Berlin, 26.11.2023

NEWSLETTER

November 2023

Ausgestellt von:

NenConsulting IT and Security GmbH

Mühlenstrasse 8a,

14167 Berlin (Zehlendorf), Deutschland

INTERN

www.itandsec.com

NenConsulting IT and Security GmbH
Mühlenstrasse 8a, 14167 Berlin, GERMANY
office@itandsec.com, www.itansec.com

INHALTSVERZEICHNIS

1. NEUES AUS DEM CYBER-SICHERHEIT WELT 3

1.1. Unternehmen im besonderen öffentlichen Interesse (UBI) 3

1.2. Wichtige Aspekte und Fortschritte bei der Umsetzung der NIS-2-Richtlinie 4

1.3. Neue Horizonte im IT-Sicherheitsmanagement: Die IT-Grundschutz Edition 2023 6

1.4. Das neue Energieeffizienzgesetz – Wichtige Informationen und Fristen für Unternehmen 8

WIR UNTERSTÜTZEN SIE GERNE BEI DER BEWÄLTIGUNG DER NEUEN PFLICHTEN UND ANFORDERUNGEN.

NenConsulting IT and Security GmbH
Mühlenstrasse 8a, 14167 Berlin, GERMANY
office@itandsec.com, www.itansec.com

1. NEUES AUS DEM CYBER-SICHERHEIT WELT

1.1. Unternehmen im besonderen öffentlichen Interesse (UBI)

Am 5. Oktober 2023 gab das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Veröffentlichung eines zentralen Informationsflyers bekannt, der gezielt an Unternehmen im besonderen öffentlichen Interesse (UBI) gerichtet ist. Dieses Dokument klärt die Kriterien für die Klassifizierung als UBI gemäß § 2 Absatz 14 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) und unterteilt diese Unternehmen in drei Hauptkategorien:

- **UBI 1 (AWV-UBI):** Betrifft Hersteller und Entwickler von Gütern gemäß § 60 der Außenwirtschaftsverordnung, insbesondere in den Bereichen Waffen, Munition, Rüstungsmaterial und IT-Sicherheitsprodukte. Seit dem 1. Mai 2023 sind diese Unternehmen verpflichtet, IT-Sicherheitsvorfälle zu melden, sich beim BSI zu registrieren, eine Kontaktstelle zu benennen und alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit einzureichen.

- **UBI 2 (Wertschöpfungs-UBI):** Beinhaltet die größten Unternehmen Deutschlands gemessen an der inländischen Wertschöpfung und deren wesentliche Zulieferer. Anmerkung: Die notwendige Rechtsverordnung für die Umsetzung dieser Kategorie steht noch aus.

- **UBI 3 (Störfall-UBI):** Umfasst Betreiber von Betriebsbereichen der oberen Klasse laut Störfall-Verordnung oder diesen gleichgestellten Betreiber. Für diese Unternehmen besteht seit dem 1. November 2021 die Pflicht, IT-Sicherheitsvorfälle zu melden; die Registrierung und Benennung einer Kontaktstelle ist allerdings freiwillig.

Zusätzlicher Hinweis für Betreiber Kritischer Infrastrukturen (KRITIS): Unternehmen, die als Betreiber Kritischer Infrastrukturen gemäß BSI-Gesetz eingestuft sind, unterliegen den Vorschriften des BSI-Gesetzes für KRITIS-Betreiber und nicht den Regelungen für Unternehmen im besonderen öffentlichen Interesse. Ein Unternehmen kann nicht gleichzeitig als Betreiber einer Kritischen Infrastruktur und als Unternehmen im besonderen öffentlichen Interesse klassifiziert werden.

