PRESSEMITTEILUNG

NIS2-Konformität mit A-Trust

Wien, 05. August 2024 – Ziel der NIS2-Richtlinie ist es, das Niveau der Cybersicherheit in der Europäischen Union zu erhöhen und mit der sich stetig weiterentwickelnden Bedrohungslandschaft Schritt zu halten. Bis spätestens 17. Oktober 2024 müssen die betroffenen Unternehmen und Organisationen Maßnahmen umsetzen, welche die Vertraulichkeit, Verfügbarkeit und Integrität ihrer Netzwerke und IT-Systeme garantieren. Österreichs führender Vertrauensdiensteanbieter A-Trust leistet mit seinen Lösungen einen wichtigen Beitrag dazu, die Sicherheit der Systeme zu erhöhen und die Einhaltung der gesetzlichen Vorgaben sicherzustellen. Als Qualifizierter Vertrauensdiensteanbieter unterliegt das Unternehmen ja auch selbst der strengen NIS2-Richtlinie und kennt daher die Anforderungen genau.

Erweiterter Geltungsbereich und strengere Vorgaben

NIS2 erweitert den bisherigen Geltungsbereich des Gesetzes zur Netz- und Informationssicherheit auf 18 Sektoren. Der Richtlinie unterliegen große sowie mittlere Unternehmen (siehe Infokästen unten), doch auch kleine Unternehmen können über Sonderbestimmungen oder über die Lieferkette betroffen sein. Und Verstöße gegen die Vorschriften können für die Geschäftsführung eines Unternehmens oder Leitungsorgane einer Organisation teuer werden: Sie müssen die Umsetzung und Einhaltung der Risikomanagementmaßnahmen gewährleisten und überwachen und haften persönlich.

NIS2 nimmt nun auch das ganze Unternehmen in den Fokus. Es reicht nicht mehr, die nötigen Risikomanagementmaßnahmen ausschließlich für den wesentlichen Dienst vorzunehmen, sondern die gesetzlichen Regelungen müssen im gesamten Unternehmen umgesetzt werden. Denn wenn etwa ein Energieerzeuger großes Augenmerk auf den Schutz seiner Anlagen richtet, in der Administration aber Einfallstore für Hacker:innen übersehen werden, nützt die Investition in Anlagensicherheit recht wenig.

Höchste Compliance durch Hash2Sign

Markus Vesely, CEO von A-Trust: „Damit der starke Fokus auf die Sicherheit nicht Prozesse verkompliziert oder den Workflow verlangsamt, bietet A-Trust eine breite Palette an digitalen Lösungen an, die wesentlich zur NIS2-Konformität beitragen. So bereitet zum Beispiel unsere neue Hash2Sign-Software Dokumente schnell und einfach für die Qualifizierte Elektronische Signatur auf."

Durch die Übermittlung nur des Hash-Werts bleibt der Inhalt der zu signierenden Dokumente stets vertraulich und dank der einfachen Einbindung über eine REST-Schnittstelle lässt sich Hash2Sign mühelos in die bestehenden Workflow-Lösungen der Kund:innen integrieren, ohne dass zusätzliche Hardware erforderlich ist. „Hash2Sign in Kombination mit der eIDAS-konformen Signatur von A-Trust garantiert auch von NIS2 betroffenen Unternehmen höchste technische und rechtliche Sicherheit", so **Vesely**.

Sichere SmartCards mit Mehrwert

Cyberkriminelle attackieren jede denkmögliche Schwachstelle, und sei es der ungesicherte Zugang zur Besenkammer, durch die unbefugte Personen in kritische Bereiche vordringen könnten. Zu den Maßnahmen, die zur von NIS2 eingeforderten Risikominimierung beitragen, gehört daher auch die Umsetzung von Zutritts- und Zugriffskontrollen. Die elektronischen Mitarbeiterausweise von A-Trust bieten hier volle Sicherheit bei zugleich maximaler Flexibilität.

„Unsere SmartCards mit kontaktlosem RFID-Chip können zum Öffnen von Türen oder für den sicheren Login am PC verwendet werden, damit werden unbefugte Zutritte bzw. Zugriffe verhindert“, erläutert **Markus Vesely**: „Mit einem qualifizierten Zertifikat verbunden, ermöglichen sie auch eine schnelle und einfache qualifizierte elektronische Signatur und verbinden Sicherheit und Effizienz mit europaweiter Rechtsgültigkeit.“

NIS2 kurz zusammengefasst:

Von NIS2 betroffen

- **11 Sektoren mit hoher Kritikalität**: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Digitale Infrastruktur, Verwaltung von IKT-Diensten (B2B), öffentliche Verwaltung und Weltraum.
- **7 sonstige kritische Sektoren:** Post- und Kurierdienste, Abfallbewirtschaftung, Chemie, Lebensmittel, verarbeitendes/herstellendes Gewerbe, Anbieter digitaler Dienste und Forschung.

