Wie Cyolo und BearingPoint Sie bei der Einhaltung der Vorschriften unterstützen: NIS2-Richtlinie

EINLEITUNG

Die NIS2-Richtlinie ist eine gesetzliche Vorgabe, die darauf abzielt, die Cyber-Resilienz kritischer Infrastrukturen in der Europäischen Union (EU) zu stärken. Sie legt verbindliche Mindestanforderungen an die Cybersicherheit fest, die von allen EU-Mitgliedstaaten in nationales Recht umgesetzt und auf betroffene Unternehmen angewendet werden müssen.

Die NIS2 ersetzt ihren Vorgänger, die ursprüngliche NIS1-Richtlinie, und baut darauf auf. Der Anwendungsbereich wurde ausgeweitet und zusätzliche Anforderungen wurden eingeführt, um auf die steigende Häufigkeit und zunehmenden Auswirkungen von Cyberangriffen auf kritische Infrastrukturen in der EU in den letzten Jahren zu reagieren.

Dieses Dokument beschreibt die Unterstützung von Cyolo und BearingPoint bei der Einhaltung der NIS2-Richtlinie und bietet einen entsprechenden Leitfaden für Sicherheits- und Risikofachleute in der EU und darüber hinaus.

KEY NIS2 COMPLIANCE REQUIREMENTS

Die Mindestanforderungen für die NIS2-Compliance für wesentliche und wichtige Einrichtungen im Geltungsbereich sind wie folgt:

Maßnahmen zum Cybersecurity-Risikomanagement: Unternehmen müssen laut NIS2-Richtlinie 10 Schlüsselmaßnahmen umsetzen, um Cyberrisiken für Netzwerke, Systeme und/oder andere digitale oder physische Vermögenswerte, die an der Erbringung wesentlicher oder wichtiger Dienste in der EU beteiligt sind, zu verwalten und zu reduzieren.

Diese Maßnahmen umfassen:

1. Richtlinien zur Risikoanalyse und zur Sicherheit von Informationssystemen.
2. Behandlung von Vorfällen (Vorbeugung, Erkennung und Reaktion von Vorfällen).
3. Krisenmanagement und Geschäftskontinuität, z. B. Backup- und Recovery-Management.
4. Sicherheit der Lieferkette für die Beziehungen zwischen den betroffenen Unternehmen und ihren Lieferanten oder Dienstleistern.
5. Sicherheit bei der Beschaffung, Entwicklung und Wartung von Netzwerken und Informationssystemen, einschließlich des Umgangs mit Schwachstellen und deren Offenlegung.
6. Richtlinien und Verfahren zur Bewertung der Wirksamkeit desCybersicherheitsrisikomanagements.
7. Grundlegende Praktiken der Cyber-Hygiene und Cybersicherheitsschulungen.

8. Richtlinien und Verfahren für den Einsatz von Kryptographie und gegebenenfalls Verschlüsselung.
9. Sicherheit der Personalressourcen, Zugangskontrollrichtlinien und Vermögensverwaltung.
10. Verwendung von Mehrfaktor-Authentifizierungs oder kontinuierlichen Authentifizierungslösungen, gesicherte Sprach-, Video- und Textkommunikation sowie gesicherte Notfallkommunikationssysteme

ÜBERSICHT ÜBER CYOLO PRO

Cyolo PRO (Privileged Remote Operations) ist eine fortschrittliche, infrastrukturunabhängige sichere Fernzugriffslösung, die die Risiken des Fernzugriffs auf geschäftskritische Anlagen minimiert. Cyolo PRO's dezentralisierte Architektur bietet außergewöhnliche Flexibilität und kann sich nahtlos an alle Umgebungen (Cloud-verbunden, Cloud-averse und offline) ohne Änderungsmanagement anpassen.

- Gewährleistung von schnellem, sicherem und gefahrlosem Support und Wartung für OT-Umgebungen
- Sichere Anbindung von Drittanbietern an OT-Umgebungen, ohne dass Agenten oder Downloads für Endbenutzer erforderlich sind
- Hinzufügen von Multi-Faktor-Authentifizierung (MFA) auf Altsystemen, die keine moderne Identitätsauthentifizierung unterstützen können
- Absicherung aller Zugangspunkte zu geschäftskritischen Anlagen, ob remote oder on-prem
- Implementierung von Segmentierung, Überwachung, Sitzungsaufzeichnung und anderen Anforderungen der Branche und regionaler Compliance-Vorgaben

CYOLO PRO/NIS2 ABGLEICH

Cyolo PRO erfüllt die Anforderungen von NIS2 mit den folgenden Funktionen und Eigenschaften:

Risikomanagement-Maßnahme	Cyolo PRO-Fähigkeiten	Kontrolltyp
Richtlinien zur Risikoanalyse und zur Sicherheit von Informationssystemen	Granulare Kontrollrichtlinien liefern Benutzer-, Sitzungs-, Anwendungs- und Geräteinformationen, um die Einhaltung von Richtlinien zu überprüfen.	**SUPPORTS**
Behandlung von Vorfällen (Vorbeugung, Erkennung und Reaktion von Vorfällen).	Funktionen wie Zero-Trust-Zugriff, MFA für alle Systeme sowie Sitzungsüberwachung und -aufzeichnung verringern die Wahrscheinlichkeit eines Sicherheitsvorfalls. Werden verdächtige Aktivitäten festgestellt, kann der Zugriff in Echtzeit eingeschränkt oder beendet werden. Nahtlose Integration mit SOAR, SIEM, XDR und anderen Tools für zusätzliche Funktionen zur Reaktion auf Vorfälle.	**PROVIDES**

