Robin Data

Cyber-Attacken betreffen zunehmend Energieversorger

Cyber-Attacken haben sich in den letzten Jahren stark professionalisiert und sorgen allein in Deutschland für bis zu 220 Milliarden Euro Schaden pro Jahr. Laut einer Bitkom-Studie hat sich die Schadenssumme seit 2018 verdoppelt. Cyber-Attacken verursachen den Ausfall von Informations- und Produktionssystemen oder die Störung von internen Abläufen, oftmals durch den Einsatz von Ransomware über Phising-Angriffe.

Insbesondere im Fokus solcher Angriffe stehen Organisationen mit **kritischer Infrastruktur (KRITIS)**, denn hier drohen neben Versorgungsengpässen in der Folge eines Angriffs erhebliche Störungen der öffentlichen Sicherheit und Versorgung. Laut der Bundesregierung wurden im Zeitraum von Januar bis Anfang November 2020 171 erfolgreiche Hackerangriffe auf Einrichtungen der Kritischen Infrastruktur gezählt, 2019 waren es noch 62, das ergibt einen Anstieg um 175 Prozent. In den letzten Jahren sind **Energieversorger** immer häufiger durch Cyber-Attacken angegriffen wurden.

Cyber-Angriffe auf Energieversorger in 2021

Mai
USA
Cyber-Atacke auf Benzin-Pipeline Colonial
Der Betrieb der Pipeline, die 45 Prozent der US-Ostküste versorgt, war komplett eingestellt. Es wurde ein Lösegeld von 3,6 Millionen Euro gezahlt.

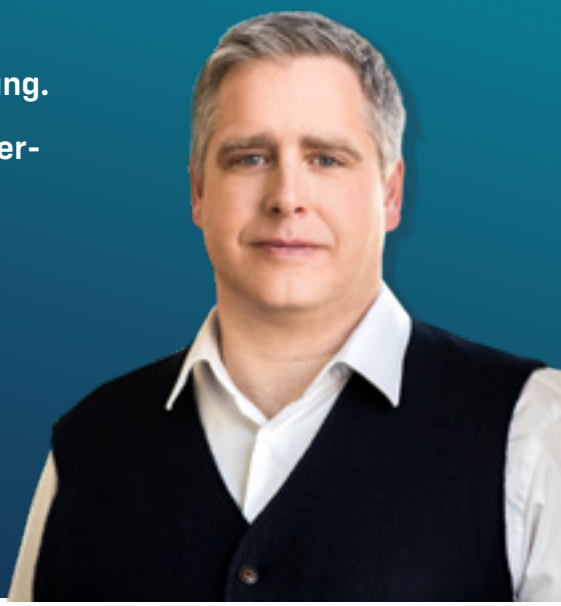
Oktober
Deutschland
Cyber-Attacke Stadtwerke Wismar
Bis heute sind die Stadtwerke im Notbetrieb und können nicht auf Service-, Kunden- und kaufmännische Daten zugreifen.

Oktober
Iran
Cyber-Attacke Bezahlsystem Tankstellen
Bezahlsystem an Tankstellen wurde landesweit lahmgelegt und die Benzinversorgung dadurch blockiert.

Unsere moderne Gesellschaft ist in hohem Maße von einer funktionierenden Energieversorgung abhängig. Betreiber von Energieversorgung unterliegen daher einer großen Verantwortung. Investieren Sie jetzt in das Management Ihrer Informationssicherheit und Ihres Datenschutzes und sichern Sie diese Daten nachhaltig vor Cyber-Attacken.

Wir unterstützen Sie dabei pragmatisch und zielorientiert!

