osanta

NIS-2-RICHTLINIE: HANDLUNGSBEDARF FÜR UNTERNEHMEN IN DEUTSCHLAND

Sind Sie eines der 30.000 betroffenen Unternehmen?

Handeln Sie jetzt – Was Sie wissen müssen und was Sie tun sollten!

Inklusive weiterführender Links

Erhöhung des Cybersicherheitsniveaus in der EU:
Ein umfassender Überblick über die kommenden Herausforderungen und Pflichten

Die NIS-2-Richtlinie der EU soll das Cybersicherheitsniveau in der EU erhöhen. Die Anforderungen an die Cybersicherheit steigen massiv, sowohl für KMU als auch für Zulieferer und Dienstleister von Wirtschaftsunternehmen.

Starten Sie jetzt mit der Umsetzung Ihrer IT-Sicherheitsmaßnahmen, da die EU-Vorgaben bis Oktober 2024 in deutsches Recht überführt werden!

BSKI
Bundesverband für den Schutz Kritischer Infrastrukturen e. V.

bitmi Bundesverband IT-Mittelstand e.V.

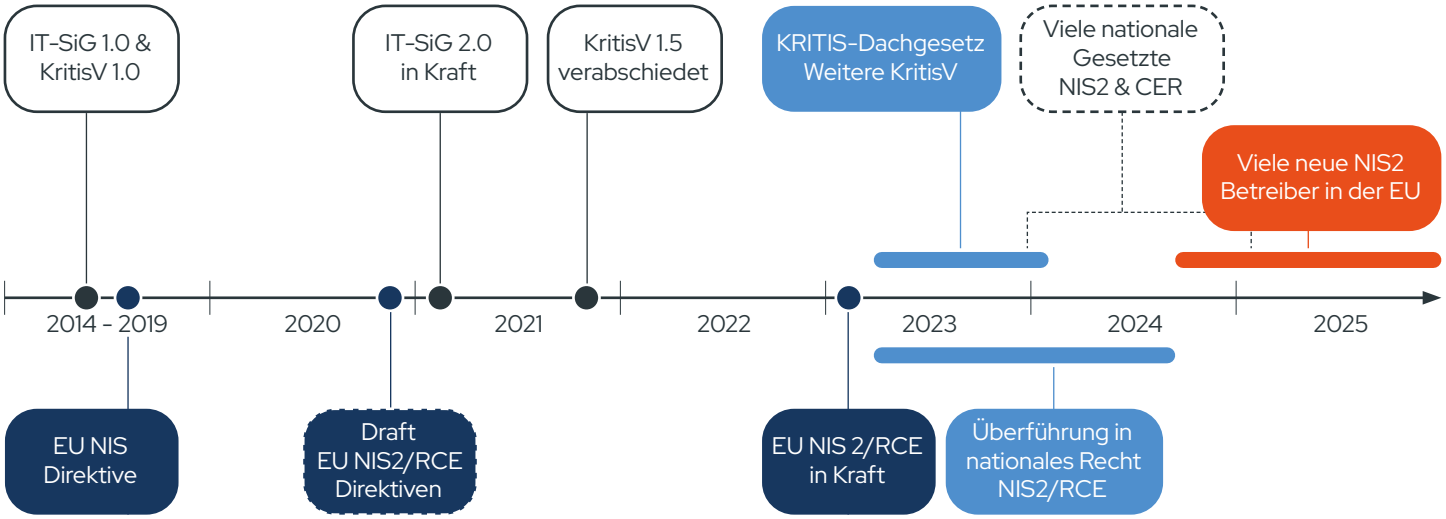
Allianz für Cyber-Sicherheit

Inhaltsverzeichnis

MANAGEMENT SUMMARY

Deutlich mehr Unternehmen betroffen, höhere Bußgelder drohen

Bis Oktober 2024 müssen die EU-Mitgliedsstaaten die „Network and Information Security Directive“ – kurz NIS-2-Direktive – der EU in nationales Recht überführen. Dies wird auch zu Änderungen am BSI-Gesetz, dem IT-Sicherheitsgesetz und der KRITIS-Verordnung führen.



