Umsetzungshinweise

OMICRON StationGuard und NIS Fact Sheet 9/2022

Autoren

Christian Brauner | christian.brauner@omicronenergy.com

Benjamin Teudeloff | benjamin.teudeloff@omicronenergy.com

Datum

28. September, 2023

Beschriebenes OMICRON-Produkt

StationGuard / GridOps

Anwendungsbereiche

Cybersecurity für KRITIS-Unternehmen

Schlagwörter

NISV

Kurzfassung

Das Dokument beschreibt die konkrete Anwendung der OMICRON Lösungen StationGuard und GridOps bezüglich NIS Fact Sheet 9/2022 sowie der rechtlichen Anforderungen gemäß NIS-Verordnung 2019. Sämtliche schwarz geschriebenen Textteile der nachfolgenden Erklärung wurden unverändert vom NIS Fact Sheet 9/2022[1] übernommen.

1) Siehe dazu: NIS Fact Sheet 9/2022; https://www.nis.gv.at/dam/jcr:bbe1c393-ba27-43b3-8d38-890610cfcc75/NIS_Factsheet_9_2022_1_0.pdf

OMICRON ist Ihr Partner für Cyber-Security-Lösungen

Wir sind seit über 30 Jahren verlässlicher Partner der Energieversorger und Netzbetreiber und verfügen über fundierte, langjährige Erfahrung in der Branche. Ein engagiertes Team aus über 1000 Mitarbeiter:innen an 24 Standorten unterstützt unsere Kund:innen in mehr als 171 Ländern. Unser technischer Support kümmert sich 24 Stunden am Tag, 7 Tage die Woche um Sie.

OMICRON arbeitet mit Leidenschaft an wegweisenden Ideen, um Energiesysteme sicherer und zuverlässiger zu machen. Mit unseren neuartigen Lösungen stellen wir uns den aktuellen und zukünftigen Herausforderungen unserer Branche. Wir zeigen vollen Einsatz bei der Unterstützung unserer Kund:innen:

Wir gehen auf ihre Kundenbedürfnisse ein, bieten ihnen hervorragenden Vor-Ort-Support und teilen unsere langjährige Expertise und unsere Erfahrungen mit ihnen. In der OMICRON-Gruppe entwickeln wir innovative Technologien für alle Bereiche elektrischer Energiesysteme. Im Fokus stehen Cyber-Security-Lösungen sowie elektrische Prüfungen an Mittel- und Hochspannungsbetriebsmitteln, Schutzprüfungen und Prüfungen digitaler Schaltanlagen.

Kund:innen in aller Welt vertrauen auf unsere einfach zu bedienenden Lösungen und schätzen deren Genauigkeit, Schnelligkeit und Qualität.

Wie wir Sie konkret bei der Umsetzung der „Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste“ gemäß NIS Fact Sheet 9/2022 unterstützen zeigen wir Ihnen unter folgenden Punkten auf:

- Ziffer 3.1 Systemkonfiguration
- Ziffer 3.2 Vermögenswerte
- Ziffer 6.1 Systemwartung und Betrieb
- Ziffer 6.2 Fernzugriff
- Ziffer 8.1 Erkennung von Vorfällen
- Ziffer 8.2 Protokollierung und Monitoring
- Ziffer 8.3. Korrelation und Analyse
- Ziffer 9.2 Vorfallsmeldung

OMICRON

Inhaltsverzeichnis

Einleitung

Hintergrund

Die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union („NIS-Richtlinie“) zielt darauf ab, ein höheres Sicherheitsniveau von Netz- und Informationssystemen in der EU zu erreichen.

Österreich setzt die NIS-Richtlinie mit dem am 28. Dezember 2018 kundgemachten Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG) um.

Mit einer Verordnung zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV) legt der Bundesminister für EU, Kunst, Kultur und Medien, im Einvernehmen mit dem Bundesminister für Inneres, Sicherheitsvorkehrungen für Betreiber wesentlicher Dienste fest.

Das vorliegende NIS Fact Sheet dient der näheren Erläuterung der in der Anlage 1 der NISV genannten Sicherheitsmaßnahmen, um Betreiber wesentlicher Dienste bei der Umsetzung der Vorgaben aus dem NISG und der NISV zu unterstützen. Diese werden den Beschreibungen jeweils vorangestellt, um den direkten Bezug zwischen NISV und dem vorliegenden NIS Fact Sheet zu ermöglichen.

Anwendbarkeit

Das NIS Fact Sheet hält sich weitgehend an die im Leitfaden der europäischen NIS-Kooperationsgruppe[1] formulierten Empfehlungen für Sicherheitsvorkehrungen, berücksichtigt aber auch nationale Besonderheiten und Erfahrungen aus den Sektorengesprächen. Aus Sicht des Bundeskanzleramts und des Bundesministeriums für Inneres stellt dieses NIS Fact

Sheet eine detailliertere Beschreibung der Sicherheitsmaßnahmen der NISV, die in ihrer Gesamtheit die Sicherheitsvorkehrungen bilden, dar.

Bei allen im NIS Fact Sheet beschriebenen Sicherheitsmaßnahmen ist bei der Umsetzung im Sinne des § 17 Abs. 1 NISG auf ein angemessenes Verhältnis zwischen dem feststellbaren Ausmaß einer Bedrohung und der wirtschaftlichen Belastung Wert zu legen. Wenn aus technischen oder betrieblichen Gründen die Umsetzung der die Sicherheitsmaßnahmen beschreibenden Ausführungen nicht gänzlich möglich ist, sind die dadurch bedingten Abweichungen bei der Umsetzung durch risikominimierende und/oder kompensierende Maßnahmen auszugleichen und dies entsprechend in den zu erbringenden Nachweisen (Aufstellung samt Prüfbericht) darzustellen und glaubhaft zu begründen.

NIS-Kooperationsgruppe

Um den Austausch zwischen den EU-Mitgliedstaaten im Bereich der Sicherheit von Netz- und Informationssystemen zu unterstützen, die strategische

1) CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services, abrufbar unter https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

Zusammenarbeit zu erleichtern und die Entwicklung von Grundsätzen für die europäische Zusammenarbeit bei Cyberkrisen zu fördern, wurde eine Kooperationsgruppe aus Vertretern der Mitgliedstaaten, der Europäischen Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) eingerichtet („NIS-Kooperationsgruppe").

Reference document on security measures for OES

Im Rahmen der Kooperationsgruppe werden in Work Streams Leitfäden und Referenzdokumente zu diversen informationssicherheitsrelevanten Themenbereichen erarbeitet. In dem Work Stream „Security measures for Operators of Essential Services (OES)" haben Mitgliedstaaten mit Unterstützung von ENISA einen Leitfaden für Betreiber wesentlicher Dienste erstellt, welcher als Grundlage zur Unterstützung für die Absicherung wesentlicher Dienste freiwillig verwendet werden kann. Dieses Referenzdokument ist auf der Homepage der Kooperationsgruppe zum Download verfügbar.[2]

Mapping internationaler Informationssicherheitsstandards und Best Practises

Die NIS-Richtlinie gibt vor, dass die Mitgliedstaaten bei der Umsetzung die Anwendung europäischer oder international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen zu fördern haben, um eine einheitliche Anwendung der Richtlinie zu gewährleisten.[3] Auf Basis dessen wurde innerhalb des Work Streams

„Security measures for Operators of Essential Services (OES)" eine Grundlage für ein Mapping erarbeitet und für die Mitgliedstaaten zur Verfügung gestellt. Dieses Mapping wurde mit nationalen Informationssicherheitsstandards erweitert und enthält demnach folgende Informationssicherheitsstandards und Best Practises:

- IEC 62443 Teil 3-3 („System security requirements and security levels", edition 1.0, 2013-08)
- IEC 62443 Teil 2-1 ("Security program requirements for IACS asset owners", draft - CDV, 2019-08)
- ÖNORM A 7700-4 (Ausgabe vom 2019-10-01)
- Österreichisches Informationssicherheitshandbuch – Version 4.3.0 (ÖISHB)
- ISO 27001
- CIS CSC 8.0
- KSÖ Cyber Risk Rating
- EN 50600

Es wird ausdrücklich darauf hingewiesen, dass die die in den folgenden Kapiteln angeführte beispielhafte Gegenüberstellung pro Sicherheitsmaßnahme keine direkte Verknüpfung zwischen den in der NISV definierten Sicherheitsmaßnahmen und etwaigen Standards und Normen darstellt. Diese beispielhaften Gegenüberstellungen mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises dienen zur Orientierung und Unterstützung bei der Umsetzung und Evaluierung von Sicherheitsmaßnahmen. Sicherheitsvorkehrungen bzw. Sicherheitsmaßnahmen sind lt. § 17 NISG dem Risiko angepasst und wirtschaftlich zu implementieren und zu überprüfen.

