IKARUS security software

Leitfaden

Unterstützung und Einhaltung der NIS-Richtlinien & Gesetze

Management von Sicherheitsrisiken, Schutz vor Cyberangriffen,
Erkennung von Sicherheitsvorfällen und Minimierung ihrer Auswirkungen

NOZOMI NETWORKS

powered by IKARUS

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Inhalt

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Einleitung

Die Verordnungen über Netz- und Informationssysteme (NIS-Verordnungen), die im Rahmen der NIS-Richtlinie der Europäischen Union (EU) entwickelt wurden, verpflichten die Anbieter dazu, kritische Dienste durch verbesserte Cybersicherheit zu schützen.

Die Verordnungen gelten für alle EU-Mitgliedstaaten und decken alle Operationen innerhalb des Geltungsbereichs ab, unabhängig vom Land des Eigentümers. Internationale Organisationen müssen sicherstellen, dass die Einrichtungen und Tätigkeiten im Geltungsbereich der NIS-Richtlinie konform sind.

Die Einhaltung ist verpflichtend und kann bei Nichtbeachtung zu erheblichen Geldstrafen führen. Jeder Mitgliedsstaat muss Strafen für die Nichteinhaltung festlegen – in Österreich können sie bis zu 100.000 Euro betragen.

Die NIS-Verordnung ist im Mai 2018 in Kraft getreten. Sie zielt darauf ab sicherzustellen, dass Betreiber kritischer Infrastrukturen für die zunehmenden Cyber-Bedrohungen gerüstet sind. Anders als Ansätze, die auf der Einhaltung von Vorschriften basieren, umreißt die NIS-Richtlinie eine Reihe von Grundsätzen, die bei der Entscheidungsfindung konsequent angewendet werden können, um ein hohes Niveau an Sicherheit von Netzwerken und Informationssystemen zu erreichen und aufrecht zu erhalten.

Dieser Leitfaden zeigt, wie die Technologien von Nozomi Networks powered by IKARUS die NIS-Ziele unterstützen, und hilft Organisationen bei der Implementierung einer effektiven OT- und IoT-Cyber Security Politik. Die Einführung einer messbaren, zielgerichteten Cybersicherheitsstrategie sollte letztendlich dazu führen, dass eine Organisation nachweisbare Indikatoren für vorbildliche Lösungen hat und die Ziele der NIS-Richtlinie erfüllt.

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

1. Anwendungsbereich der NIS Richtlinie / NIS Verordnungen

Die NIS-Richtlinien wenden sich an alle Betreiber kritischer Infrastrukturen in allen EU-Mitgliedstaaten, wobei die folgenden Sektoren ausdrücklich genannt werden:

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasserversorgung
- Digitale Infrastruktur

In den genannten Branchen ist die Einhaltung der NIS-Richtlinie verpflichtend. Sie kann jedoch von jeder Organisation als Leitfaden benutzt werden, um die Lage der eigenen Cybersicherheit anhand eines anerkannten Rahmenplans zu messen und zu verbessern.

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

2. Einhaltung der NIS-Richtlinie

Die NIS-Richtlinie ist ein prinzipienbasierter Ansatz. Wie kann die „Einhaltung“ dieser Prinzipien nachgewiesen werden?

Die NIS-Richtlinien verlangen einen risikobasierten Ansatz für die Cybersicherheit. Dementsprechend braucht eine Organisation ein effektives Risikomanagementverfahren, eine definierte Steuerungsstruktur sowie zugewiesene Rollen und Verantwortlichkeiten in Bezug auf die Cyber-Resilienz.

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

3. Wie die Nozomi Networks Lösung die NIS-Richtlinie unterstützt

Wirksame Cybersicherheit – und NIS-Konformität – dreht sich um drei Grundprinzipien: Menschen, Prozesse und Technologie. Konzentriert man sich nur auf eines, ist mit Lücken in der Cybersicherheitslage des Unternehmens zu rechnen.

Ein vertrauenswürdiger Sicherheitsrahmen wie der der NIS-Richtlinie sowie fortgeschrittene Technologien für Sichtbarkeit, Monitoring und Risikoidentifizierung unterstützen Organisationen dabei, Sicherheit in ihre Prozesse zu integrieren und ihre Cyber-Resilienz zu verbessern.

