VON NIS2 BIS StromVV

Worauf es im Spannungsfeld der Cyberregulierung wirklich ankommt

Warum Cybersicherheit jetzt wichtiger denn je ist

Ohne Stromversorgung funktioniert nichts. Strom ist die Lebensader unserer modernen Gesellschaft, auf die nicht nur Haushalte, sondern auch essenzielle Branchen wie Telekommunikation, Gesundheitswesen, Wasserversorgung und Finanzsysteme angewiesen sind.

Diese Erkenntnis ist nicht neu, aber aktueller denn je. Tägliche Schlagzeilen und Berichte der europäischen ENISA, dem österreichischen Bundeskanzleramt oder dem deutschen BSI zeigen, wie stark die Gefährdungslage zunimmt. Besonders Energieunternehmen stehen immer häufiger im Fokus von Cyberangriffen.

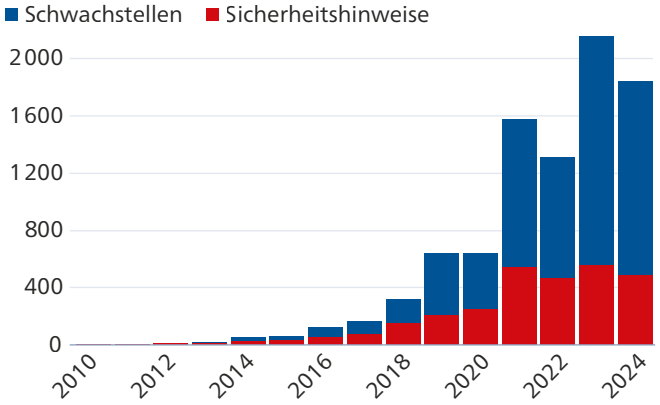
Mit der Digitalisierung hat sich die Energiewirtschaft grundlegend verändert. Neue Technologien eröffnen Chancen, erhöhen aber auch die Risiken. Die zunehmende Vernetzung kritischer Infrastrukturen und ihre Abhängigkeit von IT-Systemen machen sie verwundbarer denn je.

Ein Blick auf die bekannten Schwachstellen zeigt die Dimension des Problems: Hersteller von OT-Systemen veröffentlichen regelmäßig Sicherheitshinweise zu ihren Produkten. Die Anzahl gemeldeter Schwachstellen ist in den letzten Jahren deutlich gestiegen – ein klares Signal, dass sich Bedrohungen im Cyberspace weiter verschärfen. Der Schutz versorgungskritischer Unternehmen vor Cyberangriffen, aber auch vor physischen Attacken ist deshalb lebenswichtig.

Aktuelle Entwicklung der Cybersicherheitsgesetze

Die EU-Richtlinie NIS2 hat seit ihrer Verabschiedung im Jahr 2022 intensive Diskussionen und Auseinandersetzungen zum Thema Cybersicherheit ausgelöst. Sie fordert von den Mitgliedsstaaten, die erweiterten Sicherheitsvorgaben bis Oktober 2024 in nationales Recht umzusetzen – ein Ziel, das von 23 der 27 EU-Staaten bisher verfehlt wurde.

Diese Verfehlung ist bemerkenswert, insbesondere da das Thema Cybersicherheit keineswegs neu ist. Bereits die 2016 eingeführte NIS-Richtlinie verpflichtete die Mitgliedstaaten, ihre kritischen Systeme besser zu schützen.
Mit NIS2 wurde diese Verantwortung verstärkt und auf zusätzliche Wirtschaftssektoren ausgeweitet, darunter die Lebensmittelindustrie und der öffentliche Verkehr.



Anzahl der Schwachstellen und Sicherheitshinweise pro Jahr

*»Die Anzahl gemeldeter Schwachstellen ist in den letzten Jahren deutlich gestiegen – **ein klares Signal, dass sich Bedrohungen im Cyberspace weiter verschärfen.«***

DOCH NICHT NUR IN DER EU SCHREITEN GESETZLICHE REGELUNGEN ZUR CYBERSICHERHEIT VORAN:

USA

Im Mai 2023 aktualisierte die US-Regierung die Umsetzungsplanung ihrer nationalen Cybersicherheitsstrategie. Ziel ist es, kritische Infrastrukturen gezielt gegen Cyberbedrohungen zu schützen. Ein konkretes Beispiel dafür ist die Executive Order 14028, die eine Stärkung der Software-Supply-Chain-Sicherheit vorschreibt.

