EU-RICHTLINIE ZUR VERHINDERUNG VON CYBER-ATTACKEN

NIS2 mit Gelassenheit umsetzen

ConSecur

[security and consulting]

NIS2 ist die neue Richtlinie der Europäischen Union, die mit einheitlichen Sicherheitsstandards die Cybersicherheit von Unternehmen stärkt und Cyberangriffe verhindern soll.

Die geforderten Security-Maßnahmen müssen bis Oktober 2024 umgesetzt werden. Die EU-Richtlinie gilt für 18 konkret benannte Sektoren aus Industrie und öffentlichen Versorgern. Die betroffenen Unternehmen und Organisationen müssen angemessene Cyber-Sicherheitsmaßnahmen ergreifen und schwerwiegende Vorfälle melden.

FINDEN SIE HERAUS, OB IHR UNTERNEHMEN BETROFFEN, WELCHE MASSNAHMEN UMZUSETZEN SIND, UND ERFAHREN SIE WIE CONSECUR SIE BEI DER UMSETZUNG UNTERSTÜTZEN KANN.

Was sollten Unternehmen jetzt tun?

1. **NUTZEN SIE DIE NIS2 BETROFFENHEITSPRÜFUNG VOM BSI PRÜFEN SIE ZUNÄCHST, OB IHR UNTERNEHMEN VON DER NIS2 RICHTLINIE BETROFFEN IST.**

2. **MASSNAHMEN IDENTIFIZIEREN UND UMSETZEN PRÜFEN SIE IHRE VORHANDENEN MASSNAHMEN UND IDENTIFIZIEREN SIE, WELCHE MASSNAHMEN ZEITNAH UMGESETZT WERDEN MÜSSEN.**

Gerne beraten wir Sie, wie Sie NIS-2-Anforderungen in Ihrem Unternehmen umsetzen können. Mit Hilfe einer GAP-Analyse können wir vorhandene Lücken identifizieren und bei deren Bearbeitung unterstützen.

Welche Maßnahmen zur NIS-2 Konformität müssen umgesetzt werden?

REGISTRIERUNGSPFLICHT
Betroffene Institutionen müssen sich beim BSI registrieren und hierzu geforderte Informationen bereitstellen.

Risikomanagement: Die NIS2 Richtlinie definiert Mindestanforderungen an das Risikomanagement und nennt konkrete Anforderungen für IT-Sicherheitsmaßnahmen zur Risikoreduzierung. Ziele sind u.a.

- das Management von Zwischenfällen,
- eine verbesserte Sicherheit der Lieferkette,
- angemessene Maßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen,
- verbesserte Netzwerksicherheit,
- bessere Zugangskontrolle und Datenverschlüsselung.

VERANTWORTLICHKEIT DES MANAGEMENTS
Die Geschäftsführung ist verantwortlich für die Umsetzung der gemäß §30 geforderten Maßnahmen sowie für die Überwachung dieser Umsetzung. Darüber hinaus ist die Geschäftsführung zur Einschätzung von Risiken in der Sicherheit der Informationstechnik verpflichtet sowie hur regelmäßigen Teilnahme an Schulungen zur Cybersicherheit. Verstöße können zu empfindlichen Sanktionen führen.

MELDUNG VON VORFÄLLEN
Betroffene Unternehmen müssen die zuständigen Behörden innerhalb vorgegebener Zeiträume über Sicherheitsvorfälle sowie über die Bearbeitungserfolge sowie nach Beendigung des Vorfalls informieren.

GESCHÄFTSKONTINUITÄTSPLAN
Unternehmen brauchen Pläne für den Umgang mit größeren Cyber-Vorfällen, einschließlich Systemwiederherstellung, Notfallverfahren und die Einrichtung eines Krisenreaktionsteams.

REGELMÄSSIGE SCHULUNGEN
Geschäftsleitungen sind verpflichtet Risikomaßnahmen umzusetzen und die Umsetzung zu überwachen. Hierzu sind regelmäßige Cybersicherheitsschulungen für Mitarbeiter notwendig.

