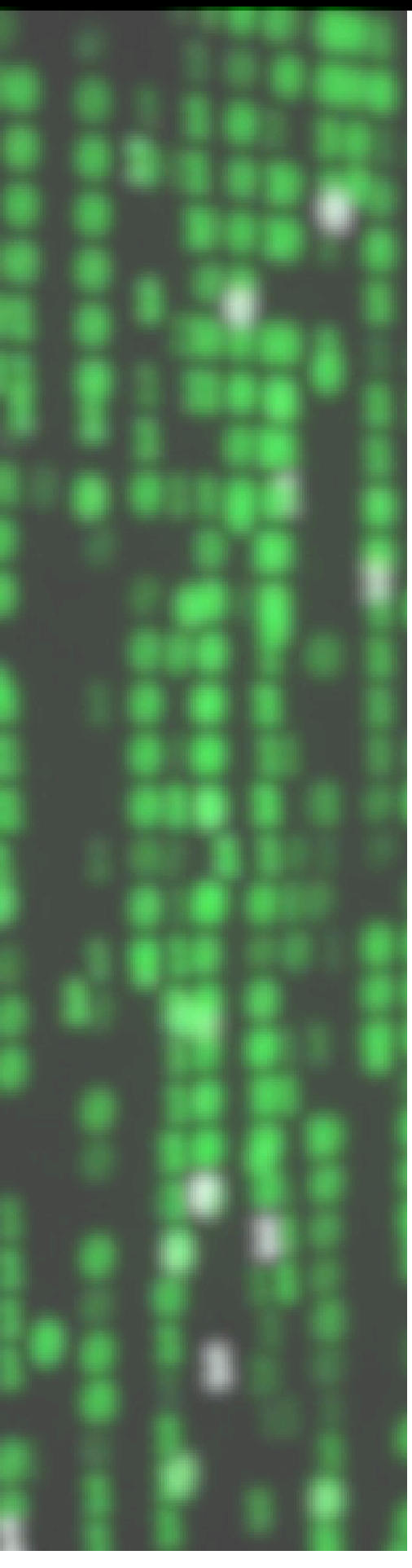
IN 3 PHASEN ZU NIS2

Der Praxisleitfaden für **Energieunternehmen**

BlackMount



INHALT

VORWORT

Cybersicherheit war für Energieunternehmen schon immer mehr als eine technische Aufgabe. Sie ist Teil der Versorgungssicherheit und längst eine Managementverantwortung. Mit der neuen NIS2-Richtlinie wird diese Verantwortung jetzt gesetzlich festgeschrieben: Energieversorger, Netzbetreiber und ihre Zulieferer müssen ihre Sicherheitsstrukturen überprüfen, anpassen und nachweisen können.

Viele Unternehmen stehen dabei vor einer Herausforderung: Die Richtlinie ist umfangreich, die Umsetzung komplex, und die Fristen sind eng. Wer sich jetzt nicht vorbereitet, riskiert nicht nur Bußgelder, sondern auch erhebliche Auswirkungen auf den Netz- und Anlagenbetrieb: von Störungen in Leitstellen über Ausfälle in SCADA-/Leittechniksystemen bis hin zu Einschränkungen im Einspeise- oder Redispatch-Prozess.

Dieser Leitfaden soll Orientierung geben . Verständlich, praxisnah und ohne Juristendeutsch. Er erklärt, was hinter NIS2 steckt, welche Anforderungen speziell auf die Energiebranche zukommen und wie Sie Ihr Unternehmen rechtzeitig in eine sichere Position bringen.

Jannik Christ
Geschäftsführer
CISSP | CCSP | CISM | ISO/IEC 27001 Lead Auditor / Lead Implementer
§8a Prüfverfahrenskompetenz (KRITIS)

NIS2 IM ÜBERBLICK

Was sich ändert und warum es wichtig ist

Die NIS2-Richtlinie (Network and Information Security Directive) ist die überarbeitete EU-Gesetzgebung zur Cybersicherheit. Sie ersetzt die bisherige NIS-Richtlinie aus dem Jahr 2016 und hebt die Anforderungen an Unternehmen deutlich an. Ziel ist es, das Sicherheitsniveau in ganz Europa zu vereinheitlichen und kritische Infrastrukturen, wie die Energieversorgung, besser vor Cyberangriffen zu schützen.