NenConsulting IT and Security GmbH
Mühlenstrasse 8a, 14167 Berlin, GERMANY
office@itandsec.com, www.itansec.com

1.2. Wichtige Aspekte und Fortschritte bei der Umsetzung der NIS-2-Richtlinie

Am 26. Oktober 2023 wurde ein umfassendes Diskussionspapier des BMI im Rahmen eines Werkstattgesprächs erstellt, das sich mit der Umsetzung der NIS-2-Richtlinie befasst. Im Mittelpunkt stehen die Harmonisierung mit bestehenden Gesetzen wie dem KRITIS-Dachgesetz, Klarstellungen zu Begrifflichkeiten, und die Definition von Schlüsselbegriffen wie "besonders wichtige Einrichtungen". Es wurden 37 Stellungnahmen der Verbände und sonstiger interessierter Institutionen angehört. Nachfolgende Vorschläge zur Harmonisierung mit dem KRITIS-Dachgesetz wurden durch das Bundesministerium für Inneres übernommen:

- **Harmonisierung mit dem KRITIS-Dachgesetz:** Diskussionen bezogen sich auf die Harmonisierung von Begrifflichkeiten, Schwellenwerten, Zuordnungskriterien und Registrierungsanforderungen zwischen NIS2UmsuCG und KRITIS-DachG.

- **Klarstellungen zu verwendeten Begriffen:** wie "Cyberhygiene", "Rechenzentrumsdienst", Definition von IKT-Produkten und Anforderungen entlang der Lieferkette.

- **Definition besonders wichtige Einrichtung/wichtige Einrichtung:** Anwendung spezieller Anforderungen an "kritische Anlagen" nur auf betroffene Unternehmensteile und Umgang mit Querverbundsunternehmen.

- **Anwendung des Size-Caps:** Es wurde abgelehnt, dass kleine und mittlere Unternehmen umfänglich von der Regulierung auszunehmen sind und nur die Haupttätigkeit des jeweiligen Unternehmens bei der Anwendung zu berücksichtigen ist.

- **Bereichsausnahmen:** Anpassung der Bereichsausnahmen für Finanzunternehmen, Betreiber von öffentlichen Telekommunikationsnetzen, Energieversorgungsnetzen und Energieanlagen werden weiter ausformuliert werden.

- **Nachweispflichten:** Vorschläge zur Verlängerung von Übergangsfristen nach Inkrafttreten und zur Einführung einer Dokumentationspflicht für wichtige und besonders wichtige Einrichtungen. und konkretisieren frühestens drei Jahre, sowohl für KRITIS als auch für wichtige und besonders wichtige Einrichtungen.

- **Verpflichtender Einsatz zertifizierter Produkte:** Streichung bestimmter Vorschriften und die Möglichkeit, den Einsatz zertifizierter Produkte zu einer Kann-Vorschrift zu machen.

- **Billigung- Überwachungs- und Schulungspflicht für Geschäftsleiter:** Erörterung der Haftungsrisiken, Schulungspflichten und der Möglichkeit der Delegation an IT-Fachkräfte. Hinweis: Der § 38 Abs. 1 bezieht sich auf die Haftungsrisiken für Leiter nationaler Unternehmensteile eines multinationalen Konzerns. Es geht um die Befürchtung, dass diese Leiter unbilligen Risiken ausgesetzt sein könnten, insbesondere im Hinblick auf die Einhaltung von Cybersicherheitsgesetzen. Dies kann besonders problematisch sein, da die Einhaltung in verschiedenen Ländern mit unterschiedlichen Vorschriften eine komplexe und möglicherweise überfordernde Aufgabe darstellt. Der Abschnitt hebt die Notwendigkeit hervor, eine Balance zwischen Sicherheitserfordernissen und der praktischen Durchführbarkeit für Geschäftsleiter in multinationalen Konzernen zu finden. Die NIS-2-Richtlinie legt spezifische Schulungspflichten für die Geschäftsleitung fest. Diese umfassen die Verantwortung für die Umsetzung und Überwachung von Maßnahmen zur Cybersicherheit. Es besteht zudem eine Verpflichtung für die Geschäftsführung und Leitungsorgane, selbst an Schulungen teilzunehmen und diese auch den Mitarbeitenden anzubieten. Das Ziel dieser Schulungen ist es, ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie entsprechende Managementpraktiken im Bereich der Cybersicherheit zu vermitteln.

