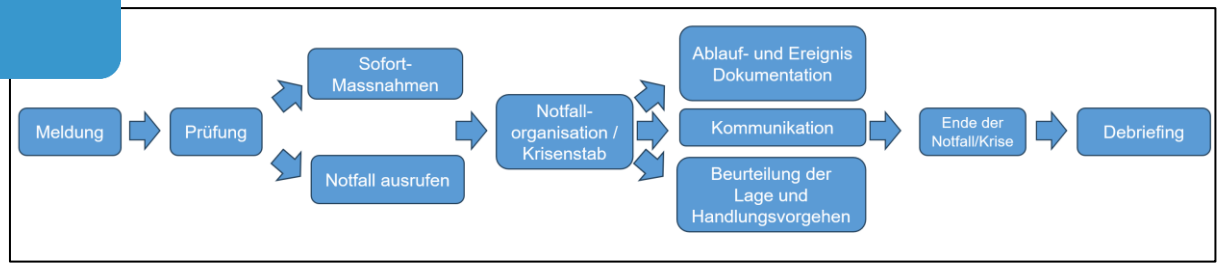


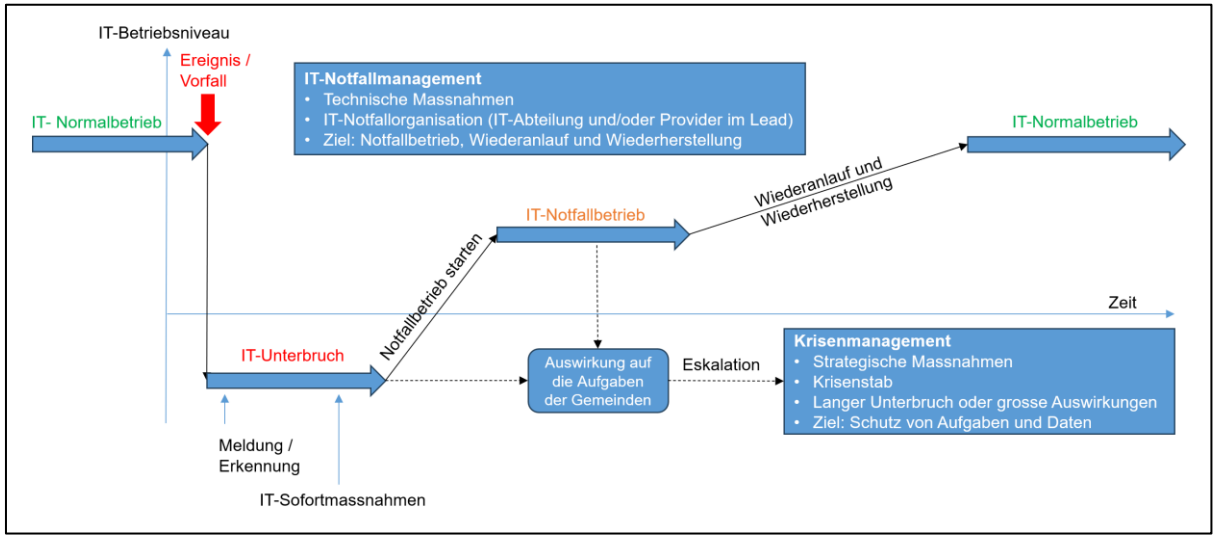
IT-Notfall- und Krisenplan von Gemeinde [NAME]

Die vorliegende IT-Notfall- und Krisenplan-Vorlage darf flexibel an die spezifischen Anforderungen der Gemeinde angepasst werden.[1]

