
WHITEPAPER

# CYBER RESILIENCE LEITFADEN FÜR DAS TOP MANAGEMENT

Was Sie im Verwaltungsrat und in der Geschäftsleitung vor, bei und nach einem Sicherheitsvorfall zwingend unternehmen müssen.

InfoGuard
SWISS CYBER SECURITY

Executive Summary

# Cyberrisiken als grösste Gefahr für Unternehmen – was tun?

Unternehmen in der Schweiz stehen verstärkt im Fokus von Cyberkriminellen. Die Meldungen in der Presse überschlagen sich. Oftmals erleiden Firmen drastische Schäden durch Cyberattacken wie Ransomware, Phishing oder DDoS. Ganze Netzwerke und zugehörige Systeme werden kompromittiert, Daten entwendet sowie Firmen lahmgelegt und erpresst. Nicht selten sind ganze Existenzen gefährdet. **Die Anzahl Cyberattacken nehmen dramatisch zu, die Schadenssummen sind immens.** Tendenz steigend. Besonders erschreckend ist die Tatsache, dass die Unternehmensgrösse dabei keine Rolle spielt.

Cyber Security ist ein enorm wichtiges Thema für den Geschäftserfolg einer Firma. Führende Risiko-Studien zeigen, dass CEOs und das Top Management Cyberrisiken als die grösste Gefahr für Unternehmen erachten. Die Gründe liegen u.a. in der fortschreitenden Digitalisierung und Vernetzung – Stichwort Homeoffice, IoT/IIoT, Remote Access und Cloud –, in der stark zunehmenden Cyberkriminalität («Cybercrime-as-a-service») und in den steigenden Compliance-Vorgaben.

Und genau deshalb gehört Cyber Resilience – sprich die Verschmelzung von Cyber Security, Risikomanagement, Geschäftskontinuität und Resilienz-Praktiken, die die Fähigkeit eines Unternehmens fördern, einem Cyberangriff standzuhalten und sich davon wieder zu erholen – auf Ihre Traktandenliste. Als VR eines renommierten Unternehmens kommt Ihnen eine entscheidende Rolle zu: Gemäss Schweizer Obligationenrecht ist jeder Verwaltungsrat dazu verpflichtet, ein integrales Risikomanagement auszugestalten, es zu implementieren und zu überwachen. Nun die Frage an Sie:

**Wie effektiv ist die Cyber-Resilience-Strategie in Ihrem Unternehmen und welche Rolle nehmen Sie als VR ein?**

Dieser eigens für VR und GL konzipierte Leitfaden samt Checkliste zeigt auf, wie es um Ihre Cyber Resilience steht und wie Sie die Widerstandsfähigkeit gegen Cyberrisiken in Ihren Unternehmen erhöhen. Zudem beinhaltet er einen 7-Punkte-Plan für den Notfall und verdeutlicht, was Sie bei respektive nach einem Sicherheitsvorfall unternehmen müssen. **Wir wünschen eine erfolgreiche Umsetzung und stehen Ihnen gerne mit Rat und Tat zur Seite.**

**Thomas Meier**
CEO & VR-Delegierter

**Peter Letter**
VR-Präsident

# Inhalt

# 01 | Die 12 elementaren Fragen für den Verwaltungsrat

Das Verständnis vom Verwaltungsrat für die Cyberbedrohung und die Mitwirkung an der Ermittlung der Reaktion sind sowohl im Hinblick auf die Rolle des Verwaltungsrates als Unternehmensstratege, als auch auf seine Aufsichtsfunktion von entscheidender Bedeutung.

**Aus unserer Sicht sollten Sie als VR deshalb Klarheit über die folgenden Themen erlangen:**

1. Welches sind die neuen Cyberbedrohungen und –risiken und inwiefern betreffen diese unser Unternehmen?
2. Genügt unser Cyber-Resilience-Programm den stetig wachsenden Herausforderungen, die sich aus der heutigen und zukünftigen Cyber-Bedrohungslage ergeben?
3. Ist unser Unternehmen genügend vorbereitet, um einen Angriff zu erkennen und darauf angemessen reagieren zu können?
4. Haben wir einen Prozess für die Datensicherung implementiert, um sicherzustellen, dass regelmässig Backups erstellt und diese auch offline aufbewahrt werden? Wenn ja, werden diese auch regelmässig auf die Wirksamkeit (Wiederherstellbarkeit) geprüft?
5. Verfügen wir über einen externen kompetenten Partner, der uns im Bedarfsfall umgehend und umfassend mit Expertise und Ressourcen (24/7) zur Seite steht? Und haben wir die Zusammenarbeit vorsorglich geklärt?
6. Verstehen wir unsere heutigen Schwachstellen – auch in Bezug auf unsere Lieferanten und Dienstleister – und welche Prozesse haben wir implementiert, um die identifizierten Cyberrisiken zu adressieren?
7. Hält unser Unternehmen die gesetzlichen und regulatorischen Verpflichtungen zum Schutz von Daten ein, beispielsweise hinsichtlich dem Datenschutz? Liegt eine ausreichende Dokumentation vor?
8. Welche Indikatoren von Schlüsselrisiken und Leistungskennzahlen müssen wir auf VR-Ebene beobachten, um unsere Aufsichtsfunktion erfolgreich wahrnehmen zu können?
9. Ist Cyber-Resilienz (Widerstandsfähigkeit des Unternehmens im Hinblick auf Cyberattacken) Teil unserer strategischen Besprechungen im VR? Wenn ja, wann haben wir uns das letzte Mal mit der Cyberbedrohung befasst?
10. Welche Aufgaben müssen wir im Verwaltungsrat selber ausführen und welche Aufgaben können delegiert werden?
11. Wie entwickeln wir unser Unternehmen von einer reaktiven zu einer aktiven, antizipierenden Herangehensweise in Bezug auf die Cyberbedrohung?
12. Sind wir unseren wichtigsten Mitbewerbern voraus? Falls ja, wie können wir dies als Wettbewerbsvorteil nutzen?