Schweiz

Mit der Stromversorgungsverordnung (StromVV) wurde am 1. Juli 2024 der IKT-Minimalstandard verpflichtend. Dieser definiert grundlegende Sicherheitsmaßnahmen für Betreiber kritischer Infrastrukturen und andere Unternehmen. Beispiele hierfür sind verpflichtende Schwachstellenanalysen und die Implementierung von Netzwerksegmentierung.

Australien

Die Cybersicherheitsstrategie 2023–2030 bietet einen klaren Rahmen, der durch das Cyber Security Bill 2024 konkretisiert wird. Dieses Gesetz legt neue Standards für die Cybersicherheit von Unternehmen und kritischen Infrastrukturen fest.

Singapur

Mit einem speziell auf OT ausgelegten Cybersecurity Masterplan hat Singapur die Absicherung industrieller Steuerungssysteme als nationale Priorität definiert.

Die Vielzahl dieser existierenden und geplanten Regularien zeigt, dass Cybersicherheit in der Energiewirtschaft keine Option mehr ist, sondern Pflicht. Welche Unternehmen konkret betroffen sind, wird in den Verordnungen der jeweiligen Mitgliedsstaaten definiert. Mit NIS2 werden beispielsweise volkswirtschaftlich wichtige, besonders wichtige und kritische Unternehmen adressiert. Derlei Ausarbeitung der Regelung steht jedoch in vielen Ländern noch aus.

Inhalt der NIS2-Richtlinie

Die NIS2-Richtlinie legt verbindliche Mindestmaßnahmen zur Cybersicherheit fest, die Unternehmen umsetzen müssen. Diese umfassen unter anderem:

- Meldung und Bearbeitung von Sicherheitsvorfällen: Unternehmen müssen Vorfälle in kurzer Zeit an die zuständigen Behörden melden.
- Risikomanagement: Verpflichtung zur Identifizierung und Bewertung von Sicherheitsrisiken.
- Schwachstellenmanagement: Erkennung und Beseitigung von Schwachstellen in IT- und OT-Systemen.

Viele dieser Maßnahmen orientieren sich an anerkannten Standards wie ISO 27001, BSI IT-Grundschutz oder dem NIST Cybersecurity Framework. Verstöße werden mit empfindlichen Sanktionen geahndet, was die Einhaltung der Vorgaben zur geschäftskritischen Aufgabe macht.

Bedeutung für Unternehmen: Wirtschaftliche und sicherheitstechnische Implikationen

Auch ohne die neuen gesetzlichen Anforderungen war es aus unternehmerischer Sicht schon immer ratsam, in Cybersicherheit zu investieren. Jedoch blieben die Renditen solcher Investitionen oft schwer messbar, da verhinderte Betriebsunterbrechungen oder Imageschäden schwer zu beziffern sind.

Mit den neuen gesetzlichen Vorgaben werden Cybersicherheitsmaßnahmen für alle Marktteilnehmer verbindlich. Das sorgt nicht nur für mehr Sicherheit, sondern auch für Chancengleichheit: Unternehmen, die in Sicherheit investieren, erleiden dadurch keinen Wettbewerbsnachteil mehr.

Dadurch werden Investitionen in Sicherheitsstandards, die dem Stand der Technik entsprechen, betriebswirtschaftlich immer sinnvoller. Ein Verstoß gegen die Vorgaben führt nicht nur zu hohen Kosten durch erfolgreiche Angriffe, sondern auch zu Sanktionen.

RELEVANTE GESETZE FÜR DIE ENERGIEWIRTSCHAFT

Cybersicherheitsvorgaben spielen in der Energiewirtschaft eine zentrale Rolle und sind weltweit in zahlreichen Gesetzen geregelt. Eine Auswahl:

- **Energiewirtschaftsgesetz (EnWG) – Deutschland:** Dieses Gesetz regelt unter anderem die Anforderungen an die Sicherheit der Energieinfrastruktur. Es wird mit Inkraftsetzung des NIS2-Umsetzungsgesetzes um gleichwertige Vorgaben ergänzt werden.
- **Stromversorgungsgesetz und -verordnung – Schweiz:** Hier legt der IKT-Minimalstandard verbindliche Maßnahmen für Netzbetreiber, Energieerzeuger und Dienstleister fest.
- **NIS-Umsetzungsgesetz – Österreich:** Das derzeit gültige NIS-Gesetz von 2018 wird durch eine NIS2-Version ersetzt, die aktuell in Entwicklung ist.
- **Critical Infrastructure Cybersecurity Act – USA:** Dieses Gesetz richtet sich speziell auf den Schutz kritischer Infrastrukturen, einschließlich der Energiewirtschaft.
- **Critical Entities Resilience (CER) – EU:** Diese Verordnung verpflichtet Unternehmen, physische Schutzmaßnahmen zur Absicherung kritischer Infrastrukturen zu ergreifen.
- **Cyber Resilience Act (CRA) – EU:** Dieses Gesetz stellt Anforderungen an die Sicherheit digitaler Produkte und an deren Hersteller, um Cyberbedrohungen für die Produktnutzer:innen zu minimieren.