Risikomanagement-Maßnahme	Cyolo PRO-Fähigkeiten	Kontrolltyp
Krisenmanagement und Geschäftskontinuität, z. B. Sicherungs- und Wiederherstellungsmanagement	Die einzigartige dezentralisierte Architektur besteht aus selbstreplizierenden Komponenten, welche die Geschäftskontinuität, ununterbrochene Betriebszeit und Datenwiederherstellung von einzelnen Komponenten ermöglicht.	**PROVIDES**
Sicherheit der Lieferkette für die Beziehungen zwischen den betroffenen Unternehmen und ihren Lieferanten oder Dienstleistern.	Die Zero-Trust-Architektur schützt Anwendungen und Ressourcen vor direkter Konnektivität. Der Zugriff auf Anwendungsebene verhindert laterale Bewegungen und begrenzt den Schaden, den ein potenzieller Angreifer verursachen könnte. Überwachungskontrollen wie überwachter Zugriff und Sitzungsaufzeichnung gewährleisten die Sicherheit für die gesamte Dauer der der Verbindung. Das agentenlose Bereitstellungsmodell der Lösung ist ideal für die Sicherung des Zugriffs durch Dritte.	**SUPPORTS**
Richtlinien und Verfahren zur Bewertung der Wirksamkeit des Risikomanagements im Bereich der Cybersicherheit	Plattforminterne Analysen zeigen die Wirksamkeit der Richtlinien für Cybersicherheit und Risikomanagement.	**SUPPORTS**
Grundsätze und Verfahren für den Einsatz von Kryptographie und gegebenenfalls Verschlüsselung	TLS-Verbindung gewährleistet vollständige Ende-zu-Ende-Verschlüsselung vom Benutzer bis zur Anwendung. Alle Daten, Geheimnisse und Kodierungsschlüssel bleiben innerhalb der der vertrauenswürdigen Grenzen des Kunden und werden niemals in der Cyolo-Cloud gespeichert oder entschlüsselt.	**SUPPORTS**
Sicherheit der Personalressourcen, Zugangskontrollrichtlinien und Vermögensverwaltung	Robuste und granulare Zugangskontrollen umfassen MFA, Passwort-Manager, Geräteüberprüfungen, Ende-zu-Ende-Verschlüsselung, kontinuierliche Autorisierung und Identitätsföderation.	**SUPPORTS**
Einsatz von Lösungen für die Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung, gesicherte Sprach-, Video- und	MFA erweitert alle Benutzerkonten (Service, gemeinsam genutzte, individuelle, etc.) in allen Umgebungen (Cloud-verbunden, Cloud-averse, offline).	**PROVIDES**

Risikomanagement-Maßnahme	Cyolo PRO-Fähigkeiten	Kontrolltyp
Textkommunikation sowie gesicherte Notfallkommunikationssysteme	MFA-Funktionen können zu Altsystemen hinzugefügt werden ohne dass Upgrades oder Änderungsmanagement erforderlich sind.	

Kontrolltyp Beschreibung

PROVIDES: Liefert Informationen, die direkt an den Prüfer weitergegeben werden oder Daten in ein Nachweisdokument eingespeist werden können.
REVIEWED: Kann verwendet werden, um nachzuweisen, ob eine andere Kontrolle vorhanden ist und/oder funktioniert.
SUPPORTS: Leitet Informationen an ein anderes System oder Prozesse weiter, die die Anforderungen erfüllen.

ÜBER CYOLO

Cyolo verfolgt einen ganzheitlichen Ansatz für die Cybersicherheit, der sich eng an das Konzept der NIS2-Richtlinie anlehnt. Die anpassungsfähige, infrastrukturunabhängige Lösung von Cyolo wurde speziell für die Sicherung, Überwachung und Prüfung privilegierter Fernverbindungen zu kritischen Infrastrukturen und OT-Systemen entwickelt.

Mit Cyolo können Unternehmen wie das Ihre die hier beschriebenen Schritte proaktiv und ohne Betriebsunterbrechung umsetzen, ohne dass Änderungen an der bestehenden Infrastruktur erforderlich sind. Vereinbaren Sie einen Termin für eine Demo und beginnen Sie noch heute mit der Umsetzung der NIS2-Konformität.

Erfahren Sie mehr unter **Cyolo.io**

ÜBER BEARINGPOINT

BearingPoint ist Österreichs größte Management- und Technologie Beratung.
Mit mehr als 500 MitarbeiterInnen entwickeln wir innovative Strategien für neue und bestehende Geschäftsmodelle, designen und implementieren digitale Lösungen oder Services für führende Unternehmen und Organisationen aller Branchen sowie Organisationen der öffentlichen Hand.
Mit unserer Kompetenz in den Bereichen Management Beratung, Agile Transformation, technologiebasierte Business Services und smarte BearingPoint Software-Lösungen, entwickeln wir gemeinsam mit unseren Kunden und Partnern innovative Geschäftsmodelle. Zu BearingPoints Kunden gehören Österreichs führende Unternehmen und Organisationen. Das globale Netzwerk von BearingPoint mit mehr als 10.000 Mitarbeitern unterstützt Kunden in über 75 Ländern.

Erfahren Sie mehr unter **BearingPoint.com**