IKARUS security software

Whitepaper

Verbesserung der operativen **Resilienz und Cybersicherheit** für Rechenzentren nach **NIS2**

www.IKARUSsecurity.com

IKARUS Security Software GmbH | Blechturmgasse 11 | 1050 Wien | Österreich | Tel.: +43 1 589 95-0
office@ikarus.at | Firmenbuchnummer: FN 64708i | Gerichtsstand Wien | UID-Nr.: ATU15191405

Inhalt

Einführung

Rechenzentren spielen eine zentrale Rolle in der digitalen Wirtschaft. Sie speichern und verarbeiten Informationen für eine Vielzahl von Branchen und müssen dabei strenge Anforderungen an den Betrieb und Schutz der eigenen Systeme erfüllen. Von der unterbrechungsfreien Stromversorgung über die Belüftung von Kühlsystemen bis hin zur Löschanlage gilt es jeden Bestandteil abzusichern, um Ausfälle oder einen gänzlichen Stillstand der Systeme zu verhindern.

Gerade ihre wesentliche Funktion für den sicheren Betrieb unserer digitalen Wirtschaft sowie ihre zunehmende Komplexität und Vernetzung mit OT- und IoT-Geräten machen Rechenzentren zu beliebten Zielen von Cyberkriminellen. Dennoch ist nach wie vor eine Vielzahl an Verwaltungstools und Anwendungen von Rechenzentren öffentlich im Internet erreichbar. Fehlende Updates, der Einsatz von Standard-Passwörtern und mangelhaftes Monitoring machen es Angreifern weitaus leichter als notwendig.

Cybersicherheits-Herausforderungen im Rechenzentrum

- **Wachsende Cyberbedrohungen**: Rechenzentren sind ständig wachsenden Bedrohungen wie DDoS-Angriffen, Ransomware oder APTs (Advanced Persistent Threats) ausgesetzt. Diese Bedrohungen können zu erheblichen Betriebsstörungen, -ausfällen und Datenverlusten führen.

- **Schwachstellen in OT- und IoT-Systemen**: Viele OT- und IoT-Geräte wie Videoüberwachungssysteme, Zugangskontrollsysteme oder Brandschutzsysteme verfügen nicht über grundlegende Sicherheitsfunktionen und werden so zu leichten Zielen für Cyberangriffe. Fehlende Updates und schwache Authentifizierung verschärfen das Risiko noch weiter.

- **Risiken durch Drittanbieter**: Durch die Integration von OT- und IoT-Systemen von Drittanbietern mit ihrer eigenen Software, die möglicherweise nicht den höchsten Sicherheitsstandards entspricht, steigen die Risiken von Schwachstellen.

Motive für Cyberangriffe auf Rechenzentren

Finanzielle Interessen sind nur ein mögliches Motiv hinter Cyberangriffen auf Rechenzentren. Staatlich gesponserte Gruppen können politische Ziele verfolgen, während es Hacktivisten möglicherweise auf ein einzelnes Unternehmen, das das Rechenzentrum nutzt, abgesehen haben. Andere wiederum spezialisieren sich auf den Diebstahl von Informationen.

Typische OT- und IoT-Systeme in Rechenzentren

OT-Systeme (Operational Technology)

- **SCADA-Systeme:** Überwachung und Steuerung industrieller Prozesse
- **PLC (Programmierbare Logiksteuerungen):** Steuerung und Automatisierung von Maschinen und Prozessen
- **DCS (Verteilte Steuerungssysteme):** Steuerung komplexer Prozesse durch vernetzte Steuerungseinheiten
- **Gebäudetechnik:** HVAC, Feuerlöschanlagen, Zugangskontrollsysteme

IoT-Systeme (Internet of Things)

- **Sensoren und Aktoren:** Temperatur-, Feuchtigkeits-, Drucksensoren
- **Überwachungssysteme:** Sicherheitskameras, Bewegungsmelder
- **Zugangskontrollsysteme:** Biometrische Scanner, RFID-Leser
- **Energie- und Umweltmanagement:** Smart Meter, Umweltüberwachung