2) CG Publication 01/2018 - Reference document on security measures for Operators of Essential Services, abrufbar unter https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
3) Vgl. Art. 19 der NIS-Richtlinie.

1 Governance und Risikomanagement

1.1 Risikoanalyse

> NIS-Verordnung:
>
> Eine Risikoanalyse der Netz- und Informationssysteme ist durchzuführen. Dabei sind spezifische Risiken auf Grundlage einer Analyse der betrieblichen Auswirkungen von Sicherheitsvorfällen zu ermitteln und hinsichtlich der hohen Bedeutung des Betreibers wesentlicher Dienste für das Funktionieren des Gemeinwesens zu bewerten.

Der Betreiber führt eine Risikoanalyse durch und aktualisiert sie regelmäßig. Die Analyse identifiziert jene Netz- und Informationssysteme, die der Betreiber für die Bereitstellung des wesentlichen Dienstes (oder der wesentlichen Dienste) nutzt, sowie die dazugehörigen Risiken. Die Risiken umfassen alle Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit der identifizierten Netzund Informationssysteme haben, und die mit vernünftigem Aufwand feststellbar sind.

Diese Analyse bildet die Basis für die Fokussierung und Priorisierung von Sicherheitsmaßnahmen und -aktivitäten. Die Durchführung der Risikoanalyse beinhaltet, die oben erwähnte laufende Aktualisierung im Rahmen eines kontinuierlichen Verbesserungsprozesses (KVP).

Bei der Aktualisierung der Analyse werden insbesondere neue Bedrohungen, der Effektivitätsverlust umgesetzter Maßnahmen sowie Änderungen der Risikosituation, beispielsweise durch Änderungen in der Systemarchitektur, berücksichtigt.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- ÖISHB: Risikoanalyse
- ISO/IEC 27001: Information security risk assessment, Information security risk treatment
- IEC 62443 2-1: Security assessments and reviews
- EN 5600-1 und 50600-2-1: Risikoanalyse

1.2 Sicherheitsrichtlinie

> NIS-Verordnung:
>
> Eine Sicherheitsrichtlinie ist zu erstellen und periodisch zu aktualisieren.

Der Betreiber erstellt, pflegt und aktualisiert eine Sicherheitsrichtlinie, welche strategische Sicherheitsziele festlegt, das Risikomanagement beschreibt und auf alle relevanten weiteren spezifischen Sicherheitsvorgaben (Richtlinien, Guidelines etc.) verweist.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- > ÖISHB: Informationssicherheitsmanagementsystem, Informationssicherheitspolitik
- > ISO/IEC 27001: Information security policies
- > IEC 62443 2-1: Security related organization and policies

1.3 Überprüfungsplan der Netz- und Informationssysteme

NIS-Verordnung:

Die Durchführung der periodischen Überprüfung der Netz- und Informationssystemsicherheit ist zu planen und festzulegen.

Gemäß dem definierten Überprüfungsplan überprüft der Betreiber eigenständig die identifizierten Netz- und Informationssysteme.

Im Rahmen des Überprüfungsplans und in Abhängigkeit von der Risikoanalyse werden Überprüfungen der Netz- und Informationssysteme durchgeführt. Diese Prüfungen zielen darauf ab, die Anwendung, Wirksamkeit und Angemessenheit der definierten Sicherheitsmaßnahmen zu validieren.

Der Betreiber sorgt für eine Übersicht und eine laufend aktualisierte Dokumentation der durchgeführten Überprüfungen.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- > ÖISHB: Umsetzung des Informationssicherheitsplans, Informationssicherheit im laufenden Betrieb
- > ISO/IEC 27001: Information security Reviews, Information systems Audit considerations
- > IEC 62443 2-1: Security assessments and reviews
- > CIS CSC v8.0: Penetration Testing, Application Software Security

1.4 Ressourcenmanagement

NIS-Verordnung:

Die periodische Überprüfung des Informationssicherheitsmanagementsystems ist festzulegen und durchzuführen.

Der Betreiber stellt die kurz-, mittel- und langfristige Verfügbarkeit aller für die Funktionsfähigkeit der Netz- und Informationssysteme erforderlichen personellen, finanziellen sowie technischen Ressourcen sicher.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- > ISO/IEC 27001: Operational procedures and responsibilities
- > IEC 62443 2-1: System availability and intended functionality
- > CIS CSC v8.0: Audit Log Management

1.5 Informationssicherheitsmanagementsystemprüfung

NIS-Verordnung:

Die periodische Überprüfung des Informationssicherheitsmanagementsystems ist festzulegen und durchzuführen.

Anhand einer Reihe von Indikatoren und Methoden evaluiert der Betreiber die Einhaltung seiner Sicherheitsrichtlinie. Indikatoren können sich beispielsweise auf die Angemessenheit und Effektivität des Risikomanagements des Betreibers, die Wartung und den Betrieb von Ressourcen unter sicheren Bedingungen, die Zugriffsrechte der Benutzer sowie die Authentifizierung des Zugriffs auf Ressourcen und die Ressourcenverwaltung beziehen.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Security Compliance, Interne ISMS Audits
> ISO/IEC 27001: Information Security Reviews, Performance evaluation
> IEC 62443 2-1: Security assessments and reviews

1.6 Personalwesen

NIS-Verordnung:

Sicherheitsrelevante Aspekte sind in den Prozessen des Personalwesens zu berücksichtigen und umzusetzen.

Der Betreiber stellt sicher, dass Mitarbeiter vertrauenswürdig und sich ihrer Verantwortung bewusst sind. Der Betreiber stellt des Weiteren sicher, dass Mitarbeiter für die ihnen zugewiesenen Rollen qualifiziert sind.

Für die Fort- und Weiterbildung in sicherheitsrelevanten Themengebieten gibt es ein entsprechendes Schulungs- bzw. Ausbildungsprogramm.

Eine Sensibilisierung in Sicherheitsfragen für alle Mitarbeiter sowie ein spezielles Sicherheitstrainingsprogramm für Mitarbeiter mit spezifischer Verantwortung für Netz- und Informationssysteme wird durchgeführt.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Personelle Sicherheit
> ISO/IEC 27001: Human resource security
> IEC 62443 2-1: Security related organization and policies

2 Umgang mit Dienstleistern, Lieferanten und Dritten

Hinweis: Es macht hinsichtlich der Prüfanforderungen keinen Unterschied, ob Netz- und Informationssysteme, von denen der wesentliche Dienst abhängt, vom jeweiligen Betreiber selbst oder von einem Dienstleister betrieben werden. Eine Überprüfung durch eine qualifizierte Stelle ist jedenfalls notwendig.

Wenn das bei oder von einem Dienstleister betriebene Netz- und Informationssystem durch eines beim jeweiligen Betreiber betriebene Netz- und Informationssystem soweit ersetzt werden kann, dass der Ausfall bzw. die Nichtaufrechterhaltung der Integrität des Dienstleisters keine erheblichen Auswirkungen auf den wesentlichen Dienst hat, ist dieses Netz- und Informationssystem des Betreibers und das diesbezügliche Konzept bzw. der diesbezügliche Prozess einer Überprüfung durch eine qualifizierte Stelle zu unterziehen.

