etengo
SMART FREELANCING

NIS-2

Wie Ihr Unternehmen der europäischen Cybersecurity-Richtlinie gerecht wird.

Für mehr Cybersecurity: NIS-2

Die NIS-2 Richtlinie ist ein zentrales Regelwerk, mit dem die **Cybersecurity** und der **Schutz kritischer Infrastrukturen** innerhalb der Europäischen Union gestärkt wird.

Indem NIS-2 klare Regeln und Maßnahmen für Unternehmen festlegt sowie **verbindliche Sicherheitsstandards** und rechtliche Vorgaben definiert, stärkt die Richtlinie europaweit die **Resilienz gegen Cyberbedrohungen**.

Die zukünftige Richtlinie erfordert unter anderem eine schnelle Reaktion auf Cybersicherheitsvorfälle, die für die meisten Unternehmen ohne Vorbereitung nicht realisierbar ist.

Unternehmen sollten daher jetzt handeln, um die Anforderungen der NIS-2 Richtlinie zu erfüllen:

Um ihre Unternehmenswerte zu schützen!

Um rechtliche Konsequenzen zu vermeiden!

Inhalt

Management Summary

Die NIS-2 Richtlinie – die Abkürzung NIS-2 steht für Network-and-Information-Security-Richtlinie 2.0 – ist ein zentrales Regelwerk, mit dem die Cybersicherheit und der Schutz kritischer Infrastrukturen innerhalb der Europäischen Union durch die Etablierung strengerer Cybersicherheitsstandards geschützt werden soll.

Die NIS-2 Richtlinie erweitert unter anderem den Kreis der Unternehmen, die verpflichtet sind, sich aktiv um ihren Cyberschutz zu kümmern, deutlich. Sie definiert strengere Sicherheitsvorgaben, stärkt das Meldewesen und optimiert das Krisenmanagement.

Ist Ihr Unternehmen von NIS-2 betroffen, sind Sie dazu verpflichtet, die Sicherheitsmaßnahmen umgehend umzusetzen.
Denn bei Verstößen drohen hohe Bußgelder.
Achtung: Führungskräfte haften persönlich!

Das NIS-2 Umsetzungsgesetz ist am 06.12.2025 in Kraft getreten.

Spätestens ab dem 6. März 2026 müssen sich betroffene Unternehmen in Deutschland beim BSI (Bundesamt für Sicherheit in der Informationstechnik) registrieren und geeignete Maßnahmen zur Vorbeugung und Abwehr von Cyberattacken einrichten.

Als spezialisierter Personaldienstleister für den projektbasierten Einsatz von Digital- und IT-Experten unterstützt Sie Etengo bei der erfolgreichen Umsetzung der NIS-2 Richtlinie und der Implementierung notwendiger Maßnahmen.

Wachsende Bedrohung

NIS-2 ist die Antwort auf die wachsende und immer komplexer werdende Bedrohungslage im digitalen Raum, die Unternehmen – aller Größen und aller Branchen – sowie staatliche Einrichtungen in ganz Europa bedroht. Jedes zweite Unternehmen war bisher von einem Cyberangriff betroffen. Tendenz steigend. Unternehmen sind heute mit verschiedenen Entwicklungen konfrontiert, die eine stärkere Cybersecurity und höhere Resilienz gegenüber Cyberangriffen erfordern, mit denen Cyberkriminelle Netzwerke stören, Dienste lahmlegen, geistiges Eigentum, sensible oder personenbezogene Daten stehlen bzw. Finanzdaten manipulieren wollen.

Wachsende Professionalisierung der Cyberkriminellen

Die Anzahl der schwerwiegenden und hochprofessionell ausgeführten Cyberangriffe nimmt Jahr für Jahr zu.

Professionellere Tools

Potente KI-Tools und illegale Plattformen machen es Cyberkriminellen heute einfacher denn je, auch hochkomplexe Angriffe auszuführen.

Anstieg von Remote-Work

Die steigende Nutzung von ungeschützten privaten Endgeräte und unzuverlässigen Verbindungen potenziert die Möglichkeiten von Cyberkriminellen.