Neu ist vor allem der erweiterte Geltungsbereich. Die Richtlinie erfasst nahezu alle Unternehmen, die an der Erzeugung, Verteilung, Speicherung oder Abwicklung energiewirtschaftlicher Prozesse beteiligt sind. Von Kraftwerksbetreibern über Netzbetreiber bis hin zu IT-/OT-Dienstleistern, Messstellenbetreibern und Marktpartnern.
Damit rückt ein deutlich größerer Teil der Branche in die Verantwortung.

Ebenso verschärft wurden die Pflichten für Geschäftsführungen und Vorstände. Sie müssen nicht nur sicherstellen, dass geeignete Schutzmaßnahmen vorhanden sind, sondern auch deren Wirksamkeit regelmäßig prüfen und dokumentieren. Versäumnisse können künftig persönliche Konsequenzen nach sich ziehen.

Die Richtlinie legt außerdem konkretere Sicherheitsanforderungen fest, von Risikomanagement und Incident Response bis hin zu Meldepflichten und Audit-Nachweisen.
Unternehmen müssen in der Lage sein, Sicherheitsvorfälle schnell zu erkennen, zu melden und nachweislich darauf zu reagieren.
Kurz gesagt: NIS2 ist ein regulatorischer Meilenstein, der sowohl IT- als auch OT-Systeme energiewirtschaftlicher Unternehmen betrifft: von der Leittechnik über Betriebsführungssysteme bis zur Marktkommunikation.
Die Richtlinie verlangt nicht nur Schutzmaßnahmen, sondern ein belastbares Sicherheitsniveau über die gesamte Wertschöpfungskette hinweg.
Sie fordert, Cybersicherheit als Teil der Unternehmensführung zu begreifen und jetzt die Strukturen zu schaffen, die langfristig Stabilität, Vertrauen und Compliance sichern.

DIE ENERGIEBRANCHE IM FOKUS

Warum Ihr Unternehmen jetzt handeln muss

Kaum eine Branche steht im Mittelpunkt der NIS2-Richtlinie so stark wie die Energieversorgung. Strom-, Gas- und Wärmenetze bilden die Grundlage der gesamten Wirtschaft – ein Ausfall hätte unmittelbare Folgen für Industrie, Bevölkerung und nationale Sicherheit. Entsprechend hoch stuft die EU die Verantwortung dieser Unternehmen ein.

Mit NIS2 werden nun auch viele Akteure in der zweiten Reihe erfasst: Netzbetreiber, Energiehändler, technische Dienstleister, IT-Provider und Zulieferer. Wer zur Aufrechterhaltung der Versorgung beiträgt, fällt in den Anwendungsbereich. Unabhängig davon, ob das Unternehmen direkt als „kritische Infrastruktur“ definiert ist oder nicht.

Damit steigt der Druck auf die gesamte Branche, Cybersicherheit nicht länger isoliert in der IT zu verorten, sondern als Teil der Unternehmensstrategie zu behandeln. Hackerangriffe, Lieferkettenvorfälle oder Systemausfälle können heute nicht nur Betriebsstörungen, sondern auch rechtliche und wirtschaftliche Konsequenzen nach sich ziehen.

Viele Energieunternehmen arbeiten bereits nach hohen Sicherheitsstandards, doch NIS2 verlangt mehr: eine durchgängig dokumentierte Sicherheitsorganisation, die IT und OT abdeckt, klare Rollen, vom Netzführungsverantwortlichen bis zum Informationssicherheitsbeauftragten sowie Prozesse, die auch im Störungsfall zuverlässig funktionieren.

Kurzum: Die Energiebranche steht nicht nur im Fokus der Richtlinie, sondern auch im Fokus der Behörden, insbesondere die Bundesnetzagentur (BNetzA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI), die künftig häufiger prüfen und Nachweise einfordern werden.

DIE WICHTIGSTEN PFLICHTEN

Die NIS2-Richtlinie definiert erstmals verbindlich, welche Sicherheits- und Organisationsmaßnahmen Unternehmen umsetzen müssen, um ihre Systeme und Daten zu schützen. Für Energieunternehmen bedeutet das eine klare Pflicht, Strukturen und Prozesse messbar sicher zu gestalten.

Funktionierendes Risikomanagement

Das Risikomanagement umfasst nicht nur klassische IT-Systeme, sondern insbesondere OT-Umgebungen wie Netzleitstellen, SCADA-/ Leittechniksysteme, Schutztechnik, Fernwirktechnik und Anlagensteuerungen. Risiken müssen regelmäßig bewertet und in einer für Behörden nachvollziehbaren Form dokumentiert werden. Dazu gehören unter anderem Zugriffskontrollen, Notfallpläne, Backup-Konzepte und Verfahren zur Wiederherstellung des Betriebs.

