27001 einen Mehrwert bringen. Auch Betreiber, welche die festgelegten KRITIS-Schwellenwerte noch nicht überschritten haben, können von einer freiwilligen Zertifizierung profitieren.

Wer selbst einmal den vollständigen Prozess einer Zertifizierung durchlaufen hat, kann zum Beispiel besser einschätzen, ob Zulieferer und Subunternehmer für die Zusammenarbeit wichtige Sicherheitsstandards einhalten. Eine zusätzliche freiwillige Zertifizierung fördert auch langfristige und vertrauensvolle Beziehungen mit Geschäfts- und Endkunden.

Manche Versicherungen verbessern die Konditionen für Kunden, die einen höheren als den gesetzlich notwendigen Sicherheitsstandard einhalten. Die Kür lohnt, wenn IT- und Cyber-Sicherheit als Prozesse dauerhaft mitgedacht und mitgeplant werden. Da sich die Bedrohungslage dynamisch entwickelt, sollten auch die ISMS-Prozesse nach dem Plan-Do-Check-Act-Verfahren kontinuierlich überprüft und falls nötig angepasst werden.

Faktor Mensch im Blick behalten

Ein System zur Angriffserkennung ersetzt nicht die Sensibilisierung der Mitarbeitenden – hierauf zielt auch das BSI mit seiner Orientierungshilfe explizit ab. Ein in den Grundlagen geschultes, stets waches Auge zählt zu den wirksamsten Schutzmaßnahmen, um beispielsweise verdächtige E-Mail-Anhänge, Phishing-Versuche oder Social-Engineering-Angriffe als solche zu erkennen. Um mögliche Einfallstore abzusichern, müssen Mensch und Technik deshalb Hand in Hand arbeiten. ■

Alle Vorschriften auf dem Radar

Das Compliance-Werkzeug Rechtskataster-Online unterstützt KRITIS-Betreiber der Energiewirtschaft bei der Optimierung ihrer IT-Sicherheit. Die Plattform fasst gesetzliche Anforderungen zusammen und ermöglicht es, deren Einhaltung zu überprüfen und zu dokumentieren.

Betreiber Kritischer Infrastrukturen (KRITIS) sind durch mehrere Gesetze auf nationaler und EU-Ebene verpflichtet, sich vor Cyber-Angriffen zu schützen und Störungen in den von ihnen betriebenen Infrastrukturen zu vermeiden. Die relevanten Anforderungen werden derzeit durch das BSI-Gesetz (BSIG) sowie durch das Energiewirtschaftsgesetz (EnWG) und das Telekommunikationsgesetz (TKG) auf nationaler Ebene geregelt, auf EU-Ebene durch die Richtlinien NIS und NIS2.

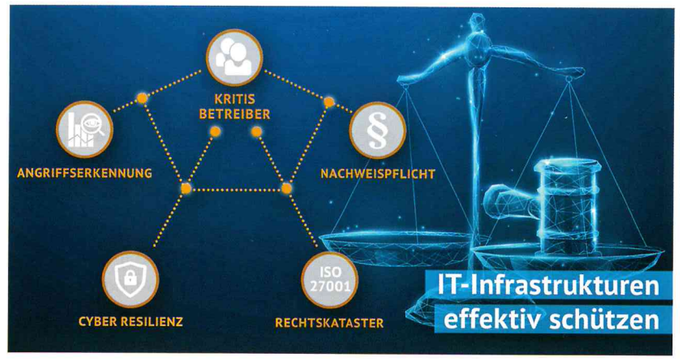
Aktuell sind die besonderen Pflichten für die IT-Sicherheit in § 8a BSIG festgelegt. KRITIS-Betreiber der Energiewirtschaft müssen demnach angemessene organisatorische und technische Vorkehrungen treffen, um die von ihnen betriebene Infrastruktur vor Cyber-Angriffen, wie zum Beispiel Hacking, Malware und Datendiebstahl, zu schützen. Alle zwei Jahre müssen sie gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) belegen, dass ihre IT-Sicherheit auf dem Stand der Technik ist, und einen Nachweis darüber erbringen, dass in Bezug auf die IT-Systeme, -Prozesse und -Komponenten angemessene Vorkehrungen getroffen wurden. Dazu bestehen seit Mai 2023 Meldepflichten gegenüber dem BSI. Dieses führt entsprechende Kontrollen durch und kann Verstöße mit Bußgeldern ahnden. Um für einen solchen Nachweis alle relevanten Gesetze und Vorschriften automatisch im Blick zu haben, nutzen bereits viele Unternehmen ein Compliance-Werkzeug wie Rechtskataster-Online, ein Projekt der Firmen SR Managementberatung und ITC. Die Plattform bündelt die rechtlichen Anforderungen für das Energie-, Umwelt- und Arbeitsschutz-Management sowie den Rechtsbereich Datenschutz.