Es wird empfohlen, frühzeitig mit der Umsetzung zu beginnen, um sicherzustellen, dass alle erforderlichen Maßnahmen rechtzeitig umgesetzt werden können. Denn NIS-2 wird die betroffenen Unternehmen zu einigen neuen IT Sicherheitsstandards verpflichten.
Schon jetzt lassen sich die erforderlichen Änderungen und Ergänzungen voraussehen: Sie werden unter anderem die Bereiche Risikomanagement, Vorfallsmeldungen, technische Maßnahmen und Governance betreffen.

Deutlich mehr Unternehmen müssen NIS-2 umsetzen

Der Kreis der Unternehmen, die von der NIS-2 Regulatorik betroffen sind, erweitert sich deutlich. So wird die neue Cybersecurity-Regulierung mindestens 30.000 Unternehmen in Deutschland betreffen, die bisher keine expliziten Vorgaben umsetzen mussten.

Neben den Betreibern kritischer Anlagen (KRITIS) wird es die Klassifizierungen *wesentliche Einrichtungen, wichtige Einrichtungen, Bundeseinrichtungen* und einige Sonderfälle geben.

Was kommt auf die Unternehmen zu?

- Staatliche Befugnisse erweitern sich durch Registrierungspflicht, Nachweis- und Meldepflichten sowie einen verbindlichen Informationsaustausch.
- Bei Nichteinhaltung der Vorschriften drohen erweiterte Sanktionen sowie höhere Bußgelder von bis zu 20 Millionen Euro.
- Sanktionen können gar bis zu einer temporären Einstellung des Geschäftsbetriebs reichen.
- Führungskräfte müssen zukünftig für Security-Vorfälle persönlich haften.

Von den strengeren Vorgaben profitieren

Statt über die Folgen von NIS-2 zu hadern oder mir großem Aufwand die Vorgaben zu umgehen, können Unternehmen durchaus von den strengeren Regeln profitieren. Auch wenn die IT-Security immer auf C-Level aufgehängt sein sollte, wird NIS-2 allein aus Haftungsgründen jetzt ganz oben auf Geschäftsleitungsebene angesiedelt werden müssen. Das macht die Bahn frei für Veränderungen!

Um möglichst schnell und effizient zur NIS-2-Compliance zu gelangen, empfiehlt sich die Zusammenarbeit mit einem erfahrenen Managed Security Service Provider. Dieser entwickelt eine passgenaue Security-Strategie, wählt den geeigneten Technologie-Stack aus und kann die Security-Landschaft zum Fixpreis betreiben. Angesichts des Fachkräftemangels in der IT-Branche kann das ein großer Vorteil insbesondere für kleine und mittelständische Unternehmen sein.

GELTUNGSBEREICH VON NIS-2

Wen betrifft NIS-2?

Während bisher nur große Organisationen aus dem direkten KRITIS-Umfeld betroffen waren, wurden die KRITIS-Sektoren von 11 auf 18 erweitert. Zudem gilt NIS-2 jetzt auch für privatwirtschaftliche Unternehmen.

Im Vergleich zur ursprünglichen NIS unterscheidet die NIS-2 nicht mehr zwischen Betreibern, die wesentliche Dienste anbieten und Betreibern, die digitale Dienste anbieten. Stattdessen werden die Einrichtungen nach ihrer Bedeutung in zwei Kategorien eingeteilt: wesentliche und wichtige Einrichtungen, die jeweils unterschiedlichen Aufsichtsregelungen unterliegen.

Alle in der NIS-2 aufgeführten Sektoren und Organisationen sind für die Mitgliedstaaten der Europäischen Union von grundlegender Bedeutung. Es wird davon ausgegangen, dass eine Störung bzw. Verhinderung der unternehmerischen Leistungserbringung der Gesellschaft schweren Schaden zufügen würde.

Die Unterscheidung in zwei Kategorien trägt der Tatsache Rechnung, dass der Effekt eines Sicherheits-vorfalls auf die Gesellschaft von Sektor zu Sektor unterschiedlich ausgeprägt sein kann.

