Cyber-**Sicherheit** in **KRITIS**-**chen** Zeiten

Tankstellenunternehmen sind als KRITIS eingestuft und müssen sich im Bereich Cybersicherheit mit verschiedenen Fragestellungen beschäftigen. Welche gesetzlichen Anforderungen bestehen, verrät uns ein Experte.

TEXT: LISA LEVY **FOTOS:** STOCK.ADOBE.COM/TIPPAPATT; AUDACO IT-REVISION GBR; VERENA FOTOGRAFIERT; VODAFONE

Laut dem Digitalverband „Bitkom" liegen die Schäden durch Cyber-Angriffe in Deutschland bei 148 Milliarden pro Jahr. Reputationsschaden, Versicherungsverlust, Produktionsstillstand – so lauten die Albträume der Unternehmer. Für Tankstellen kommen die gesetzlichen Vorschriften für die Cybersicherheit hinzu, denn sie sind als KRITIS eingestuft. „Hier sind Kontrollen durch das Bundesamt für Informationssicherheit (BSI) möglich, zum Beispiel KRITIS-Prüfungen, Tiefenprüfungen durch das BSI, Lieferantenaudits und mehr", sagt Jörg Karner, geschäftsführender Partner bei der „audaco IT-Revision GbR".

Die Komplexität der betrieblichen Abläufe erfolgt durch die zunehmende Vernetzung der Systeme mit dem Internet. Seine Office-IT heutzutage sicher zu gestalten, sei aber machbar, so Jörg

Karner: „Die Möglichkeiten der Systeme, aktuell auch durch KI, wachsen rasant, sodass Mitarbeiter oft nicht das Wissen zur richtigen Nutzung besitzen." Neben technischen und organisatorischen Maßnahmen müssten personelle Maßnahmen eingeleitet werden, die zum Schutz der Office-IT beitragen.

Sicherheits-Maßnahmen

Als Basis müsse die IT-Infrastruktur auf dem aktuellen Stand der Technik betrieben werden. „Dazu gehören aktuelle Betriebssysteme auf Servern, PC, Laptops, Netzkomponenten", so Jörg Karner. „Der IT-Betrieb muss Verfahren zum Patch- und Changemanagement sowie zur Schwachstellenerkennung etabliert haben." Die IT-Architektur müsse unterschiedliche Netzsequenzierungen beinhalten, die voneinander geschützt administriert werden. „Eine Trennung von IT-Systemen und Betriebstechnologie-Systemen (OT) in eigenen Netzen ist zwingend", so der Experte. Außerdem wichtig: „Die regelmäßige Schulung und Sensibilisierung der Mitarbeiter für Gefahren und den richtigen Umgang mit IT-Systemen ist zu planen und zielgruppenorientiert umzusetzen", so der geschäftsführende Partner bei „audaco IT-Revision GbR".

> *Unsere Beratung der IT-Sicherheit deckt alle kritischen Bereiche ab, einschließlich KRITIS §8A-Anforderungen.*

Jörg Karner, geschäftsführender Partner, „audaco IT-Revision GbR"

Eine schriftliche Dokumentation gehört ebenfalls zu den Maßnahmen, die gesetzlich verpflichtend sind. „Bei Fehlen einer angemessenen Dokumentation kann es im Schadensfall zu Organisationsverschulden und zur Haftung des Geschäftsführers führen", sagt Jörg Karner. „Privatvermögen eingeschlossen, da Versicherungen in diesem Fall gegebenenfalls nicht leisten."

Protokollierung der IT-Sicherheit

Aus der Compliance-Sicht kann ein KRITIS-Unternehmen die IT-Sicherheit nur durch eine externe Prüfung protokollieren, zum Beispiel zur Umsetzung der KRITIS §8a VO oder ISO27001:2022.

„Aus der IT-technischen Sicht ist die Protokollierung sehr vielsichtig, da alle IT-Systeme in irgendeiner Weise Logfiles erstellen und nach definierten Zeiten aufbewahren", so Jörg Karner. „Protokolle dienen oft als Quelle bei technischen Problemen oder zur Klärung von Sicherheitsereignissen. Bei Sicherheitsvorfällen müssen sie gegebenenfalls Ermittlungsbehörden zur Verfügung gestellt werden. Das Thema Protokollierung hat mit der gesetzlichen Umsetzungspflicht für KRITIS-Betreiber gemäß der Angriffsfrüherkennung eine neue Bedeutung gewonnen. Unternehmen müssen demnach seit 1. Mai 2023 in der Lage sein, Cyber-Angriffe zu protokollieren, zeitnah zu identifizieren und umgehend zu reagieren."

Aufbewahrungsfristen

Aufbewahrungsfristen sind abhängig von den protokollierten Daten. Sind die Daten kaufmännischen Prozessen zuzuordnen, gelten andere Aufbewahrungsfristen als bei technischen Protokolldaten. „Bei personenbezogenen Daten sind die Zweckgebundenheit gemäß EU-DSGVO zu berücksichtigen, ebenso entsprechende Löschfristen bei den Protokollen." ■

Marc Beck
Inhaber & Partner, „Eye-Level-Consulting"

Für kleine und mittlere Unternehmen ist es sinnvoll, sich beim Thema Cybersicherheit von einem vertrauenswürdigen Partner beraten zu lassen, der über die nötige Expertise verfügt. Marc Beck, der uns für diesen Beitrag den Experten Jörg Karner empfohlen hat, vermittelt IT-Freelancer oder Festangestellte für spezifische Branchenunternehmen. „Wir bringen die besten Köpfe in Ihr Unternehmen. ‚Eye-Level-Consulting' vereint Branchenexpertise mit effizienter Personalvermittlung."

www.eye-level-consulting.de

Andreas Vorbau
Senior Manager Business Rahmenverträge, „Vodafone"

„Die dargestellte Bandbreite an Themen und Aufgaben verdeutlicht: Wer sich nicht intensiv und regelmäßig mit allen Aspekten dieser komplexen Materie beschäftigt, ist schnell überfordert oder verliert den Anschluss an den aktuellen Stand der Technik. Hauseigene Konzepte bergen das Risiko, wichtige Teilaspekte zu übersehen. Suchen Sie sich in guten Zeiten einen vertrauenswürdigen Partner, der Sie in Cyber Security unterstützt, damit Sie in Krisenzeiten gut vorbereitet sind und schnell auf Bedrohungen reagieren können."