**Hand aufs Herz:** Konnten Sie eine grosse Mehrheit der Fragen mit einem überzeugenden «Ja» beantworten? Oder sind einzelne Punkte für Ihr Unternehmen noch eine Art Blackbox? So oder so, dieser Leitfaden unterstützt Sie einerseits aktiv in Ihrem Anliegen, ein hohes Level an Cyber Resilience in Ihrem Unternehmen zu erreichen. Andererseits dient er – auch dank der Checkliste – als konkrete Hilfestellung, was es für Sie vor, bei und nach einem Sicherheitsvorfall zwingend zu tun gilt. Doch erst der Reihe nach:

# 02 | **Cyber Resilience als Aufgabe des Verwaltungsrates**

Cyberrisiken klettern nicht zuletzt dank den zahlreichen Vorfällen und Medien-Berichterstattungen in jüngster Vergangenheit auf der Traktandenliste vieler Verwaltungsratssitzungen nach oben. Wir sagen: Absolut zu Recht. Der Grund ist schnell erläutert. Die Auswirkungen bei den betroffenen Unternehmen sind schwerwiegend, nicht selten stehen Existenzen auf dem Spiel oder das Resultat solcher Attacken gipfelte in Konkursen. Nebst grossen Unternehmen trifft es in der Schweiz aktuell immer öfters auch KMU. Aus einem Cyberangriff können schnell massive Schäden resultieren. Nur um einige (gravierende) zu nennen:

- **Verlust von Kundenvertrauen und Reputation**
- **Umsatzeinbussen**
- **Folgekosten für Ersatz und Wiederherstellung**
- **Rechtskosten und Bussen**
- **Haftung, Schadenersatz, Kompensationszahlungen für Verspätungen**
- **Zeitverlust, verspäteter Markteintritt**
- **Konkurs**

Es versteht sich von selbst, dass es nicht Ihre Aufgabe ist, im Detail mit den neuesten Technologien vertraut zu sein und operative Massnahmen vorzugeben oder diese zu überprüfen. Vielmehr geht es darum, dass Sie – auch mithilfe dieses Leitfadens – in der Lage sind, von Ihren IT- und Sicherheitsverantwortlichen durch gezielte Fragen die Informationen zu erhalten, anhand derer Sie beurteilen können, wie widerstandsfähig und effektiv Ihr Unternehmen gegen Cyberbedrohungen ist. Oder wo Sie gegebenenfalls intervenieren und reagieren müssen.

Cyber Resilience bedeutet auch eine strategische Chance für Ihr Unternehmen! Nutzen Sie diese, um sich von Ihren Mitbewerbern abzuheben und zu differenzieren. Verantwortungsbewusstes Management von Cyberrisiken oder ein gut gemanagter Cybervorfall können das Vertrauen der Stakeholder eines Unternehmens stärken – seien dies Kunden, Investoren, Lieferanten oder Aufsichtsbehörden. Dabei reicht es nicht aus, sich alleine auf die Abwehr zu konzentrieren. Entscheidend ist die Widerstandsfähigkeit gesamthaft zu stärken und Angriffe schnell zu erkennen und noch schneller zu reagieren. Damit dies alles gelingt, empfiehlt es sich frühzeitig einen geeigneten, professionellen und kompetenten Partner zu evaluieren und an Board zu holen. Klären Sie die Zusammenarbeit vorsorglich.