Als „wichtige" Einrichtung zählen Betriebe bereits ab 50 Mitarbeitern oder/und mehr als 10 Millionen Euro Jahresumsatz. Einige Unternehmen fallen unabhängig von ihrer Größe unter die Direktive, weil sie zu den „kritischen Organisationen" zählen.

BETROFFENE BRANCHEN

Wesentliche Einrichtungen

Große Organisationen in Sektoren mit **hoher Kritikalität** sowie Sonderfälle

Was sind große Organisationen?

> 250 Mitarbeiter
> 50 Millionen € Umsatz
> 43 Millionen € Bilanzsumme

Sektoren mit hoher Kritikalität

- Bankwesen
- Abwasser
- Trinkwasser
- Öffentliche Verwaltung
- Finanzmarktstruktur
- Verkehr
- Gesundheitswesen
- Energie
- Verwaltung von IKT-Diensten
- Digitale Infrastruktur
- Weltraum

Wichtige Einrichtungen

Große Organisationen sonstiger kritischer Sektoren und **mittlere Unternehmen**

Was sind mittlere Unternehmen?

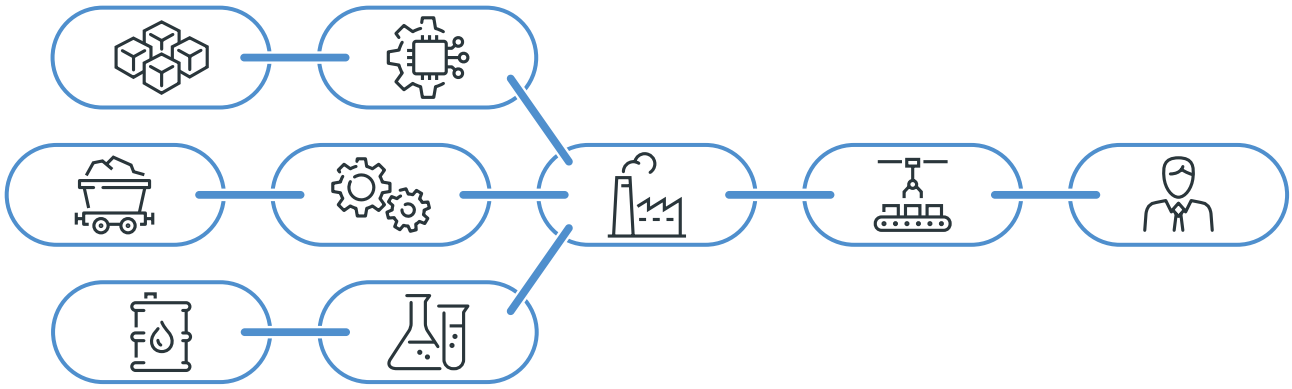
50 - 250 Mitarbeiter
10 - 50 Millionen € Umsatz
< 43 Millionen € Bilanzsumme

Sonstige kritische Sektoren

- Anbieter digitaler Dienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Forschung
- Post- und Kurierdienste
- Verarbeitendes Gewerbe/Herstellung von Waren (elektronische Ausrüstungen und andere)
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln

NEUE PFLICHTEN BEI LIEFERKETTEN

NIS-2 wirkt sich auf eine breite Masse von Unternehmen aus, von denen viele erst auf den zweiten Blick feststellen, dass sie betroffen sind.



Neu ist auch, dass Unternehmen die Cybersicherheit ihrer Zulieferer überprüfen und die Einhaltung der relevanten Regularien durchgängig sicherstellen müssen. Aufgrund der zunehmenden Komplexität in der globalen Wertschöpfungslogistik kann der Ausfall bereits eines Glied seiner Lieferkette zu kritischen Engpässen und weitreichenden Folgeeffekten führen. Wie gefährlich Supply-Chain-Angriffe sein können, hat zum Beispiel der Solarwinds-Hack Ende 2020 gezeigt.
Über ein kompromittiertes Update konnten Angreifer in viele Systeme verschiedener Unternehmen eindringen. Sogar das US-Finanz- und Handelsministerium wurde gehackt.

SCHRITTE ZUR COMPLIANCE

Was wird gefordert?