Meldepflicht bei Sicherheitsvorfällen

Unternehmen müssen erhebliche Störungen innerhalb von 24 Stunden an die zuständigen Behörden melden und anschließend einen detaillierten Bericht zur Ursachenanalyse vorlegen.

Klare Rollen- und Verantwortlichkeitsverteilung

Geschäftsführung und Sicherheitsbeauftragte müssen nachweisen können, dass sie angemessen über Risiken informiert sind, Schulungen erhalten und die Einhaltung der Sicherheitsvorgaben aktiv überwachen.

Umfassende Dokumentations- und Nachweispflicht

Alle Maßnahmen, Prozesse und Zuständigkeiten müssen so festgehalten sein, dass sie im Rahmen eines Audits jederzeit überprüfbar sind. Unternehmen müssen jederzeit belegen können, wie sie Risiken steuern, Vorfälle behandeln, Leitstellen- und Betriebssysteme absichern, Dienstleister bewerten und technische Maßnahmen im IT- und OT-Bereich überwachen.

VOM GESETZ ZUR PRAXIS

So gehen Sie NIS2 richtig an

Nach der Analyse der Anforderungen steht für Energieunternehmen nun die entscheidende Frage im Raum: Wie lässt sich NIS2 konkret umsetzen?

Die Antwort liegt in einem strukturierten, schrittweisen Vorgehen, das das Thema von Beginn an strategisch verankert.

Zunächst braucht es eine klare Bestandsaufnahme. Unternehmen sollten prüfen, welche Systeme, Prozesse und Dienstleister unter die Richtlinie fallen und welche Schutzmaßnahmen bereits existieren. Eine realistische Bewertung des aktuellen Reifegrads schafft die Grundlage für jede weitere Maßnahme.

Darauf aufbauend folgt die Integration in bestehende Managementstrukturen. NIS2 lässt sich nicht isoliert umsetzen. Es muss mit etablierten Prozessen aus IT-Sicherheit, Compliance und Risikomanagement verzahnt werden. Nur so entstehen Synergien statt Doppelstrukturen.

Im nächsten Schritt gilt es, Verantwortlichkeiten und Kommunikationswege festzulegen. Es muss eindeutig festgelegt sein, wer bei Störungen im Netzbetrieb, in Erzeugungsanlagen oder in der Leittechnik handelt, wer Vorfälle technisch bewertet und wer Meldungen an BSI oder BNetzA auslöst. Klare Eskalationspfade verhindern Verzögerungen in kritischen Situationen.

Wesentlicher Erfolgsfaktor ist zudem die Schulung der Mitarbeitenden. NIS2 verlangt kein Spezialwissen für alle, aber ein gemeinsames Grundverständnis für Sicherheit und Meldeprozesse.

Regelmäßige Trainings schaffen Bewusstsein und fördern eine Sicherheitskultur, die über bloße Richtlinientreue hinausgeht.

Abschließend sollten alle Maßnahmen laufend überprüft und dokumentiert werden. Dazu gehören u. a. OT-spezifische Härtungstests, Restore-Tests in Leitstellenumgebungen, Red-/Blue-Team-Übungen, Tests der Fernwirktechnik sowie strukturierte interne Audits.

So entsteht ein Prozess, der nicht auf kurzfristige Compliance zielt, sondern auf nachhaltige Resilienz. Und das ist letztlich der Kern von NIS2.

TECHNISCHE UND ORGANISATORISCHE ANFORDERUNGEN

Während NIS2 den rechtlichen Rahmen vorgibt, entscheidet die praktische Umsetzung darüber, ob Energieunternehmen tatsächlich widerstandsfähig gegen Cyberrisiken sind. Besonders in der Energiewirtschaft in der physische und digitale Infrastrukturen eng miteinander verknüpft sind, müssen technische und organisatorische Schutzmaßnahmen ineinandergreifen.

Ein zentrales Element ist die Absicherung kritischer Systeme und Netzwerke. Dazu zählen u. a.:

- die Segmentierung zwischen
- IT, OT und Leitstellenumgebungen
- die Härtung von SCADA-/Leittechniksystemen und Schutzgeräten
- die Überwachung energiewirtschaftlicher Kommunikationsschnittstellen
- ein kontinuierliches Schwachstellenmanagement, das auch langlebige OT-Komponenten berücksichtigt

Automatisierte Überwachungssysteme helfen, Anomalien frühzeitig zu erkennen und Angriffe zu stoppen, bevor sie Betriebsprozesse beeinträchtigen.