### Die drei Erfolgsfaktoren

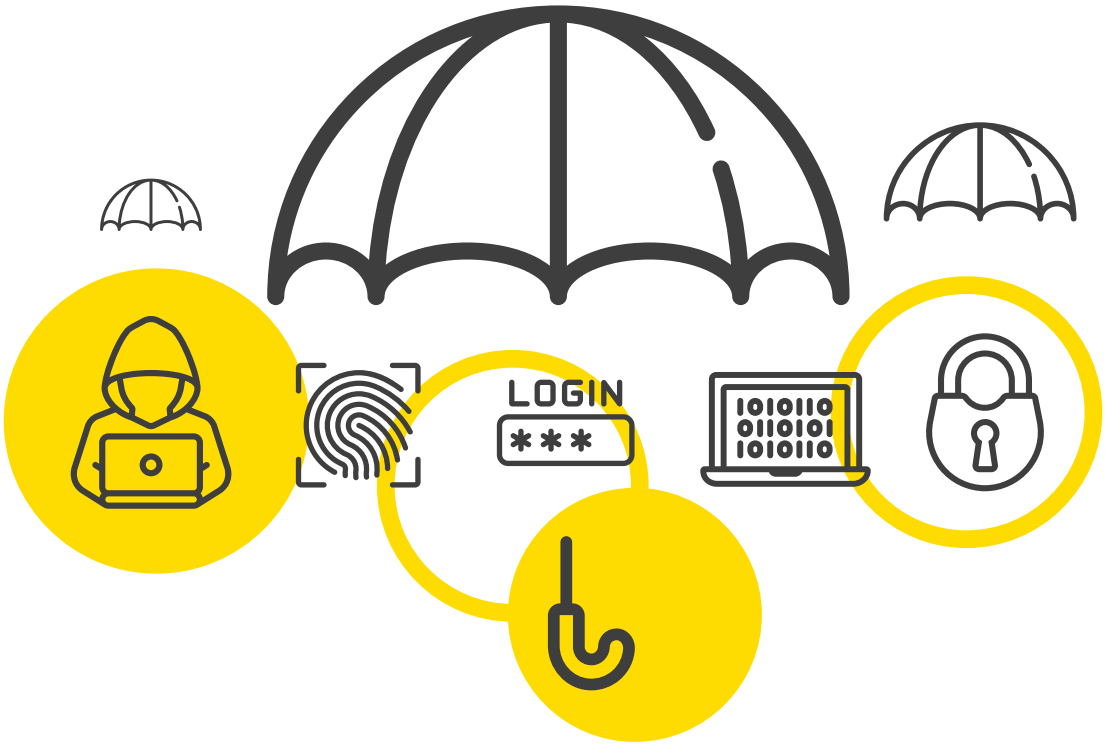
- ✓ Nehmen Sie Cyber Resilience auf oberster Unternehmensebene wahr.
- ✓ Beziehen Sie Cyber Resilience in die unternehmensweite Risikobetrachtung ein.
- ✓ Bauen Sie geeignete Cyber-Resilience-Massnahmen auf und kontrollieren Sie die Umsetzung.

## 02.1 | **Nehmen Sie Cyber Resilience auf oberster Unternehmensebene wahr**

Sie sind sich ganz bestimmt bewusst, dass Sie im Verwaltungsrat die Verantwortung für die Identifikation, Einschätzung, Steuerung und Überwachung von Cyberrisiken und der entsprechenden Widerstandsfähigkeit tragen. Dabei können Sie die Handlungsverantwortung selber übernehmen oder diese an ein bereits bestehendes Gremium (z.B. Prüfungs- oder Risikoausschuss) oder an ein spezifisches Cyber-Resilience-Expertenteam delegieren. Die Führungsverantwortung dagegen kann nicht delegiert werden. Aus Erfahrung empfehlen wir Ihnen den Umfang und die Zuständigkeiten sowie die Art und Weise, in der diese Zuständigkeiten wahrgenommen werden sollten, schriftlich festzulegen. Einschliesslich der Struktur und Prozesse zur Überprüfung der Cyber Resilience.

## 02.2 | **Beziehen Sie Cyber Resilience in die unternehmensweite Risikobetrachtung ein**

Als VR obliegt es in Ihrer Verantwortung sicherzustellen, dass das Management die Cyber Resilience und Cyber-Risikobewertung in die allgemeine Geschäftsstrategie und das unternehmensweite Risikomanagement sowie die Budgetierung und Ressourcenallokation integriert hat. Ebenso ist es von zentraler Bedeutung, dass Sie regelmässig über aktuelle Bedrohungen und Trends informiert werden und dies auch dokumentiert wird. Ziehen Sie dazu bei Bedarf unabhängige externe und ausgewiesene Experten bei.
Auf uns können Sie zählen. Wir von der InfoGuard unterstützen Sie dabei sehr gerne!



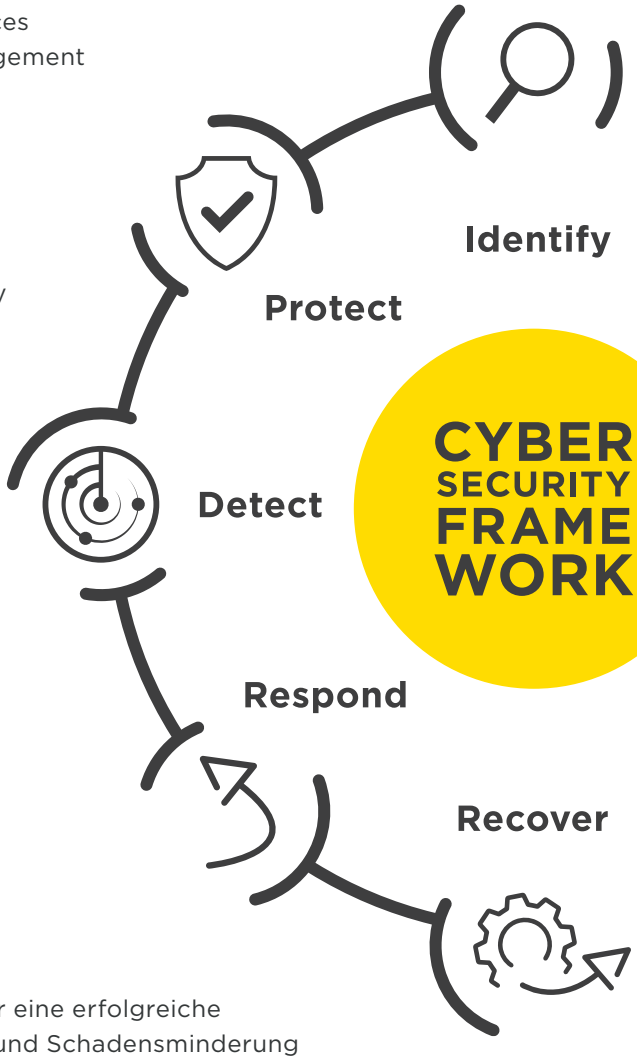
# 02.3 | **Bauen Sie geeignete Cyber-Resilience-Massnahmen auf und kontrollieren Sie die Umsetzung**

