IT-Sicherheit im Service-Bereich

Service-Verband KVD appelliert an KMU

19.06.2025 · Quelle: Pressemitteilung · 2 min Lesedauer ·

Auch Unternehmen, die technische Dienstleistungen anbieten, sind Cyberrisiken ausgesetzt. Allerdings lässt das Bewusstsein dafür dem Service-Verband KVD zufolge noch zu wünschen übrig. Der Verband gibt Handlungsempfehlungen.

Der Berufsverband für Beschäftigte im Kundendienst und Service KVD legt es besonders KMU aus der technischen Dienstleistungsbranche ans Herz, ihre IT-Sicherheitsmaßnahmen aufzubessern – hinsichtlich der Awareness der Mitarbeitenden und als Vorbereitung auf NIS 2 und den EU AI Act.
(Bild: © ipopba - stock.adobe.com)

Ausgefallene Ticketsysteme, fehleranfällige Chatbots oder unautorisierte Fernzugriffe: Cyberangriffe sind dem Service-Verband KVD zufolge keine Seltenheit mehr im Service-Alltag. Deshalb warnt der Berufsverband für Beschäftigte im Kundendienst und Service vor dieser unterschätzten digitalen Gefahr. Denn viele Managed Service Provider, technische Kundendienstleister und IT-Support-Anbieter würden die Bedrohung für den technischen Service durch Cyberkriminelle nicht ernst genug nehmen. „Die technologische Entwicklung hat enorme Effizienzgewinne ermöglicht, aber auch die Abhängigkeit von funktionierenden, geschützten Infrastrukturen massiv erhöht", sagt Verbandsgeschäftsführer Carsten Neugrodda. „Wer Cybersicherheit nicht ganz oben auf die Agenda setzt, riskiert Stillstand, Vertrauensverlust und langfristige wirtschaftliche Schäden." Gerade bei kleinen und mittelständischen Unternehmen (KMU) sehe der Verband enormen Handlungsbedarf.

Handlungsbedarf hinsichtlich Security-Awareness

Der KVD sieht die Verantwortung für die Cybersecurity nicht allein bei der IT-Abteilung, sondern bei der gesamten Organisation. Als besonders kritisch sieht Neugrodda die Automatisierung, die zunehme, während Mitarbeitende weniger zu Cybergefahren geschult würden. Gerade in mittel-großen Unternehmen ist das Bewusstsein für Bedrohungen aus dem Netz eher geringer als in großen Unternehmen mit mehr als 1.000 Beschäftigten, so eine Studie von G Data. Darüber hinaus haben 23 Prozent der Befragten einer Umfrage des Marktforschungsinstituts Censuswide Sorge, einen Fehler zu machen, der zu einem Cyberangriff führen könnte. Deshalb sieht der KVD hinsichtlich Sensibilisierung, Kompetenzaufbau und Prävention noch Luft nach oben.

> *„Sicherheit beginnt beim Menschen – im Service, im Vertrieb, in der Führung. Nur wenn alle mitziehen, entsteht Resilienz."*
>
> Carsten Neugrodda, Verbandsgeschäftsführer des KVD

Empfehlungen des KVD

Vor allem hinsichtlich zunehmender Regulierungen durch Vorgaben wie die NIS-2-Richtlinie und den EU AI Act, wachse der Druck auf Unternehmen. Wer noch keine Cybersicherheitsstrategie hat, könnte Probleme bekommen. Denn künftig müssen Unternehmen – auch IT-Dienstleister – nachweisen, dass sie in der Lage sind, Risiken zu identifizieren, zu bewerten, zu steuern und zu dokumentieren. Deshalb empfiehlt der KVD die Einführung von Informationssicherheitsmanagementsystemen (ISMS) nach ISO 27001. Daneben weist der Verband auf den „CyberRisikoCheck" des BSI hin, ein Angebot, das sich speziell an KMU richtet und diese dabei unterstützt, ihren Sicherheitsstatus zu analysieren und konkrete Maßnahmen abzuleiten.