Die Funktionen von Nozomi Networks für industrielle Cyber Security und Visibilität unterstützen alle drei Säulen effektiver Cybersicherheit. Sie bieten beispielsweise Netzwerkintelligenz in Echtzeit, Überwachung und KI-gestützte Bedrohungserkennung und ermöglichen einen proaktiven Ansatz zur Risikominimierung. Außerdem werden Echtzeitwarnungen zu Bedrohungen und Anomalien innerhalb eines industriellen Kontrollnetzwerks bereitgestellt.

Die Lösung umfasst ein flexibles und intuitives Interface für das Netzwerk-Monitoring und Reporting. So können Organisationen einen Reifegrad von Cybersicherheit entwickeln, der mit der NIS-Richtlinie übereinstimmt und deren Einhaltung nachweist.

Die Gesamtlösung von Nozomi Networks powered by IKARUS liefert alle Informationen, um einen intelligenten und zielgerichteten Ansatz für Cybersicherheit in OT- und IoT-Umgebungen zu ermöglichen. Das Ergebnis ist schnelle Risikominderung für die kritischsten Anlagen einer Organisation.

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

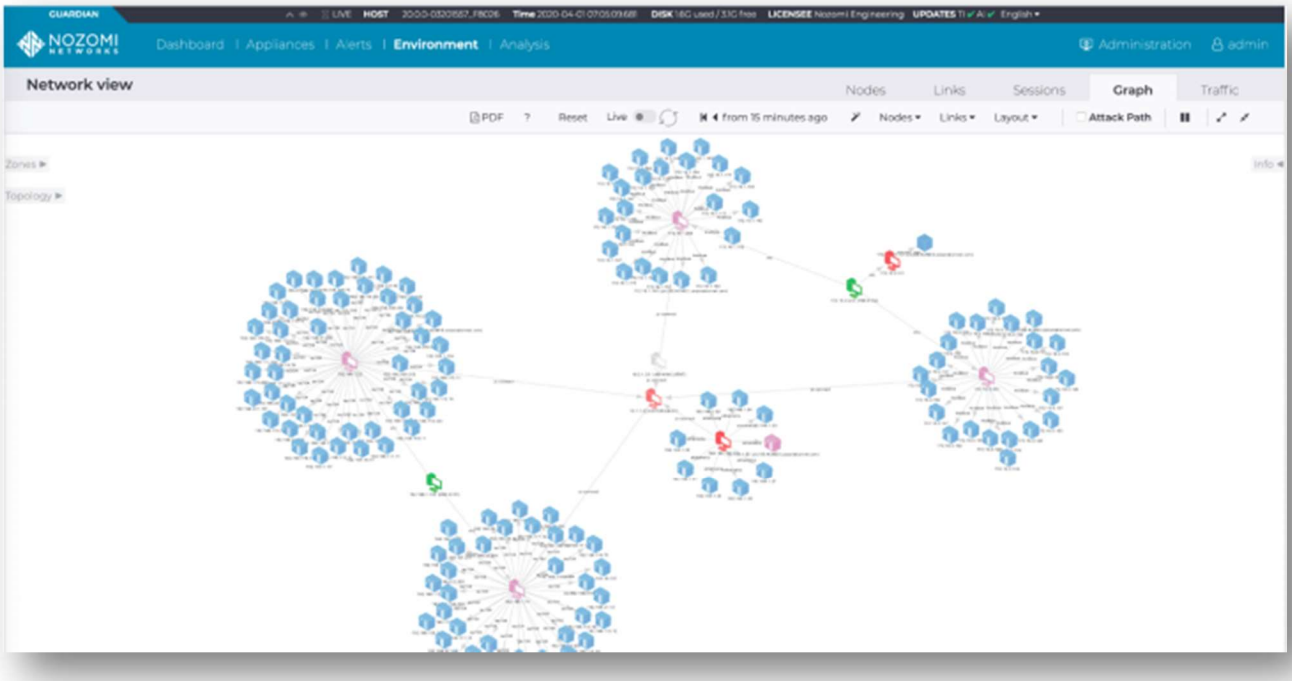
4. Unterstützung der NIS Zielsetzungen

Ziele	Richtlinien	Zusammenfassung	Unterstützt von Nozomi/IKARUS
Verwaltung von Sicherheitsrisiken	Steuerung	Die Organisation verfügt über angemessene Managementrichtlinien und Prozesse, um ihren Ansatz zur Sicherheit von Netzwerken und Informationssystemen zu steuern.	teilweise
	Risikomanagement	Die Organisation ergreift geeignete Maßnahmen für die Identifizierung, Bewertung und das Verständnis von Sicherheitsrisiken für Netzwerk und Informationssysteme, die die Erbringung wesentlicher Dienste unterstützen.	vollständig
	Anlagenverwaltung	Alles, was zur Bereitstellung, Wartung oder Unterstützung von Netzwerken und Informationssystemen für wesentliche Dienste benötigt wird, wurde festgelegt und verstanden.	vollständig
	Lieferkette	Die Organisation versteht und verwaltet die Sicherheitsrisiken, die aus der Abhängigkeit von externen Lieferanten entstehen und Netzwerke sowie Informationssysteme, die die Erbringung wesentlicher Dienste unterstützen, betreffen.	teilweise
Schutz vor Cyber-Angriffen	Sicherheitsrichtlinien und -prozesse	Die Organisation definiert, implementiert, kommuniziert und setzt geeignete Richtlinien und Prozesse, die auf die Sicherung von Systemen und Daten zur Unterstützung wesentlicher Dienste ausgerichtet sind.	vollständig
	Identitäts- und Zugangskontrolle	Die Organisation versteht, dokumentiert und verwaltet den Zugang zu Systemen und Funktionen, die die Erbringung von wesentlichen Diensten unterstützen.	teilweise
	Datensicherheit	Elektronisch gespeicherte oder übermittelte Daten sind geschützt vor Aktionen wie unbefugtem Zugriff, Veränderung oder Löschung, die zu einer Unterbrechung der wesentlichen Dienste führen können.	vollständig