Herausforderungen in der OT- und IoT-Security

Komplexität der Gebäudetechnik

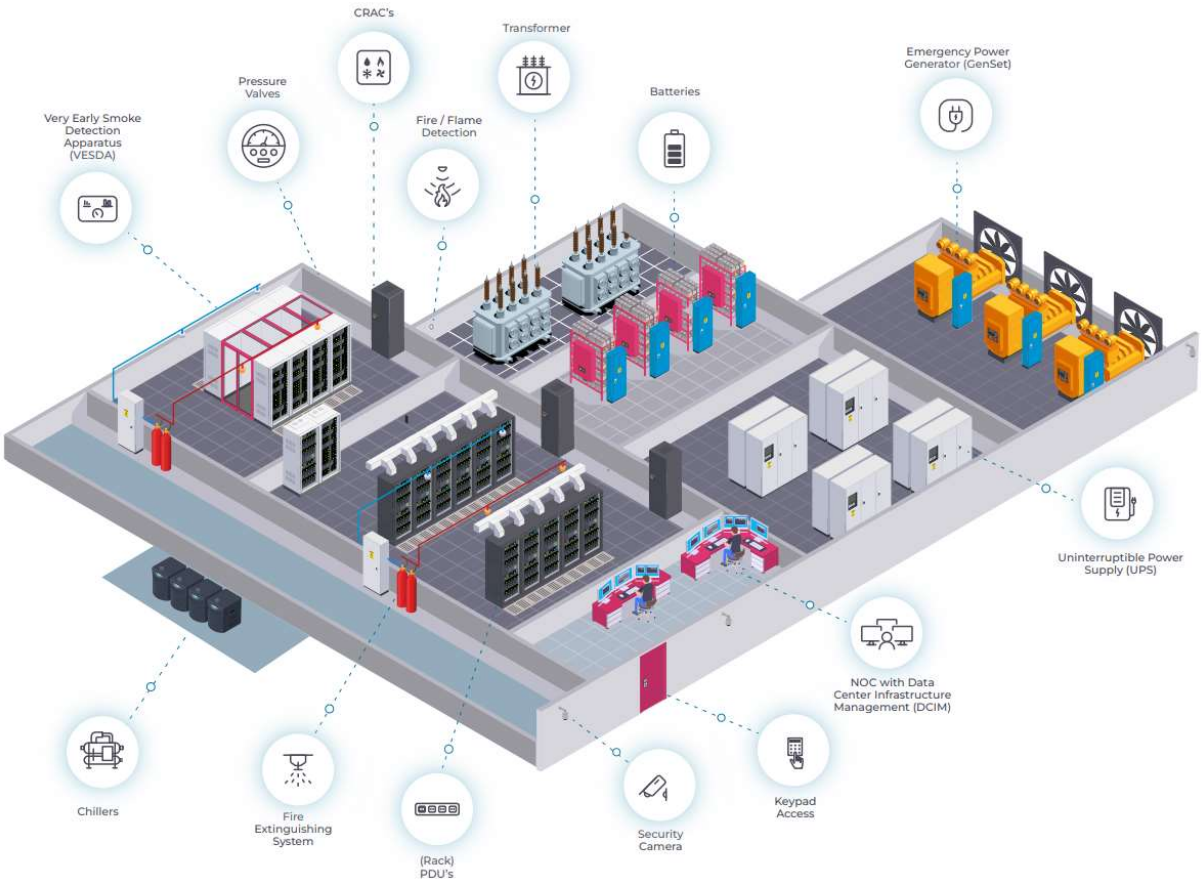
Gebäudetechnische Systeme in Rechenzentren umfassen eine Vielzahl von Subsystemen, die nahtlos zusammenarbeiten müssen. Die Sicherung dieser Systeme erfordert umfassende Kenntnisse über ihre Funktionsweise und potenzielle Schwachstellen.

