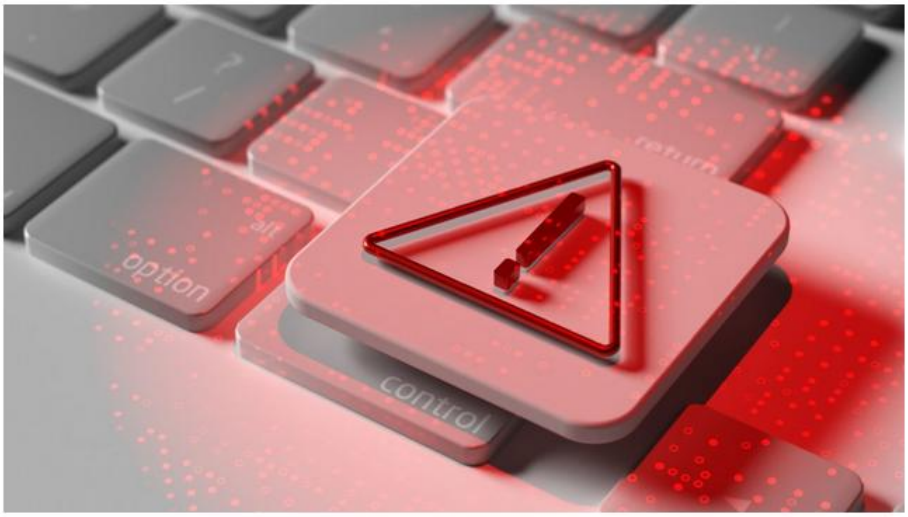
it-daily.net

Cybersicherheit im technischen Service

Wenn Angriffe den Kundendienst lahmlegen

14. August, 2025 05:40



Ausgefallene Ticketsysteme, gestörte Fernzugriffe, kompromittierte KI-Vorschläge: Der technische Service wird zur Angriffsfläche, mit fatalen Folgen für Verfügbarkeit und Kundenzufriedenheit.

Um handlungsfähig zu bleiben, müssen Serviceorganisationen ihre digitale Resilienz gezielt stärken.

Ein Maschinenstillstand. Der Techniker ist beim Kunden vor Ort. Doch statt Lösungen zu liefern, beginnt die Fehlersuche im eigenen Haus: Aufgrund gezielter Angriffe ist die sichere Kommunikationsverbindung zur Zentrale unterbrochen, der Fernzugriff auf die Steuerung der Anlage bricht ab, und die KI-basierte Software schlägt auf Basis veralteter, ungesicherter

Daten eine risikobehaftete Reparaturmaßnahme vor. Solche Bedrohungsszenarien sind im Service-Alltag längst Realität – gerade in hochvernetzten Serviceumgebungen, in denen Systeme eng verzahnt arbeiten. Die Folgen derlei Attacken sind oft gravierend: Reaktionsverzögerungen, Datenlecks, Reputationseinbußen und nicht selten hohe wirtschaftliche Schäden. Was kann der technische Service also tun, um sich resilienter aufzustellen?

Cyberangriffe zielen auf operative Systeme

Angriffe auf den technischen Service folgen einer klaren Logik. Dort, wo kritische Daten fließen und produktionsnahe Prozesse laufen, lassen sich mit vergleichsweise geringem Aufwand große Störungen verursachen. Besonders gefährdet sind mobile Schnittstellen, cloudbasierte Serviceportale, Remote-Wartungssysteme oder KI-gestützte Supportstrukturen – also genau die Bereiche, die Unternehmen für ihren Kundenservice modernisiert haben. Zusätzlich wirken viele Angriffe indirekt: durch manipulierte Ersatzteildaten, den Ausfall von Kommunikationssystemen oder verzögerte Eskalationen. Der Schaden ist nicht immer sofort sichtbar, aber operativ meist hochrelevant.

Sicherheit als Teil der Servicearchitektur

Die Konsequenz: IT-Sicherheit darf sich nicht nur auf den Schutz klassischer Infrastrukturen konzentrieren. Unternehmen müssen sie vielmehr als funktionalen Bestandteil der digitalen Servicearchitektur verstehen – von der Applikationsebene bis zur Kundenschnittstelle.

Das betrifft nicht nur technologische Aspekte, sondern auch organisatorische Fragen. Wer trägt im Störungsfall die Verantwortung? Wie ist der Zugriff auf sensible Kunden- und Anlagendaten geregelt? Und welche Rolle spielt IT-Sicherheit in Schulungen, Briefings oder im operativen Tagesgeschäft? Gerade hier liegen die strukturellen Schwächen vieler Unternehmen. Laut einer Bitkom-Studie bieten zwar 73 Prozent der Unternehmen Weiterbildungen zu digitalen Themen aber, aber nur 11 Prozent tun dies flächendeckend. Das bedeutet: Auch viele Servicemitarbeiter agieren in hochdigitalisierten Umgebungen ohne ein einheitliches Verständnis für Risiken und Schutzmaßnahmen. Hinzu kommen regulatorische Anforderungen wie NIS2 oder der EU AI Act, die Nachweise über den sicheren Betrieb kritischer Systeme und KI-gestützter Entscheidungen verlangen.

Hebel für mehr IT-Sicherheit im Servicealltag

Gerade kleine und mittlere Unternehmen fühlen sich von diesen steigenden Anforderungen an IT-Sicherheit oft überfordert. Der CyberRisikoCheck des BSI bietet hier einen niedrigschwelligen Einstieg – inklusive individueller Empfehlungen und staatlicher Förderung. So entsteht eine belastbare Grundlage, um gezielt in digitale Resilienz zu investieren.