Bedrohungen aus dem Ausland

Durch globale Spannungen und nationale Konflikte nehmen staatlich finanziertes Hacking, Cyber-Spionage und Cyber-Kriegsführung zu.

Steigende Bedrohung von Schlüsselindustrien.

Diese Zunahme von Cyberbedrohungen gefährdet besonders Schlüsselindustrien und wichtige Branchen. Diese sind vor allem daher lohnenswerte Ziele für Cyberkriminelle, da hier jede Serviceunterbrechung sofort behoben werden muss. Diese Dringlichkeit macht sie unter anderem anfällig für Erpressungen.

Ziele von NIS-2

Um der Bedrohungslage gerecht zu werden, stärkt NIS-2 die digitale Resilienz und geht beim Bedrohungsmanagement über die 2016 eingeführte Vorgänger-Richtlinie NIS-1 hinaus. NIS-2 dient darüber hinaus als Roadmap für störungsfreie Geschäftsabläufe, für die Optimierung der Zusammenarbeit und für die Förderung einer Sicherheitskultur, in der die Mitarbeitenden sichere Verhaltensweisen verinnerlichen.

Mit NIS-2 soll Folgendes erreicht werden:

- Identifikation kritischer Informationssysteme durch Asset-Management-Verfahren
- Planung und Etablierung von Risikomanagement-Abläufen
- Absicherung der Lieferkette
- Definition und Umsetzung von Cybersicherheits-Strategien
- Sensibilisierung der Mitarbeitenden durch regelmäßige Schulungen
- Ausarbeitung von Reaktionsplänen & Protokollen für die Abwicklung von Vorfällen
- Gewährleistung der durchgängigen Verfügbarkeit kritischer Dienste bei Sicherheitsvorfällen
- Gewährleistung einer schnellen und effizienten Reaktion auf Zwischenfälle
- Zuverlässige Meldung von Vorfällen bei zuständigen Stellen

Ist Ihr Unternehmen betroffen?

NIS-2 betrifft öffentliche und private Einrichtungen, Organisationen und Unternehmen, die wesentliche oder kritische Services für Wirtschaft und Gesellschaft erbringen. Und das direkt sowie indirekt, da auch die jeweiligen Lieferketten geschützt werden müssen.

Unternehmen müssen selbständig prüfen, ob sie NIS-2 betrifft und sich auch selbstständig registrieren.

Es erfolgt keine Information von offizieller Stelle. Prüfen Sie jetzt selbst, ob Ihr Unternehmen betroffen ist:

www.bsi.bund.de

NIS-2 gilt für „wesentliche“ und „wichtige“ Einrichtungen

Die NIS-2 Richtlinie unterscheidet zwischen wesentlichen und wichtigen Einrichtungen, wobei die Sicherheitsanforderungen identisch sind, Unterschiede werden nur bei der notwendigen Ausprägung und den drohenden Sanktionen gemacht.

Wesentliche Einrichtungen

Energie
Stromversorgung
Fernwärme/-kälte
Kraftstoff, Heizöl, Gas

Wasser
Trinkwasser
Abwasser

Finanzinstitute
Banken
Finanzmarkt-infrastruktur

Transport (Infrastruktur)
Luftverkehr
Schienenverkehr
Schiffahrt
Straßenverkehr

Gesundheit
Dienstleistung
Referenzlabore
F&E
Pharma & Medizinprodukte

IT & TK
IXPs, DNS,
Cloud Provider
Kommunikation
Security Services
Rechenzentren

Weltraum
Bodeninfrastruktur

Wichtige Einrichtungen

Transport
Paketdienste
Kurierdienste
Expressdienste

Entsorgung
Abfall-bewirtschaftung

Chemie
Herstellung & Vertrieb
Produktion
Handel & Vertrieb

Lebensmittel
Großhandel
Produktion
Verarbeitung

Verarbeitendes Gewerbe
Medizin
Diagnostik
Maschinenbau
Fahrzeugbau
KFZ-Zulieferer