Operative Resilienz und NIS2-Compliance

Die operative Resilienz von Rechenzentren muss gewährleistet werden, um Ausfallzeiten zu minimieren und den Betrieb aufrechtzuerhalten. Die NIS2-Richtlinie der EU stellt neue Anforderungen an die Cybersicherheit und Resilienz kritischer Infrastrukturen, die es zu erfüllen gilt.

Integration von Drittanbieter-Systemen

Die Integration von Drittanbietersystemen erhöht die Komplexität und das Risiko, da diese Systeme potenziell anfällig für Cyberangriffe sind. Eine enge Zusammenarbeit und klare Sicherheitsstandards sind unerlässlich, um diese Risiken zu minimieren.



© Nozomi Networks

Anforderungen an die OT-Sicherheit

- ✓ Frühzeitige Warnungen bei Störungen oder Stabilitätsproblemen, um Probleme beheben zu können, bevor sie die Server beeinflussen
- ✓ Schnellere und effizientere Fehlerdiagnose bei OT-Vorfällen
- ✓ Echtzeit-Überwachung von OT-Systemen über die gesamte Systemlandschaft des Rechenzentrums

- ✓ Umsetzbare Informationen, um Schwachstellen und Bedrohungen zu priorisieren, Antworten zu beschleunigen und Ausfallzeiten zu reduzieren

Anforderungen an die IoT-Sicherheit

- ✓ Umfassende Sichtbarkeit über alle IoT-Geräte unabhängig von ihrem Anbieter
- ✓ Klare Identifizierung und Priorisierung der relevantesten Bedrohungen und Schwachstellen
- ✓ Echtzeitüberwachung von Wartungssystemen (Überwachungssystemen, Sensoren u. ä.)
- ✓ Verringerung der Sicherheitsrisiken in einer sich ständig verändernden Bedrohungslandschaft inkl. gezielter Angriffe (APT)

Die Lösung von Nozomi Networks

Nozomi Networks bietet eine umfassende Plattform, die speziell für die Sicherheitsbedürfnisse von kritischen Infrastrukturen entwickelt wurde und auf Sichtbarkeit, Bedrohungserkennung und Skalierbarkeit setzt.

Umfassende Sichtbarkeit

Administratoren benötigen einen Überblick über alle Industrie-, Gebäudeautomatisierungs- und virtuelle Anlagen im Netzwerk., um Bedrohungen zu diagnostizieren und Schwachstellen zu erkennen, bevor sie sich auf den Betrieb auswirken.

- **Asset Discovery:** Automatische Erkennung und Inventarisierung aller verbundenen Geräte
- **Netzwerkvisualisierung:** Darstellung von Netzwerkverkehr und Geräteinteraktionen