2.1 Beziehungen mit Dienstleistern, Lieferanten und Dritten

NIS-Verordnung:

Anforderungen an Dienstleister, Lieferanten und Dritte für den Betrieb von, einen sicheren Zugang zu und Zugriff auf Netz- und Informationssysteme sind festzulegen und periodisch zu überprüfen.

Der Betreiber erstellt ein Gesamtbild seines Ökosystems, einschließlich Dienstleister und Lieferanten mit vertraglichen Beziehungen sowie Dritter, insbesondere solcher, die Zugang zu den Netz- und Informationssystemen haben oder diese verwalten.

Der Zweck dieses Gesamtbilds ist es, Risiken und Abhängigkeiten, die sich aus den Beziehungen zu den Dienstleistern, Lieferanten und Dritten ergeben, zu identifizieren und zu bewerten. Um diese Bewertung durchzuführen, berücksichtigt der Verantwortliche zumindest die folgenden Fragestellungen:

> Reife: Über welche technischen Fähigkeiten verfügen die Dienstleister, Lieferanten und Dritten in Bezug auf Cybersicherheit?
> Vertrauen: Kann ich davon ausgehen, dass die Absichten des Dienstleisters, Lieferanten und Dritten mir gegenüber vertrauenswürdig und diese selbst zuverlässig sind?
> Zugriffsebene: Welche Zugangsrechte haben die Dienstleister, Lieferanten und Dritten zu Netz- und Informationssystemen?
> Abhängigkeit: Inwieweit ist die Beziehung zu Dienstleistern, Lieferanten und Dritten für die Tätigkeit entscheidend?

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Zusammenarbeit mit Externen, Evaluierung von Zertifizierungen, Lieferantenbeziehungen
> ISO/IEC 27001: Information security in supplier relationships
> IEC 62443 2-1: Supply chain security
> CIS CSC v8.0: Service Provider Management
> KSÖ Cyber Risk Rating: Anforderungen für A bzw. B Rating

2.2 Leistungsvereinbarungen mit Dienstleistern und Lieferanten

NIS-Verordnung:

Die Leistungsvereinbarungen mit Dienstleistern und Lieferanen sind periodisch zu überprüfen und zu überwachen.

Der Betreiber legt eine Richtlinie für seine Beziehungen zu Dienstleitern und Lieferanten fest, um die identifizierten Risiken zu minimieren. Ein besonderer Fokus wird hierbei auf Schnittstellen zwischen deren Netz- und Informationssystemen und jenen des Betreibers gelegt.

Generell müssen für Netz- und Informationssysteme, die von Dienstleistern betrieben werden, Sicherheitsanforderungen identifiziert und definiert werden. Der Betreiber stellt durch Service Level Agreements (SLA) und/oder Prüfmechanismen sicher, dass seine Dienstleister und Lieferanten ebenfalls angemessene Sicherheitsmaßnahmen umsetzen, um den Sicherheitsanforderungen des Betreibers zu entsprechen.

Der Betreiber definiert mit seinen Dienstleistern und Lieferanten

Reaktions- und Wiederherstellungsprozesse nach (Sicherheits-)Vorfällen und überprüft diese periodisch.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- ÖISHB: Zusammenarbeit mit Externen, Lieferantenbeziehungen
- ISO/IEC 27001: Information security in supplier relationships
- IEC 62443 2-1: Supply chain security
- CIS CSC v8.0: Service Provider Management
- KSÖ Cyber Risk Rating: Anforderungen für A bzw. B Rating

3 Sicherheitsarchitektur

3.1 Systemkonfiguration

NIS-Verordnung:

Netz- und Informationssysteme sind sicher zu konfigurieren. Diese Konfiguration ist strukturiert zu dokumentieren. Die Dokumentation ist aktuell zu halten.

Der Betreiber verwendet nur Ressourcen (z.B. Dienste und Geräte), die für den Betrieb der Netz- und Informationssysteme notwendig sind.

Bei der Installation und im gesamten Lebenszyklus verfolgt der Betreiber einen Systemhärtungsansatz.

Zudem sorgt der Betreiber dafür, dass die Konfiguration aller relevanten Komponenten dokumentiert wird. Der Betreiber aktualisiert diese Dokumentation regelmäßig.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- ÖISHB: Dokumentation
- ISO/IEC 27001: Operational procedures and responsibilities, Control of operational software
- IEC 62443 2-1: Secure development and support, System segmentation, Devices and Media, Malware protection, Protection of Data, Identification and authentication
- CIS CSC v8.0: Secure Configuration of Enterprise Assets and Software, Application Software Security

So unterstützt Sie OMICRON bei der Systemhärtung

StationGuard erkennt und stellt alle Dienste und Geräte im Netzwerk dar. Zusätzliche, nicht für den Betrieb erforderliche Dienste können hierdurch leicht identifiziert werden. Zum Beispiel nicht unbedingt benötigte Dienste auf Windows-PCs im Netzwerk, wie IPv6 und Dateifreigabe. Diese werden erkannt und gemeldet. Noch nicht oder nicht ausreichend gehärtete Geräte oder PC können somit einfach identifiziert und Risiken minimiert werden.

3.2 Vermögenswerte

NIS-Verordnung:

Vermögenswerte, die im Zusammenhang mit Netz- und Informationssystemen stehen, sind strukturiert zu analysieren und zu dokumentieren.

Der Betreiber erstellt ein geeignetes Konzept zur Verwaltung von Vermögenswerten (Assets) für die Identifizierung, Klassifizierung und Inventarisierung der IT-Prozesse, -Systeme, -Komponenten sowie Softwareplattformen/-Lizenzen und Applikationen. Im Inventar sind je Vermögenswert klare Rollen und Verantwortlichkeiten definiert und diese im Hinblick auf ihre Kritikalität klassifiziert.

Das Inventar unterstützt unter anderem das Ausrollen von Updates und Patches und ermöglicht gegebenenfalls eine Ermittlung, welche Komponenten von neuen Sicherheitsproblemen oder Schwachstellen betroffen sind.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- ÖISHB: Vermögenswerte und Klassifizierung von Informationen, Lizenzverwaltung und Versionskontrolle von Standardsoftware
- ISO/IEC 27001: Asset management
- IEC 62443 2-1: Inventory management of IACS hardware/software components and network communication
- CIS CSC v8.0: Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Access Control Management

So unterstützt Sie OMICRON beim Assetmanagement

Die StationGuard-Lösung identifiziert und inventarisiert alle im OT-Netzwerk detektierten Geräte und stellt das gesamte OT-Netzwerk mit allen zugehörigen Geräten grafisch dar. Mit unserer Benutzeroberfläche können Sie von einer zentralen Übersicht auf Netzebene aus in die detaillierte Visualisierung eines einzelnen OT-Netzwerks abtauchen. Dafür steht das gewohnte ZeroLine-Diagramm von StationGuard zur Verfügung und kann bei Bedarf auf ihre Betreiberanlage angepasst werden.

GridOps erstellt ein standortübergreifendes, durchsuchbares Anlageninventar, das alle Ihre von sämtlichen StationGuard Sensoren im Netz erkannten Geräte auflistet. Die Assets bzw. Betriebsmittel werden mit den zugehörigen Eigenschaften in einer Tabelle aufgelistet, welche laufend in Echtzeit aktualisiert wird.

In Verbindung mit den beispiellosen Möglichkeiten von StationGuard, genaueste Detailinformationen über jedes Betriebsmittel abzurufen (beispielsweise durch Importieren von SCL-Dateien oder von Arbeitsblättern mit den Betriebsmitteldaten aus der Anlagendokumentation), bietet Ihnen GridOps eine leistungsstarke Lösung für die Verwaltung Ihres Anlageninventars dar. Das automatische Anlageninventar funktioniert auch für StationGuard Sensoren, die nur temporär aktiv sind, wie beispielsweise die mobile Version von StationGuard auf der MBX1-Plattform.