- **Sektorspezifische Themen**: Spezifische Regelungen und Anpassungen für die Sektoren Gesundheit, Transport und Verkehr, Energie (Definition Wasserstoff, Anlehnung der Begrifflichkeiten and das EnWG).

Weiteres Vorgehen: Erstellung des zweiten Referentenentwurfs, Einleitung der zweiten Runde der Ressortabstimmung, Länder- und Verbändeanhörung, Einleitung des parlamentarischen Verfahrens, und der Start der 3-Jahresfrist für Nachweise nach Inkrafttreten. Das Ende der Umsetzungsfrist der NIS-2-Richtlinie ist für den 17. Oktober 2024 geplant

https://intrapol.org/wp-content/uploads/2023/10/BMI-Werkstattgespraech-NIS-2-Dokumentation.pdf

1.3. Neue Horizonte im IT-Sicherheitsmanagement: Die IT-Grundschutz Edition 2023

Die IT-Grundschutz Edition 2023 nun offiziell verfügbar ist. Dies markiert einen entscheidenden Schritt vorwärts im kontinuierlichen Bestreben, die IT-Sicherheitsstandards zu verbessern und zu aktualisieren. Die Edition 2023 bringt signifikante Neuerungen, die sicherstellen, dass die IT-Sicherheit mit den heutigen Herausforderungen Schritt hält.

Allgemeine Änderungen: Es gab Anpassungen in Zuordnungen und Überarbeitungen bestehender sowie Aufnahme neuer Bausteine. Insgesamt sind 21 Bausteine betroffen, wobei einige umfassend angepasst wurden, darunter OPS.1.1.2 (Ordnungsgemäße IT-Administration) und APP.2.1/2.2 (Allgemeiner Verzeichnisdienst/Active Directory Domain Service).

Neue Bausteine in der Edition 2023:

- CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)
- OPS.1.1.1 Allgemeiner IT-Betrieb
- OPS.2.3 Nutzung von Outsourcing (dieser Baustein ersetzt OPS.2.1 Outsourcing für Kunden)
- OPS.3.2 Anbieten von Outsourcing (dieser Baustein ersetzt OPS.3.1 Outsourcing für Dienstleister)
- APP.5.4 Unified Communications und Collaboration (UCC)
- SYS.1.2.3 Windows Server
- SYS.1.9 Terminalserver
- SYS.2.5 Client-Virtualisierung
- SYS.2.6 Virtual Desktop Infrastructure
- NET.3.4 Network Access Control

Entfallene Bausteine:

- SYS.2.2.2 Clients unter Windows 8.1: Der Support für das Betriebssystem endete am 10.01.2023. Windows 8.1 sollte daher nicht mehr eingesetzt werden.
- OPS.2.1 Outsourcing für Kunden: Der Baustein wird durch OPS.2.3 Nutzung von Outsourcing ersetzt
- OPS.3.1 Outsourcing für Dienstleister: Der Baustein wird durch OPS.3.2 Anbieten von Outsourcing ersetzt

Überarbeitete Bausteine:

- ORP.1 Organisation
- CON.1 Kryptokonzept
- CON.2 Datenschutz

- OPS.1.1.2 Ordnungsgemäße IT-Administration
- OPS.1.1.3 Patch- und Änderungsmanagement
- OPS.1.2.5 Fernwartung
- APP.1.2 Webbrowser
- APP.2.1 Allgemeiner Verzeichnisdienst
- APP.2.2 Active Directory: (Der Baustein wurde in „Active Directory Domain Services“ umbenannt)
- APP.2.3 OpenLDAP
- APP.5.3 Allgemeiner E-Mail-Client und -Server
- SYS.1.1 Allgemeiner Server
- SYS.2.1 Allgemeiner Client
- SYS.2.3 Clients unter Linux und Unix
- SYS.2.2.3 Clients unter Windows 10: Der Baustein wurde in „Clients unter Windows“ umbenannt und behandelt nun mit Windows 10 und 11 die einzigen beiden Versionen von Windows für Client-Systeme, die durch Microsoft Support erhalten.
- SYS.4.3 Eingebettete Systeme
- SYS.4.5 Wechseldatenträger
- IND.3.2 Fernwartung im industriellen Umfeld
- INF.1 Allgemeines Gebäude
- INF.2 Rechenzentrum sowie Serverraum
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum

Anpassung und Korrektur: Bei der Implementierung dieser Änderungen müssen die existierenden Systeme und Sicherheitskonzepte entsprechend angepasst und die Modellierung überprüft werden. Besonderes Augenmerk liegt auf der Härtung der Systeme, die in den neuen Bausteinen hervorgehoben wird.

NenConsulting IT and Security GmbH
Mühlenstrasse 8a, 14167 Berlin, GERMANY
office@itandsec.com, www.itansec.com

1.4. Das neue Energieeffizienzgesetz – Wichtige Informationen und Fristen für Unternehmen

Das Energieeffizienzgesetz, das am 17. November 2023 in Kraft trat, ist ein bedeutender Schritt in Richtung Energieeffizienz und stellt Unternehmen vor neue Herausforderungen. Mit diesem Gesetz werden nicht nur die Anforderungen der europäischen Energieeffizienzrichtlinie umgesetzt, sondern es werden auch konkrete Verpflichtungen für Unternehmen, Rechenzentren und öffentliche Stellen festgelegt. Das Gesetz sieht vor, dass der Endenergieverbrauch bis 2030 um 26,5 % und der Primärenergieverbrauch um 45 % gegenüber 2008 reduziert wird. Das Gesetz enthält zudem Anforderungen an Rechenzentren, die ihre Energieeffizienz steigern und erneuerbare Energien nutzen müssen, sowie spezifische Vorgaben für die Nutzung von Abwärme und die Implementierung klimaneutraler Betriebsstandards.

Für Unternehmen bedeutet dies vor allem die Einführung und Umsetzung von Energiemanagementsystemen. Unternehmen mit einem durchschnittlichen Gesamtendenergieverbrauch von über 7,5 GWh in den letzten drei Jahren müssen bis zum 18. Juli 2025 ein Energiemanagementsystem nach ISO 50001:2018 einführen. Darüber hinaus sind Unternehmen mit einem Verbrauch von mehr als 2,5 GWh verpflichtet, innerhalb von drei Jahren nach dem Gesetz konkrete Pläne zur Energieeinsparung zu entwickeln und umzusetzen, basierend auf Energieaudits oder dem Energiemanagementsystem ISO 50001:2018. **Der Stichtag hierfür ist der 18. Juli 2025.**

Diese Maßnahmen sollten auf Ergebnissen von Energieaudits nach DIN EN 16247-1 oder aus Energiemanagementsystemen nach ISO 50001:2018 basieren und müssen spätestens innerhalb von drei Jahren umgesetzt werden. Die Pläne sind durch externe Zertifizierer, Umweltgutachter oder zugelassene Energieauditoren zu verifizieren.

Für Nicht-KMU Unternehmen bleibt die vierjährige Energieauditpflicht nach dem EDL-G bestehen. Auch Unternehmen mit einem Endenergieverbrauch von unter 7,5 GWh könnten somit einer Auditpflicht unterliegen.

Angesichts dieser umfangreichen Anforderungen und Fristen ist es für Unternehmen essenziell, zeitnah die notwendigen Schritte zu ergreifen, um die Einhaltung der Vorgaben zu gewährleisten. Unternehmen, die sich dieser Herausforderung stellen, können nicht nur zur Reduzierung des Energieverbrauchs beitragen, sondern auch ihre Betriebskosten langfristig senken und ihre Wettbewerbsfähigkeit verbessern.