Prof. Dr. Andre Döring, CEO der Robin Data GmbH
Ihr Experte für Datenschutz und Informationssicherheit



Robin Data GmbH | sales@robin-data.io | +49 (0) 3461 4798960 | www.robin-data.io

Robin Data

KRITIS-Sektor Energie: Pflichten, Vorgaben, Gesetzgebung

Selbstüberprüfung mittels interner Audits

- Energieversorger müssen die **Anforderungen des § 8a Absatz 1 BSIG** umsetzen
- Diese Anforderungen beinhalten die Umsetzung eines **Management-Systems für Informationssicherheit (ISMS)** im Geltungsbereich ihrer KRITIS-Anlagen, um KRITIS-Risiken zu mindern. Betreiber können ISMS nach ISO 27001, BSI IT-Grundschutz oder Branchen-Standards in den KRITIS-Anlagen umsetzen.
- Weiterhin sind Energieversorger aufgefordert **Selbstüberprüfungen des ISMS zur Überwachung** des laufenden Betriebes durchzuführen, die Überprüfungen werden auch als interne Audits bezeichnet und finden mindestens jährlich statt.

Interne Audits gemäß Anforderungskatalog zur Konkretisierung der Kriterien des § 8a Absatz 1 BSIG

Nr.	Anforderung an die Betreiber Kritischer Infrastrukturen (KRITIS-Betreiber)	Grundlage (C5 #)
86.	**Interne Überprüfungen der Compliance von IT-Prozessen mit internen Informationssicherheitsrichtlinien und Standards** Qualifiziertes Personal (z. B. Interne Revision) oder durch den **Betreiber der kritischen Dienstleistung beauftragte sachverständige Dritte überprüfen jährlich** die Compliance der internen IT-Prozesse mit den entsprechenden internen Richtlinien und Standards sowie der für den Betrieb der kritischen Dienstleistung rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen. Die identifizierten Abweichungen werden priorisiert und in Abhängigkeit ihrer Kritikalität Maßnahmen zur Behebung zeitnah definiert, nachverfolgt und umgesetzt. Die Prüfung wird regelmäßig durchgeführt. Die Prüfung umfasst auch die Einhaltung der Anforderungen dieses Anforderungskatalogs.	SPN-02
87.	**Prüfungen in anderen, anderweitig vorgegebenen Prüfzyklen – interne IT-Prüfungen** Qualifiziertes Personal (z. B. Interne Revision) des KRITIS-Betreibers oder **durch den KRITIS-Betreiber beauftragte sachverständige Dritte überprüfen mindestens jährlich** die Compliance der IT-Systeme, soweit diese ganz oder teilweise im Verantwortungsbereich des KRITIS-Betreibers liegen und für die Entwicklung oder den Betrieb der kritischen Dienstleistung relevant sind, mit den entsprechenden internen Richtlinien und Standards sowie der für die kritischen Dienstleistungen relevanten rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen. Die identifizierten Abweichungen werden priorisiert und in Abhängigkeit ihrer Kritikalität werden Maßnahmen zur Behebung zeitnah definiert, nachverfolgt und umgesetzt. Der KRITIS-Betreiber verpflichtet seine Unterauftragnehmer zu solchen Prüfungen und lässt sich die Prüfberichte im gleichen Turnus vorlegen und verwertet sie bei seinen Überprüfungen.	SPN-03

Robin Data

Audits gemäß IT-Grundschutz für Energieversorger

Professionelles Audit durch zertifizierte Experten in ganz Deutschland. Profitieren Sie von der langjährigen Erfahrung durch kompetente und praktische Beratung.

Ablauf des Informationssicherheits-Audits

In einem 1-tägigen Workshop führt ein Informationssicherheit-Experte der Robin Data GmbH ein Audit bei Ihnen vor Ort durch. In dem Audit wird der aktuelle Reifegrad des Managementsystems für Informationssicherheit (ISMS) gegen den Standards des IT-Grundschutzes für die Energieversorgung begutachtet. Ergänzend wird auch der aktuelle Reifegrad des Datenschutz-Managementsystems betrachtet.

1

Vorbereitung und Angebot
In einem kostenfreien Erstgespräch mit Robin Data beraten wir Sie unverbindlich zum Thema ISMS-Audit und den Umfang Ihrer Anforderungen. Zur Vorbereitung auf das Audit werden auf Basis einer Anforderungsliste des Kunden die vorhandene Dokumentation und verwendete Richtlinien des ISMS abgefragt.