Für ein erfolgreiches Schwachstellen- und Risikomanagement analysiert und bewertet GridOps automatisch alle Daten der einzelnen Assets/Betriebsmittel. Schwachstellen in der von OMICRON gepflegten Vulnerabilitäts-Datenbank werden automatisch mit den Produktnamen und Firmwareständen der Betriebsmittel abgeglichen und -falls zutreffend- dem Benutzer als relevante Schwachstelle mitgeteilt. In der Datenbank sind die im OT-Bereich verbreiteten Produkte wie Feldleitgeräte, Schutzgeräte, industrielle Switche, etz. enthalten und werden von den OMICRON Spezialisten laufend aktualisiert. Grundlage der Datenbank sind die von den Herstellern veröffentlichten Schwachstellen (CVE Security Advisories).

3.3 Netzwerksegmentierung

NIS-Verordnung:

Eine Segmentierung der Netzwerke ist innerhalb der Netz- und Informationssysteme abhängig vom Schutzbedarf vorzunehmen.

Der Betreiber trennt seine Systeme physisch oder logisch je nach Schutzbedarf und Klassifikation, um Auswirkungen von (Sicherheits-)Vorfällen innerhalb seiner Systeme einzudämmen.

Der Betreiber gestattet nur Verbindungen zwischen Systemen mit unterschiedlichem Schutzbedarf und unterschiedlicher Klassifikation, die für das Funktionieren der Netz- und Informationssysteme von signifikanter Bedeutung sind.

Für solche Schnittstellen (z.B. Schnittstellen zwischen den Netz- und Informationssystemen von Lieferanten und Kunden) dokumentiert der Betreiber angemessene Sicherheitsmechanismen und setzt diese um. Dies umfasst unter anderem Prozesse und Verfahren für einen sicheren Zugriff, Fernzugriff, Monitoring oder Datenaustausch.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Sicherheitsmanagement in der Kommunikation
> ISO/IEC 27001: Communications security
> IEC 62443 2-1: Network and communications security
> CIS CSC v8.0: Network Infrastructure Management

3.4 Netzwerksicherheit

NIS-Verordnung:

Die Sicherheit innerhalb der Netzwerksegmente und der Schnittstellen zwischen den Netzwerksegmenten ist zu gewährleisten.

Der Betreiber filtert den eingehenden und ausgehenden Netzwerkverkehr und begrenzt diesen auf das für das Funktionieren der Netz- und Informationssysteme unbedingt erforderliche Maß.

Der Betreiber filtert auch den Netzwerkverkehr innerhalb des Netzwerks und verbietet jeglichen Netzwerkverkehr, der für das Funktionieren seiner Systeme nicht erforderlich ist und potenzielle Angriffe erleichtern kann.

Hierzu definiert und aktualisiert der Betreiber die Filterregeln regelmäßig nach Netzadresse, Portnummer, Protokoll usw.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Sicherheitsmanagement in der Kommunikation
> ISO/IEC 27001: Communications security
> IEC 62443 2-1: Network and communications security
> CIS CSC v8.0: Network and communications security, Network Monitoring and Defense

3.5 Kryptographie

NIS-Verordnung:

Vertraulichkeit, Authentizität und Integrität von Informationen sind durch den angemessenen und wirksamen Einsatz kryptographischer Verfahren und Technologien sicherzustellen.

Der Betreiber legt Richtlinien und Verfahren für den Einsatz von Kryptographie und Schlüsselmanagement fest, um deren angemessene und wirksame Verwendung zum Schutz der

Vertraulichkeit, Authentizität und/oder Integrität von Informationen und Systemen in seinen Netz- und Informationssystemen sicherzustellen.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- ÖISHB: Kryptographie
- ISO/IEC 27001: Cryptography
- IEC 62443 2-1: Protection of Data
- CIS CSC v8.0: Data Protection, Application Software Security

4 Systemadministration

4.1 Administrative Zugangsrechte

NIS-Verordnung:

Administrative Zugangsrechte sind eingeschränkt nach dem Minimalrechtsprinzip zuzuweisen. Diese Zuweisungen sind periodisch zu überprüfen und gegebenenfalls anzupassen.

Der Betreiber richtet – soweit dies vom System unterstützt wird – dedizierte und personalisierte Konten für die Administration ein, die zum Zweck der Installation, Konfiguration, Verwaltung, Wartung usw. verwendet werden dürfen. Diese Konten werden auf einer stets aktualisierten Liste dokumentiert und in einem regelmäßigen Review-Prozess überprüft, wobei eine solche Liste auch für nicht administrative Konten geführt wird.

Die erteilten administrativen Berechtigungen werden individualisiert auf den funktionalen und technischen Aufgabenbereich des jeweiligen administrativen Benutzerkontos beschränkt. Diese Benutzerkonten werden nur zum Zweck der Administration selbst und für die Verbindung zu administrativen Systemen verwendet. Ein Einsatz für nicht administrative Tätigkeiten wird untersagt.

Bei der Vergabe von administrativen Konten werden Anforderungen der Pflichtentrennung berücksichtigt und administrative Tätigkeiten protokolliert.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- ÖISHB: Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung, Protokollierung und Monitoring
- ISO/IEC 27001: User access management
- IEC 62443 2-1: Authorization and access control

8) Eigenes oder das eines Dienstleisters

9) Das CVSS (Common Vulnerability Scoring System) ist der Industriestandard zur Bewertung des Schweregrades von möglichen Schwachstellen oder Sicherheitslücken.

> CIS CSC v8.0: Account Management, Access Control Management, Audit log Management

4.2 Systeme und Anwendungen zur Systemadministration

NIS-Verordnung:

Systeme und Anwendungen zur Systemadministration sind ausschließlich für Tätigkeiten zum Zweck der Systemadministration zu verwenden. Die Sicherheit dieser Systeme und Anwendungen ist zu gewährleisten.

Für die Durchführung von Administrationstätigkeiten werden nur Systeme eingesetzt, die der Betreiber oder Dienstleister für diesen Zweck vorgesehen hat. Hardund Software, die für administrative Tätigkeiten verwendet werden, werden vom Betreiber oder gegebenenfalls vom Dienstleister, den der Betreiber zur Durchführung von administrativen Tätigkeiten autorisiert hat, verwaltet und sicher konfiguriert.

Administrative Systeme werden ausschließlich zur Durchführung von administrativen Tätigkeiten verwendet und nicht für andere Tätigkeiten genutzt. Insbesondere werden sie nicht für den Zugriff auf das Internet verwendet. Benutzer und Benutzerinnen verbinden sich keinesfalls über eine Softwareumgebung, die für andere Funktionen als die Administration eingesetzt wird, mit einem System, das für administrative Tätigkeiten verwendet wird. Hinsichtlich der Nutzung von sog. „Jumpservern"/„Jumphosts" zur Durchführung administrativer Tätigkeiten siehe Kapitel 6.2 Fernzugriff.

Der Betreiber richtet ein dediziertes logisches oder physisches Netzwerk ein, um die administrativen Systeme mit den zu verwaltenden Systemen zu verbinden.

Für administrative Tätigkeiten werden sichere, den aktuellen Stand der Technik berücksichtigende Protokolle, Authentifizierungs- und Verschlüsselungsmechanismen eingesetzt.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Fernzugriff, Zugriff auf Betriebssysteme, Zugriff auf Anwendungen und Informationen Protokollierung und Monitoring
> ISO/IEC 27001: System and application access control
> CIS CSC v8.0: Audit Log management, Network Infrastructure Management

5 Identitäts- und Zugriffsmanagement

5.1 Identifikation und Authentifikation

NIS-Verordnung:

Es sind Verfahren umzusetzen und Technologien einzusetzen, die die Identifikation und Authentifikation von Benutzern und Diensten gewährleisten.

Zur Identifikation richtet der Betreiber entsprechend einem definierten und dokumentierten Verfahren eindeutige Konten für Benutzer oder für

automatisierte Prozesse ein, die auf Netz- und Informationssysteme zugreifen müssen. Nicht genutzte oder nicht mehr benötigte Konten müssen deaktiviert werden. Hierzu wird ein regelmäßiger Überprüfungsprozess eingerichtet.