Auf organisatorischer Ebene spielt die Vorbereitung auf Sicherheitsvorfälle eine entscheidende Rolle. Unternehmen sollten festgelegte Abläufe für die Erkennung, Bewertung und Reaktion auf Vorfälle definieren, inklusive klarer Eskalationswege und Kommunikationsrichtlinien. Diese Prozesse müssen regelmäßig getestet werden, etwa durch simulierte Angriffsübungen oder Notfallproben.

Ein weiteres Kernelement ist die Absicherung der Lieferkette. Da die Energiewirtschaft stark von spezialisierten Dienstleistern abhängt, fordert NIS2 eine systematische Bewertung der Cybersicherheitsstandards von Partnern. Das bedeutet: Verträge sollten Sicherheitsanforderungen enthalten, und Risiken entlang der gesamten Wertschöpfung müssen bewertet werden.

Schließlich darf die dokumentierte Nachvollziehbarkeit nicht fehlen. Technische Maßnahmen sind nur dann wirksam im Sinne der Richtlinie, wenn sie belegt werden können, etwa durch Auditprotokolle, Risikoanalysen oder Nachweise über Mitarbeiterschulungen.

NIS2 verlangt nicht nur moderne Technik, sondern eine integrierte Sicherheitsarchitektur, die sowohl IT- als auch OT-Perspektiven verbindet und sicherstellt, dass energiewirtschaftliche Prozesse auch unter Angriffsdruck stabil bleiben.

AUDITS, NACHWEISE & BEHÖRDEN

Was Sie wissen müssen

Mit der Umsetzung der NIS2-Richtlinie entstehen neue Kontroll- und Nachweispflichten, die weit über bisherige Eigenverantwortung hinausgehen. Künftig wird Cybersicherheit nicht nur gefordert, sondern auch regelmäßig überprüft. Für Energieunternehmen bedeutet das: Die Einhaltung von Sicherheitsstandards muss jederzeit prüfbar und dokumentiert sein.

Die Aufsicht über die Umsetzung obliegt in Deutschland dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sowie branchenspezifischen Behörden, wie der Bundesnetzagentur (BNetzA). Diese Instanzen können Audits anordnen, Unterlagen anfordern oder Sicherheitsprüfungen vor Ort durchführen. Entscheidend ist, dass Unternehmen alle relevanten Nachweise strukturiert und aktuell vorlegen können – von Risikoanalysen über Meldeprotokolle bis hin zu Schulungsnachweisen.

Ein Audit prüft dabei nicht nur, ob Maßnahmen existieren, sondern vor allem deren Wirksamkeit im realen Netz- und Anlagenbetrieb. Behörden erwarten, dass Sicherheitsprozesse gelebt werden. Etwa durch regelmäßige Übungen, dokumentierte Krisenstabsaktivitäten oder Prüfungen der marktseitigen Kommunikationsschnittstellen.

Wichtig ist eine lückenlose Dokumentationsstrategie. Jedes sicherheitsrelevante Ereignis, ob Schwachstellenbewertung, Software-Update oder Awareness-Training, sollte protokolliert werden. Diese Aufzeichnungen bilden im Ernstfall den Beleg, dass Pflichten erfüllt und Risiken aktiv gesteuert wurden.

Unternehmen sollten sich zudem frühzeitig auf mögliche Überprüfungen und Stichproben vorbereiten. Eine interne Auditplanung oder externe Vorprüfung hilft, Schwächen zu erkennen, bevor sie von Behörden festgestellt werden. So wird aus einer Kontrollanforderung ein wertvolles Instrument zur Qualitätssicherung.

Gut vorbereitete Audits sind kein bürokratisches Übel, sondern eine Chance, Vertrauen zu stärken, gegenüber Aufsichtsbehörden ebenso wie gegenüber Partnern und Kunden.
Wer Transparenz zeigt, beweist, dass Sicherheit im eigenen Unternehmen gelebt wird. Und das ist letztlich der beste Nachweis, den NIS2 verlangt.

KOSTENFALLE VERMEIDEN

Was NIS2-Richtlinien wirklich kosten können

Die NIS2-Richtlinie sieht für Verstöße empfindliche Sanktionen vor. Unternehmen, die ihre Pflichten nicht erfüllen oder Sicherheitsvorfälle verspätet melden, riskieren Bußgelder von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes. Je nachdem, welcher Betrag höher ist.