## Identify / Identifizieren

- Betreiben eines angemessenen Risikomanagements und Identifizierung von Sicherheitsrisiken
- Zuweisen von Aufgaben, Kompetenzen und Verantwortlichkeiten
- Kennen der unternehmenskritischen Daten und Geschäftsprozesse
- Inventarisieren der IT-Systeme und Software (auch Internet der Dinge, IoT) mit den entsprechenden Abhängigkeiten zu Ihren Business-Services
- Vendor Management: Lieferketten Überwachung & Management sowie Managed Services & Outsourcing

## Protect / Schützen

- Sensibilisierung der Mitarbeitenden
- Aufbau eines Sicherheits-Frameworks nach anerkannten Standards, beispielsweise ISO-27001, NIST Cyber Security Framework, IKT-Minimalstandard
- Identitäts- und Zugriffsmanagement, inklusive Monitoring
- Implementation von angemessenen Sicherheits- und Abwehrmassnahmen, professioneller Betrieb und Cyber-Security-Architektur (auch bei der Zusammenarbeit mit Dritten)
- Regelmässiges Patch- & Schwachstellen-Management aller IT-Systeme




## Detect / Erkennen

- Security Überwachung / Monitoring zur Erkennung von Angriffsspuren, Lateral-Movement und typischen Vorgehensweisen anhand der Cyber-Killchain
- Segmentierung und Überwachung der Netzwerke
- Periodische/kontinuierliche technische Sicherheitstests, auch in der Software- und Produktentwicklung

## Respond / Reagieren

- Entwicklung und Testen/Üben der Vorfall-Notfallpläne für eine erfolgreiche Reaktionsplanung, Kommunikation, Analyse der Vorfälle und Schadensminderung
- Implementierung eines kontinuierlichen Verbesserungsprozesses zur Optimierung der Cyber Resilience

## Recover / Wiederherstellen

- Entwicklung und Testen/Üben der Cyber-Notfall-Wiederherstellungsplanung inkl. Kommunikation, Nachbearbeitung zur kontinuierlichen Verbesserung der eigenen Cyber Resilience
- Regelmässige offline Sicherungen / Backups von Systemen, durchgeführt, bewirtschaftet und getestet (inklusive Rückspielbarkeit der Backups)

Die Geschäftsleitung steuert dabei die Umsetzung von Massnahmen (Definition, Implementierung, Prüfung und kontinuierliche Verbesserung der Massnahmen und Prozesse) zur Verbesserung der Cyber Resilience und schaut, dass diese im gesamten Unternehmen aufeinander abgestimmt sind.

# 02.4 | **Checkliste zur Einschätzung Ihrer Cyber Resilience**

Wir haben für Sie eine Checkliste erarbeitet, die es Ihnen als VR ermöglichen soll eine realistische Selbsteinschätzung bezüglich der Cyber Resilience in Ihrem Unternehmen vorzunehmen.

**Die nachfolgenden Fragen sollten Sie im Verwaltungsrat für Ihr Unternehmen mit gutem Gewissen mit «Ja» beantworten können.**

- ✓ Werden Sie regelmässig über Themen der Cyber Resilience informiert und können Sie die Auswirkungen auf das eigene Unternehmen abschätzen?
- ✓ Besteht ein dokumentiertes Datenschutz- und Cybersicherheitsprogramm, das aus angemessenen und geeigneten Richtlinien und Verfahren besteht? Versteht und befolgt die gesamte Belegschaft diese Richtlinie?
- ✓ Haben Sie die Handlungsverantwortung festgelegt und wer trägt diese?
- ✓ Sind Ihre wichtigsten Informationswerte identifiziert und die Anfälligkeit für Cyberangriffe gründlich bewertet?
- ✓ Werden regelmässig unabhängige Bewertungen / Audits Ihrer Cyber Resilience durchgeführt und werden Ihnen die relevanten Ergebnisse – also jene mit hoher Priorität – kommuniziert?
- ✓ Haben Sie eine Risikobewertung für die Cybersicherheit durchgeführt?
- ✓ Kennen Sie Ihre aktuelle Risikolage, Schwachstellen und die Auswirkungen auf Ihre Cyber Resilience?
- ✓ Wird Ihre Cyber-Resilience-Strategie periodisch überprüft, einschliesslich der Frage, ob die wichtigsten Cybersicherheitsrisiken angemessen bewertet, priorisiert und minimiert wurden?
- ✓ Werden die Auswirkungen des Cyberrisikos auf das Geschäft, wie z.B. Geschäftsunterbrechungen, Auswirkungen auf die Qualität von Produkten/Dienstleistungen, Reputation etc., hinreichend berücksichtigt?
- ✓ Evaluieren Sie die Auswirkungen auf das Cyberrisiko im Vorfeld von neuen Geschäftsvorhaben (z.B. Fusionen, Übernahmen und Joint Ventures) oder auch neuen Produkten oder Technologien?
- ✓ Verfügen Sie über grundlegende Cyber-Resilience-Vorgaben, einschliesslich Business Continuity und Disaster Recovery, Incident Response sowie für die kontinuierliche Verbesserung und Kommunikation?
- ✓ Setzen Sie bewährte Sicherheitsmechanismen zur Abwehr und Monitoring-Systeme zur frühzeitigen Erkennung von Cyberangriffen ein?
- ✓ Haben Sie im Falle eines Cybervorfalls einen Notfallplan? Wird der Notfallplan regelmässig geübt? Und sind Backups und Offline-Backups der relevanten Assets zeitnah verfügbar?
- ✓ Verfügen Sie über Experten zur Optimierung der Cyber Resilience (Identifizieren, Schützen, Erkennen, Reagieren, Wiederherstellen von Cyberattacken)? Haben Sie Verfahren etabliert, um im Bedarfsfall auf externe Experten zurückgreifen zu können?
- ✓ Werden zur kontinuierlichen Verbesserung der Cyber Resilience KPIs verwendet und rapportiert (z.B. Reaktionszeiten auf Sicherheitsereignisse, Reaktionszeiten auf Schwachstellen)?