Für die Authentifikation schützt der Betreiber den Zugriff auf Ressourcen seines Netz- und Informationssystems durch Benutzer oder automatisierte Prozesse mit einem sicheren Authentifikationsmechanismus. Der Betreiber definiert die Regeln für die Verwaltung der Authentifizierungsdaten.

Wann immer es erforderlich ist, ändern die Benutzer ihre Authentifizierungsdaten entsprechend definierten Vorgaben regelmäßig. Insbesondere ändert der Betreiber vor Inbetriebnahme eines Systems die vom Hersteller/Lieferanten installierten Standard-Authentifizierungsdaten.

Der Einsatz von Verfahren zur Zwei-Faktor-Authentifizierung wird vom Betreiber in seiner Architektur berücksichtigt und gezielt vorangetrieben.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- ÖISHB: Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung
- ISO/IEC 27001: Access Control
- IEC 62443 2-1: User access control
- CIS CSC v8.0: Account Management, Access Control Management

5.2 Autorisierung

NIS-Verordnung:

Es sind Verfahren umzusetzen und Technologien einzusetzen, die unautorisierte Zugriffe auf Netz- und Informationssysteme unterbinden.

Der Betreiber gewährt definierten Regeln folgend Benutzern oder automatisierten Prozessen nur dann Zugriffsrechte, wenn deren Zugriff für die Erfüllung von Aufgaben oder die Durchführung automatisierter Prozesse unbedingt erforderlich ist. Eine Vergabe von Zugriffsrechten erfolgt immer unter Anwendung des definierten Rechteanforderungsprozesses, in dem die Pflichtentrennung entsprechend berücksichtigt wird. Es werden Maßnahmen umgesetzt, um die Einhaltung des Grundsatzes „Need-to-know“ bzw. des Minimalrechtsprinzips zu gewährleisten.

Der Betreiber überprüft diese Zugriffsrechte mindestens einmal jährlich, wobei er die Benutzerkonten, deren zugehörige Zugriffsrechte und die entsprechenden Systeme oder Funktionalitäten, auf die mit diesen Zugriffsrechten zugegriffen wird, überprüft.

Der Betreiber führt und aktualisiert eine Liste der privilegierten Konten (z.B. von administrativen Konten). Der Betreiber überprüft jede mögliche Änderung an einem privilegierten Benutzerkonto, um sicherzustellen, dass die Zugriffsrechte auf Systeme und Funktionalitäten dem Minimalrechteprinzip entsprechen und für die Nutzung des Benutzerkontos angemessen sind.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- > ÖISHB: Zugriffskontrolle, Berechtigungssysteme, Schlüssel- und Passwortverwaltung
- > ISO/IEC 27001: Access Control
- > IEC 62443 2-1: User access control
- > CIS CSC v8.0: Account Management, Access Control Management

6 Systemwartung und Betrieb

6.1 Systemwartung und Betrieb

NIS-Verordnung:

Abläufe und Vorgänge zur Gewährleistung eines sicheren Systembetriebs von Netz- und Informationssystemen sind einzuführen und periodisch zu überprüfen.

Der Betreiber definiert Verfahren und Bedingungen, unter denen die Sicherheit seiner Netz- und Informationssysteme im Betrieb sichergestellt ist. Unter anderem wird auch ein Verfahren definiert, um Informationen über Schwachstellen und zugehörige Patches, die Netz- und Informationssysteme betreffen, zu sammeln und davon abgeleitet entsprechende Schritte zu setzen. Ein entsprechendes Verfahren kann sowohl manuelle als auch automatische Komponenten enthalten. Es wird explizit keine spezifische technische Maßnahme vorgegeben, da das entsprechende Verfahren von der Systemumgebung und Risikobeurteilung abhängt.

Der Betreiber stellt sicher, dass die eingesetzten Systemversionen aus sicherheitstechnischer Sicht auf dem aktuellen Stand sind. Der Betreiber überprüft Herkunft und Integrität der jeweiligen Systemversion vor ihrer Installation beziehungsweise vor ihrer Aktualisierung und analysiert die technischen und betrieblichen Auswirkungen dieser Version auf das betreffende Netz- und Informationssystem.

Der Betreiber stellt sicher, dass Komponenten der Netz- und Informationssysteme regelmäßig entsprechend ihrer Wartungsintervalle gewartet werden und protokolliert die Durchführung.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- > ÖISHB: Informationssicherheit im laufenden Betrieb, Sicherheitsmanagement im Betrieb, Wartung
- > ISO/IEC 27001: System acquisition, development and maintenance, Equipment
- > IEC 62443 2-1: Component Security, Inventory management of IACS hardware/software components and network communication
- > CIS CSC v8.0: Secure configuration of Enterprise Assets and Software, Continuous Vulnerability Management

10) Dieser Abschnitt wird perspektivisch in die OH Nachweise integriert.

11) Bei der Wahl geeigneter Maßnahmen zur Erfüllung der Anforderungen ist der Betreiber frei.

So unterstützt Sie OMICRON bei der Systemwartung und dem Betrieb

StationGuard ist ein Angriffserkennungssystem (engl. Intrusion Detection System, IDS) und erfüllt u.a. alle rechtlichen und technischen Anforderungen des IT-SiG 2. 0 der Bundesrepublik Deutschland für ein System zur Angriffserkennung (SzA) und schützt ihre Betreiberanlage vor Cyber Risiken und Bedrohungen in Ihrem OT-Netzwerk.

Eine zusätzliche Besonderheit unseres StationGuard ist die integrierte Funktionsüberwachung. Hierdurch können Sie den ordnungsgemäßen Betrieb ihrer Automatisierungssysteme und Netzwerke überwachen und damit Abweichungen vom Normalzustand feststellen. Dies können beispielsweise sein (Auszug):

- die Überwachung der Konfigurationsrevisionsfelder von Nachrichten im Netzwerk,
- die Detektion und Alarmierung von Änderungen an der Konfiguration von IEDs,
- die Überwachung der IEC-61850-Konfigurationsparameter mit ihrer Einsatzumgebung oder SCL-Datei,
- die Detektion von Konfigurationsfehlern von IEDs (falsche VLAN-Konfiguration, falsche Datasets, fehlerhafte GOOSE-Parameter, etc.),
- die Detektion von Überlast, aufgrund eines DOS-Angriffs oder eines unerwartet langsamen Netzwerks,
- die Detektion fehlerhafter und fehlgeschlagener Zeitsynchronisation,
- die Detektion fehlgeschlagener Steuerbefehle (z.B. in MMS, IEC-60870-5-104),
- die Detektion von Protokoll- und Interoperabilitätsproblemen (z.B. in GOOSE-, Sampled-Values-Einstellungen, etc.),
- Detektion nicht vorhandener und ausgefallener GOOSE-Kommunikation,
- die Überwachung und Protokollierung von Dateiübertragungen, z.B. bei Störschrieben und Protokollierung von Schaltbefehlen (z.B. in MMS, IEC-60870-5-104) sowie
- die Aufzeichnung von Rohdaten (PCAP-Daten) für jedes Ereignis zur weiteren Analyse und forensischen Auswertung.

So unterstützt Sie OMICRON beim Schwachstellen- und Vulnerabilitymanagement

Unsere StationGuard-Lösung verfügt über eine Vulnerability-Datenbank, mit der alle Assets hinsichtlich Schwachstellen Live überwacht werden können. Diese Datenbank enthält für jedes Asset alle CVE-Schwachstellen die durch den Hersteller der Geräte veröffentlicht wurden.

Dank unseres integrierten Schwachstellenmanagements veranschaulicht Ihnen GridOps

- welche ihrer Schutz- und Automatisierungsgeräte von einer offengelegten Schwachstelle (CVE oder Security Advisory) betroffen sind,
- bewertet automatisch auf Basis des CVSS deren Kritikalität und
- zeigt Ihnen die Möglichkeit für Gegenmaßnahmen wie zum Beispiel ein Firmware-Update oder Konfigurationshinweise auf.

Unsere Vulnerability-Datenbank kann offline oder online upgedatet werden.