Digitale Dienste
Marktplätze
Suchmaschinen
Soziale Netzwerke

Forschung
MPI
RKI
Fraunhofer

Folgen bei Nichteinhaltung

In der NIS-2 Richtlinie sind grundlegende Sanktionen für Verstöße im Hinblick auf die Cyber-Sicherheitsmaßnahmen und Meldepflichten festgelegt. Die Strafen für Unternehmen, die die vereinbarten Fristen nicht einhalten, können unterschiedliche Formen haben. Die konkrete Art der Strafe variiert je nach Organisation und Abweichung zwischen der geforderten und der tatsächlichen Implementierung.
Bei Verstößen drohen folgende Konsequenzen:

Nicht-Monetäre-Rechtsmittel

Dazu gehören Compliance-Verfügungen, verbindliche Anweisungen, Umsetzungsverordnungen für Sicherheitsprüfungen und Verfügungen für Bedrohungsmeldungen an Ihre Kunden.

Geldbußen

Je nachdem, welcher Betrag höher ist, können bei Verstößen wesentliche Einrichtungen mit einer Geldbuße bis zu 10 Mio. Euro oder 2% des weltweiten Umsatzes und wichtige Einrichtungen mit einer Geldbuße bis zu 7 Mio. Euro oder 1,4% des weltweiten Umsatzes geahndet werden.

Private Haftung

NIS-2 nimmt das Top-Management ab C-Level in die Verantwortung: Wenn aufgrund grober Fahrlässigkeit der Organisation ein Cybervorfall auftritt, haften Geschäftsführer und Vorstände persönlich.

Als spezialisierter Personaldienstleister für den projektbasierten Einsatz von Digital- und IT-Experten unterstützt Sie Etengo bei der erfolgreichen Umsetzung der NIS-2 Richtlinie und der Implementierung notwendiger Maßnahmen.

Konkrete Anforderungen

NIS-2 soll die Resilienz und die Reaktion auf Sicherheitsvorfälle des öffentlichen und privaten Sektors in der EU verbessern. Falls Ihr Unternehmen zu den betroffenen Einrichtungen zählt, müssen Sie verschiedene aufeinander aufbauende Anforderungen erfüllen und Management-Maßnahmen ergreifen. Das Topmanagement haftet dafür.

Wie und wo sind Sie verwundbar?

Implementierung einer zentralen Plattform für das effektive Management von identifizierten Schwachstellen sowie das Steuern von Penetrationstests.

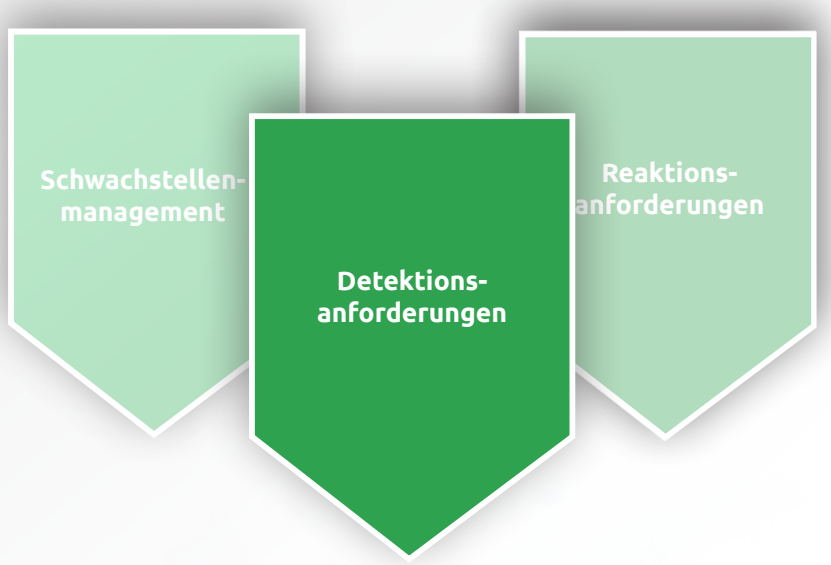
Was müssen Sie alles überwachen?

- Netzwerkverkehr
- Anmeldevorgänge
- Administrative Aktivitäten
- Datenabflüsse
- Richtlinienverstöße
- Datenintegrität
- uvm.