NIS-2 verpflichtet alle betroffenen Organisationen, sicherheitsrelevante technische und organisatorische Maßnahmen zu ergreifen. Grundlegende Elemente sind die Etablierung eines Mindest-Niveaus an Fachwissen, die Übernahme von Verantwortung durch die Führungskräfte sowie ein wirksames Risikomanagement. Die aktive Einsteuerung effektiver Maßnahmen durch das Management ist somit von zentraler Bedeutung für die Umsetzungsqualität im Sinne der NIS-2 Regulatorik.

Zur Umsetzung der IT-Sicherheitsanforderungen gehören neben der Implementierung von Sicherheitsmechanismen ebenfalls die Umsetzung internationaler Standards wie ISO 27001 oder das NIST-Framework.
Zudem gelten strenge Meldepflichten – ähnlich wie bei der DSGVO – wenn es zu Cybervorfällen kommt. Dabei gelten definierte Meldefristen für die Anzeige des Incidents beim BSI.

Zu den konkreten Vorgaben gehören:

- Reaktion auf Sicherheitsvorfälle
- Absicherung der Lieferkette
- Sicherheit in der Entwicklung, Beschaffung und Wartung
- Verschlüsselung
- Management und Offenlegung von Schwachstellen
- Wirksame Risikoanalysen
- Prüfung und Auditierung von Strategien für die Cybersicherheit
- Erstellung von Krisenmanagement-Plänen zur Aufrechterhaltung des Betriebs
- Meldung von Sicherheitsvorfällen innerhalb von 24 Stunden sowie Detailinfos innerhalb von 72 Stunden
- Schulungen in den Themengebieten Cybersicherheit und Cyberhygiene
- Multi-Faktor Authentisierung und kontinuierliche Authentisierung
- Sichere Kommunikation (Sprach, Video- und Text)
- Sichere Notfallkommunikation

MASSNAHMEN UND IMPLEMENTIERUNG

Welche Maßnahmen müssen Unternehmen angehen?

Artikel 21 der NIS-2-Regel beschreibt grundlegende Kriterien für Cybersicherheitsmaßnahmen, um die Leistungsfähigkeit von IT-Architekturen zu schützen. Demnach sollten die Unternehmen folgende Punkte bei der Umsetzung berücksichtigen:

- Implementierung basierend auf State-of-the-Art Technologien
- Aufbau eines Informationssicherheits-Managementsystems (ISMS), in dem Regeln, Prozesse, Methoden, Tools und Verantwortlichkeiten definiert sind
- Aufbau eines ganzheitlichen und gefahrenübergreifenden Konzepts
- Berücksichtigung europäischer und internationaler Normen

Wichtige Orientierungshilfen bieten unter anderem der BSI-Grundschutz und die ISO/IEC 27001.

Die meisten Unternehmen haben bisher nur Puzzleteile eines ISMS etabliert. Zunächst ist es daher wichtig, Lücken zu identifizieren und diese dann Schritt für Schritt zu schließen. Zahlreiche Rollen müssen besetzt und Policies definiert werden. All das ist meist aufwändiger als gedacht und erfordert Zeit.

So setzen Sie NIS-2 um

Analysieren Sie Sicherheitsrichtlinien und -verfahren sowie die Konfiguration der Netzwerk-Infrastruktur NIS-2 schreibt den Schutz vor Ransomware ausdrücklich vor.

Schulen Sie Ihre Mitarbeiter angemessen technisch und rechtlich – beispielsweise für Phishing per E-Mail, per Facebook-Message oder QR-Code-Betrug.

Schwachstellenmanagement sollte automatisiert dauerhaft laufen.

Sie benötigen Zugriffsbeschränkungen und privilegierte Konten. Aktualisieren Sie besonders Admin-Passwörter regelmäßig.

Verwenden Sie starke Authentifizierungsmethoden, segmentieren Sie Netzwerke. Validieren Sie Zugriffsversuche und analysieren Sie Bedrohungen.

Entwickeln Sie einen Notfallplan: Stellen Sie sicher, dass kritische Systeme auch bei einem Ausfall einzelner Applikationen oder physischer Infrastrukturkomponenten betreibbar bleiben.

Dokumentieren Sie alle Maßnahmen und Prozesse.