	Systemsicherheit	Netz- und Informationssysteme und -technologien, die für die Erbringung wesentlicher Dienste kritisch sind, werden vor Cyberangriffen geschützt. Ein organisatorisches Verständnis des Risikos für wesentliche Dienste bildet die Grundlage für den Einsatz robuster und zuverlässiger Sicherheitsmaßnahmen.	vollständig
	Widerstandsfähige Netzwerke und Systeme	Die Organisation entwickelt Widerstandsfähigkeit gegen Cyberangriffe und Systemausfälle in der Entwicklung, der Implementierung, dem Betrieb und der Verwaltung von Systemen, die die Erbringung wesentlicher Dienste unterstützen.	vollständig
	Mitarbeiter- und Bewusstseins-schulung	Die Mitarbeitenden verfügen über ein angemessenes Bewusstsein sowie Wissen und Fähigkeiten, um ihre organisatorischen Aufgaben in Bezug auf die Sicherheit von Netz- und Informationssystemen zur Unterstützung der Erbringung wesentlicher Dienste zu erfüllen.	teilweise

Ziele	Richtlinien	Zusammenfassung	Unterstützt von Nozomi/IKARUS
Erkennen von Cyber Security Vorfällen	Security Monitoring	Die Organisation überwacht den Sicherheitsstatus der Netzwerke und Systeme, die die Bereitstellung wesentlicher Dienste unterstützen, um potenzielle Sicherheitsprobleme zu erkennen und die Wirksamkeit von Sicherheitsschutzmaßnahmen zu verfolgen.	**vollständig**
	Proaktive Erkennung von Sicherheits-ereignissen	Die Organisation erkennt in Netzwerken und Informationssystemen böswillige Aktivitäten, die die Bereitstellung wesentlicher Dienste beeinträchtigen oder beeinträchtigen könnten, selbst wenn die Aktivität signaturbasierte Sicherheitslösungen zur Verhinderung/Erkennung umgeht oder es aus irgendeinem Grund nicht möglich ist, signaturbasierte Erkennung einzusetzen.	**vollständig**
Minimierung der Auswirkungen von Cyber Security Vorfällen	Planung von Reaktion und Wiederherstellung	Es gibt gut definierte und erprobte Prozesse für Incident Response, die darauf abzielen, die Kontinuität der wesentlichen Dienste im Falle eines System- oder Dienstausfalls zu gewährleisten. Es gibt auch Maßnahmen zur Schadensbegrenzung, um die Auswirkungen einer Kompromittierung zu begrenzen.	**vollständig**
	Gewonnene Erkenntnisse	Tritt ein Vorfall auf, werden Schritte unternommen, um die Ursachen zu verstehen und um sicherzustellen, dass geeignete Abhilfemaßnahmen ergriffen werden, um zukünftige Vorfälle zu vermeiden.	**vollständig**

4.1. Zielsetzung: Verwaltung von Sicherheitsrisiken

Nozomi Networks bringt maximale Transparenz und Bereitschaft für Risikostrategien. Industrielle Kontrollsysteme werden aus der Sicherheitsperspektive oft unzureichend verwaltet. Manchmal haben sie keine oder ungenaue Anlageninventuren, oder es fehlen detaillierte Netzwerkarchitektur- und Datenflussdiagramme. Diese fehlenden Daten bedeuten, dass die Organisation nicht über die erforderlichen Informationen für eine gezielte Steuerung und ein effektives Risikomanagement verfügt. Infolgedessen sehen sich die Unternehmen mit der unüberwindbaren Aufgabe konfrontiert, diese Informationen zu generieren und zu verwalten.