Fortgeschrittene Bedrohungserkennung

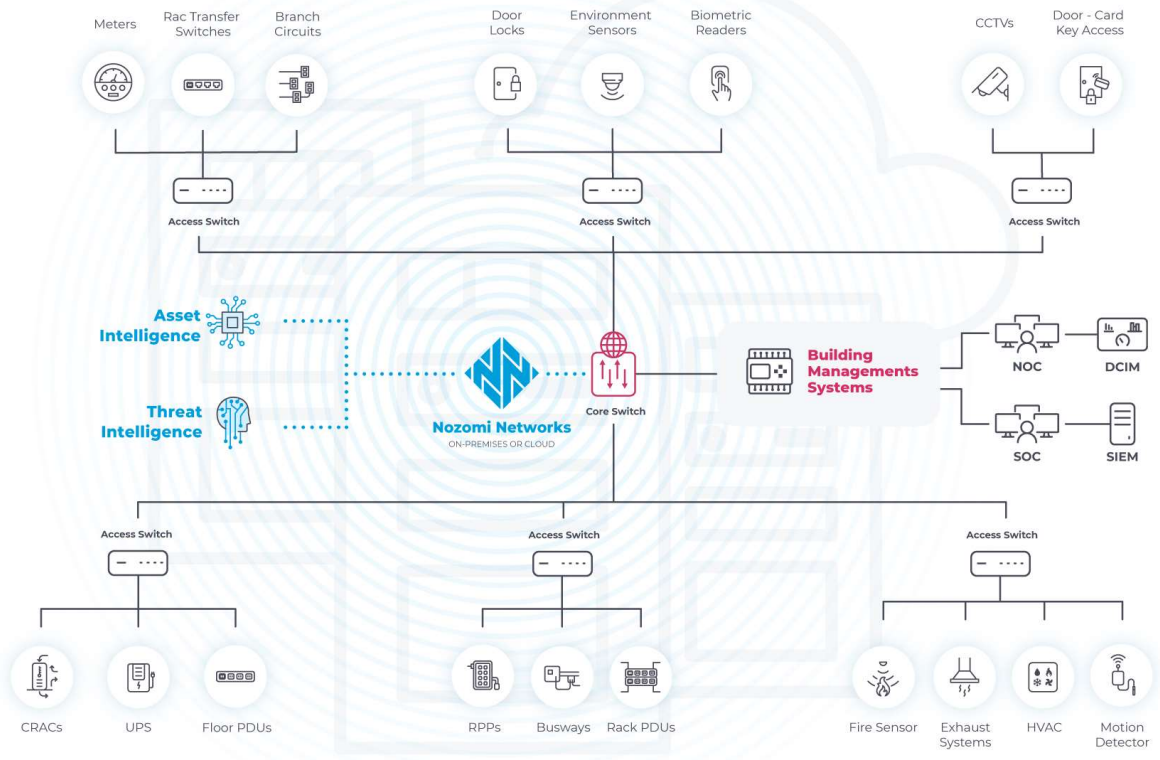
Die Vielzahl unterschiedlicher Protokolle und Hersteller in OT-Netzwerken vergrößert die Angriffsfläche. Mit den neuesten Bedrohungsdaten zu Zero-Day-Angriffen, Malware, Botnets und Geräteschwachstellen sind Administratoren den Hackern einen Schritt voraus.

- **Anomalie-Erkennung:** Identifikation ungewöhnlicher Verhaltensmuster mithilfe von KI
- **Bedrohungsinformationen:** Zugriff auf eine umfangreiche Datenbank spezifischer Schwachstellen- und Bedrohungsinformationen

Umsetzbare Informationen

Mit umsetzbaren Informationen und forensischen Werkzeugen können Administratoren schneller und gezielter auf Sicherheitsvorfälle reagieren und damit deren Auswirkungen und Folgekosten reduzieren.

- **Vorfallreaktion:** Nutzung vordefinierter Playbooks und forensischer Werkzeuge
- **Time Machine:** Erneute Wiedergabe von Netzwerkereignissen zur Ursachenanalyse



Beispiel für die Architektur eines Deployments im Rechenzentrum (© Nozomi Networks)

Die Rollen von IKARUS und Nozomi Networks

IKARUS übernimmt die Integration und den Betrieb der Nozomi Networks Technologie in Ihrem Rechenzentrum. Wir begleiten Sie vor, während und nach der Implementierung Ihrer Sicherheitslösung, um eine nahtlose und störungsfreie Integration der Nozomi Networks-Technologien in Ihre Systemlandschaft zu ermöglichen. Wir stellen sicher, dass das Projekt zu Ihrer vollsten Zufriedenheit umgesetzt wird und Ihre Teams mit den neuen Technologien und Werkzeugen vertraut gemacht werden.

- **Beratung und Planung:** Analyse Ihrer bestehenden Infrastruktur und Identifizierung der Sicherheitsanforderungen
- **Implementierung:** Installation und Konfiguration der Nozomi Networks Lösung
- **Schulung und Support:** Schulung Ihres Personals und kontinuierlicher Support zur Sicherstellung eines reibungslosen Betriebs

Nozomi Networks stellt die Technologie bereit, die zur Sicherung Ihres Rechenzentrums erforderlich ist. Ihre Plattform bietet die notwendigen Werkzeuge, um umfassende Sichtbarkeit, präzise Bedrohungserkennung und schnelle Reaktionsfähigkeit in OT- und IoT-Systemen zu ermöglichen.