Passen Sie Ihre Security-Budgets gegebenenfalls nach oben an.

Bauen Sie ein Security Operation Center (SOC) auf oder nutzen Sie das SOC eines Managed Security Service Providers (MSSP) wie Cosanta.

Teil des SOCs ist eine Security Information and Event Management (SIEM)-Software, die Logdaten sammelt und analysiert.

Setzen Sie Mindeststandards mit konkreten Anforderungen und Erfüllungskriterien für Ihre Lieferanten und Partner. Um eine erfolgreiche Auditierbarkeit zu gewährleisten, ist es empfehlenswert, Reifegrad 3 im Reifegradmodell zu erreichen.
Nach dem Reifegradmodell gehören zu Reifegrad 3 unter anderem:

- formalisierte Richtlinien, Verfahren und Prozesse
- Messung und Überwachung von Risiken
- Suche nach Outsourcing-Möglichkeiten
- Integration von Sicherheitsoperationen in Unternehmenssystemen und -funktionen

Reifegrade und ihre Merkmale (Reifegradmodell BSI)

Reifegrad	Kennzeichen
0	Es existiert kein Prozess, es gibt auch keine Planungen hierzu.
1	Es gibt Planungen zur Etablierung eines Prozesses, jedoch keine Umsetzungen.
2	Teile des Prozesses sind umgesetzt, es fehlt jedoch an systematischer Dokumentation.
3	Der Prozess ist vollständig umgesetzt und dokumentiert.
4	Der Prozess wird darüber hinaus auch regelmäßig auf Effektivität überprüft.
5	Zusätzlich sind Maßnahmen zur kontinuierlichen Verbesserung vorhanden.

VOM PROOF OF CONCEPT ZUM BETRIEB

In 4 Wochen vom Proof of Concept zum Betrieb:

Da jetzt schon weitgehend klar ist, welche Standards durch NIS-2 erfüllt werden müssen, sollten betroffene Organisationen zügig mit den Vorbereitungen beginnen, um nicht unter Zeitdruck zu kommen. Insbesondere für Unternehmen, die bei angespanntem Fachkräftemarkt über geringe Inhouse-Expertise verfügen, bieten sich Managed Security Services wie die der Cosanta an. Sie halten die Anfangsinvestitionen in Grenzen und ermöglichen den späteren Betrieb weitestgehend zu kalkulierbaren, monatlichen Fixpreisen.

Mit einem standardisierten Methodenansatz von der Analyse über den Proof of Concept bis hin zum Betrieb der notwendigen Lösungen werden Unternehmen in die Lage versetzt, die Anforderungen von NIS 2 innerhalb eines Zeitfensters von nur 4 Wochen zu erfüllen.

Analyse

- Bestandsaufnahme
- Asset Gruppierung & Schutzbedarfsfeststellung
- IT & Security Prozesse
- Asset-management
- Roll-Out Infrastruktur

Proof of Concept

- Roll-Out der Agents
- Schärfung der Loganalyse & Incident-Erkennung
- Klärung der Berichtswege
- Ggf. Anpassung der Prozesse
- Optimierung

Betrieb

- Übernahme in den Betrieb, basierend auf ISO27001 & IT-Grundschutz der BSI
- Kontinuierliche Schärfung der Loganalyse
- Meldung & Reporting
- Optional 24/7

Der erste Schritt umfasst eine Bestandsaufnahme aller IT-Komponenten, die mit den Core-Systemen vernetzt und angreifbar sind. Dazu zählt auch die Analyse der Logfiles, also der Auswertung aller protokollierten Vorgänge innerhalb des IT-Verbunds. Es werden alle Aktivitäten von Servern, Anwendungen und Mitarbeitenden sowie ihre „Endpoints" dokumentiert. Dazu können neben dem Zugriff über Desktops auch Logs über Smartphones, Tablets oder Laptops gehören sowie Maschinen, die automatisiert Daten an zentrale Systeme senden.