Ausschnitt aus der interaktiven Netzwerkvisualisierung.

Guardian powered by IKARUS erstellt ein Netzwerkdiagramm mit präzisen und detaillierten Asset Informationen. Diese Daten werden passiv und automatisch abgerufen, wenn die Appliance mit einem Span- oder Mirror-Port des industriellen Netzwerks verbunden ist. Sie ermöglichen einer Organisation, schnell die Gefährdung durch neue und bestehende Schwachstellen zu bewerten, die Ausfallsicherheit durch kritisches Ersatzteilmanagement zu verwalten und Audit-Funktionen durchzuführen. Eine detaillierte Datenflusskarte wird ebenfalls generiert, die Unternehmen hilft, die Übereinstimmung mit internen und Industriestandards zu verstehen – beispielsweise die Anforderungen der IEC 62443 für die Geräte-Kommunikation zwischen den Ebenen des Purdue-Modells.

Anhand der von Guardian powerd by IKARUS bereitgestellten Details kann eine Organisation beginnen, Folgendes zu verstehen und zu identifizieren:

- Anlagen, die für das Funktionieren kritischer Infrastrukturen entscheidend sind
- Sicherheitsmängel

Cyber-Bedrohungen für kritische Infrastrukturen werden sichtbar und Risikoentscheidungen fundiert. Abhilfemaßnahmen führen zu nachweisbaren Risikominderungen, die Stakeholdern und Prüfenden klar kommuniziert werden können.

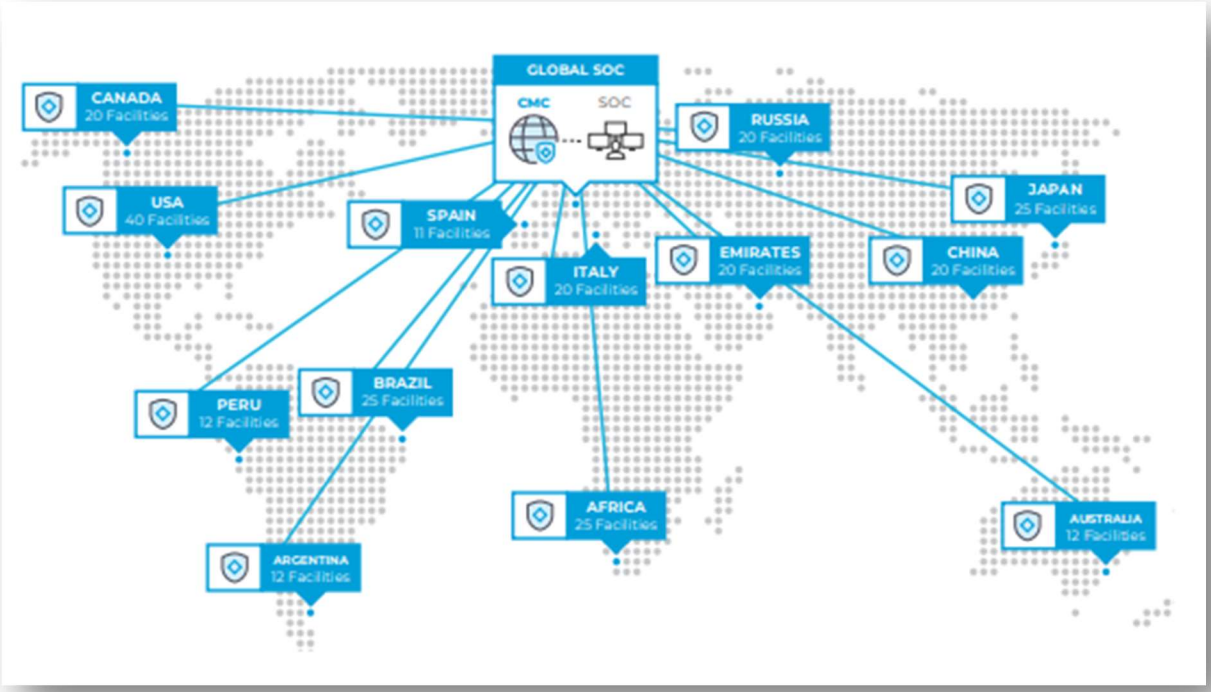
4.2. Zielsetzung: Verwaltung von Sicherheitsrisiken