Gleichzeitig hängen viele Cyberversicherungen von der Einhaltung dieser Standards ab. Wer die erforderlichen Maßnahmen (z. B. Notfallmanagement, Backup-Management, Virenschutz) nicht umsetzt, riskiert reduzierten oder gar keinen Versicherungsschutz – was wiederum ein neues Risiko darstellt.

Was sollte man zunächst tun?

Auch ohne finale Klärung der rechtlichen Anforderungen können bereits Vorbereitungen getroffen werden, die die Cybersicherheitsposition Ihres Unternehmens erheblich stärken.

- **Betroffenheitsprüfung durchführen:** Wenn unklar ist, ob Ihr Unternehmen von der NIS2-Gesetzgebung betroffen ist oder sein wird, sollten Sie eine kostenlose Prüfung durch nationale Sicherheitsinstitutionen wie das BSI (Deutschland) oder den WKO Online Ratgeber (Österreich) in Anspruch nehmen.
- **Verantwortlichkeiten definieren:** Benennen und schulen Sie Verantwortliche für die Informationssicherheit der IT- und OT-Systeme. Diese Personen sollten auch als zentrale Kontaktstelle der zu erwartenden Meldepflichten fungieren.
- **Unternehmensleitung einbeziehen:** Die Geschäftsführung muss die Verantwortung für Cybersicherheit übernehmen und dies im gesamten Unternehmen kommunizieren.
- **Sicherheitsstatus ermitteln:** Nutzen Sie Anforderungskataloge wie ISO 27001 Annex A, NIST CSF oder den IKT-Minimalstandard, um den Sicherheitsstatus Ihres Unternehmens zu bewerten und Maßnahmen zu priorisieren. Dienstleister bieten dahingehend auch spezielle Cyber Risk Assessments an.

»Insbesondere in der Anfangsphase können externe Expert:innen bei der Etablierung von Sicherheitsprozessen unterstützen. ***Wichtig ist jedoch, dass das erarbeitete Wissen nachhaltig ins Unternehmen integriert wird.«***

Ein vollständiges Asset-Inventar ist die Grundlage für effektives Risikomanagement und Schwachstellenmanagement, besonders im Bereich OT. Nach dem Prinzip „Nur was ich kenne, kann ich schützen" sollte die Erstellung eines solchen Inventars oberste Priorität haben.

Insbesondere in der Anfangsphase können externe Expert:innen bei der Etablierung von Sicherheitsprozessen unterstützen. Wichtig ist jedoch, dass das erarbeitete Wissen nachhaltig ins Unternehmen integriert wird.

Konkrete Umsetzungshinweise am Beispiel NIS2

Das Managen von Cyber-Risiken ist die zentrale Anforderung an Unternehmen, die unter die NIS2-Gesetzgebung fallen. Wie bereits erwähnt, sollte zunächst das Cyber-Risiko ermittelt werden. Der Prozess umfasst mehrere Schritte:

1. **Identifikation der wesentlichen Betriebsabläufe:** Welche Prozesse sind essenziell für Ihr Unternehmen oder die Erbringung volkswirtschaftlich wichtiger Dienstleistungen?
2. **Ermittlung der relevanten IT-/OT-Komponenten:** Zuordnung der Prozesse zu den entsprechenden Unternehmenswerten wie IT-/OT-Assets oder Gebäuden inklusive Verantwortlichkeiten.
3. **Durchführung der Risikoanalyse:** Mit dem erstellten Asset-Inventar ermitteln Sie Schadenshöhen und Eintrittswahrscheinlichkeiten von Risiken. Hierfür können, müssen aber nicht, einschlägige Standards (ISO 27005, BSI IT-Grundschutz) angewendet werden.
4. **Planung von Maßnahmen:** Reduzieren Sie die Risiken auf ein akzeptables Maß durch Maßnahmen, die dem Stand der Technik entsprechen. Gesetzlich vorgeschriebene Maßnahmen, wie Systeme zur Angriffserkennung in Deutschland, sollten priorisiert umgesetzt werden.
5. **Dokumentation:** Alle Vorgaben, Planungen und Maßnahmenumsetzungen müssen dokumentiert werden. Dies umfasst auch die regelmäßige Kontrolle der Wirksamkeit der getroffenen Maßnahmen.