Neben finanziellen Strafen drohen operative Schäden massive Auswirkungen auf den Energie- und Netzbetrieb:
Ausfälle in Leitstellen, Störungen in SCADA-/Leittechniksystemen, Manipulationen an Schutzgeräten, Fehlsteuerungen im Einspeise- oder Redispatch-Prozess oder Unterbrechungen der Marktkommunikation können schnell zu erheblichen Folgekosten führen – technisch, wirtschaftlich und regulatorisch.

Für Geschäftsführungen kommt hinzu, dass NIS2 sie ausdrücklich in die Pflicht nimmt.
Fehlendes Sicherheitsmanagement in kritischen OT-Umgebungen, mangelnde Überwachung energiewirtschaftlicher Kernprozesse oder unzureichende Meldewege können individuelle Haftungsrisiken für technische Leiter, Netzverantwortliche und Vorstände nach sich ziehen.

Viele Kosten entstehen jedoch schon vor einem Vorfall, durch hektische Nachbesserungen, wenn Unternehmen zu spät reagieren. Wer rechtzeitig in Planung, Schulung und technische Modernisierung investiert, reduziert Risiken und langfristig auch Ausgaben.

Ein geordnetes Vorgehen ist daher wirtschaftlich sinnvoller als reaktive Maßnahmen. Frühe Investitionen in Sicherheit schützen nicht nur vor Strafen, sondern stärken Stabilität und Vertrauen. Zentrale Faktoren für die Wettbewerbsfähigkeit in einer zunehmend digitalisierten Energiebranche.

3-PHASEN-PLAN

zur Umsetzung in Ihrem Unternehmen

Die Anforderungen der NIS2-Richtlinie wirken auf den ersten Blick komplex. Mit einem strukturierten Vorgehen lassen sie sich jedoch systematisch und effizient umsetzen. Der folgende 3-Phasen-Plan zeigt, wie Energieunternehmen schrittweise vorgehen können, um Compliance sicherzustellen und gleichzeitig ihre Sicherheitsorganisation zu stärken.

Phase 1: Analyse

Der erste Schritt ist eine gründliche Bestandsaufnahme in Form einer GAP-Analyse.
Gewinnen Sie Klarheit darüber, welche Systeme, Prozesse und Partner unter die Richtlinie fallen.

- Erfassen Sie alle IT- und OT-Systeme sowie deren Verknüpfungen.
- Bewerten Sie, welche dieser Systeme für die Aufrechterhaltung der Energieversorgung kritisch sind.
- Prüfen Sie bestehende Sicherheitsmaßnahmen und Richtlinien.
- Dokumentieren Sie Lücken in einer Gap-Analyse.

3-PHASEN-PLAN

zur Umsetzung in Ihrem Unternehmen

Phase 2: Planung

Legen Sie Verantwortlichkeiten und Ressourcen fest, um die NIS2-Pflichten gezielt umzusetzen.

- Ernennen Sie einen Verantwortlichen (z. B. CISO oder Informationssicherheitsbeauftragten).
- Definieren Sie Rollen und Meldewege intern und gegenüber Behörden.
- Erstellen Sie einen Maßnahmenplan mit Zeitrahmen, Prioritäten und Budgets.
- Schulen Sie Management und Schlüsselpersonal zu neuen Pflichten und Meldeprozessen.
- Integrieren Sie die Maßnahmen in bestehende Sicherheits- und Compliance-Systeme (z. B. ISO 27001 oder IT-Grundschutz).

3-PHASEN-PLAN

zur Umsetzung in Ihrem Unternehmen

Phase 3: Umsetzung und Prüfung

Sie setzen alle definierten Sicherheitsmaßnahmen um, dokumentieren sie sorgfältig und überprüfen Ihre Maßnahmen regelmäßig.

- Implementieren Sie technische Schutzmaßnahmen (Zugriffskontrollen, Patch-Management, Netzsegmentierung).
- Richten Sie Prozesse für Incident-Management, Risikobewertung und Lieferantenprüfung ein.
- Führen Sie interne Audits und Übungen durch – z. B. Leitstellenübungen, Wiederanlaufproben, Red-/Blue-Team-Übungen für OT-Systeme oder Test-meldungen an BSI/BNetzA
- Melden und dokumentieren Sie sicherheitsrelevante Vorfälle gemäß Vorgabe.
- Etablieren Sie eine Routine zur regelmäßigen Aktualisierung Ihrer Sicherheitsstrategie.