- **Große Unternehmen** mit mindestens 250 Beschäftigten oder über 50 Mio. Euro Jahresumsatz und über 43 Mio. Euro Jahresbilanzsumme
- **Mittlere Unternehmen** mit 50 bis 249 Beschäftigten oder zwischen 10 und 50 Mio. Euro Jahresumsatz bzw. zwischen 10 und 43 Mio. Euro Jahresbilanzsumme
- **Kleine Unternehmen** sind grundsätzlich nicht im direkten Anwendungsbereich, können aber über **Sonderbestimmungen** im Anwendungsbereich oder über die **Lieferkette** betroffen sein.

Erforderliche Maßnahmen

- Entwicklung von Konzepten für Risikoanalysen und die Sicherheit von Informationssystemen sowie Konzepte und Verfahren zur Bewertung der Wirksamkeit der Risikomanagementmaßnahmen
- Maßnahmen, die zur Erkennung und Minimierung von Sicherheitsvorfällen beitragen
- die Sicherstellung der Geschäftskontinuität durch Backup- und Krisenmanagementmaßnahmen
- Maßnahmen zur Gewährleistung der Sicherheit der Lieferketten
- Cyberhygieneverfahren sowie Schulungen, Fort- und Weiterbildungen im Bereich der Cybersicherheit
- der Einsatz von Kryptografie und Verschlüsselungstechnologie
- Personalsicherheit, Zugriffskontrollen und Management von Anlagen
- Lösungen für Multi-Faktor-Authentifizierungen oder kontinuierliche Authentifizierungen
- Verwendung von sicherer Sprach-, Video- und Textkommunikation

Vorgehen bei Sicherheitsvorfällen

- Sobald ein Problem erkannt wurde, muss **binnen 24 Stunden** gemeldet werden, ob der Vorfall auf einer rechtswidrigen oder böswilligen Handlung beruht bzw. grenzübergreifende Auswirkungen haben kann (Frühwarnung).
- **Binnen 72 Stunden** muss eine erste Einschätzung des Cybersicherheitsvorfalls abgegeben werden.
- **Ein Monat** nach der Meldung muss ein Zwischen- bzw. Abschlussbericht mit einer ausführlichen Beschreibung des Cybersicherheitsvorfalls übermittelt werden.

Sanktionen & Bußgelder

Geschäftsführung eines Unternehmens oder Leitungsorgane einer Organisation müssen die Umsetzung und Einhaltung der Risikomanagementmaßnahmen gewährleisten und überwachen. Sie können persönlich haftbar gemacht werden. Im Extremfall kann ein Bußgeld von bis zu 10 Mio. Euro oder bis zu 2 Prozent des weltweiten Umsatzes (je nachdem, welcher Betrag höher ist) anfallen.

Über A-Trust
Compliance, Integrität, Komfort und vor allem Sicherheit: A-Trust ist ein zuverlässiges Partnerunternehmen, wenn es um Sicherheit im digitalen Raum geht, und steht für innovative und professionelle Zertifikats- und Signaturlösungen. Das Unternehmen ist ein qualifizierter Vertrauensdiensteanbieter für elektronische Zertifikate auf Basis der eIDAS-Verordnung und in der EU-Trusted List eingetragen.

Mit mehr als 20 Jahren Erfahrung im Zertifikatsbereich und mehr als 4 Millionen aktiven Nutzer:innen einer A-Trust-QES (z.B. ID Austria) steht A-Trust für Beständigkeit und Investitionssicherheit und ist auch im Heimatmarkt Österreich zum Branchenführer avanciert. Gemeinsam mit verschiedenen internationalen Partner:innen bietet A-Trust erfolgreich sichere und komfortable Signaturlösungen für zahlreiche Kund:innen in der DACH-Region und in ganz Europa an.
www.a-trust.at

Rückfragehinweis

A-Trust GmbH
Mag. Eva Kleinbrod, MSc
Head of Marketing & PR
Landstraßer Hauptstraße 1b / E02
1030 Wien
Tel.: +43 1 713 21 51 341
E-Mail: eva.kleinbrod@a-trust.at

corporate identity prihoda gmbh
mag. irmgard dober
pr consultant
peter-jordan-straße 74
1190 wien
tel.: +43 1 479 63 66–22
e-mail: irmgard.dober@cip.at