TAGESSPIEGEL
BACKGROUND

Gesundheit & E-Health

Digitalisierung der Pflege erhöht Risiko durch Cyberangriffe

von **Gunnar Göpel**

veröffentlicht am 17.08.2022

Vor allem kleine und mittelständische Unternehmen (KMU) im Gesundheits- und Sozialwesen müssen zunehmend **sensibler für Cybersicherheit** werden. Dazu rät der Fachverband für Informationstechnologie in Sozialwirtschaft und Sozialverwaltung (FINSOZ). Den KMU stünden üblicherweise nur begrenzte IT-Ressourcen zur Verfügung und IT-Infrastrukturen seien tendenziell auf einem älteren Stand. Gleichzeitig sei die Vielzahl hochsensibler personenbezogener Daten für Angreifer umso attraktiver. Art und Anzahl der Bedrohungen hätten zugenommen. „Insbesondere durch die **fortschreitende Digitalisierung in der Pflegebranche** wächst auch das Risiko für Einrichtungen, Opfer von Cyberattacken zu werden“, sagte die FINSOZ-Vorstandsvorsitzende Michaela Grundmeier gestern zu Tagesspiegel Background.

Im „1. Lageberichts IT-Sicherheit in der Sozialwirtschaft 2022“ hat die verbandsinterne Fachgruppe „IT-Compliance“ – darunter Datenschützer:innen, Jurist:innen, IT-Sicherheitsbeauftragte, IT-Verantwortliche und QM-Beauftragte – die Sicherheitslage mit speziellem Fokus auf die Sozialwirtschaft untersucht. Sie kamen zu dem Schluss, dass **insbesondere Ransomware, neben Bedrohungen wie Phishing, Malware**

und DDoS (Distributed Denial-of-Service), eine „akute Herausforderung“ für die Sozialwirtschaft darstelle. 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.

Umso dringlicher seien daher die Implementierung und der Ausbau von IT-Sicherheit auch in den Organisationen der Pflegebranche, führte Grundmeier weiter aus, die auch Co-Autorin des Berichts ist. Dies wäre ein **wichtiger Schritt, um auch für zukünftige Innovationen wie die Telematik-Infrastruktur** gut gerüstet zu sein. „Perspektivisch gesehen führt jedoch kein Weg daran vorbei, IT-Sicherheit zukünftig als einen zentralen Aspekt **im Betrieblichen Risiko- und Compliance-Management zu verankern**“, so die Vorstandsvorsitzende.

Die Autor:innen verweisen darauf, dass nicht zwingend Einrichtungen der kritischen Infrastruktur, beispielsweise Maximalversorger wie Universitätskliniken, von Cyberangriffen betroffen sein müssten, damit „erhebliche Störungen und Schäden“ entstehen könnten. *gg*