Wer langfristig widerstandsfähig sein will, sollte – basierend auf den Empfehlungen des BSI – vier Handlungsfelder im Blick behalten:

- **Technologie absichern:** Sicherheitsupdates konsequent einspielen (Patchmanagement), sensible Systeme logisch voneinander trennen (Netzwerksegmentierung), Fernzugriffe mit Multi-Faktor-Authentifizierung schützen und Kommunikation durchgängig verschlüsseln.
- **Prozesse etablieren**: Klare Notfall- und Wiederanlaufpläne entwickeln, Rollen und Zugriffsrechte eindeutig regeln, Eskalationspfade definieren und sicherstellen, dass sicherheitsrelevante Vorgänge nachvollziehbar dokumentiert sind.

- **Menschliche Faktoren stärken:** Mitarbeiter regelmäßig für Cyberrisiken sensibilisieren, realistische Angriffsszenarien (z. B. Phishing-Tests) simulieren und Sicherheitsverantwortung im Team verankern.
- **Governance & Compliance integrieren:** Ein Informationssicherheits-Managementsystem (ISMS) nach ISO 27001 einführen, den Umgang mit KI-Systemen dokumentieren und gesetzlichen Nachweispflichten nachkommen – etwa im Zuge neuer Regulierungen wie NIS2 oder dem EU AI Act, wenn KI-gestützte Entscheidungen revisionssicher nachvollzogen werden müssen.

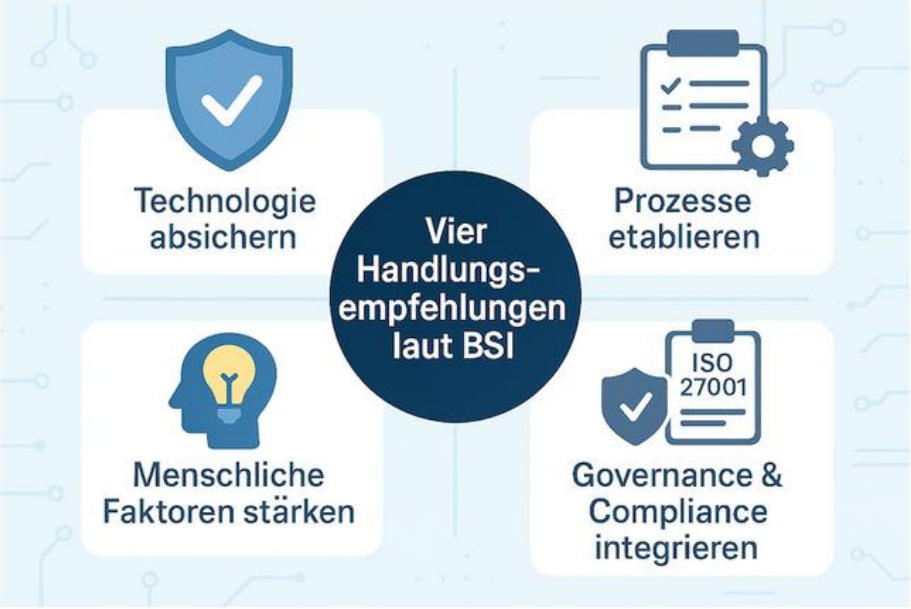


Bild 1: Diese vier Handlungsfelder sollten Serviceorganisationen im Blick behalten. (Bildquelle: ChatGPT)

Praxisnah umgesetzt kann das wie folgt aussehen:

Das technische Service-Team eines Maschinenbauunternehmens stieß nach einem Fernwartungsausfall auf Sicherheitslücken in der Zugriffskontrolle. In Zusammenarbeit mit den IT-Verantwortlichen führte das Team gestufte Zugriffsrechte ein, erweiterte die Multi-Faktor-Authentifizierung und definierte ein klares Eskalationsschema für Störungen. Zusätzlich erhielten alle Servicemitarbeiter ein gezieltes Training zur Erkennung von Phishing-Versuchen. Die Maßnahmen betteten die Verantwortlichen in die bestehende Governance-Struktur ein. Das Ergebnis: eine deutlich schnellere Reaktion auf kritische Vorfälle und ein klar abgegrenztes, besser gesichertes Servicenetzwerk.

Sicherheit als Schlüssel zur Servicequalität

Technischer Service nimmt mittlerweile eine strategische Schlüsselrolle ein. Er ist Kundenschnittstelle, Wertschöpfungspartner und zunehmend ein sicherheitskritischer Bereich. Wer ihn zuverlässig digital betreiben will, braucht mehr als funktionierende Tools. Benötigt wird eine Sicherheitsarchitektur, die Technologie, Prozesse, Menschen und Governance strategisch und skalierbar zusammenführt. Nur so lassen sich Systeme schützen, Ausfallrisiken minimieren und die Kundenzufriedenheit langfristig sichern. Denn ohne wirksame Sicherheitsmaßnahmen verliert selbst der beste Techniker seine Handlungsfähigkeit – und das Unternehmen seine Servicequalität.

Cyberangriff | Cybersicherheit | Kundendienst

Carsten Neugrodda

Geschäftsführer
Service-Verband KVD

Carsten Neugrodda ist seit 2021 Geschäftsführer des Kundendienst-Verband Deutschland e.V. (Service-Verband KVD). Der Diplom-Ökonom bringt über 20 Jahre Führungserfahrung in Marketing, Vertrieb und Business Development in multinationalen Konzernen und mittelständischen Unternehmen mit.