FAZIT & HANDLUNGS-EMPFEHLUNGEN

Die NIS2-Richtlinie markiert einen Wendepunkt für die Cybersicherheit in der Energiebranche. Was lange als „Best Practice“ galt, wird jetzt zur Pflicht und betrifft nahezu alle Bereiche der Energieversorgung: Netzführung, Erzeugung, Messwesen, Marktkommunikation sowie alle daran angebundenen IT- und OT-Systeme.

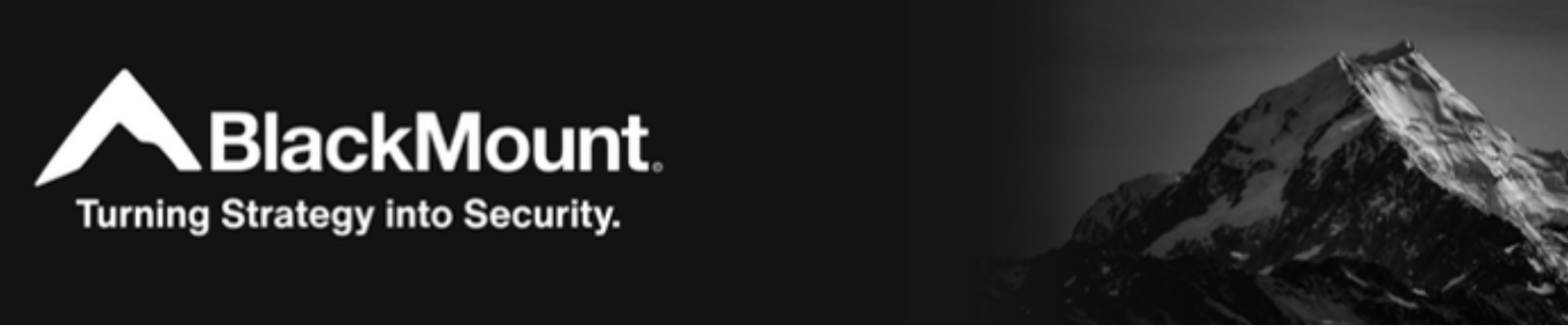
Unternehmen, die frühzeitig handeln, verschaffen sich einen klaren Vorteil: Sie reduzieren Risiken, vermeiden Sanktionen und stärken das Vertrauen von Kunden, Partnern und Behörden.

Starten Sie jetzt mit einer realistischen Bestandsaufnahme, einem klaren Maßnahmenplan und einer gelebten Sicherheitskultur.

Jede Investition in Cybersicherheit ist eine Investition in die Zukunftsfähigkeit Ihres Unternehmens und in die Sicherheit der gesamten Energieversorgung. NIS2 ist kein rein regulatorisches Projekt, sondern eine Chance, die eigene Resilienz zu erhöhen und damit das, was in der Energiewirtschaft am meisten zählt: die Versorgungssicherheit.

BlackMount.

Turning Strategy into Security.



In einer Welt, in der Cyberrisiken zum Tagesgeschäft gehören und gesetzliche Anforderungen stetig steigen, reicht es nicht mehr aus, Informationssicherheit nur technisch zu betrachten.

Unser Antrieb ist es, Informationssicherheit ganzheitlich zu denken: als Zusammenspiel aus unternehmerischer Strategie, Prozessen, Menschen und Technologie. Wir sind davon überzeugt, dass Informationssicherheit dann besonders wirksam ist, wenn sie strategisch im Unternehmen verankert ist, zum Geschäftsmodell passt und nicht als notwendiges Übel betrachtet wird.

Was uns dabei antreibt? Unsere Leidenschaft für exzellente Beratung, unser Anspruch an nachhaltige Wirksamkeit und unser tiefes Verständnis für die realen Herausforderungen in Unternehmen.

Ihr kostenloses NIS 2 Expertengespräch für die Energiebranche

Sie möchten wissen, inwieweit Sie von NIS2 betroffen sind oder benötigen Hilfe zur Umsetzung der Anforderungen in Ihrem Unternehmen?
Buchen Sie sich gerne ein kostenloses Expertengespräch mit einem Experten für kritische Infrastruktur, um Ihre individuellen Fragestellungen zu klären.

Termin buchen

Kontakt

info@blackmount.de

+49 (0) 800 / 5200 112

www.blackmount.de