**NIS2 - Trendartikel**

**Der Weg zur digitalen Sicherheit: ein Blick auf die NIS2-Richtlinie der EU**

**Cyberbedrohungen und die europäische Antwort**

Die zunehmende Digitalisierung bringt nicht nur Fortschritt. Sie bringt auch ein zunehmendes Risiko mit sich: Cyberangriffe. Um dem zu begegnen, hat die Europäische Union 2016 die NIS-Richtlinie (Netz- und Informationssicherheit) eingeführt. Ziel war es, die Cybersicherheit in strategisch wichtigen Sektoren zu stärken: insbesondere in den Bereichen Energie, Verkehr, Banken, Finanzmärkte, Gesundheitswesen, Wasser und digitale Infrastruktur.

Seitdem haben sich jedoch grundlegende Veränderungen in der Gesellschaft ergeben, insbesondere nach der COVID. Die massenhafte Einführung von Videokonferenz-Tools (wie MS Teams, Zoom oder Google Meet) in Verbindung mit der gestiegenen Nachfrage nach E-Commerce und Lieferdiensten haben den Übergang zur digitalen Welt intensiviert. Tatsächlich schätzt McKinsey, dass die Pandemie die Digitalisierung um 3 bis 4 Jahre beschleunigt hat. Diese Entwicklungen brachten neue Herausforderungen für die Cybersicherheit mit sich - und so musste die EU ihre Richtlinie aktualisieren.

**NIS2: Strengere Regeln für eine sicherere Welt**

Im November 2022 verabschiedete die EU die neue NIS2-Richtlinie. Diese Richtlinie erweitert den Geltungsbereich der ursprünglichen Rechtsvorschriften erheblich und verschärft die Sicherheitsmaßnahmen. Zusätzlich zu den sieben ursprünglichen Sektoren deckt NIS2 nun auch neue Bereiche wie das verarbeitende Gewerbe, Post-/Kurierdienste, Wissenschaft, Forschung und Bildung ab.

NIS2 verpflichtet Unternehmen und Organisationen in all diesen Sektoren, Cyberrisiken zu erkennen und zu bewältigen, Informationssysteme zu sichern und Mitarbeiter regelmäßig zu schulen. Eine der neuen Verordnungen sieht sogar die Verpflichtung vor, schwerwiegende Sicherheitsvorfälle innerhalb von 24 Stunden nach ihrer Entdeckung zu melden, wobei ein detaillierter Bericht innerhalb von 72 Stunden und ein Abschlussbericht innerhalb von 30 Tagen zu erstellen ist.

In der Richtlinie werden Organisationen in zwei Kategorien eingeteilt - „wesentliche“ und „kritische“ Einrichtungen, wobei für jede Kategorie spezifische Verpflichtungen gelten. Die Strafen für die Nichteinhaltung der Vorschriften können sehr streng sein. Wesentliche Einrichtungen müssen mit Geldbußen von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes rechnen, je nachdem, welcher Betrag höher ist. Gegen bedeutende Unternehmen können Geldbußen von bis zu 7 Mio. € oder 1,4 % des Umsatzes verhängt werden.

Die NIS2 spielt somit eine Schlüsselrolle bei der Gewährleistung der Cybersicherheit in der EU. Die Organisation setzt sich für die Einführung neuer Maßnahmen und die Einhaltung strenger Vorschriften zum Schutz kritischer Infrastrukturen wie Energienetze, Wasserversorgung und Gesundheitswesen ein. Dadurch wird sichergestellt, dass wichtige Dienstleistungen, auf die sich die Menschen verlassen, auch im Falle eines Cyberangriffs funktionieren und sicher sind.

**Wie bereitet sich 2N auf die NIS2 vor?**

2N muss die NIS2 einhalten: Es gilt als Verpflichteter (mehr als 250 Beschäftigte und ein Jahresumsatz von mehr als 10 Mio. EUR) und fällt unter mehrere regulierte Sektoren wie „Herstellung von elektronischen Geräten und Ausrüstungen“, „Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste“ und auch „Anbieter von Cloud-Computing-Diensten“.

Das Unternehmen beschäftigt sich seit langem mit dem Thema Cybersicherheit und verfügt über die Zertifizierung nach ISO 27001, die es regelmäßig bei Überwachungs- und Rezertifizierungsaudits aufrechterhält. Dieses Jahr hat 2N auch die Sicherheitszertifizierung IEC 62443-4-1 erhalten, die für seine Aufzugsprodukte gilt.