Wie müssen Sie reagieren können?

Etablierung von strukturierten Reaktionen auf Sicherheitsvorfälle, die eine schnelle und wirksame Bewältigung gewährleisten, sowie von Prozessen die eine Meldung im Rahmen der gesetzten Fristen sicherstellen.

Neue Detektionsanforderungen durch NIS-2



Relevante Bausteine und dafür benötigte Expertise

Protokollierung & Überwachung

Planung & Implementierung einer kontinuierlichen Überwachung und Protokollierung sicherheitsrelevanter Ereignisse.

Senior Cybersecurity Consultant

- Protokollierung & Speicherung (Splunk, Elastic, Sysmon)
- Strategische IT-Security Beratung (Architektur, Design, Implementierung einer ganzheitlichen Protokollierung)

SIEM-System

Implementierung eines SIEM-Systems für die Bereitstellung von Detektion, Analyse, Reaktion und Dokumentation um auftretende Sicherheitsvorfälle im Netzwerk Ihres Unternehmens zu erkennen und zu visualisieren.

Senior Cybersecurity Consultant

- SIEM-System (Splunk, Elastic, QRadar, MS Sentinel)
- Strategische IT-Security Beratung (Architektur, Design, Implementierung eines SIEM-Systems)
- Schnittstellen Anbindung

Threat Intelligence

Integration von TI-Feeds um kontinuierlich aktuelle Daten über Cyberbedrohungen, Schwachstellen und Angriffstechniken zu erhalten.

Senior Cybersecurity Consultant

- Threat Intelligence (MISP, Anbindungen, IOC-Bewertung)
- Strategische IT-Security Beratung (Architektur und Design einer TI-Integration)
- Schnittstellen Anbindung

Endpoint Detection & Response (EDR)

Implementierung einer EDR-Lösung für einen effektiven & effizienten Schutz der Endpunkte im gesamten Unternehmen.

Senior Cybersecurity Consultant

- EDR-Lösung (Crowdstrike, Microsoft APT, paloalto Cortex XDR)
- Strategische IT-Security Beratung (Architektur und Design einer EDR-Lösung)
- Schnittstellen Anbindung

Neue Schwachstellenmanagement-Anforderungen durch NIS-2

Relevante Bausteine und dafür benötigte Expertise

Regelmäßige Schwachstellenscans

Um potenzielle Sicherheitslücken Systemen und Netzwerken zu identifizieren.

Cybersecurity Consultant

- Schwachstellen Management Experte (Qualys, Tenable, Pentera)
- Bewertung und Qualitätssicherung der Schwachstellenscans

Schwachstellenbewertung & -priorisierung

Etablierung von Prozessen zur Bewertung und Priorisierung der identifizierten Schwachstellen, um eine rechtzeitige Behebung der Schwachstellen auf Basis ihrer Kritikalität sicherzustellen.

Cybersecurity Consultant

- Schwachstellen Management Experte (Qualys, Tenable, Pentera)
- Bewertung und Priorisierung der Schwachstellenscan-Ergebnisse

Penetrationstests

Durchführung von Penetrationstests, um die Sicherheit der Systeme zu überprüfen und Schwachstellen zu identifizieren, die durch die regelmäßigen Scans möglicherweise nicht entdeckt wurden.

Penetrationstester

- Manuelle Penetrationstests
- Automatisierte Penetrationstests (Pentera)
- Identifizieren und bewerten von Schwachstellen
- Red Team Experte