# 03 | **Erste Hilfe bei einem Sicherheitsvorfall**

Angesichts der heutigen Lage wäre die Annahme als fahrlässig zu bezeichnen, dass ausgerechnet Ihr Unternehmen für Hackerangriffe uninteressant sei. **Heute gilt der Grundsatz: Es ist nicht die Frage ob, sondern wann Ihr Unternehmen Ziel einer erfolgreichen Cyberattacke sein wird.** Dessen sind Sie sich bestimmt bewusst und gerade deshalb ist es existenziell wichtig, dass Sie entsprechendeVorkehrungsmassnahmen zur Bewahrung der Cybersicherheit getroffen haben.

Von zentraler Bedeutung ist die Erkennung, Analyse und Reaktion auf Cyberangriffe – und zwar rund um die Uhr. Ein CSIRT (Computer Security Incident Response Team) aus einem professionellen Cyber Defence Center (CDC) hilft Ihnen dabei, die Dauer eines Sicherheitsvorfalls und den dadurch verursachten Schaden zu minimieren sowie den Business Impact drastisch zu reduzieren.

Hierbei ist die Erstellung eines Incident-Response-Plans eine der wichtigsten Aufgaben, um ein effektives Incident Management aufzubauen. In einem Vorfallreaktionsplan wird dokumentiert, wer, wie, welche Massnahmen beim Eintreten eines Sicherheitsvorfalls ergreift. Ausserdem werden darin die notwendigen Abläufe, Richtlinien, Rollen, Verantwortlichkeiten und nicht zuletzt auch Kommunikations- und Eskalationswege definiert.

Als VR müssen Sie dafür sorgen, dass ein solcher Prozess aufgebaut, dokumentiert und auch entsprechend geübt wird. **Die Erkenntnisse daraus müssen im Sinne einer kontinuierlichen Optimierung natürlich auch wieder zurückfliessen.**

Bei der Bewältigung einer solchen Situation braucht auch Ihr Unternehmen den sofortigen Zugriff auf Spezialisten. Denn nebst technischen Hürden gilt es, auch die Kunden, Geschäftspartner und nicht zuletzt die Mitarbeitenden sowie eventuell die Öffentlichkeit zu informieren.

Sie gewinnen wertvolle Zeit, wenn Sie auf Ihren bewährten Partner setzen können – und nicht erst noch einen geeigneten Partner evaluieren sowie die vertraglichen Details für die Unterstützung bei der Bewältigung eines Cyberangriffs klären müssen. Mit Hilfe eines CSIRT (Computer Security Incident Response Team) – wie beispielsweise von InfoGuard – lassen sich die Dauer eines Sicherheitsvorfalls und der dadurch verursachte Schaden minimieren. Denn wir bei InfoGuard legen grossen Wert auf den schnellen Wiederaufbau und die schnelle Wiederherstellung der Produktions-, respektive Geschäftsfähigkeit der betroffenen Unternehmen.

# 03.1 | **7-Punkte-Plan für den Notfall**

Ein Sicherheitsvorfall kann jederzeit und bei jedem Unternehmen auftreten. Unabhängig von der Grösse oder Branche. Meist trifft es die Verantwortlichen ganz unvermittelt und nicht selten sind diese mit der Situation überfordert – was unser CSIRT fast täglich erfährt.

**Aus diesem Grund haben wir für Verwaltungsrät*innen wie Sie einen 7-Punkte-Plan erarbeitet:**

**1. Richten Sie einen Krisenstab ein.**
Binden Sie frühzeitig relevante interne Stellen ein, zum Beispiel in Form eines Krisenstabes.

**2. Planen Sie regelmässige Sitzungen.**
Planen Sie regelmässige Beratungsphasen des Krisenstabes im Wechsel mit Arbeitsphasen. Empfohlene Traktanden sind beispielsweise die Situationsanalyse und Faktensammlung, Sofortmassnahmen, Risiken-Chancen-Analyse, Handlungsoptionen, Entscheidung, Timing, Verantwortlichkeiten sowie die Überprüfung der Zielerreichung.