Mit Guardian powered by IKARUS kann die Umsetzung von Richtlinien und Verfahren überprüft werden. Die daraus resultierenden Metriken belegen die Risikominderung, z. B. die Reduzierung kritischer Schwachstellen, die Verringerung der Anzahl der nicht unterstützten Betriebssysteme, etc.

Durch die Bereitstellung detaillierter und genauer Informationen in Echtzeit erlernt Guardian powered by IKARUS den normalen Betrieb von Netzwerk und Prozess. Sobald der Lernprozess abgeschlossen ist, schaltet das System in den Schutzmodus, der die Benutzer auf Änderungen im Prozess- und Netzwerkverhalten aufmerksam macht. In den Datenfluss im Netzwerk können auch Next-Generation-Firewalls integriert werden, wodurch ein virtualisierter Ansatz zur Netzwerksegmentierung entsteht.

Guardian powered by IKARUS und die Central Management Console (CMC) überwachen Kommunikationspfade zwischen den Netzwerkressourcen und ermöglichen so Echtzeitinformationen zur Unterstützung einer Zugriffsmanagement-Strategie.

Guardian-Geräte können mit der CMC aggregiert werden, um Assets über geografisch verteilte, abteilungsübergreifende Installationen zu überwachen.



Die CMC bietet konsolidierten Zugriff auf die Daten aller Guardian-Einsätze auf Feld- oder Werksebene.

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Durch die Kombination aus KI und verhaltensbasierter Analytik mit einem regelbasierten Mechanismus erkennt Guardian die Ausnutzung von Schwachstellen. Dies bietet Schutz vor bekannten Schwachstellen in einer Umgebung, in der ein routinemäßiges Patchen nicht möglich ist. Die gleichen Mechanismen bieten auch Schutz vor bekannten Bedrohungen, Malware und Zero-Day-Bedrohungen.

Dieser Ansatz für die Netzsicherheit bedeutet, dass im Falle eines Versagens konventioneller Schutzmechanismen Zugriffsversuche entdeckt und die Auswirkungen von Angriffen minimiert werden, die andernfalls unentdeckt blieben.

Die Netzwerkabbildungs- und -visualisierungsfunktionen von Guardian powered by IKARUS unterstützen ein gutes Netzwerk-Design – zum Beispiel mit der Nutzung von Informationen darüber, wie der Verkehr im bestehenden Netzwerk fließt.

Die virtuelle Segmentierung kann zur Entwicklung einer geeigneten Segmentierungsstrategie genutzt werden, die sowohl realisierbar als auch wartbar ist. Dieser Ansatz der virtuellen Segmentierung kann den Verkehrsfluss durchsetzen oder Warnungen bei Richtlinienverstößen ausgeben, wodurch im Einklang mit einem „Defense-in-Depth“-Ansatz eine zusätzliche Sicherheitsebene eingezogen wird.

Die Netzabbildung unterstützt auch die NIS-Vorschriften in Bezug auf die Datenspeicherung und die Abbildung von Systemabhängigkeiten. Mit diesen Informationen kann eine Organisation die Auswirkungen einer Beschädigung oder eines Verlusts der Datenverfügbarkeit besser verstehen und einen gezielten und risikobasierten Ansatz für den Schutz kritischer Dienste wählen. Prozesse zur Reaktion auf Vorfälle können gezielt eingesetzt werden, um kritische Dienste nach einer Unterbrechung schnell wiederherzustellen.

Guardian powered by IKARUS bringt die Überwachung auf Netzwerk- und Prozessebene auf ein neues Niveau. Dank Echtzeitwarnungen bei Änderungen von Prozessdaten, Kommunikationsverbindungen oder Anlagen kann ein bisher nicht gekanntes Maß an Prozessintegrität erreicht werden. Mit der branchenführenden Integration in traditionelle IT-Sicherheitsanwendungen können Sicherheitsteams die Lösung mit ihren bestehenden Tools nutzen.