6.2 Fernzugriff

NIS-Verordnung:

Fernzugriff ist eingeschränkt nach dem Minimalrechtsprinzip und zeitlich beschränkt zu vergeben. Die Fernzugriffsrechte sind periodisch zu überprüfen und gegebenenfalls anzupassen. Die Sicherheit des Fernzugriffs ist zu gewährleisten.

Der Betreiber etabliert Prozesse zur Verwaltung von Fernzugriffen. Insbesondere stellt er Techniken zur Verfügung, die Fernzugriffe auf Netz- und Informationssysteme nur nach dem Minimalrechtsprinzip autorisiert und zeitlich beschränkt ermöglichen.

Die Authentifizierung im Rahmen des Fernzugriffs wird mittels Zwei-Faktor-Authentifizierung umgesetzt. Jeglicher unautorisierte Zugriff wird unterbunden.

Für Wartungsarbeiten, die über Fernzugriffe erfolgen, stellt der Betreiber sicher, dass alle Tätigkeiten und Operationen aufgezeichnet und dokumentiert werden. Alle Zugriffe externer Personen können nur unter Kontrolle der Systemverantwortlichen erfolgen.

Der Einsatz von sog. „Jumpservern"/„Jumphosts", bspw. für die Durchführung administrativer Tätigkeiten, ist durchaus möglich. Die Konfiguration der Jumpserver/Jumphosts für die Nutzung durch MitarbeiterInnen, welche sich aus einem Netzwerkabschnitt mit geringerem Schutzbedarf von einem Gerät verbinden bzw. der Einsatz von Sicherheitsmaßnahmen bei ebenjenen, hat den Vorgaben zur Fernwartung von Externen zu entsprechen.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Fernzugriff
> ISO/IEC 27001: Mobile devices and teleworking
> IEC 62443 2-1: Secure remote access
> CIS CSC v8.0: Network Infrastructure Management

So unterstützt Sie OMICRON bei der Überwachung der Fernzugriffe

StationGuard verfügt über eine separate Betriebsart „Wartung":

Während einer (Fern-)Wartung tritt im Anlagennetzwerk typischerweise Verkehr auf, der während des Normalbetriebs nicht vorhanden ist, also beispielsweise Verkehr von Konfigurationstools, die sich mit IEDs verbinden und deren Einstellungen anpassen. Um zu verhindern, dass durch solchen Verkehr zusätzliche Alarme ausgelöst werden, können Sie StationGuard bekannt geben, dass das System aktuell gewartet wird. Dann wird eine Detektionskonfiguration verwendet, die zusätzlich zu den Berechtigungen für den normalen Betrieb noch weitere spezifische Berechtigungen für den während der Wartung auftretenden Verkehr enthält.

Andererseits führen unautorisierte Fernwartungszugriffe – z.B. wenn sich die Anlage nicht im Wartungsmodus befindet oder der Zugriff durch eine nicht freigegebene IP/MAC Adresse bzw. Protokollservice erfolgt - automatisch zu einem Alarm.

7 Physische Sicherheit

7.1 Physische Sicherheit

NIS-Verordnung:

Der physische Schutz der Netz- und Informationssysteme, insbesondere der physische Schutz vor unbefugtem Zutritt und Zugang, ist zu gewährleisten.

Der Betreiber verhindert unbefugten physischen Zugang zu, Zugriff auf, Beschädigung von und Eingriffe in Netz- und Informationssysteme. Insbesondere erstellt der Betreiber ein physisches Sicherheitskonzept inkl. einer entsprechenden Definition unterschiedlicher Sicherheitszonen und definiert Verfahren für den sicheren Umgang mit Besuchern und betriebsfremdem Personal (wie etwa Wartungstechniker, Dienstleister, Lieferanten oder Dritte).

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Physische und umgebungsbezogene Sicherheit
> ISO/IEC 27001: Physical and environmental security
> IEC 62443 2-1: Security of physical access
> EN 50600-2-1 und 50600-2-5: Gebäudekonstruktion, Sicherungssysteme

8 Erkennung von Vorfällen

8.1 Erkennung

NIS-Verordnung:

Mechanismen zur Erkennung und Bewertung von Vorfällen sind umzusetzen.

Der Betreiber richtet ein System zur Erkennung von sicherheitsrelevanten Ereignissen ein. Die hierzu im Netzwerk und auf Systemkomponenten eingerichtete Sensorik analysiert übertragene Daten, Datenströme, Protokolle sowie das Verhalten einzelner Systeme oder Komponenten selbst, um Ereignisse zu erkennen, welche die Sicherheit der Netz- und Informationssysteme beeinträchtigen können. Dieses System ist so einzurichten, dass es zumindest alle zwischen den Netz- und Informationssystemen des Betreibers und denen der Lieferanten und Dienstleister ausgetauschten Datenströme erfasst. Der Betreiber definiert Standardwerte für zulässige System- und Netzwerkoperationen und zu erwartende Datenflüsse und Aktivitäten.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- ÖISHB: Schutz vor Schadprogrammen und Schadfunktionen, Protokollierung und Monitoring
- ISO/IEC 27001: Logging and monitoring, Protection from malware
- IEC 62443 2-1: Event and incident management, Security assessments and reviews
- CIS CSC v8.0: Network Monitoring and Defense, Malware Defenses

So unterstützt Sie OMICRON bei der Erkennung von Vorfällen

StationGuard überwacht und validiert den gesamten OT-Netzwerkverkehr bis ins kleinste Detail und erkennt unverzüglich sicherheitsrelevante Ereignisse und Bedrohungen für ihre OT/IT. Darüber hinaus detektiert StationGuard automatisch evtl. vorhandene Funktionsstörungen sowie Kommunikations- und Konfigurationsfehler innerhalb ihrer Betreiberanlage.

Ferner unterstützt Sie unsere Deep Packet Inspection (DPI) mit einer effektiven Anomalieerkennung, um Sie frühzeitig vor Cyber Angriffen zu schützen. Wir analysieren detailliert die übertragenen Datenpakete und der Inhalte in Ihrem OT-Netzwerk.

Unterstützte OT-Protokolle (Auszug):	Unterstützte IT-Protokolle (Auszug, mehr als 300):
> IEC 60870-5-104 > IEC 61850 (MMS, GOOSE) > IEC 60870-6 TASE.2/ICCP > Modbus TCP > DNP3 > IEC 62439-3 PRP und HSR (mit RedBox) > IEC 62056 (DLMS/COSEM) > IEEE C37.118 (Synchrophasor Protocol) > IEEE 1703-2012 / ANSI C12.22 (AMI Protocol) > EtherNet/IP > CIP > OPC UA > S7 Protocol > Profinet > EtherCAT > …	> FTP > HTTP > SSH, HTTPS (Applikationserkennung ohne Entschlüsselung) > RDP > NTP > SNMP > STP, CDP > netbios (Windows Dateifreigabe) > ARP, DHCP > MySQL, MSSQL, PostgreSQL > telnet > ICMP, ICMPv6 > RIPv2 > SSDP > MDNS > ...

So unterstützt Sie OMICRON bei der Bewertung von Vorfällen

StationGuard erkennt und meldet sicherheitsrelevante Ereignisse in Ihrem OT-Netzwerk, wenn eine Abweichung vom Sollverhalten der Anlage detektiert wird. Für jeden Eintrag im Ereignisprotokoll werden

> der Schweregrad (Information, Warnung, Fehler oder kritischer Alarm),
> der Zeitpunkt der Detektion (Datum und Uhrzeit),
> die beteiligten Geräte und
> eine beschreibende Meldung angegeben.

Ihre Mitarbeiter können die Alarmmeldungen jederzeit einsehen und bei Bedarf den Alarmierungsmechanismus anpassen, d.h. das zugrundeliegende Ereignis in die Allowlist mit aufnehmen und damit zukünftig eine False-Positive-Alarmierung dieses Ereignisses zu verhindern. Sofern erforderlich, kann die Allowlist aufgrund sich ändernder Systembedingungen oder rechtlicher Anforderungen von Ihren Mitarbeitern angepasst werden. OMICRON unterstützt Sie hierbei gerne.