**3. Kommunizieren Sie regelmässig.**
Die interne und externe Kommunikation ist eines der wichtigsten Tools für die nach aussen sichtbare Bewältigung des Vorfalls und gleichzeitig eine der grössten Herausforderungen. Unsere Empfehlung an Sie:

- Überlassen Sie die Kommunikation den Spezialisten!
- Identifizieren Sie die Stakeholder und stimmen Sie die Sprachregelung ab!
- Befolgen Sie den Grundsatz: Interne Kommunikation vor externer Kommunikation!
- Zentralisieren Sie den Informationsfluss und nutzen Sie FAQs!
- Seien Sie sich bewusst: Für «blame, name, shame» und «bashing» ist in der Krise kein Platz!
- Sagen Sie öffentlich sowie gegenüber Ihren Mitarbeitenden jederzeit die Wahrheit!

**4. Denken Sie an Meldepflichten.**
Bei Datenschutz-Verstössen ist die Meldeverpflichtung gegenüber der Aufsichtsbehörde zwingend zu beachten. Eine Meldung hat i.d.R. innerhalb von 72 Stunden zu erfolgen. Informieren Sie zudem frühzeitig Ihre Cyber-Versicherung. Und ziehen Sie spezialisierte Rechtsanwälte bei.

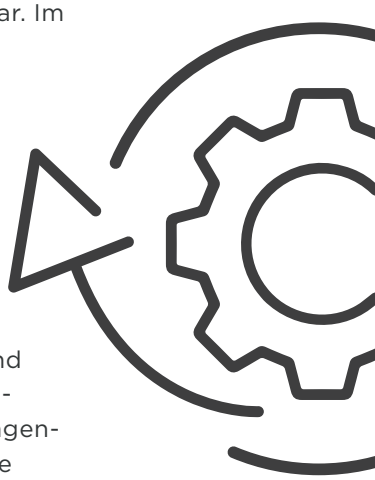
**5. Holen Sie sich frühzeitig externe Unterstützung.**
Oft besitzen betroffene Unternehmen nicht genug interne Expertise oder Ressourcen für die erfolgreiche Bewältigung von solchen Sicherheitsvorfällen. Externe Spezialisten unterstützen Sie auch in juristischen Fragen und bei der Verhandlung mit den Angreifern. Sehr oft kann die Höhe des Lösegelds massiv reduziert werden (sollte dies nötig sein).

**6. Stellen Sie Ihre Handlungsfähigkeit wieder her.**
Es ist unerlässlich, dass Sie regelmässig Backups erstellen und diese auch offline aufbewahren. Dies kann im Falle eines Ransomware-Angriffs den Fortbestand des Unternehmens sichern. Kurzfristig können sich für den Notbetrieb wichtige Daten allenfalls auch an abgesetzten Aussenstellen oder auf Systemen von Mitarbeitenden im Urlaub befinden, welche (noch) nicht betroffen sind.

**7. Vergessen Sie die Nachbearbeitung nicht.**
Denken Sie an eine professionelle Nachbesprechung zur Auswertung und Optimierung. Definieren Sie allfällige langfristigen Sicherheitsmassnahmen und planen Sie eine Revision Ihrer IT durch externe Experten, sobald diese Massnahmen umgesetzt sind. Last but not least: Danken Sie Ihren Vertragspartnern und Kunden für das Verständnis, die Geduld und die Unterstützung. Planen Sie mit etwas Abstand ein «Dankeschön» für alle beteiligten Mitarbeitenden.

# 03.2 | **Rückkehr aus dem Not- in den Normalbetrieb**

Für jedes Unternehmen ist es von entscheidender Bedeutung, einen Prozess für Backup und Recovery zu implementieren. Dieser ist ein wesentlicher Bestandteil der Disaster-Recovery-Strategie eines Unternehmens, denn Ihre Daten sind zu wertvoll und geschäftskritisch. Dabei geht es nicht nur um Prozesse, Technologien und Verfahren zur Erstellung regelmässiger Kopien von Daten und Anwendungen auf ein separates, sekundäres Gerät. Sondern auch um die Wiederherstellung selbiger im Falle eines Datenverlustes/-beschädigung sowie der für die Datenverarbeitung nötigen IT-Umgebung der darauf basierenden Geschäftsabläufe, von denen Sie abhängig sind. In der heutigen diversifizierten und vielschichtigen IT-Umgebung stellt dies eine grosse Herausforderung dar. Im Grossen und Ganzen gibt es drei Dinge, die Sie tun respektive veranlassen müssen:



1. **Planen: Erstellen eines Plans als Grundlage: WAS, WANN** (Wiederherstellungspunkt-Ziele (RPO), Wiederherstellungszeit-Ziele (RTO) und Service Level Agreements (SLAs)), WER.
2. **(Schnelles) Wiederherstellen der Systeme und Daten.**
3. **Testen des Plans sowie kontinuierliche Verbesserung.**

Erfahrungsgemäss nimmt die Rückkehr zum Normalbetrieb nach einem Incident beträchtliche Zeit in Anspruch. Im Voraus gezielt die Zuordnung von Ressourcen und Aktivitäten auf die verfügbare Zeit zu planen, erlaubt eine raschmöglichste und zielgerichtete Wiederherstellung gemäss definierter Prioritäten, Reihenfolgen und Mengengerüste. Besonderes Gewicht sollten Sie darauflegen, die Aktivitäten in dieser Phase genauestens zu überwachen und zu protokollieren, um improvisiertes und unkoordiniertes Handeln der Beteiligten möglichst zu verhindern. Diese aus der Planung und Tests gewonnenen Erkenntnisse und Informationen ermöglichen Ihnen eine Optimierung der Recovery-Phase hinsichtlich Effektivität und Effizienz.