4.3. Zielsetzung: Erkennen von Cybersicherheitsvorfällen

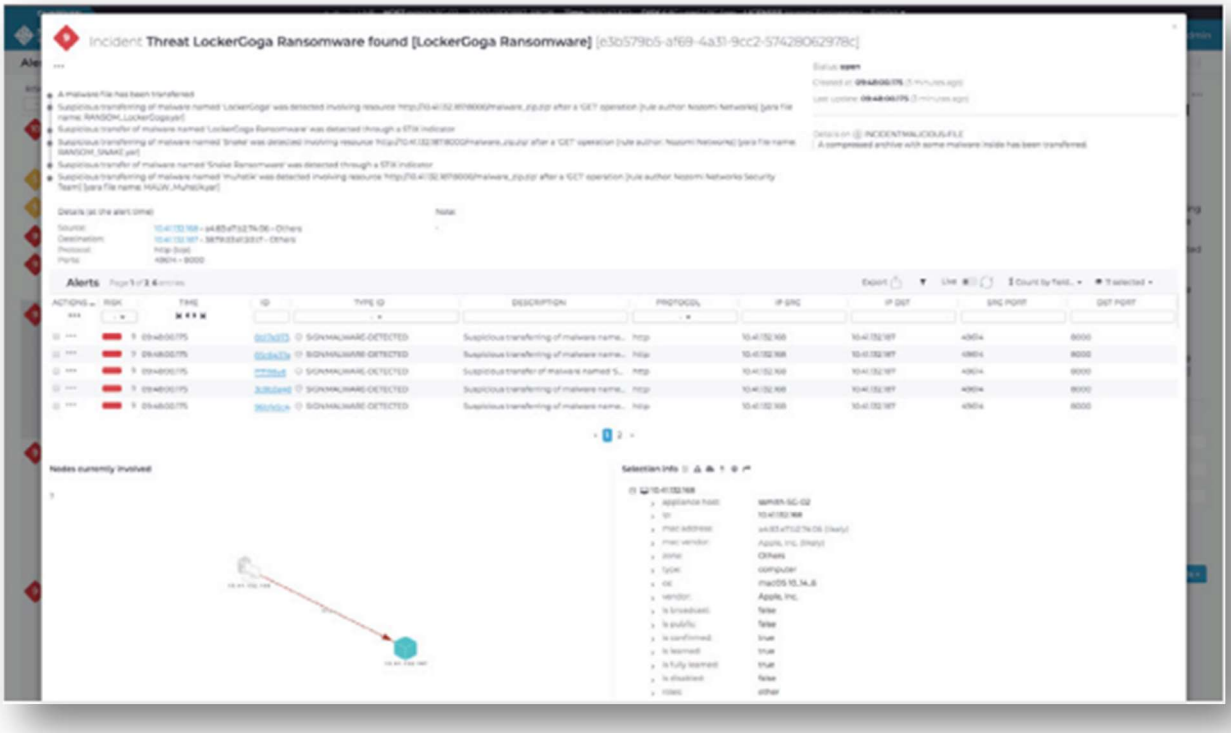
Basierend auf umfassenden verhaltensbasierten KI-Analysen und signaturbasierten Engines erkennt Guardian powered by IKARUS zuverlässig Sicherheitsvorfälle, Richtlinienverstöße und Prozessanomalien, die die Bereitstellung wichtiger Dienste beeinträchtigen könnten. Guardian powered by IKARUS deckt die gesamte Netzwerkumgebung ab und lernt und versteht normales Netzwerk- und Prozessverhalten. Abweichungen von bekannten Zuständen führen zu Warnmeldungen, so dass Benutzer bekannte Gefährdungsindikatoren (Indicators of Compromise) und Zero-Day-Bedrohungen erkennen können.

Die Lösung von Nozomi Networks ist so aufgebaut, dass sie die volle Kontrolle über die gesamte Technologieplattform hat – zusätzlich zur der Softwarelösung selbst auch über die Firmware und das Betriebssystems auf der physischen Appliance. Das System ist gehärtet und Bestandteil regelmäßiger eingehender Sicherheitsüberprüfung. Systempatches werden bei Bedarf als Produkt-Updates eingespielt. So werden die Gesamtbetriebskosten reduziert und zugleich eine hochsichere Plattform bereitgestellt.

Die Lösung bietet außerdem branchenführende Warnfunktionen für das Management von Sicherheitsvorfällen. Warnungen können priorisiert, behoben und gekennzeichnet werden, um sich auf die tatsächlich relevanten Sicherheitsprobleme konzentrieren zu können.

