IT-SICHERHEIT IN DER SOZIALWIRTSCHAFT

FINSOZ veröffentlicht 1. Lagebericht & Leitfaden zu Prävention und Abwehrmechanismen von Cyberattacken.

Die Sensibilität für Cybersicherheit in den Organisationen der Sozialwirtschaft wächst – und die Art und Anzahl der Bedrohungen ebenso. Vor allem kleine und mittelständische Unternehmen im Gesundheits- und Sozialwesen stellen ein attraktives Angriffsziel dar: begrenzte IT-Ressourcen, tendenziell veraltete IT-Infrastruktur und der Vielzahl hochsensibler personenbezogener Daten laden Angreifer förmlich ein.

Das ist das erste Fazit des vom Digitalverband FINSOZ im Juni herausgegebenen 1. Lageberichts IT-Sicherheit in der Sozialwirtschaft 2022.

Die Autoren der verbandsinternen Fachgruppe „IT-Compliance“ hatten die Sicherheitslage mit speziellem Fokus auf die Sozialwirtschaft erstmals im Jahr 2022 untersucht und im Fazit Nummer zwei festgestellt, dass insbesondere Ransomware – neben Bedrohungen wie Phishing, Malware und DDoS (Distributed Denial-of-Service) – eine akute Herausforderung für die Branche darstellt. Sicherheitslücken in den Organisationen und die zunehmend hochprofessionalisierten Strukturen der Angreifer, die Cyberkriminalität längst als Dienstleistungsmarkt ansehen (Cybercrime-as-a-Service, CaaS), führten zu einer steigenden Anzahl von Vorfällen, so die Autoren weiter. „Auch wenn es sich bei der Vielzahl der Bedrohungen für die IT-Sicherheit in der Sozialwirtschaft bislang häufig nicht um Einrichtungen oder Organisationen im Bereich der „kritischen Infrastruktur“ handelt, kann ein Ausfall zu erheblichen Störungen und Schäden führen“ – so Fazit Nummer drei. Ihre Empfehlung: IT-Sicherheit sollte zukünftig zu einem zentralen Aspekt im betrieblichen Risiko- und Compliance-Management werden.

In dem 53-seitigen Lagebericht, der als erster Leitfaden IT-Sicherheit für die Sozialwirtschaft gilt, werden beispielhaft reale Datenschutz- und IT-Sicherheitsvorfälle in der Branche aufgezeigt und beschrieben, auf welchen Wegen Cyberkriminelle ins Netzwerk der Organisationen eindrangen, wie sie Zugangsbeschränkungen umgingen, Zugriffe erhielten oder wo sich ausgewählte Schwachstellen in der Rekonstruktion finden ließen. Das Prekäre daran: Nahezu sämtliche Beispiele und beschriebenen Angriffsvektoren sind nach DSGVO und den evangelischen bzw. katholischen Kirchengesetzen zum Datenschutz als mögliche Datenpannen einzustufen und entsprechend den Aufsichtsbehörden zu melden.

Neben dem Überblick zu Datenschutz- und IT-Sicherheitsvorfällen und den Vorgehensweisen von Angreifern stellt die Autorenschaft, die aus Datenschützern, Juristen, IT-Sicherheitsbeauftragten, IT-Verantwortlichen und QM-Beauftragten besteht, auch konkrete Handreichungen zur Verfügung, beispielsweise wie Verteidigungslinien zur Abwehr errichtet werden können oder wie die aktuelle Rechtslage im Kontext der IT-Sicherheit aussieht. Abgerundet wird der Leitfaden durch eine „Checkliste IT-Notfall“ im Anhang.

Der Lagebericht richtet sich an Vorstände, Geschäftsführungen und Digitalisierungsverantwortliche sowie an IT-Sicherheitsspezialist:innen und Datenschutzbeauftragte. Er kann entgeltlich beim Digitalverband FINSOZ erworben werden unter der Mailadresse: *info@finsoz.de*
Für FINSOZ-Mitglieder steht der Lagebericht kostenfrei zur Verfügung.

FINSOZ e.V.
Digitalverband Sozialwirtschaft

FINSOZ e.V. –
Fachverband Informationstechnologie in Sozialwirtschaft und Sozialverwaltung
Mandelstraße 16, 10409 Berlin
Tel.: +49-(0)30-42084-512
E-Mail: info@finsoz.de
www.finsoz.de

BILD: © FINSOZ