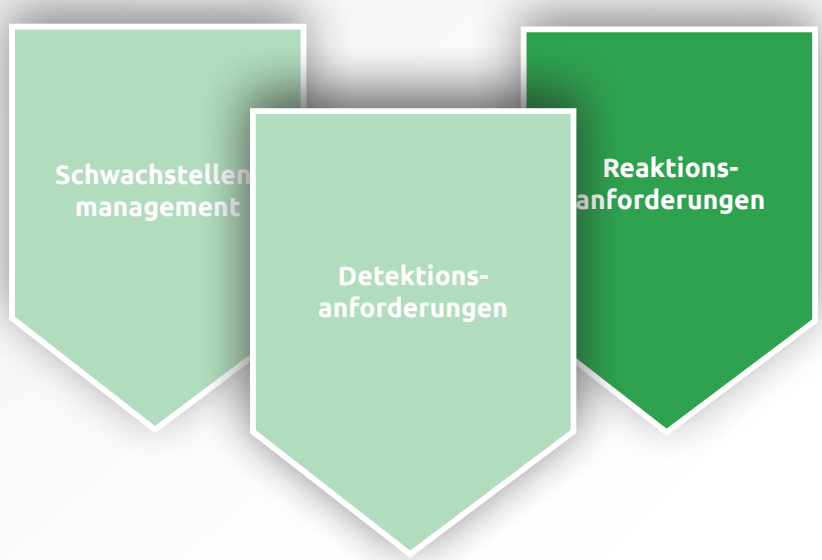
Patch-Management

Regelmäßige Prüfung der IT-Systeme auf Schwachstellen und zeitnahe Implementierung von Sicherheitsupdates. Dabei müssen Risiken bewertet, Patches getestet und Maßnahmen dokumentiert werden, um Sicherheitsvorfälle zu verhindern und Compliance-Anforderungen zu erfüllen.

Cybersecurity-Consultant

- Planung und Implementierung von Updates
- Tests und Validierung der Patches
- Dokumentation und Nachverfolgung
- Sicherstellung der Compliance

Neue Reaktionsanforderungen durch NIS-2



Relevante Bausteine und dafür benötigte Expertise

Cybersecurity Analyse

Dauerhafte Analyse und Lösung von auftretenden Sicherheitsvorfällen in einem angemessenen Zeitraum durch ein fachkundiges Analyse-Team.

Cybersecurity Analyst

- Einzelpersonen für Projektstellen
- Managed-Capacity für Cybersecurity Analysen
- Full-Managed Analyse-Leistungen

Incident Response Plan (IRP)

Entwicklung eines Incident Response Plans (IRP). Aufbau und Schulung eines Incident Response Teams (Intern/Extern/Service).

Senior Cybersecurity Consultant

- Incident Response Experte
- Incident Handling Experte (SANS 504)
- 3rd Level Cybersecurity Analyst
- Digital Forensic

SOAR

Implementierung von Automatisierungsmechanismen für die Erkennung und Reaktion auf Sicherheitsvorfälle.

Cybersecurity Consultant

- SOAR Consulting (Cortex XDR, Phantom, Swimlane)
- Strategische IT-Security Beratung (Architektur, Design und Implementierung eines SOAR)
- Schnittstellen Entwicklung

Risk-Management & Meldepflichten

Erfassung von Schwachstellen und Risikopotentialen inkl. Ableitung passgenauer Maßnahmen sowie Sicherstellung der Einhaltung von Meldepflichten über entsprechende Prozesse.

IT-Risk-Manager

- Einwertung nach anerkannten Standards (ISO 27001)
- Ableitung von Überwachungsmaßnahmen
- Erstellen von Notfallplänen inklusive Meldeprozessen

Etengo unterstützt Sie bei der erfolgreichen NIS-2 Umsetzung

Das sorgfältig gepflegte Etengo-Netzwerk umfasst mehr als 40.000 Experten mit multiplen Skillsets & Rollen. Dazu gehören Freelancer und sozialversicherungspflichtig festangestellte IT-Experten unserer Partnerunternehmen (PU) die Sie bei der fristgerechten Umsetzung der NIS-2 Anforderungen unterstützen.