Der Nozomi Networks Threat Intelligence Service liefert Guardian powered by IKARUS zur einfachen Erkennung von Bedrohungen und Schwachstellen in OT- und IoT-Umgebungen aktuelle Bedrohungsdaten. Threat Intelligence wird vom Nozomi Networks Labs Expertenteam erstellt und kuratiert. Es unterstützt auch das Hinzufügen von benutzerdefinierten Signaturen aus Industriequellen, die mit branchenspezifischen Bedrohungen arbeiten.

Der Asset Intelligence Service aktualisiert Guardian powered by IKARUS kontinuierlich mit umfangreichen OT und IoT-Geräteprofilen und Verhaltensdaten. Er ermöglicht Guardian-Appliances eine präzise Klassifizierung von Anlagen, was den Lernprozess beschleunigt und detaillierte Warnungen liefert, die wichtige Sicherheits- und Betriebsanomalien aufzeigen.



Smart Incident zeigt verwandte Warnungen und Sicherheitskontext an.

4.4. Zielsetzung: Minimierung der Auswirkungen von Cyber Security-Vorfällen

Die Technologie von Nozomi Networks liefert detaillierte Informationen über alle Aspekte eines Industrienetzwerks und unterstützt damit erweiterte Reaktionsmöglichkeiten auf Vorfälle. Detaillierte Informationen über den Netzwerkverkehr und seine Abhängigkeiten helfen bei der Planung und decken mehrere Angriffsszenarien ab.

KI und verhaltensbasierte Analysen liefern detaillierte und genaue Sicherheitswarnungen mit Ereigniskorrelation und Identifizierung der Grundursache. Informationen zu Sicherheitsereignissen sind in der Lösung verfügbar. Darüber hinaus können für eine tiefgreifende Analyse auf Datenpaketebene auch Paket Traces von der Appliance heruntergeladen und den Sicherheits- und Forensik-Teams zur Verfügung gestellt werden.

Guardian powered by IKARUS nimmt auch Daten in Form von Netzwerk-Packet-Captures (PCAPs) auf. Die Lösung kann zur Simulation eines Angriffs, als Schulungsinstrument und zur Unterstützung von Organisationen zum Üben ihrer Incident Response-Verfahren genutzt werden. Letzteres ist eine Anforderung der NIS sowie aller aktuellen Sicherheitsstandards.

Detaillierte Ereigniskorrelation und Angriffsvektoranalysen, die von der Guardian Appliance ermöglicht werden, können in die Richtlinien für die Reaktion auf Vorfälle und den Sicherheitsschutz einfließen. Dies hilft, aus Sicherheitsvorfällen zu lernen und die zukünftige Cybersicherheitslage zu stärken.

Zusammenfassung

Der Schlüssel zu einer effektiven Netzüberwachung liegt in der Nutzung von Informationen, um ein genaues Risikobild zu erstellen.