2

Durchführung des Informationssicherheits-Audits
Während des ISMS-Audits werden interne und externe Sicherheitsvorgaben (Kontrollen, Security Policy und Guidelines), Prozesse und relevante Dokumente überprüft. Offene Maßnahmen dokumentiert und am Ende des Audits priorisiert. Auf dieser Basis werden sicherheitsrelevante Abweichungen von den Standards direkt angegangen.

3

Ergebnis-Gutachten und Maßnahmenkatalog
Anschließend erfolgt die Bewertung unserer Experten über den Zustand des etablierten Informationssicherheits-Managementsystems. Sie erhalten 5-10 Werktage nach Abschluss des ISMS Audits ein zusammenfassendes Gutachten und eine Übersicht der Ergebnisse des Audits. Dieses enthält die Abweichungen zu den Norm-Kontrollen und die priorisierte Maßnahmenliste. Ein Gespräch schließt das Audit ab.

4

Maßnahmenkatalog
Ergebnis der Analyse sind konkrete Handlungsempfehlungen, um die Defizite zwischen “Ist” und “Soll” zu beheben. Die definierten Maßnahmen können bspw. die Erstellung von Richtlinien, die Überprüfung einzelner Sicherheitskonzepte, die Etablierung eines Löschkonzeptes oder die Umsetzung genereller technisch-organisatorischer Maßnahmen sein. Ihre Organisation erhält diese Analyse in Form einer Dokumentation und in Zusammenfassung als Auditbericht.

Umfassende Informationssicherheits-Audits gemäß § 8a Absatz 1 BSIG für Energieversorger

Jetzt Angebot anfordern

Robin Data GmbH | sales@robin-data.io | +49 (0) 3461 4798960 | www.robin-data.io

Robin Data

ISO-zertifizierte Lösungen für Informationssicherheit und Datenschutz bei Energieversorgern

Über 50 TÜV / DEKRA zertifizierte Experten

Beratung regional oder digital

Digitales Datenschutz-Management-System

Das sagen Kunden von Robin Data

„In dem Audit unseres Informationssicherheits-Management-Systems durch die Robin Data GmbH, wurde der aktuelle Reifegrad unseres ISMS gegen den Standard des IT-Grundschutzes auditiert. Interne und externer Prozesse und Dokumente wurden überprüft und offene Maßnahmen dokumentiert. Durch die Beratung und klare Verteilung von Verantwortlichkeiten kennen wir eventuelle Schwachstellen und können diese nun aktiv angehen.

Marco Voigt,
Leiter IT in der Stadtverwaltung Merseburg

„Herr Professor Döring wurde von uns mit der Durchführung eines Datenschutz- und Informationssicherheitsaudits im Jahre 2021 beauftragt. Wir wollten uns Aufschluss über die Angemessenheit und Wirksamkeit bereits ergriffener Maßnahmen und über etwaige Verbesserungsmöglichkeiten verschaffen. Die Zusammenarbeit mit Herrn Professor Döring gestaltete sich sowohl fachlich als auch menschlich sehr erfreulich. Das Audit wurde termingerecht und zügig durchgeführt; die Ergebnisse unverzüglich und verständlich dargelegt. Vor dem Hintergrund dieser positiven Erfahrungen haben wir nunmehr die Robin Data GmbH zum externen Datenschutz- und Informationssicherheitsbeauftragten bestellt.

Dr. Markus Reinhardt,
Geschäftsführer Zentrale Dienste der Industrie- und Handelskammer Halle-Dessau

Die einfache und gesetzeskonforme Umsetzung von Informationssicherheit

Erstberatungsgespräch buchen

Jetzt Angebot anfordern

Robin Data GmbH | sales@robin-data.io | +49 (0) 3461 4798960 | www.robin-data.io