Aber was kommt als nächstes? 2N muss die strengen NIS2-Vorschriften einhalten und die bestehenden Sicherheitsmaßnahmen gründlich und regelmäßig überprüfen. Daher führt das Unternehmen eine Lückenanalyse durch, um festzustellen, welche NIS2-Verpflichtungen es bereits erfüllt (durch die ISO 27001-Zertifizierung) und was noch umgesetzt werden muss. Da die Cybersicherheit eine der obersten Prioritäten von 2N ist, geht das Unternehmen davon aus, dass die Erfüllung der verbleibenden Anforderungen reibungslos und innerhalb der gesetzlich vorgeschriebenen Frist erfolgen wird. Wenn Sie sich für 2N entscheiden, können Sie sicher sein, dass Sie keine Nichteinhaltung der EU-Richtlinien riskieren.

**Wissen, Vertrauen und Transparenz: Schlüsselwerte**

2N stützt sich seit langem auf das umfangreiche Wissen und die Erfahrung seiner Muttergesellschaft AXIS im Bereich der Cybersicherheit. Die Experten beider Unternehmen stehen in täglichem Kontakt und tauschen bewährte Verfahren und Ideen für eine sichere Entwicklung aus.

Eines der wichtigsten Tools, das 2N übernommen hat, ist das Axis Security Development Model (ASDM), das 13 Prozesse und Sicherheitspraktiken beschreibt, die sich auf die Implementierung (und anschließende Überprüfung) von Sicherheitsmaßnahmen in jeder Entwicklungsphase konzentrieren. Dieser Ansatz minimiert das Risiko von Sicherheitsvorfällen und stärkt das Vertrauen und die Zufriedenheit der Kunden.

Vertrauen und Transparenz zwischen dem Unternehmen und seinen Kunden sind zentrale Werte für 2N. Das Unternehmen veröffentlicht alle sicherheitsrelevanten Materialien und Informationen auf seiner Website - das gewährleistet nicht nur die Sicherheit seiner Produkte und Dienstleistungen, sondern stärkt auch Ihr Vertrauen in deren Zuverlässigkeit.

**Banner - Trendartikel**

2N's Einblicke in die NIS2-Richtlinie

Erhalten Sie immer mehr Fragen über die bevorstehende NIS2-Richtlinie der EU und ihre Auswirkungen auf Unternehmen? Erfahren Sie in diesem aufschlussreichen Artikel, was sie bedeutet, wen sie betrifft und wie sich 2N, ein führender Anbieter von Zutrittskontrollsystemen, darauf vorbereitet

**>>Lesen Sie weiter**

**E-Mail – Hardening Guide**

**Thema:** Verstärken Sie Ihre Netzwerksicherheit mit dem 2N Hardening Guide

**Vorspann:** Herunterladen

Sehr geehrter [Name des Empfängers],

In der heutigen, sich schnell entwickelnden Cybersicherheitslandschaft **ist die Gewährleistung der Sicherheit Ihrer IP-basierten Geräte nicht mehr optional, sondern unerlässlich**. Angesichts der immer ausgefeilteren Cyber-Bedrohungen war die Notwendigkeit, Systeme zu schützen, noch nie so dringlich wie heute.

Damit Sie immer einen Schritt voraus sind, bieten wir Ihnen den 2N Hardening Guide an - eine umfassende Ressource, die wichtige Best Practices zur Verbesserung der Sicherheit von 2N Netzwerkgeräten beschreibt.

Ganz gleich, ob Sie Geräte in einer Hochsicherheitsumgebung wie dem Gesundheitswesen oder einer Behörde verwalten oder einfach nur ein Wohn- oder Multifunktionsgebäude sichern wollen, diese Empfehlungen sind darauf ausgerichtet, Schwachstellen zu minimieren und Ihre Abwehrkräfte zu stärken.

**Was Sie lernen werden**

* **Festlegen starker Passwörter:** Zuverlässige Anmeldedaten zum Schutz vor unbefugtem Zugriff einrichten
* **Regelmäßige Firmware-Updates:** Patches für bekannte Sicherheitslücken, um Bedrohungen vorzubeugen
* **Sichere Kommunikationsprotokolle:** Gewährleistung einer sicheren Kommunikation zwischen Geräten
* **Aktivieren von Verschlüsselung:** Schutz sensibler Daten während der Übertragung
* **Unnötige Dienste deaktivieren:** Minimierung potenzieller Angriffsflächen
* **Begrenzung des Netzwerkzugangs:** Verringerung der Gefährdung durch Beschränkung des Zugangs auf vertrauenswürdige Benutzer
* **Netzwerksegmentierung:** Isolierung kritischer Geräte vom breiteren Netzwerkverkehr zur Verbesserung der Sicherheit

Warten Sie nicht, bis eine Sicherheitslücke entsteht. Informieren Sie sich und schützen Sie Ihr System jetzt. Der 2N Hardening Guide ist Ihre unverzichtbare Ressource für die Aufrechterhaltung eines robusten, sicheren Netzwerks.

[Herunterladen]

Mit freundlichen Grüßen,