Überblick behalten

Das BSIG verweist zwar nicht explizit auf eine Zertifizierung nach ISO 27001, jedoch kann diese unter bestimmten Voraussetzungen ein wesentlicher Bestandteil eines Nachweises gemäß § 8a Absatz 3 sein. Wer bei Rechtskataster-Online die Rechtsbereiche Energie und Datenschutz bucht, erhält die für die Zertifizierung relevanten Gesetze und Vorschriften automatisch im Überblick. Die Normen können nachverfolgt, bewertet und je nach Relevanz in das unternehmenseigene Rechtskataster übernommen werden, um letztlich die im Gesetz geforderten, angemessenen und organisatorischen Vorkehrungen zu erfüllen. Die alleinige Vorlage eines solchen Zertifikats reicht allerdings als Nachweis beim BSI nicht aus.

Link-Tipp

Weitere Informationen unter:
- www.rechtskataster-online.de



iStockphoto.com/Who_I_am | ITC AG

Rechtskataster-Online hilft, IT-Infrastrukturen effektiv zu schützen.

Die NIS2-Richtlinie ist die Nachfolgerichtlinie der Cybersecurity-Richtlinie NIS aus dem Jahr 2016 und führt zusätzliche Maßnahmen und Anforderungen ein. So wird beispielsweise genauer definiert, welche Unternehmen oder Organisationen den Kritischen Infrastrukturen zugeordnet werden und in welchen Sektor sie fallen. Zudem wurde die Anzahl dieser Sektoren erweitert und Schwellenwerte für Unternehmen von mindestens 50 Mitarbeitern und zehn Millionen Euro Jahresumsatz festgelegt. Die Norm zielt darauf ab, in der gesamten EU ein gleichmäßig hohes Sicherheitsniveau in Kritischen Infrastrukturen zu gewährleisten. Bis Mitte Oktober 2024 erfolgt die nationale Umsetzung mit dem KRITIS-Dachgesetz (KRITIS-DachG). Auch die aktuelle NIS2-Richtlinie wird im Rechtskataster-Online berücksichtigt. Damit haben insbesondere KRITIS-Unternehmen der Energiewirtschaft stets alle relevanten Vorschriften auf dem Radar.

Jetzt aktiv werden

Unternehmen und kommunale Akteure sollten bestehende Schutzmaßnahmen für die Cyber-Sicherheit überprüfen und bei Bedarf anpassen sowie verbessern, um den derzeitigen und künftigen Anforderungen gerecht zu werden und drohende Sanktionen zu vermeiden. Vor diesem Hintergrund ist es wichtig, mit Rechtskataster-Online alle relevanten Änderungen im Blick zu haben. Die abonnierten Vorschriften werden im System automatisch aktualisiert. Sobald sich eine Vorschrift nach dem letzten Log-in geändert hat, wird diese farblich gekennzeichnet. Der Service wurde im Einklang mit den Anforderungen der einschlägigen Normen entwickelt. Im Rahmen von Zertifizierungsaudits wurde er zudem umfassend geprüft. Das spart KRITIS-Betreibern viel Zeit bei der Recherche und Dokumentation von Rechtsvorschriften. Zudem wird letztlich nicht nur die Resilienz gegenüber Cyber-Bedrohungen gestärkt, sondern auch eine zukunftsorientierte Sicherheitsstrategie gefördert.

Das Compliance-Werkzeug Rechtskataster-Online wird ausschließlich als Cloud-Service bereitgestellt, sodass alle Anwender automatisch von den regelmäßigen Updates profitieren. Diese beinhalten sowohl Sicherheitspatches als auch Optimierungen und neue Funktionen. Mit dem Online-Tool können Anwender einschlägige und unternehmensrelevante Gesetze, Vorschriften, Richtlinien und Verordnungen aus den Rechtsbereichen Energierecht, Umweltschutz, Arbeitsschutz und Datenschutz ermitteln, bewerten und deren Einhaltung dokumentieren. Zusätzlich können firmeninterne Vorschriften oder Vorschriften aus anderen Rechtsbereichen erfasst und bereitgestellt werden. Alle Rechtsgebiete stehen als separates Modul zur Verfügung und können frei kombiniert werden. Damit ist die Lösung auch für integrierte Management-Systeme geeignet. ■


Privat; ITC AG

Die Autoren: Volker Sonntag und Sigrid Rehak

Volker Sonntag ist bei der SR Managementberatung GmbH Prokurist, Energieauditor und Fachverantwortlicher für das Rechtskataster-Online. Sigrid Rehak arbeitet im Fachbereich Marketing/PR bei der ITC AG.