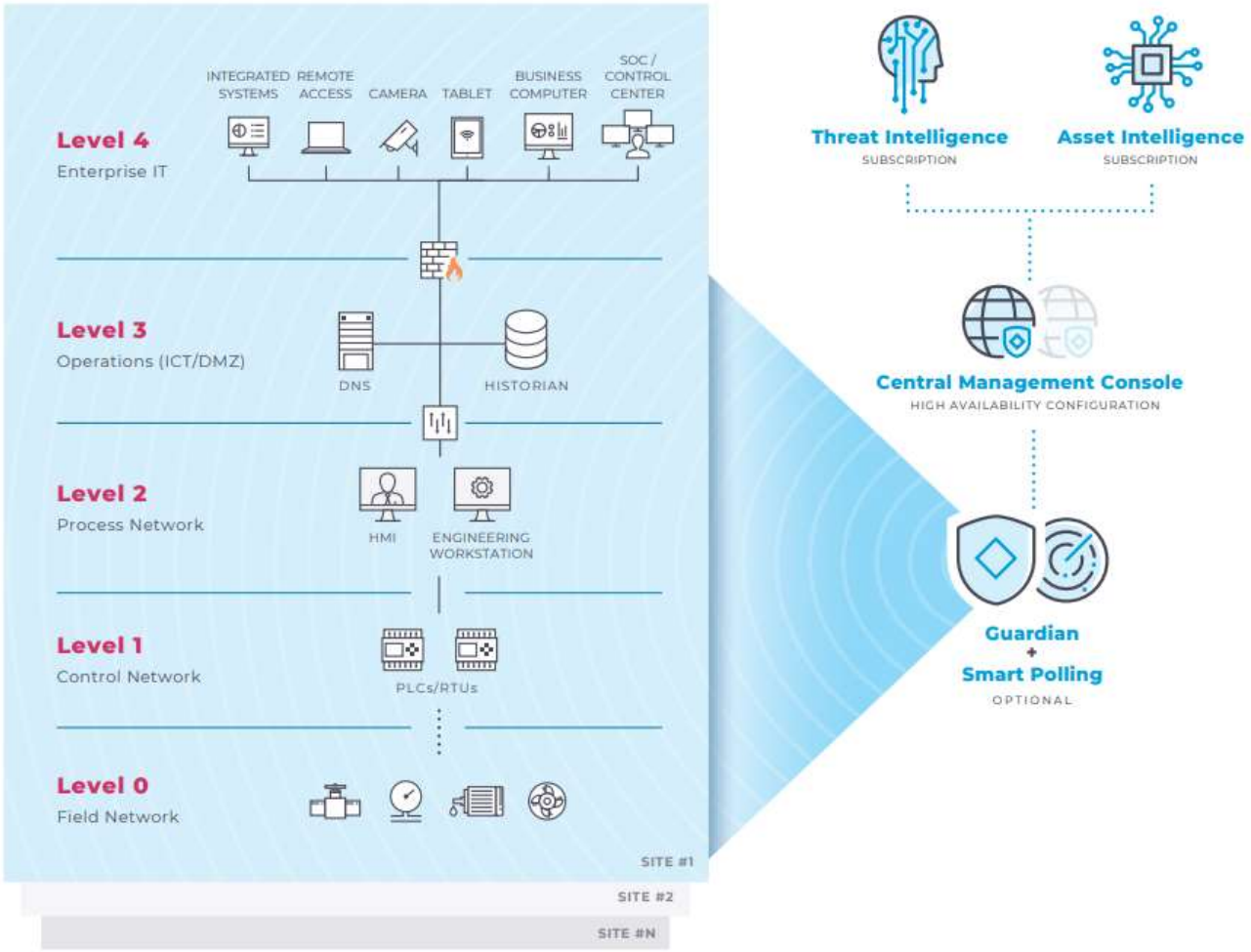
Die Lösung von Nozomi Networks bietet eine detaillierte Asset Identifizierung und Netzwerkerkennung, die Organisationen dabei hilft, einen tiefen Einblick in den Status ihrer OT und IoT-Netzwerke zu erhalten. Ausgestattet mit Informationen kann eine Organisation Risiken und Bedrohungen, die in ihren Umgebungen aktiv sind, identifizieren. Diese Einsicht ermöglicht es, ein effektives und gezieltes Programm zur Risikominderung zu implementieren, das den Einsatz begrenzter personeller Ressourcen maximiert und gleichzeitig fundierte Risikoentscheidungen, die sowohl effizient als auch effektiv sind, ermöglicht.

Die branchenführende Integration von Nozomi Networks in Standard-IT-Sicherheitsplattformen und die intuitive Benutzeroberfläche sind für Ingenieure, IT- und Sicherheitsteams gleichermaßen von Nutzen. Durch die Bereitstellung kontextbezogener Warnungen können Organisationen schnell auf Bedrohungen in ihren Automatisierungs- und Steuerungssystemen reagieren. Mit anpassbaren Dashboards und Berichten können Unternehmen eine zielgerichtete Risikominderung im gesamten Unternehmen erreichen.

Guardian powered by IKARUS ist ein grundlegendes Tool, das Organisationen dabei hilft, die NIS-Richtlinie und NIS-Verordnungen zu erfüllen.

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com

Beispiel für eine Einsatzarchitektur



Über IKARUS Security Software

Der österreichische Cyber Security-Spezialist IKARUS Security Software entwickelt und betreibt seit 1986 führende Sicherheitstechnologien: von der eigenen Scan Engine über leistungsstarke Cloud-Services für Endpoints, mobile Endgeräte und E-Mail-Gateways bis hin zur Threat Intelligence Platform (TIP). Durch Partnerschaften mit FireEye/Mandiant, Marktführer im Bereich Threat Intelligence, und Nozomi Networks, Technologieführer bei OT/IoT-Security, erweitert IKARUS das eigene Portfolio und positioniert sich als der lokale Ansprechpartner und Systemintegrator für professionelle IT-, OT- und IoT-Security.

Blechturmgasse 11 | A-1050 Wien | Tel.: +43 1 589 95-500 | E-Mail: sales@ikarus.at | www.IKARUSsecurity.com