Strategische Skillbereiche	Key-Skills	
1 Netzwerke & Infrastruktur	▪ Windows, Linux, Unix ▪ Cortex XDR, Fortinet, Cisco, Juniper, Sophos	▪ VMware, Hyper-V, Citrix, Xen ▪ Ansible, Jenkins, Docker, Kubernetes, Terraform
2 IT-Security	▪ ISMS, SIEM, ISO27001, BSI, NIST ▪ IAM, SSO, PAM, MFA, Zero Trust ▪ BCM, Desaster Recovery, IRM	▪ PKI, Kryptographie ▪ BAIT, VAIT, MaRisk ▪ DORA, NIS-2, KRITIS
3 SAP	▪ R/3, SAP S/4HANA ▪ Diverse Module (u.a. FI/CO, SD, MM, EWM, Branchenlösungen)	▪ ABAP, ABAP OO, Fiori, UI5 ▪ Basis, Netweaver, SolMan
4 Softwareentwicklung	▪ Java, Spring, JUnit, Angular, React ▪ C#, .NET, ASP.NET, VB.NET	▪ UML, MVC, MBSE ▪ XRay, Selenium, SOAP UI, HP ALM
5 Organisations- & Prozessberatung	▪ IPMA, Prince2, PMP, CSPO, Scrum ▪ BPMN, GPA, GPO	▪ ITIL, ISO/IEC20000, ITSM, SLM, SLA ▪ IREB, Spice, CMMI
6 Datenmanagement/ -analyse	▪ T-SQL, PL/SQL, OracleDB, MS SQL, MySQL, IBM DB, Mongo DB ▪ Hadoop, Spark, Cassandra, Hive, Cloudera	▪ ETL, Tableau, MS Power BI, QlikSense, IBM Cognos Analytics, Oracle BI, SAS BI
7 Cloud	▪ AWS, EC2, RDS, S3 ▪ Azure, Azure DevOps, Azure Functions ▪ Google Cloud, GKE	▪ Salesforce Cloud, IBM Cloud, Oracle Cloud, SAP-Cloud
8 UI/ UX Design	▪ SEO, SEA, SEM ▪ Figma, Sketch, Adobe XD, InVision	▪ Wordpress, Joomla, Drupal ▪ HTML, CSS, JavaScript
9 Data Science/ KI	▪ Python, R, Scala, SAS, MatLab ▪ PyTorch, Pandas, Keras, Tensorflow, Scikit-Learn, OpenAI	▪ NLP, LLM, CV ▪ Apache Airflow, MLFlow, Kubeflow, Cortex
10 Sonstiger IT-Skillbereich (CRM, ERP, MES)	▪ Salesforce ▪ MS Dynamics365	▪ Infor M3 ▪ Oracle NetSuite
11 Embedded/ Hardware Engineering	▪ C/C++, Rust, Embedded Linux ▪ CAD, Siemens NX, Eplan P8, PTC Creo ▪ SIL, ASIL, ASPICE, LTspice, ISO2626	▪ SPS/HMI, TwinCat, Siemens S7, WinCC ▪ SiL, HiL, DOORS
12 Non-IT (HR, Finance, Marketing, Sales)	▪ Recruiting, Xing, LinkedIn, Textkernel ▪ Controlling, Einkauf	▪ Kampagnenmanagement

Passende NIS-2 Experten. Für Sie.

Etengo stellt Ihnen für die erfolgreiche Umsetzung der NIS-2 Richtlinie in Ihrem Unternehmen die benötigten IT-Skills, die gesuchten digitalen Fähigkeiten kurzfristig zur Verfügung und unterstützt Sie beim Einsatz der externen Experten vollumfänglich.

Beispielhafte Profile aus unserem Portfolio

Cyber Security Analyst

Fachkenntnisse

Cyber Security Analysis

- SOC-Services: Überwachung und Reaktion auf Sicherheitsvorfälle
- Cyber Defense, Security Operations, Netzwerksicherheit
- Phishing- und Malware-Analyse, Incident Response, SIEM
- End Point Security (EDR), proaktive Bedrohungserkennung
- Threat Hunting, Schwachstellen- und Log-Analyse
- Analytische Fähigkeiten, Entwicklung von Lösungen für Sicherheitsbedrohungen
- Zusammenarbeit mit Stakeholdern, Kommunikation von Sicherheitsrisiken

