we run your business

„Ransom, Risiko, Resilienz“ – warum Unternehmen jetzt aufrüsten müssen

„Sicherheit im Unternehmen“ ist für viele Unternehmen mit Planungen, Besprechungen und Investitionen verbunden. Doch angesichts der aktuellen Lage darf dieses Thema keinesfalls zweitrangig behandelt werden.

Laut BSI-Studien waren 2023 rund 72 Prozent aller befragten Unternehmen von Cyberangriffen betroffen – 2024 bereits 81 Prozent (+9 Prozent). Gleichzeitig halten sich nur 53 Prozent der Unternehmen für gut vorbereitet auf solche Angriffe.

Deutschland – die aktuelle Situation

Die Bedrohungslage hat sich in den letzten Jahren deutlich verschärft. Bitkom-Präsident Dr. Ralf Wintergerst formulierte es so: „Die Bedrohungslage für die deutsche Wirtschaft verschärft sich und Unternehmen müssen ihre Schutzmaßnahmen weiter hochfahren.“

Die Fakten sprechen für sich[1]: 81 Prozent der Unternehmen in Deutschland wurden 2024 Opfer von Cyberangriffen – darunter Datendiebstahl, Industriespionage und Sabotage. Der Schaden: ca. 266 Mrd. Euro, ein Anstieg um 29 Prozent gegenüber dem Vorjahr.

Die häufigsten Angriffsmethoden:

- **Ransomware (Datenverschlüsselung):** 31 Prozent (+8)
- **Phishing:** 26 Prozent (-5)
- **Passwort-Angriffe:** 24 Prozent (-5)
- **Schadsoftware:** 21 Prozent (-7)

Viele Unternehmen sehen in diesen Zahlen eine existenzielle Bedrohung[2]. Und das zu Recht – nicht nur wegen der Häufigkeit, sondern auch wegen der zunehmenden Raffinesse der Angriffe. Auch der Einsatz von KI-gestützten Sprachmodellen zur Optimierung von Phishing-E-Mails erhöht das Risiko drastisch.

Cyberrisiken stellen heute einen der größten Gefährdungsblöcke für Unternehmen weltweit dar. Dennoch wäre es fahrlässig, nur digitale Risiken zu betrachten. Die Industriespionage – häufig durch staatlich gesteuerte Akteure – erlebt durch geopolitische Spannungen eine neue Hochkonjunktur. Auch Naturkatastrophen wie Überschwemmungen oder Brände gehören zu den Risiken, denen Unternehmen zunehmend ausgesetzt sind.

Deutschland – der Ausblick

Die Bedrohungslage wird voraussichtlich nicht abnehmen. Im Gegenteil: Der globale Wettbewerb und die Zahl der Konkurrenten steigen – ebenso wie die Aktivitäten staatlicher Akteure im digitalen Raum. Für Unternehmen ist das ein klarer Appell, IT-Risikomanagement strukturell zu verankern – und zwar auf Geschäftsleitungsebene. Der Grundsatz lautet: **Prepare for the worst and hope for the best.**

Auch das BSI stuft die Bedrohungslage als „besorgniserregend“ ein – doch Unternehmen sind dieser Situation nicht hilflos ausgeliefert. Es gibt wirksame Mittel, um Resilienz aufzubauen.

Zwei zentrale Strategien

1. **Angriffsabwehr (Prävention)**: Ein solides Sicherheitsniveau basiert auf einer Strukturanalyse und gezielter Risikobehandlung in den Unternehmensprozessen. **Ziel: Risikominimierung**.
2. **Notfallmanagement (Mitigation)**: Auch das sicherste System kann kompromittiert werden. Eine strukturierte Notfallplanung – basierend auf derselben Strukturanalyse – ermöglicht die Aufrechterhaltung elementarer Prozesse. **Ziel: Schadenminimierung.**

Beide Maßnahmen sind Grundpfeiler der Unternehmens Resilienz und ergänzen sich perfekt. Der **BSI-Standard** (200-1 bis 200-4) sieht sie als integralen Bestandteil eines umfassenden IT-Sicherheitskonzepts ISMS.

we run your business

Cyberversicherung oder Business Continuity Management?

Cyberversicherungen sind zwar populär, aber kein Ersatz für IT-Sicherheit. Sie sollten nur als ergänzender Baustein verstanden werden.

- **Cyberversicherung**
  - Deckt finanzielle Verluste (Lösegeld, Wiederherstellungskosten, Rechtsberatung)
- **Business Continuity Management (BCM)**
  - Sorgt für strukturierte Vorbereitung und klare Prozesse.
  - Ermöglicht schnellen Übergang in den Notbetrieb.
  - Kann Versicherungsprämien reduzieren.

Prävention oder Mitigation? Beides ist notwendig. Prävention schützt – Mitigation rettet. Zusammen ergeben sie ein belastbares IT-Sicherheitskonzept.

Fazit

Die Bedrohung durch Cyberangriffe auf deutsche Unternehmen ist real und wächst weiter. Dabei gewinnen nicht nur digitale, sondern auch analoge Risiken an Bedeutung. Unternehmen sind mehr denn je gefordert, in Sicherheitsmaßnahmen zu investieren – nicht nur aus Eigeninteresse, sondern auch zum Schutz von Geschäftsbeziehungen, Kunden und der Lieferkette. Ziel dieses Beitrags ist es, das häufig als kryptisch wahrgenommene Thema IT-Risikomanagement greifbar und verständlich für Entscheider zu machen. **Denn: Sicherheitsmaßnahmen sind kein Luxus!** Ohne Notfallplanung wird ein Cyberangriff nicht nur zum Notfall – sondern zur Krise. Und für manche Unternehmen zur existenziellen Bedrohung.

„Es kommt nicht darauf an, die Zukunft vorauszusehen, sondern auf die Zukunft vorbereitet zu sein."
– Perikles, griechischer Staatsmann (493–429 v. Chr.) –

Der Autor:
Michael Hacker, Geschäftsführer der mevalon-Datentechnik GmbH in Mannheim. Die Firma unterstützt seit 2001 Unternehmen in IT-Betrieb und -Management. Seit 2015 auch mit den Schwerpunkten Datenschutz und IT-Risikomanagement. Er selbst ist zertifizierter Datenschutz-Auditor, ISMS-Auditor, BCMS-Praktiker und BSI Grundschutz-Praktiker. Fragen rund um die Themen IT-Sicherheit und IT-Risikomanagement beantwortet er gerne unter: security@mevalon.de

---

we run your business

Quellen

[1] Bitkom „Wirtschaftsschutz 2024“

[2] Angriffe auf die deutsche Wirtschaft nehmen zu | Bitkom Research