8.2 Protokollierung und Monitoring

NIS-Verordnung:

Mechanismen zu Protokollierung und Monitoring, insbesondere von für die Erbringung des wesentlichen Dienstes essentiellen Tätigkeiten und Vorgängen, sind umzusetzen.

Der Betreiber implementiert in seinen Netz- und Informationssystemen Mechanismen zu Protokollierung und Monitoring. Die Protokollierung umfasst u.a. die Anwendungsserver, System- und Netzwerkinfrastrukturserver, Sicherheitstechnologien und -systeme, Technik- und Wartungsstationen von Industriesystemen, Netzwerkausrüstungen und administrative Arbeitsstationen, die kritische Aktivitäten unterstützen. Der Betreiber erfasst im Protokollierungssystem Ereignisse mit Zeit- und Datumsstempel (unter Verwendung synchronisierter Zeitquellen) und bewahrt die Informationen für einen definierten Zeitraum in zentralen Archiven auf.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Protokollierung und Monitoring
> ISO/IEC 27001: Logging and monitoring
> IEC 62443 2-1: Event and incident management
> CIS CSC v8.0: Network Monitoring and Defense, Audit Log Management

So unterstützt Sie OMICRON bei der Protokollierung und Monitoring

StationGuard erkennt und meldet sicherheitsrelevante Ereignisse in Ihrem OT-Netzwerk, wenn eine Abweichung vom Sollverhalten der Anlage detektiert wird. Für jeden Eintrag im Ereignisprotokoll werden.

Jedes Ereignis bzw. jeder Alarm wird Ihnen in einem Übersichtsdiagramm in der Benutzeroberfläche von StationGuard angezeigt. Für das betroffene Gerät werden folgende Informationen sofort dargestellt:

> eindeutige Zuordnung der Quelle
> Zuordnung des Ziels (betroffenes Gerät)
> Zuordnung der Kommunikationsverbindung.

Bei Anwahl des betroffenen Gerätes werden in der Detailansicht weiter detaillierte Informationen zum Ereignis bzw. Alarm angezeigt. Die konkrete Meldung kann folgende Informationen enthalten (Auszug):

> Ereignis- bzw. Alarmtext
> Schweregrad der Meldung
> Datum und Uhrzeit der Meldung
> Hilfe ID (mit Hyperlink zur StationGuard Hilfe)
> Schnittstelle des detektierenden StationGuard
> Quelle und Ziel mit Angabe von MAC/IP Adresse sowie Portnummer
> Service mit Angabe von Anwendungs-/Transport- und Vermittlungsschicht
> Freigabe und Ausnahmeinformationen

Alle Ereignisse werden in der Ereignisliste chronologisch angezeigt. Die Ereignisliste enthält drei Spalten in denen der Schweregrad, Datum und Uhrzeit sowie Ereignistext angezeigt werden. Mittels Filter- und Sortierfunktionen behalten Ihre Mitarbeiter auch bei mehreren Ereignissen stets den Überblick.

Alle von unserer StationGuard-Lösung erfassten Ereignisse werden als Rohdaten bzw. PCAP-Daten aufgezeichnet. Mittels GridOps können diese zentral gespeichert und exportiert werden.

8.3 Korrelation und Analyse

NIS-Verordnung:

Mechanismen zur Erkennung und adäquaten Bewertung von Vorfällen durch die Korrelation und Analyse der ermittelten Protokolldaten sind umzusetzen.

Zur Korrelation und Analyse verwendet der Betreiber ein System, das sicherheitsrelevante Ereignisse zusammenfasst und auswertet, um Vorfälle zu erkennen.

Der Betreiber richtet ein spezielles Informationssystem für die Korrelation, Analyse und weitere Bearbeitung von Vorfällen ein. Der Betreiber berücksichtigt bei der Konzeption dieses Systems insbesondere die Vertraulichkeit der gespeicherten Daten.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Protokollierung und Monitoring
> ISO/IEC 27001: Logging and monitoring
> IEC 62443 2-1: Event and incident management
> CIS CSC v8.0: Network Monitoring and Defense, Audit Log Management

So unterstützt Sie OMICRON bei der Korrelation und Analyse

StationGuard erkennt und meldet sicherheitsrelevante Ereignisse in Ihrem OT-Netzwerk. Jedes Ereignis (Information, Warnung, Fehler oder kritischer Alarm) bzw. jeder Alarm wird Ihnen in einem Übersichtsdiagramm in der Benutzeroberfläche von StationGuard angezeigt.

Zudem können Sie SIEM- und Ticket-Systeme (wie bspw. Splunk, FortiSiem oder ServiceNow) einfach anbinden. Dies erfolgt über integrierte Plug-ins mit denen automatisch Tickets zur Bearbeitung von IDS-Alarmen erstellt werden können. Durch den Import des Asset- bzw. Betriebsmittelverzeichnisses aus StationGuard werden die Tickets automatisch den verantwortlichen Mitarbeitern zugewiesen, die für das betreffende Betriebsmittel oder den Standort zuständig sind.

Alternativ dazu können unsere leicht verständlichen Alarmmeldungen auch über das Syslog-Protokoll weitergeleitet werden.

Die Datenübertragung zwischen StationGuard, den Benutzeroberflächen von StationGuard und GridOps bzw. den angebundenen Systemen (Ticket, SOC, SIEM, etc.) und SIEM erfolgt TLS(1.3) verschlüsselt.

9 Bewältigung von Vorfällen

9.1 Vorfallsreaktion

NIS-Verordnung:

Prozesse zur Reaktion auf Vorfälle sind zu erstellen, aufrechtzuerhalten und zu erproben.

Der Betreiber erstellt und implementiert Prozesse und Verfahren zur Reaktion auf Vorfälle, die das Funktionieren oder die Sicherheit eines Netz- und Informationssystems beeinträchtigen. Der Betreiber legt diesbezüglich klare Rollen und Verantwortlichkeiten fest. Die Prozesse und Verfahren werden regelmäßig aktualisiert und durch Tests bzw. Übungen überprüft.

Der Betreiber stellt sicher, dass forensisches Wissen und Kapazitäten entweder hausintern zur Verfügung stehen oder über einen Vertrag mit einem Dienstleister bei Bedarf abgerufen werden können.

Der Betreiber stellt sicher, dass Erkenntnisse und Lehren aus vorangegangenen Vorfällen in seine Prozesse und Verfahren einfließen (Lessons learned).

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

- ÖISHB: Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling)
- ISO/IEC 27001: Information security incident management, Controls against malware
- IEC 62443 2-1: Event and Incident Management
- CIS CSC v8.0: Incident Response Management

9.2 Vorfallsmeldung

NIS-Verordnung:

Prozesse zur internen und externen Meldung von Vorfällen sind zu erstellen, aufrechtzuerhalten und zu erproben.

Der Betreiber erstellt, implementiert und aktualisiert regelmäßig Prozesse und Verfahren zur internen und externen Meldung von Vorfällen.

Darüber hinaus entwickelt der Betreiber Prozesse und Verfahren, um bei

Vorfällen bei Dienstleistern und Lieferanten umgehend von diesen informiert zu werden, sofern die Vorfälle für das Sicherheitsniveau oder die -situation des Betreibers relevant sein könnten.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling)
> ISO/IEC 27001: Information security incident management, Controls against malware
> IEC 62443 2-1: Event and Incident Management
> CIS CSC v8.0: Incident Response Management

So unterstützt Sie OMICRON bei der Vorfallsmeldung

Unser Monitoring und Alarmierung ermöglicht eine für Ihre OT- und IT-Experten geeignete Darstellung, um rechtzeitig Behandlungsmaßnahmen einleiten zu können. Ebenso können Sie mit GridOps automatisierte E-Mail Benachrichtigungen entsprechend Ihrer Melde- und Eskalationswege an ihre verantwortlichen Mitarbeiter (und Abteilungen) senden.