Es empfiehlt sich insbesondere auch in dieser Phase auf die Unterstützung eines externen Partners zu vertrauen. Diese Expertise hilft Ihnen zu einer effizienten, sicheren und erfolgreichen Rückkehr aus dem Not- in den Normalbetrieb, ohne dass Checklisten, Massnahmenpläne usw. gänzlich neu erfunden werden müssen. Vergessen Sie dabei die Kommunikation mit Ihren internen und externen Stakeholdern nicht. Sorgen Sie dafür, dass regelmässig und transparent kommuniziert wird, so dass Zweifel, Gerüchte und Entscheidungsunsicherheiten gar nicht erst aufkommen und die Entscheidungs- und Eskalationskompetenz unbestritten bleibt.

« **Zur erfolgreichen Bewältigung eines Sicherheitsvorfalls brauchen Sie schnelle und professionelle Unterstützung durch Experten**, die Ihnen mit Ressourcen und Expertise tatkräftig zur Seite stehen. Dank der Unterstützung von InfoGuard waren wir schnell wieder handlungsfähig. Ich kann das Schweizer Cyber-Security-Unternehmen bestens empfehlen. »

**DR. STEPHAN WARTMANN,**
CEO der BRUGG GROUP AG

# 04 | Cyber Security ist unsere Leidenschaft

InfoGuard ist der Schweizer Experte für umfassende Cyber Security. Unsere über 230+ Sicherheitsspezialisten in Zug und Bern sorgen täglich für die Informationssicherheit bei über 400 Kunden in der Schweiz, Deutschland und Österreich. Wir bieten Ihnen ein ganzheitliches Lösungsangebot für die Umsetzung und Stärkung Ihrer Cyber Resilience.

Cyber Security ist eine Herausforderung – und unsere Leidenschaft. Tagtäglich setzen wir uns dafür ein, die Welt digital sicherer zu machen. Mit unserer 360°-Expertise sowie innovativen Services und Lösungen definieren wir den Benchmark. An vier Standorten sorgen über 230 Sicherheitsexpert*innen dafür, dass unsere Kunden in der Schweiz, Deutschland und Österreich rund um die Uhr umfassend geschützt sind. Langjährige Erfahrung, ein breites Lösungsportfolio, anerkannte Zertifizierungen und Attestierungen sowie qualifizierte Mitarbeitende bilden die Grundpfeiler, die ein Höchstmass an Sicherheit, Professionalität und Verlässlichkeit bieten. Dank unserer Unabhängigkeit als eigenständiges Unternehmen können wir zudem schnell und flexibel auf Veränderungen der Kundenbedürfnisse reagieren.

Unsere Vision, die Welt Tag für Tag digital sicherer zu machen, bildet das Fundament unseres Tuns und motiviert uns, alles zu geben, damit unsere Kunden geschützt sind. Dabei stehen wir für die Werte Leidenschaft, Vertrauen, Kundenzufriedenheit, Expertise und Innovation, die unsere Arbeit prägen und uns immer wieder zu Höchstleistungen anspornen.

**2001**
**Erfahrung und Expertise seit über 20 Jahren**

**100%**
**eigenständig**

**230+**
**Sicherheits-expert*innen**

**4**
**Standorte in der Schweiz, Deutschland und Österreich**

**24/7**
**Echtzeit-überwachung und Notfall-intervention**

**ISO 27001**
**ISO 14001**
**ISAE 3000** Typ 2

**Swiss CDC Cyber Defence Center**

**CSIRT Computer Security Incident Response Team**
**FIRST-Mitglied und BSI-qualifizierter APT-Response-Dienstleister**

# 05 | Cyber Security Made in Switzerland

In der heutigen digitalen Welt ist Cyber-Sicherheit von entscheidender Bedeutung. InfoGuard steht für verlässliche, innovative Services und Lösungen, die Ihre Sicherheit und Ihr Vertrauen schützen. Unsere 360°-Expertise reicht von Cyber Defence Services und Incident Response Services über Managed Security & Network Solutions bis hin zu Penetration Testing & Red Teaming sowie Security Consulting Services. Durch die Bereitstellung in der Cloud, hybrid und on-premise ermöglichen wir Flexibilität, die Ihren individuellen Anforderungen gerecht wird. Mit unserem ganzheitlichen Ansatz, hochspezialisierten Mitarbeitenden, effizienten Prozessen und modernsten Technologien sorgen wir dafür, dass Sie heute und in Zukunft in der komplexen digitalen Welt sicher sind.

## Cyber Defence

In der dynamischen, sich ständig verändernden Welt der Cyber-Bedrohungen ist es entscheidend, potenzielle Angriffe schnell zu identifizieren und zu bekämpfen – und zwar 24/7. Sämtliche Services werden aus dem ISO 27001-zertifizierten Cyber Defence Center (CDC) in der Schweiz erbracht.

## Cloud Security

Umfassende Sicherheit und Expertise in der Cloud – von der Strategie, Architektur und Transition über die professionelle Umsetzung und den sicheren Betrieb bis hin zur kontinuierlichen Optimierung und dem reibungslosen Off-Boarding.