MINDESTNIVEAU AN IT-SICHERHEIT
Betroffene Unternehmen müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen ergreifen, um IT-Störungen zu vermeiden.

Wie kann ConSecur bei der NIS-2-Umsetzung unterstützen?

ISMS ZUR ERFÜLLUNG DER COMPLIANCE VORGABEN
Zur Erfüllung der NIS 2 Richtlinie empfiehlt sich die Umsetzung eines ISMS. Ein ISMS (Informationssicherheits-Managementsystem) besitzt verbindliche Regeln und Verfahren, Informationswerte in Unternehmen und Organisationen auf Grundlage einer Risikobetrachtung angemessen und strukturiert zu schützen.

Für einzelne Sektoren stehen konkrete „branchenspezifische Sicherheitsstandards“ zur Verfügung, die konkrete Vorgaben zur Umsetzung formulieren.

SIEM ZUR PROAKTIVEN BEDROHUNGSERKENNUNG
Security Information and Event Management System zeigt die Aktivitäten innerhalb der IT-Landschaft und wertet diese nach Angriffskriterien aus. SIEM sammelt dabei Protokolldaten von Netzkomponenten wie Router, Firewalls, IT-Systemen und Anwendungen ein, wertet diese sogenannten Logs aus und schlägt Alarm, sobald eine verdächtige Kombination von Ereignissen erkannt worden ist. Ein SIEM-System hilft bei der Umsetzung der Risikobehandlung, indem es die IT-Infrastruktur permanent überwacht.

MANAGED SIEM (CYBER DEFENSE CENTER)
Im Cyber Defense Center werden Sicherheitsereignisse in der Netzwerk-Infrastruktur kontinuierlich überwacht. Es ist eine zentrale Einheit, die sich mit der kontinuierlichen Überwachung, Analyse und Reaktion auf Vorfälle beschäftigt. Die Anforderungen der NIS2 Richtlinie zur Überwachung und Erkennung von Cybersicherheitsvorfällen sowie die Reaktion darauf lassen sich mit einem Cyber Defense Center effektiv erfüllen.

SPEZIFISCHE GAP-ANALYSE ZUM START
Für den Start empfiehlt ConSecur eine spezifische GAP-Analyse. Diese berücksichtigt einerseits mögliche konkrete Anforderungen des Sektors, dem die fragliche Organisation zuzuordnen ist und andererseits auch die Einordnung „besonders wichtig“ oder „wichtig“. ConSecur ermittelt somit konkret die erforderlichen To-dos, um die NIS2 Anforderungen für die Organisation angemessen zu erfüllen.

IHREN TERMIN ONLINE RESERVIEREN

TERMIN TELEFONISCH RESERVIEREN
Kontaktieren Sie Elke Schomakers oder Doris Poppenberg gerne telefonisch für Ihren Termin.

T +49 5931 9224-0
info@consecur.de

ConSecur GmbH

In unserer digitalen Zeit ist die Information ein sehr hoher Unternehmenswert, dessen Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität wir uns verpflichtet fühlen. ConSecur konzipiert und betreibt IT-Sicherheitslösungen für Unternehmen und Organisationen, die auf vorhandene IT-Infrastrukturen abgestimmt sind und mit uns das nächste Level der Informationssicherheit erreichen. Konzeption, Aufbau und Betrieb sind unsere Stärke. IT-Sicherheitslösungen betreiben wir dauerhaft in unserem Cyber Defense Center 24/7 (Managed CDC). Ziel unserer Arbeit ist es, nur berechtigten Personen den Zugriff auf Informationen zu gewähren und Informationen vor Übergriffen Unbefugter zu schützen. Das Ergebnis ist eine IT-Infrastruktur auf höchstem Sicherheitsniveau.

ConSecur – next level information security

ConSecur
[security and consulting]

ConSecur GmbH
Nödiker Straße 118
49716 Meppen

TEL.: +49 5931 9224-0
info@ConSecur.de
www.ConSecur.de