Mehr als Cybersicherheit: Wie Sie mit Cyber-Resilienz die Geschäftskontinuität sicherstellen

Warum IT-Verantwortliche heute Strategien zur Bewältigung von Störungen entwickeln müssen, statt sich nur auf deren Vermeidung zu konzentrieren.

Cybersicherheit vs. Cyber-Resilienz

Der Schwerpunkt der Cybersicherheit liegt vor allem auf der Abwehr von Angriffen. Cyber-Resilienz hingegen gewährleistet, dass der Geschäftsbetrieb während und nach einem solchen Angriff aufrechterhalten wird.

Cybersicherheit
Prävention, Perimeter-Verteidigung und Vermeidung von Datenschutzverletzungen

Cyber-Resilienz
Anpassungsfähigkeit, Wiederherstellung, Geschäftskontinuität

Auswirkungen auf die Geschäftskontinuität in verschiedenen Branchen

Warum Cyber-Resilienz in allen kritischen Branchen wichtig ist

Ausfallzeiten und Cyberangriffe können alle Unternehmen treffen. Die Konsequenzen sind jedoch je nach Branche unterschiedlich.

Gesundheitswesen

60 %

der Gesundheitseinrichtungen geben an, dass Cybervorfälle die Patientenversorgung direkt beeinträchtigen.[1]

Warum das wichtig ist:
Ausfallzeiten können dazu führen, dass sich Behandlungen verzögern, Patienten umgeleitet werden müssen und die Sicherheit beeinträchtigt wird.

Einzelhandel

43 %

der Einzelhandelsunternehmen erlebten im vergangenen Jahr größere Ausfälle aufgrund von IT- oder Cybervorfällen.[2]

Warum das wichtig ist:
Selbst kurze Störungen beeinträchtigen den Umsatz, die Übersicht über das Inventar sowie das Kundenerlebnis.

Finanzdienstleistungen

91 %

der Finanzinstitute waren im vergangenen Jahr mindestens einmal von einem Cybervorfall betroffen.[3]

Warum das wichtig ist:
Ausfallzeiten beeinträchtigen die Verarbeitung von Transaktionen, das Kundenvertrauen und die Einhaltung gesetzlicher Vorschriften.

Transportwesen und Logistik[4]

94 %

der Unternehmen geben an, dass Störungen durch Cybervorfälle zu einer Kettenreaktion von Ausfällen in der Lieferkette führen können.[5]

Warum das wichtig ist:
Systemausfälle stoppen die Sendungsverfolgung, den Lagerbetrieb und Just-in-Time-Lieferungen.

Öffentliche Verwaltung / Regierung

60 %

der Netzwerkausfälle verursachen bei öffentlichen Einrichtungen Betriebsunterbrechungen, die mindestens eine Million USD kosten.[6]

Warum das wichtig ist:
Ausfälle beeinträchtigen Bürgerdienstleistungen, den Notfallschutz und das öffentliche Vertrauen.

Ausfallzeiten entstehen durch mangelnde Geschäftskontinuität

Ausfallzeiten beeinträchtigen Umsatz, Betrieb und Reputation – nicht nur IT-Systeme.

96 %

der Unternehmen haben in den letzten drei Jahren mindestens einen Ausfall erlebt.

80 %

gaben an, dass die Ausfälle immer schwerwiegender werden.[7]

Warum herkömmliche Redundanzstrategien bei Ransomware versagen

Redundanz schützt zwar vor Hardware-Fehlern, jedoch nicht vor intelligenten Angriffen, die sich im System ausbreiten.

Infektionen können sich durch Replikation ausbreiten

Uneinheitliche Disaster Recovery- und Backup-Lösungen schaffen Sicherheitslücken

Zu viele Einzellösungen erhöhen die Wiederherstellungszeit und den Arbeitsaufwand

Moderne Resilienz erfordert neue Kennzahlen für die Wiederherstellung

Geschwindigkeit allein reicht nicht aus. Die wiederhergestellten Daten müssen malewarefrei sein und die Wiederherstellung muss auf den Geschäftsbetrieb abgestimmt erfolgen.

Kennzahl	Bedeutung
RTO	Maximale Zeitspanne bis zur Wiederherstellung des Geschäftsbetriebs
RPO	Maximal akzeptabler Datenverlust
MTD	Maximal tolerierbare Ausfallzeit, die ein Unternehmen verkraften kann.
MTCR	Zeitspanne, die erforderlich ist, um eine verifizierte, malwarefreie Umgebung wiederherzustellen.

Eine malwarefreie Wiederherstellung ist nun eine Voraussetzung für die Geschäftskontinuität

Eine schnelle Wiederherstellung ist nutzlos, wenn die wiederhergestellten Systeme kompromittiert sind.

- Die durchschnittlichen Kosten einer Datenschutzverletzung belaufen sich derzeit auf 4,45 Mio. USD.
- Betriebsunterbrechungen sind der größte Kostenfaktor bei Datenschutzverletzungen.[8]

Was IT-Verantwortliche in Unternehmen priorisieren sollten

Resilienz ist eine wirtschaftliche und betriebliche Entscheidung.

Wichtigste Maßnahmen (höchste Priorität)

- **Schutz an die Kritikalität der Assets anpassen**
- **Testen der Wiederherstellung unter realen Bedingungen testen**
- **Validierung von Backups vor der Wiederherstellung**
- **Reduzierung von Komplexität durch einheitliche Plattformen**

Angriffe sind unvermeidlich. Mit Cyber-Resilienz sorgen Sie jedoch für Kontinuität, Vertrauen und Kontrolle.

Mit Acronis von der Cybersicherheit zur Cyber-Resilienz

Cybersicherheit erfordert mehr als nur Schutz. Sie erfordert Resilienz. Erfahren Sie, wie Acronis Sie dabei unterstützt, auf Bedrohungen vorbereitet zu sein, Angriffen standzuhalten, sich schneller zu erholen und sich an zukünftige Bedrohungen anzupassen.

Kontaktieren Sie uns

---

[1] U.S. Department of Health and Human Services (HHS)
https://www.hhs.gov/about/news/2023/12/01/ransomware-cyber-attacks-threaten-patient-safety.html

[2] Uptime Institute, „Jährliche Ausfallanalyse 2023“
https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[3] Weltwirtschaftsforum, „Global Cybersecurity Outlook 2024“
https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

[4] Weltwirtschaftsforum, „Global Risks Report 2024“
https://www.weforum.org/reports/global-risks-report-2024

[5] Ibid

[6] Intelligent CIO, „US Regierungsbehörden verlieren bei einem durchschnittlichen Netzwerkausfall oder Sicherheitsvorfall Millionen.“
https://www.intelligentcio.com/north-america/2021/01/26/us-government-organizations-lose-millions-in-an-average-network-outage-or-data-breach/

[7] Uptime Institute, „Jährliche Ausfallanalyse 2023“
https://uptimeinstitute.com/resources/research-and-reports/annual-outage-analysis-2023

[8] IBM, „Kostenbericht zu Datenschutzverletzungen 2025“
https://www.ibm.com/reports/data-breach