## Incident Response (IR)

Erfolgreiche Cyber-Angriffe können nie vollständig ausgeschlossen werden. Unser Computer Security Incident Response Team (CSIRT) ist im Ernstfall umgehend zur Stelle, um die Angreifer zu stoppen und den Schaden möglichst gering zu halten. Wir stehen Unternehmen in jeder Phase zur Seite und sorgen dafür, dass sie schnellstmöglich wieder handlungsfähig sind.

## Security Consulting

Professionelle Sicherheitsberatung ist unverzichtbar, um den vielfältigen Anforderungen gerecht zu werden und die individuellen Ziele zu erreichen – sei es im Bereich Strategie, Governance, Risk und Compliance, Architektur und Design, Security Assessments oder bei der Förderung einer sicherheitsbewussten Unternehmenskultur.

## Managed Security & Network

Cyber-Sicherheit gelingt nur mit einem stabilen, zuverlässigen Fundament. Dazu entwickeln wir IT-Sicherheitsarchitekturen, die auf modernsten Netzwerk- und Sicherheitslösungen basieren. Durch umfassende Professional Services sowie 24/7 Managed Services gewährleisten wir zudem den kontinuierlichen Schutz digitaler Infrastrukturen und die zuverlässige Verfügbarkeit.

## Penetration Testing & Red Teaming

Effektive Cyber-Sicherheit erfordert ein tiefes Verständnis der Methoden und Taktiken von Cyber-Kriminellen. Mit unserer Expertise im Bereich Penetration Testing & Red Teaming identifizieren wir nicht nur Schwachstellen, sondern entwickeln auch Tools und Verfahren, um diese zu erkennen, noch bevor potenzielle Angreifer sie ausnutzen können.

# 06 | **Fazit**

Cyberrisiken gehören zu den bedeutendsten operationellen Risiken eines Unternehmens. Die Aufgabe des Verwaltungsrates und der Geschäftsleitung ist es, ein effektives Risikomanagement-Konzept zu implementieren. Dabei ist zwingend zu empfehlen, die Cyberstrategie auf Resilienz auszurichten.

Die letzten Monate haben klar gezeigt, dass die Quantität und insbesondere auch die Qualität der Angriffe markant zugenommen haben. Auch die Gefahren werden immer komplexer und vielfältiger. So stellen wir aktuell beispielsweise sehr viele Cloud Kompromittierungen fest: Cybervorfälle im Azure Umfeld, primär im Bereich der sogenannten Business E-Mail Compromise – besser bekannt unter dem Namen «CEO Fraud». Untersuchungen zeigen, dass viele IT-Administratoren mit der Komplexität der MS Cloud Lösungen nicht umgehen können und überfordert sind. Auch im Bereich «Mergers & Acquisitions» – bei Fusionen, Unternehmenskäufen, Übernahmen und Akquisitionen – ist die Gefahr grösser denn je. Nicht selten sind die neu erworbenen Unternehmen ohne deren Wissen bereits gehackt worden und stellen so ein sehr grosses Sicherheitsrisiko dar.

Sie sehen: Die Cyber-Risiko-Landschaft ist sehr komplex und anspruchsvoll. Cybersicherheit gehört zu den unternehmerischen Schlüsselthemen und ist aus vielen Gründen strategisch relevant. Nicht zuletzt, weil Sicherheitsrisiken in der IT ein geschäftskritisches Ausmass annehmen können, gehört Cyber Resilience ohne Wenn und Aber auf die Traktandenliste von Verwaltungsrat und Geschäftsleitung. Der vorliegende Cyber-Resilience-Leitfaden samt Checkliste soll Ihnen im Verwaltungsrat als Impuls und konkrete Hilfestellung dienen. Darüber hinaus sind wir der festen Überzeugung, dass Unternehmen wie Ihres einen kompetenten und zuverlässigen Partner an der Seite weiss. Experten, die Sie mit Ressourcen und Expertise tatkräftig unterstützen.

**Wir von der InfoGuard sind für Sie da – jederzeit (24/7), mit einem umfassenden 360-Grad Cyber Security Portfolio und mit voller Begeisterung!**

## Einladung zum Erfahrungsaustausch

Lassen Sie uns in einem unverbindlichen Round-Table-Gespräch herausfinden, wo und was Ihre grössten Herausforderungen und Bedrohungen im Security-Ökosystem sind. Wir freuen uns auf den persönlichen Austausch. Von VR zu VR. Von GL zu GL. Oder von CIO zu CIO. Kontaktieren Sie uns!

**Unverbindliches Gespräch vereinbaren**

**infoguard.ch/de/cyber-resilience-strategie-fuer-vr**

# CYBER DEFENCE AUF HÖCHSTEM NIVEAU.

## Wie sicher ist Ihr Unternehmen?

InfoGuard
SWISS CYBER SECURITY

## Securing Your Digital World – Today and Beyond


**Baar (Hauptsitz)**
InfoGuard AG
Lindenstrasse 10
6340 Baar
Schweiz
+41 41 749 19 00
info@infoguard.ch
infoguard.ch

**Bern**
InfoGuard AG
Stauffacherstrasse 141
3014 Bern
Schweiz
+41 31 556 19 00
info@infoguard.ch
infoguard.ch

**München**
InfoGuard Deutschland GmbH
Landsberger Straße 302
80687 München
Deutschland
+49 899 040 5064
info@infoguard.de
infoguard.de

**Wien**
InfoGuard GmbH
Graben 19
1010 Wien
Österreich
+43 123 060 6538
info@infoguard.at
infoguard.at