Threat Hunting, Incident Respond und Network Security Analysis

- Netzwerksicherheit, Analyse und Reaktion auf Bedrohungen
- Konfiguration und Überwachung von Firewalls, IDS/IPS
- Sicherheitsaudits, Schwachstellenbewertungen, Penetrationstests
- Kenntnisse aktueller Bedrohungslandschaften, proaktive Trendverfolgung
- SIEM-Tools zur Analyse von Sicherheitsereignissen
- Erstellung technischer Dokumentationen und Sicherheits-richtlinien
- Teamarbeit und interdisziplinäre Kommunikation

Projektauszug

03/2023 – 04/2024, Security Operations Center (SOC)

- Überwachung und Analyse von SIEM-Warnungen, Incident Response
- EDR-basierte Analyse betroffener Hosts, Log-Analysen
- Aktualisierung der Bedrohungserkenntnisse, Umsetzung von Maßnahmen

Senior Cyber Security Consultant

Fachkenntnisse

Security Consulting

- Erfahrung in IT-Sicherheitsberatung, Sicherheitsarchitekturen und Prozessoptimierung
- Expertise in Cyberregulatorik (NIS-2, KRITIS) und Unterstützung bei der Compliance
- Implementierung von SOAR-Lösungen zur Automatisierung von Sicherheitsprozessen
- Schwachstellenmanagement (Qualys, Tenable, Pentera), Priorisierung und Abhilfemaßnahmen
- Schnittstellenentwicklung zur Integration von SOAR und Sicherheitstools

Vulnerability-Management, SOAR-Implementation

- Durchführung von Schwachstellenscans und Priorisierung kritischer Lücken
- Qualitätssicherung der Schwachstellenbewertungen, kontinuierliche Scans
- SOAR-Beratung und Implementierung (Palo Alto XDR, Phantom, Swimlane)
- Entwicklung von Sicherheitsprozessen und Playbooks für Incident Response

Projektauszug

12/2023 – 05/2024, Energiebranche

- Implementierung eines Sicherheitsrahmens und SOAR gemäß NIS-2-Anforderungen
- Risikoanalyse und Identifizierung kritischer Schwachstellen
- Erstellung von Sicherheitsrichtlinien und Notfallplänen

Penetration Tester

Fachkenntnisse

Pentesting

- Tiefgehende Penetration Tests (Netzwerke, Webanwendungen, APIs, Mobile Apps)
- Windows & Active Directory Exploitation, Perimeter-Sicherheit
- Schwachstellenmanagement (Tenable Nessus, Qualys)
- Red Teaming zur Simulation realer Angriffe und Identifikation von Sicherheitslücken
- Sicherheitsaudits basierend auf Standards wie OWASP, MITRE ATT&CK und weiteren Best Practices

Consulting Cyber Resilience & Red-Teaming

- Beratung zur Verbesserung der Cyber Resilience und Einführung von präventiven Sicherheitsmaßnahmen
- Durchführung von Schwachstellenscans und Priorisierung von Maßnahmen zur Reduzierung von Risiken
- Red Team Training zur Verbesserung der Sicherheitslage
- Beratung zu Compliance (ISO 27001, DORA, NIS-2, FDA, PCI, Automotive)
- Sicherheitsstrategien und Maturity Assessments nach NIST, CIS und weiteren Frameworks zur Feststellung der aktuellen Sicherheitslage und Entwicklung langfristiger Maßnahmenpläne
- Erfahrung mit der Integration von Sicherheitstools in den operativen Sicherheitsprozess
- Tools: Kali Linux, Metasploit, Nessus, Qualys

Projektauszug

03/2024 – 10/2024, Dienstleistungs-Branche

- Durchführung von tiefgehenden Penetration Tests (Netzwerke, Webanwendungen, APIs) zur Identifikation von Schwachstellen
- Red Teaming zur Simulation realistischer Cyber-Angriffe und Erkennung von Sicherheitslücken im Unternehmen
- Beratung bei der Einhaltung von ISO 27001 und NIS-2 sowie Unterstützung bei Audits und Maturity Assessments nach NIST