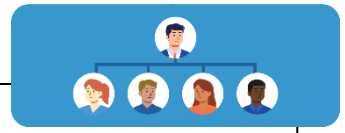
Inhaltverzeichnis

1. Akzeptierbare Auswirkungen und Kontakte ... 2
2. IT-Notfall- und Krisenplan – worum geht es? ... 3
3. Notfallvorbereitung ... 4
   3.1. Vorbereitungsaufgaben, Rollen und Verantwortung ... 4
   3.2. Notfallübungen / Verifizieren des IT-Notfall- und Krisenplanes ... 5
   3.3. Relevante Informationen ... 5
      3.3.1. Dateninventar ... 5
      3.3.2. Priorisierung bei Wiederanlauf und Wiederherstellung ... 6
      3.3.3. Kritische IT-Abhängigkeiten der Gemeinde ... 6
      3.3.4. IT-Notfall- und Krisenplan – Ablageorte ... 7
      3.3.5. Krisenstabsraum / Lagezentrum ... 7
4. Vorgehen beim IT-Notfall und Krise ... 8
   4.1. Meldung ... 9
   4.2. Notfallerkennung / Triage ... 9
   4.3. IT-Sofortmassnahmen ... 10
   4.4. Notfallorganisation ... 10
   4.5. Krisenstab ... 11
   4.6. Notfallkommunikation und Meldepflichten ... 12
      4.6.1. Offizielle Kommunikation und Meldepflichten ... 12
      4.6.2. Interne Kommunikation ... 13
      4.6.3. Externe Kommunikation ... 13
   4.7. Lagebeurteilung und Handlungsvorgehen ... 14
   4.8. Debriefing – Post Incident Review ... 15
5. Informationen zum Dokument ... 15
   5.1. Änderungshistorie ... 15





Phase 3 – Vorfallbewältigung



4.4. Notfallorganisation

Die Notfallorganisation ist ab dem Moment des Ausrufes eines Notfalls autorisiert, primär und unverzüglich alle Handlungen zur Eindämmung und Beseitigung der Gefahren und zum Wiederanlauf und der Wiederherstellung des Normalbetriebes zu unternehmen. Weiter ist sie befugt, den Notfallbetrieb zu starten. Folgende Rollen sind dabei wichtig.

Vorname, Name	Rolle in Notfallorganisation	Verantwortlichkeit / Aufgaben	Erreichbarkeit
[VORNAME, NAME]	[ROLLE]	[AUFGABEN]	[KONTAKT DATEN]
Max Muster (inkl. Stv)	*IT-Verantwortliche-r (IT-SPOC)*	*Technische Sofortmassnahmen, IT-Notfallbetrieb, Wiederherstellung der Systeme …*	*+41 7X +41 2X Messaging-Apps*
Admin Muster (inkl. Stv)	*Gemeindeschreiber/-in*	*Führt die Ablaufdokumentation, Stellt die interne Koordination der Gemeinde sicher …*	*+41 7X +41 2X Messaging-Apps*
Extern Muster (inkl. Stv)	*Externe IT-Anbieter*	*Technische Sofortmassnahmen, Forensische Analysen, IT-Notfallbetrieb, Wiederherstellung der Systeme …*	*+41 7X +41 2X Messaging-Apps*

Tabelle 7: Rollen für die Notfallorganisation.



4.6.1. Offizielle Kommunikation und Meldepflichten

Folgende Stellen müssen gegebenenfalls kurz nach dem Erkennen des Vorfalls informiert werden:

- Die Polizei (Notruf 117); es kann geprüft werden, ob eine Anzeige erstattet werden soll.
- Das Bundesamt für Cybersicherheit (BACS) gemäss Informationssicherheitsgesetz (ISG): Sofern der Vorfall mindestens einer dieser folgenden Kriterien[8] erfüllt, muss dieser, am besten über den *Cyber Security Hub*[9], innert 24 Stunden gemeldet werden:
  a) die Funktionsfähigkeit der betroffenen kritischen Infrastruktur ist gefährdet;
  b) es zu einer Manipulation oder zu einem Abfluss von Informationen kam;
  c) die Kompromittierung über einen längeren Zeitraum unentdeckt blieb, insbesondere wenn Anzeichen dafür bestehen, dass der Angriff zur Vorbereitung weiterer Cyberangriffe ausgeführt wurde; oder
  d) der Vorfall mit Erpressung, Drohung oder Nötigung verbunden ist.
- Die [kantonale Datenschutz Behörde], wenn ein Datenabfluss von Personendaten nicht ausgeschlossen werden kann.

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*
…	…	…

Fazit – Schweizer Gemeinden müssen sich auf Cyberangriffe vorbereiten

- Es ist entscheidend, sich auf einen Cybervorfall vorzubereiten, um:
  - die **Wahrscheinlichkeit** des Auftretens eines Vorfalls zu verringern
  - die internen und externen Rollen und **Verantwortlichkeiten** im Falle eines Vorfalls zu klären
  - die **Auswirkungen** eines möglichen Vorfalls zu minimieren
  - die **Dauer** eines möglichen Vorfalls zu verkürzen
  - die wesentlichen **Aufgaben der Gemeinden** im Falle eines Vorfalls sicherzustellen



Fragen?