Auf Basis dieser Daten, lässt sich dann der aktuelle Security-Status und die Widerstandsfähigkeit Ihrer IT-Infrastruktur feststellen. Dies dient als Grundlage für das technische und prozessuale Konzept und den späteren Roll-out der notwendigen Systeme und sonstigen Maßnahmen. In der Proof of Concept-Phase rollen wir die Security-Maßnahmen aus und schärfen sie anhand der Logs sowie erkannten Incidents nach, um sie auf die individuellen Erfordernisse Ihres Unternehmens zuzuschneiden. Auch wenn die Schärfung eine Daueraufgabe ist, können die Security-Systeme nach kurzer Zeit in Betrieb gehen.

KERNSYSTEME FÜR IHRE IT-SICHERHEIT

Auf Basis dieser Daten, lässt sich der aktuelle Security-Status und die Widerstandsfähigkeit der IT-Architektur feststellen. Dies dient als Grundlage für das technische und prozessuale Konzept und den späteren Roll-out der notwendigen Systeme und sonstigen Maßnahmen. In der Proof of Concept-Phase werden die Security-Maßnahmen ausgerollt und optimiert: Anhand von Logs sowie erkannter Incidents werden die Sicherheitsmaßnahmen spezifisch auf die individuellen Unternehmens-Erfordernisse zugeschnitten. Die Security-Systeme können so bereits nach kurzer Zeit in Betrieb gehen und werden anschließend fortwährend weiter geschärft.

Dazu zählen:

ISMS – Information Security Management System

Im ISMS sind Regeln, Verfahren, Maßnahmen und Tools definiert, mit denen sich die IT-Sicherheit steuern, kontrollieren, sicherstellen und optimieren lässt. Essenziell für ein ISMS ist die Umsetzung in allen Bereichen und Ebenen der Organisation. Die IT-Grundschutz-Kataloge des BSI stellen ein Konzept für die Umsetzung eines ISMS dar. Die Einführung und der Betrieb eines ISMS ist herausfordernd und bedarf meist externer Fachunterstützung.

NIDS – Network-based Intrusion Detection System

NIDS überwachen den Datenverkehr eines Unternehmensnetzes. Dabei empfiehlt sich meist, das Netzwerk in einzelne Segmente zu unterteilen und den Datenverkehr in jedem Einzelsegment zu überwachen. Die Analyse der Daten kann feststellen, ob es sich bei einem Datenverkehr um normalen Traffic oder um einen Angriff handelt. Das System nutzt dafür unter anderem eine „Rote Liste", die gefährliche Datenverkehre definiert.

SIEM – Security Information Event Management

Ein SIEM-System ist das Herzstück jedes Security-Konzepts. Es sammelt automatisiert Informationen aus IT-Infrastrukturen und wertet diese aus. Ein Großteil der im SIEM gesammelten Daten besteht aus Logfiles. Diese Logs von Serversystemen, der Netzinfrastruktur, zentralen Anwendungen und Clients werden im zentralen Log Management gesammelt und im SIEM ausgewertet. Auswertungen erfolgen aufgrund hinterlegter Policies oder über eine Anomalie-Erkennung auf Basis von statistischen Auswertungen und künstlicher Intelligenz.

Da der Aufbau und Betrieb eines SIEMs aufwändig ist, bietet es sich an, SIEM-Technologie als Managed SIEM zu buchen und von der Kompetenz eines zentralen SIEM-Betreibers zu profitieren. Für den Betrieb einer SIEM-Lösung brauchen Unternehmen gut ausgebildete Analysten. Zudem sollte eine 24x7-Überwachung und -Reaktion auf Sicherheitsvorfälle gewährleistet sein - eine Aufgabe, die für kleine und mittlere Unternehmen kaum zu stemmen ist. Weiterhin benötigt ein SIEM-System eine kontinuierliche Optimierung, um es an die ständig wechselnde Bedrohungslage anzupassen.

Die Erfahrung mit dem Eigenbetrieb eines SIEMs zeigt, dass die Fehlerrate sehr hoch ist. Dies liegt meist an knappen finanziellen, personellen und zeitlichen Ressourcen sowie fehlender Expertise. Daraus können Ineffizienzen entstehen: Wichtige Events werden nicht erkannt, oder es werden zu viele Fehlalarme ausgelöst, die wertvolle Zeit in Anspruch nehmen.

