## Immer einen Schritt voraus

# Proaktives Cybersecurity-Management

Ein proaktives Cybersecurity-Management schützt Daten und Prozesse und stärkt das Vertrauen von Kunden und Partnern.

→ **VON RETO ZBINDEN**

**DER AUTOR**

**Reto Zbinden,** Rechtsanwalt und CEO der Swiss Infosec AG, dem unabhängigen Beratungs- und Ausbildungsunternehmen für Goverance, Risk, Compliance und Security.
**www.infosec.ch**

Die rasante Digitalisierung steigert zwar die Effizienz und Wettbewerbsfähigkeit, führt aber auch zu neuen Risiken: Cyberangriffe und Datenschutzverletzungen bedrohen die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und Daten. Für KMU, die nicht über die Ressourcen grosser Konzerne verfügen, ist ein strukturiertes Cybersecurity Management überlebenswichtig.

### ZENTRALES ELEMENT: RISIKOMANAGEMENT

Ein zentrales Element des Cybersecurity Managements ist das Risikomanagement – also die systematische Identifikation, Bewertung und Priorisierung von Risiken. Eine Analyse der bestehenden IT- und Prozesslandschaften ist die Grundlage, um Schwachstellen frühzeitig zu erkennen. Hierbei werden Software- und Hardwarekomponenten, die Netzwerksicherheit, Lieferantenbeziehungen sowie menschliche und externe Einflussfaktoren überprüft und bewertet. Entscheidend ist, die relevanten Risiken für das eigene Unternehmen zu verstehen. Nur wer die Angriffsszenarien kennt und versteht, kann wirksame Schutzmassnahmen ableiten und seine Organisation nachhaltig schützen.

### MÖGLICHE BEDROHUNGEN…

Phishing-Angriffe in Form von manipulierten E-Mails, Anrufen oder Websites gehören zu den häufigsten Angriffsarten. Die Qualität der Angriffe wird durch den Einsatz von Künstlicher Intelligenz (KI) , Stichwort Deepfakes, weiter verbessert. Ransomware, also die Verschlüsselung geschäftskritischer Daten mit Lösegeldforderung, betrifft nicht nur grosse Organisationen. Gerade bei kleineren Unternehmen oder bei Gemeinden vermuten Cyberkriminelle mangelhafte Sicherheitsvorkehrungen, die sich einfach(er) umgehen lassen. Die Prävention wird schwierig, wenn Angreifer bislang unbekannte Sicherheitslücken (Zero-Day-Exploits) ausnutzen. Nicht alle Gefahren kommen von aussen: Insider-Bedrohungen entstehen durch aktuelle oder ehemalige Mitarbeitende, die unberechtigten Zugriff auf sensible Informationen und Daten haben.

### …UND WIRKUNSVOLLE MASSNAHMEN

Ein wirkungsvolles Cybersecurity Management basiert auf einem Zusammenspiel aus technischen, organisatorischen und personellen Massnahmen. Wenn alle Ebenen ineinandergreifen, wird ein widerstandsfähiges Sicherheitsniveau erreicht. Praxisnähe und Kontinuität sind bei der Umsetzung der Massnahmen entscheidend. Organisationen müssen klar definieren, wie lange geschäftskritische Prozesse im Ernstfall unterbrochen sein dürfen und innerhalb welcher Frist sie wieder anlaufen müssen.

## Checkliste Cybersecurity-Management

1. Risikobewertung und Priorisierung
2. Wiederherstellbarkeit kritischer Prozesse
3. Backup nach dem 3-2-1-0-Prinzip
4. Notfallpläne und Krisenübungen
5. Absicherung externer Zugänge
6. Sichere Konfiguration und Zugriffskontrolle
7. Regelmässige Audits und Tests
8. Anpassung an neue Bedrohungen
9. Sensibilisierung & Schulung der Mitarbeitenden
10. Nutzung bewährter Frameworks (ISO 27001, NIST)

Bild: zVg

Cybersicherheit ist ein integraler Bestandteil der Informationssicherheit und weit mehr als IT-Sicherheit.

Darauf aufbauend ist eine solide Backup-Strategie unverzichtbar. Bewährt hat sich das 3-2-1-0-Prinzip: drei Kopien wichtiger Daten, zwei unterschiedliche Speichermedien, mindestens ein Offline-Backup und null Fehler bei der Überprüfung. Diese Struktur garantiert, dass Daten auch im Fall von Ransomware, Systemausfällen oder Hardwaredefekten wiederherstellbar bleiben und der Geschäftsbetrieb schnell fortgesetzt werden kann.

## NOTFALLPLÄNE UND KONTROLLIERTE ZUGRIFFE

Klare Notfallpläne, definierte Rollen und regelmässige Übungen stellen sicher, dass im Krisenfall jeder weiss, was zu tun ist. Auch die Absicherung von Schnittstellen ist entscheidend: Externe Zugänge sollten auf das Nötigste reduziert und durch eine Mehrfaktorauthentifizierung geschützt werden. Eine sichere Konfiguration aller Endgeräte sowie eine konsequente Zugriffskontrolle bilden das Rückgrat jeder Sicherheitsarchitektur. Systeme sollten gehärtet, Standardkonfigurationen überprüft und administrative Privilegien nach dem «Least-Privilege-Prinzip» (Prinzip der minimalen Rechte) vergeben werden. Ergänzend prüfen Audits – intern wie extern – die Wirksamkeit aller Massnahmen.

## KONTINUIERLICHE WEITERENTWICKLUNG

Da sich Cyberbedrohungen laufend verändern, darf auch die Sicherheitsstrategie nicht statisch bleiben. Um auf neue Angriffsmuster frühzeitig reagieren zu können, muss sie kontinuierlich an neue Bedrohungen angepasst werden. Ebenso wichtig - leider oft vernachlässigt – ist die Sensibilisierung der Mitarbeitenden: Schulungen, Awareness-Programme und klare Richtlinien fördern eine Sicherheitskultur, die menschliche Fehler minimiert und das Bewusstsein für Risiken stärkt.

## ORIENTIERUNG AN FRAMEWORKS

Im Ernstfall können kompetente externe Partner entscheidende Unterstützung leisten. Für die strukturierte Umsetzung eines Cybersecurity Managements bieten bewährte internationale Frameworks wie ISO 27001 oder das NIST Cybersecurity Framework eine wertvolle Orientierung. Sie helfen, Risiken systematisch zu identifizieren, Schutzmassnahmen zielgerichtet umzusetzen und Informationssicherheit nachhaltig im Unternehmen zu verankern.

## IMMER EINEN SCHRITT VORAUS SEIN

Cybersicherheit ist kein Projekt mit Enddatum, sondern ein kontinuierlicher Prozess. Der Aufbau und Betrieb eines Cybersecurity ist eine strategische Notwendigkeit. Wer proaktiv handelt, reduziert Risiken, stärkt das Vertrauen in seine Organisation – und ist im entscheidenden Moment immer einen Schritt voraus. ←

**Den vollständigen Artikel finden Sie online.**


## IMPRESSUM

**Das offizielle Publikationsorgan des VIW**

**Herausgeber**:
VIW – Wirtschaftsinformatik Schweiz
→ www.viw.ch

**Podcasts, Videos & mehr:**
→ https://my.viw.ch

**VIW in den sozialen Netzwerken:**