IT Security Risk Manager

Fachkenntnisse

Security Risk Management

- Management von IT-Sicherheitsrisiken und deren Bewertung
- Entwicklung und Implementierung von Risikomanagement-Frameworks
- Identifizierung und Analyse von Bedrohungen und Schwachstellen in IT-Systemen, Netzwerken und Prozessen
- Expertise in der Einhaltung von regulatorischen Anforderungen (ISO 27001, NIST, DSGVO)
- Risikoanalysen und Bewertung von Sicherheitskontrollen zur Risikominderung
- Entwicklung von Risikominderungsstrategien und Business Continuity-Plänen

Compliance und Risikobewertung

- IT-Security-Risikobewertungen und Entwicklung von Maßnahmen zur Risikominderung
- Überwachung und Sicherstellung der Einhaltung von Compliance-Anforderungen und internen Sicherheitsrichtlinien
- Implementierung von Sicherheitsrichtlinien und Risikomanagement-Prozessen gemäß ISO 27001, NIST und weiteren Standards
- Erstellung von Risikoberichten für das Management und Entwicklung von Notfallplänen
- Bewertung der Wirksamkeit von Sicherheitsmaßnahmen und kontinuierliche Optimierung von Kontrollmechanismen

Projektauszug

12/2023 – 05/2024, Energiebranche

- Implementierung eines IT-Sicherheitsrisikomanagement-Frameworks
- Durchführung von Risikoanalysen und Compliance-Überprüfungen
- Entwicklung von Risikominderungsmaßnahmen und Notfallplänen

Was jetzt zu tun ist: Ihr Weg zur NIS-2 Compliance

Seit dem Inkrafttreten von NIS-2 sind Unternehmen verpflichtet, die geforderten Sicherheitsmaßnahmen umzusetzen. Sie müssen jetzt handeln und die notwendigen operativen Maßnahmen ergreifen, um ein effektives Information Security Management System (ISMS) zu etablieren:

NIS-2 als Projekt aufsetzen

Je nach gewählter Projektmethodik entsprechende Gremien und Rollen definieren und besetzen
Interne Stakeholder identifizieren, z.B. Legal Compliance, Risk- und Qualitymanagement
Regelmäßige Berichterstattung an die Geschäftsführung etablieren

Projektteam und Stakeholder hinsichtlich NIS-2 qualifizieren

Übergreifende NIS-2 Schulungen für Stakeholder
Vertiefende NIS-2 Schulungen für Projekt-Mitarbeitende

Durchführung NIS-2 Assessment

Durchführung eines 360° Maturity Assessments (Resilienz, Detektion, Reaktion, Recover, Meldung), um den aktuellen Stand der gesamten Organisation zu messen
Abgleich des aktuellen Standes mit den NIS-2 Anforderungen, um Lücken zu identifizieren

Erstellung Roadmap

Definition und Planung einer praxisorientierten Roadmap für die Implementierung aller notwendigen Tools und Prozesse zur Erfüllung der NIS-2 Anforderungen

Rechtzeitige Umsetzung

Basierend auf der Roadmap wird das NIS-2-Projekt mit den jeweiligen Unterprojekten wie z.B. SIEM oder Schwachstellenmanagement bezogen auf:

- die permanente Detektionanforderungen
- das kontinuierliche Schwachstellenmanagement
- die notwendigen Reaktionsanforderungen

geplant und gestartet.

Jetzt ist Zeit zu handeln

Lassen Sie uns über die Umsetzung von NIS-2 und die Erfüllung der notwendigen Detektions- und Reaktionsanforderungen sowie die Etablierung eines NIS-2-konformen Schwachstellenmanagements in Ihrem Unternehmen sprechen.

Wir unterstützen Sie auch bei der kurzfristigen Umsetzung von NIS-2. Denn als Spezialist für den projektbasierten Einsatz von hochspezialisierten Digital- und IT-Experten stellen wir Ihnen die benötigten Digital- & IT-Skills für die erfolgreiche Umsetzung innerhalb kürzester Zeit zur Verfügung und unterstützen Sie beim Einsatz der externen IT-Experten über den gesamten Projektzeitraum vollumfänglich.

Nehmen Sie jetzt Kontakt mit uns auf:

Etengo AG
Konrad-Zuse-Ring 27
68163 Mannheim

Telefon: +49 621 15 021 0
Fax: +49 621 15 021 399
kontakt@etengo.de