Folgende Themen sind gemäß der NIS2-Richtlinie in dieser Dokumentation mindestens zu berücksichtigen:

- Risikomethodik für Analyse, Bewertung und Behandlung;
- Vorgaben zur Cybersicherheit von IT- und OT-Komponenten;

- Abläufe und Verantwortlichkeiten für die Behandlung von Sicherheitsvorfällen;
- Geschäftskontinuität, z. B. Backup-Management, Notfallwiederherstellung und Krisenmanagement;
- Sicherheit der Lieferkette und der Beziehungen zu Dienstleistern;
- Sicherheit bei der Beschaffung, Entwicklung und Wartung von Systemen, insbesondere Umgang mit Schwachstellen;
- Strategien zur Bewertung der Wirksamkeit von Cybersicherheits-Maßnahmen;
- Grundlegende Cyber-Hygiene und Schulungen;
- Einsatz von Kryptographie und Verschlüsselung, wo notwendig;
- Sicherheit des Personals, Zugangskontrollen und Asset-Management;
- Verwendung von Multi-Faktor-Authentifizierung oder anderen Authentifizierungsmethoden

Diese Vorgaben sind aus Standards wie ISO 27001 oder dem BSI IT-Grundschutz bekannt und bilden den Kern eines Informationssicherheitsmanagementsystems (ISMS). Für OT-Bereiche, die bisher nicht im Anwendungsbereich solcher Systeme standen, können jedoch Herausforderungen entstehen. Es ist daher sinnvoll, bestehende Prozesse aus der IT-Sicherheit an die Anforderungen der OT-Sicherheit anzupassen.

Fazit

Die neuen Cybersicherheitsgesetze stellen Unternehmen vor große Herausforderungen, bieten jedoch auch eine Chance, den Geschäftsbetrieb nachhaltig zu sichern. Eine strukturierte Herangehensweise ermöglicht die Erfüllung gesetzlicher Anforderungen und die Etablierung eines robusten Sicherheitsniveaus, das nicht nur den gesetzlichen Anforderungen genügt, sondern auch das Vertrauen von Kund:innen und Partner:innen stärkt.

UNTERSTÜTZUNG DURCH OMICRON

Wir bieten umfassende Lösungen, um Ihr Unternehmen bei der Erfüllung der NIS2-Anforderungen zu unterstützen:

StationGuard-Lösung

- **Angriffserkennungssystem:** BSI-zertifiziertes System für Umspannwerke und Leitstellen mit intuitiver Bedienung und SIEM-Integration.
- **Asset-Management:** Automatische Erfassung von IT-/OT-Systemen reduziert den Aufwand für die Erstellung und Pflege von Inventaren.
- **Schwachstellenmanagement:** Präzise Identifikation betroffener OT-Systeme erleichtert das Patchmanagement erheblich.
- **Funktionsüberwachung:** Erkennung von Fehlkonfigurationen und Steigerung der Ausfallsicherheit.

ADMO/Insight

- **Workflow-Optimierung:** Verbesserung von Arbeitsabläufen und Sicherstellung der Datenintegrität und -verfügbarkeit.
- **Datenverwaltung:** Zentralisierte Planung und Organisation von Engineering-, Prüf- und Wartungsaufgaben.

Trainings & Technische Services

- **Risikobewertung:** Durchführung von Security Risk Assessments und Auditvorbereitungen
- Unterstützung bei Erstellung und Realisierung von **Sicherheitskonzepten**
- Sichere OT-Netzwerk-Konfiguration
- **Reaktion auf Vorfälle:** 24/7-Support bei Sicherheitsvorfällen
- **Schulungen:** Maßgeschneiderte Trainings für IT- und OT-Fachkräfte

Unsere Lösungen erleichtern nicht nur die Automatisierung von Sicherheitsprozessen, sondern helfen auch bei der Einhaltung von Normen wie ISO 27001 und den Anforderungen der NIS2-Richtlinie. Weitere Informationen finden Sie unter:

omicroncybersecurity.com