9.3 Vorfallsanalyse

NIS-Verordnung:

Prozesse zur Analyse und Bewertung von Vorfällen und zur Sammlung relevanter Informationen sind zu erstellen, aufrechtzuerhalten und zu erproben, um den kontinuierlichen Verbesserungsprozess zu fördern.

Der Betreiber etabliert Prozesse und implementiert Verfahren, um die Analyse und Bewertung von erkannten und/oder vermuteten Vorfällen zu ermöglichen. Des Weiteren definiert der Betreiber Prozesse zur Sammlung und Bewertung analyserelevanter Informationen und erprobt diese.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Sicherheitsvorfälle bzw. Informationssicherheitsereignisse (Incident Handling)
> ISO/IEC 27001: Information security incident management, Controls against malware
> IEC 62443 2-1: Event and Incident Management
> CIS CSC v8.0: Incident Response Management

10 Betriebskontinuität

10.1 Betriebskontinuitätsmanagement

NIS-Verordnung:

Die Wiederherstellung der Erbringung des wesentlichen Dienstes auf einem zuvor festgelegten Qualitätsniveau nach einem Sicherheitsvorfall ist zu gewährleisten.

Der Betreiber definiert Ziele und strategische Richtlinien für das Betriebskontinuitätsmanagement im Falle eines Sicherheitsvorfalls. Der Betreiber verantwortet den Aufbau eines leistungsfähigen Notfall- und Krisenmanagements zur systematischen Vorbereitung auf die Bewältigung von Sicherheitsvorfällen bzw. Schadereignissen, insbesondere der Wiederherstellung der Erbringung des wesentlichen Dienstes.

Als Grundlage des Notfall- und Krisenmanagements führt der Betreiber eine Business Impact Analyse seiner Netz- und Informationssysteme durch und aktualisiert diese regelmäßig.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Disaster Recovery und Business Continuity
> ISO/IEC 27001: Information security aspects of business continuity management
> IEC 62443 2-1: System integrity and availability
> CIS CSC v8.0: Data Recovery
> EN 50600-2-1 bis 5: Verfügbarkeit

10.2 Notfallmanagement

NIS-Verordnung:

Notfallpläne sind zu erstellen, anzuwenden, regelmäßig zu bewerten und zu erproben.

Der Betreiber erstellt ein Notfallhandbuch und stellt sicher, dass die in diesem definierten Notfallprozesse dementsprechend durchgeführt werden. Der Betreiber stellt sicher, dass Erkenntnisse und Lehren aus früheren Sicherheitsvorfällen in die Notfallpläne einfließen.

Der Betreiber führt regelmäßige Notfallübungen durch, um die Wirksamkeit von Maßnahmen im Bereich der Notfallvorsorge zu prüfen.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Disaster Recovery und Business Continuity
> ISO/IEC 27001: Information security aspects of business continuity management
> IEC 62443 2-1: System integrity and availability
> CIS CSC v8.0: Data Recovery

11 Krisenmanagement

11.1 Krisenmanagement

NIS-Verordnung:

Rahmenbedingungen und Prozessabläufe des Krisenmanagements sind für die Aufrechterhaltung des wesentlichen Dienstes vor und während eines Sicherheitsvorfalls zu definieren, umzusetzen und zu erproben.

Der Betreiber definiert die Organisation und Verantwortlichkeiten für das Krisenmanagement bei Sicherheitsvorfällen, erstellt geeignete Alarmierungspläne und implementiert geeignete Prozesse und Verfahren zur Krisenbewältigung.

Der Betreiber stellt sicher, dass Aktivitäten im Rahmen des Krisenmanagements mit internen und externen Partnern (z.B. Internet Service Providern, CERT, Behörden, Systemintegratoren etc.) koordiniert werden.

Beispielhafte Gegenüberstellung mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises:

> ÖISHB: Disaster Recovery und Business Continuity
> ISO/IEC 27001: Information security aspects of business continuity management
> IEC 62443 2-1: System integrity and availability
> CIS CSC v8.0: Data Recovery

Versionshistorie

Das vorliegende Dokument ist eine Zusammenführung folgender NIS Fact Sheets:

- NIS Fact Sheet 8/2018: Mapping-Tabelle von IKT-Sicherheitsstandards und Cyber Security Best Practices
- NIS Fact Sheet 8/2019: Sicherheitsmaßnahmen für Betreiber wesentlicher Dienste

Änderungen, Anpassungen sowie Detaillierungen in der vorliegenden Version gegenüber der zwei ursprünglichen NIS Fact Sheet (siehe oben) ergeben sich aus den folgenden Grün- den:

- IEC 62443 Update
- CIS CSC 8.0 Update
- Aufnahme KSÖ Cyber Risk Rating
- Aufnahme EN 50600
- Überarbeitung und Verallgemeinerung der beispielhaften Gegenüberstellung pro Sicherheitsmaßnahmen mit nationalen und internationalen Informationssicherheitsstandards sowie Best Practises (vormals „Mapping Tabelle").
- Detailierung der Sicherheitsmaßnahmenbeschreibungen bei 2, 4.2, 6.1, 6.2.

Impressum

Medieninhaber, Verleger und Herausgeber:

Bundeskanzleramt, Ballhausplatz 2, 1010 Wien

Autoren: Bundeskanzleramt Abteilung I/8 (Cyber Security, GovCERT, NIS-Büro und ZAS) und BMI/IV/S/2 (Netz- und Informationssystemsicherheit)

Wien, 2022. Stand: 12. September 2022

Abschließende Anmerkungen:

Es wird darauf hingewiesen, dass Änderungen vorbehalten sind.

Alle in diesem NIS Fact Sheet verwendeten personenbezogenen Bezeichnungen gelten gleichermaßen für alle Geschlechter.

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an nis@bka.gv.at und post@nis.gv.at.

Support

Für Ihre Arbeit mit unseren Produkten stellen wir Ihnen ein umfangreiches Spektrum an optimal abgestimmten Zusatzleistungen bereit. Für all Ihre Fragen stehen wir Ihnen gerne jederzeit zur Verfügung.

24/7 Technical Support - Erhalten Sie Unterstützung

https://www.omicronenergy.com/de/support

Über unsere technische Hotline erreichen Sie kompetente, best-ausgebildete Techniker für die Beantwortung all Ihrer Fragen - rund um die Uhr und kostenlos.

Nutzen Sie unsere internationalen technischen - 24/7 - Hotlines:

Europa / Mittlerer Osten / Afrika	+43 59495 4444
Amerikanischer Kontinent	+1 713 830-4660 +1 800-OMICRON
Asien- Pazifik-Raum	+852 3767 5500

Darüber hinaus finden Sie auf unserer Webseite alle unsere Service Center oder Vertriebspartner in Ihrer Nähe.

Kundenportal – Bleiben Sie informiert

https://my.omicronenergy.com/

Das Kundenportal auf unserer Webseite ist eine Plattform für den internationalen Wissensaustausch. Hier können Sie die neuesten Software-Aktualisierungen für alle unsere Produkte herunterladen und in unserem User-Forum Ihre Erfahrungen mit anderen Anwendern teilen.

Durchsuchen Sie die Wissensbibliothek. Dort finden Sie Anwendungsberichte, Vorträge von Konferenzen, Erfahrungen aus der täglichen Arbeitspraxis, Benutzerhandbücher und mehr.

OMICRON Academy – Bilden Sie sich weiter

https://omicron.academy/

Das Kundenportal auf unserer Webseite ist eine Plattform für den internationalen Wissensaustausch. Hier können Sie die neuesten Software-Aktualisierungen für alle unsere Produkte herunterladen und in unserem User-Forum Ihre Erfahrungen mit anderen Anwendern teilen.

Durchsuchen Sie die Wissensbibliothek. Dort finden Sie Anwendungsberichte, Vorträge von Konferenzen, Erfahrungen aus der täglichen Arbeitspraxis, Benutzerhandbücher und mehr.

Mehr Informationen, eine Übersicht der verfügbaren Literatur und detaillierte Kontaktinformationen unserer weltweiten Niederlassungen finden Sie auf unserer Website.

www.omicroncybersecurity.com

www.omicronenergy.com