Gemanagtes SIEM

Es wird daher empfohlen, ein gemanagtes SIEM – z.B. von Cosanta - zu nutzen, das in folgenden Schritten aufgebaut wird:

1. **Kickoff-Workshop**
   Bestandsaufnahme der IT-Infrastruktur, Erfassen aller protokollierenden Systeme im IT-Verbund sowie Durchführung einer IT-Sicherheitsanalyse.

2. **POC (Proof of Concept)**
   Ausrollen der für das SIEM benötigten Agents auf Testsysteme und Netze. Im POC wird die Funktionalität der Komponenten demonstriert.

3. **Begleitetes Rollout**
   Erweiterung des Agent-Rollouts auf die gesamte IT-Infrastruktur. Dieser Vorgang wird durch einen Cyber Security-Experten durchgeführt – das SIEM wird in Betrieb genommen.

4. **Begleitete Lernphase**
   In der KI-Lernphase des SIEM-Systems wird das Regelwerk optimiert und ein aussage-kräftiges Reporting aufgesetzt.

5. **SIEM Incident Response & mehr**
   Je nach gebuchtem SLA werden kritische Incidents aktiv gemeldet. Optional wird das SIEM als Managed Security Service bis hin zum Full Service-SOC im 24/7-Betrieb begleitet.

SOC – Security Operation Center

Einen Schritt weiter geht ein Security Operation Center, in dem SIEM und Schwachstellenmanagement vereint sind. Ein Managed SOC spart Erstinvestitionen sowie laufende Ressourcen, ist schnell betriebsbereit und hat das SIEM als grundlegenden Services mit im Gepäck.
Ein Managed SOC entlastet Ihre eigenen IT-Mitarbeitenden, ist skalierbar und bietet Ihnen mit regelmäßigen Reports und einem Zugriff auf das auf Sie zugeschnittene Dashboard jederzeit eine hohe Transparenz über die aktuelle Sicherheitslage. Wir nutzen dafür aktuelle Tools und die neuesten Technologien mit KI.

GEMEINSAM ZUR NIS-2 COMPLIANCE: COSANTAS EXPERTISE FÜR IHR UNTERNEHMEN

Cosanta steht Unternehmen als kompetenter Dienstleister im Bereich der Cyber-Sicherheit zur Seite, um den Anforderungen der NIS-2-Richtlinie gerecht zu werden. Durch gezielte Beratung und dem Einsatz intelligenter SOC-Dienste unterstützt Cosanta Firmen als externes IT-Sicherheitsteam. Besonders im Fokus steht dabei die Unterstützung von Unternehmen aus kritischen Bereichen, um erhöhte Sicherheitsstandards gemäß KRITIS, IT-Grundschutz und ISO 27001 zu erfüllen.

Mit Cosanta erhalten Unternehmen eine klare Anleitung und praktische Unterstützung, um die notwendigen Sicherheitsmaßnahmen zu implementieren und stets aktuell zu halten. Cosanta bringt dabei umfassende Erfahrung und Verständnis für die spezifischen Sicherheitsherausforderungen mit, die mit NIS-2 einhergehen. Unternehmen profitieren von einem erfahrenen Partner, der hilft, die IT-Sicherheit fortlaufend zu verbessern und an neue Bedrohungen anzupassen.

Die Zusammenarbeit mit Cosanta bedeutet für Sie, einen zuverlässigen Begleiter an Ihrer Seite zu haben, der Sie nicht nur auf dem Weg zur Einhaltung der Richtlinie unterstützt, sondern auch dabei, eine Kultur der Cybersicherheit zu etablieren. Cosanta bietet somit einen klaren Pfad, um die NIS-2 Compliance sicher und ohne Umwege zu erreichen.

BSKI
Bundesverband für den Schutz Kritischer Infrastrukturen e. V.

bitmi Bundesverband IT-Mittelstand e.V.

Allianz für Cyber-Sicherheit

KONTAKT

Cosanta

Büroadresse und Besucherempfang:
Cosanta GmbH, c/o Coworking Orangery
Prinzenstraße 2a
42697 Solingen

Sales@Cosanta.de
0212 / 520 8232 0