Vorteile der Implementierung

Durch die Implementierung der Nozomi Networks Lösung profitieren Rechenzentren von:

- **Erhöhter Sicherheit:** Schutz kritischer Infrastrukturen und sensibler Daten vor einer Vielzahl von Cyberbedrohungen
- **Betrieblicher Widerstandsfähigkeit:** Proaktive Erkennung und Behebung potenzieller Probleme
- **Regulatorischer Konformität:** Erfüllung von Branchenvorschriften und -standards
- **Kosteneffizienz:** Reduzierung der finanziellen Auswirkungen von Cybervorfällen

Fallstudien

Fallstudie 1: Finanz-Rechenzentrum

Herausforderung: Ein großes Finanzinstitut benötigte eine robuste Sicherheitslösung für sein Rechenzentrum, um den zunehmenden Bedrohungen durch Cyberangriffe entgegenzuwirken. Das Ziel war es, die Betriebskontinuität zu gewährleisten und den Schutz sensibler Kundendaten zu sichern.

Lösung: IKARUS implementierte die Nozomi Networks Plattform zur Echtzeit-Überwachung und Bedrohungserkennung. Dies umfasste die vollständige Sichtbarkeit aller OT- und IoT-Geräte, Anomalie-Erkennung und die Integration von Bedrohungsdatenbanken.

Ergebnisse:

- ✓ **Erhöhte Sichtbarkeit**: Vollständige Transparenz über alle Netzwerkanlagen und deren Kommunikationsmuster
- ✓ **Schnelle Reaktion**: Frühzeitige Erkennung und Abwehr von Bedrohungen, bevor sie den Betrieb beeinträchtigen können
- ✓ **Compliance**: Einhaltung regulatorischer Anforderungen und Verbesserung der Cybersicherheitsstandards

Fallstudie 2: Gesundheitswesen-Rechenzentrum

Herausforderung: Ein führender Gesundheitsdienstleister wollte die Cyberabwehr und operative Resilienz seines Rechenzentrums stärken, um Patientendaten zu schützen und die Integrität der Gesundheitssysteme sicherzustellen. Die zunehmende Anzahl von IoT-Geräten stellte eine zusätzliche Herausforderung dar.

Lösung: Durch die Implementierung der Nozomi Networks Lösung konnte das Gesundheitsunternehmen umfassende Sicherheitsmaßnahmen integrieren. Dazu gehörten die automatische Erkennung und Inventarisierung von Geräten, Echtzeit-Überwachung und detaillierte Bedrohungsanalysen.

Ergebnisse:

- ✓ **Verbesserte Sicherheitslage**: Erhöhung der Sicherheitsstandards und Schutz sensibler Patientendaten
- ✓ **Operative Resilienz**: Sicherstellung der Betriebsbereitschaft durch schnelle Bedrohungserkennung und -abwehr
- ✓ **Regulatorische Einhaltung**: Erfüllung der NIS2-Richtlinien und anderer regulatorischer Anforderungen im Gesundheitswesen

Fazit

Rechenzentren vor Cyber-Bedrohungen zu schützen, erfordert eine robuste und flexible Lösung. IKARUS und Nozomi Networks bieten gemeinsam eine umfassende Sicherheitslösung, die speziell auf die Bedürfnisse von kritischen Infrastrukturen und Rechenzentren zugeschnitten ist.

Durch die Kombination der Expertise und Dienstleistungen von IKARUS mit den innovativen Technologien von Nozomi Networks stellen wir sicher, dass Ihr Rechenzentrum sicher, widerstandsfähig und zukunftssicher bleibt.

Informationen und Beratung:

Tel.: +43 1 58995-500
E-Mail: sales@ikarus.at

www.IKARUSsecurity.com/industrial-cyber-security