NIS2 – verschärfte Cybersicherheit in der Produktion

Empfindliche Strafen ab 2024: Wissen Sie, ob Ihr Unternehmen compliant ist?

Whitepaper

AUVESY-MDT
We secure the world's automation

VORWORT

Unsere Handlungsempfehlungen und Lösungsansätze zur neuen EU-Direktive im Überblick

Zehn Millionen Euro oder zwei Prozent des weltweit im Vorjahr getätigten Umsatzes – mit diesem maximalen Strafmaß will die EU wesentliche Einrichtungen zur Einhaltung neuer Cybersicherheitsstandards bringen. Die neue Cybersicherheitsdirektive soll Angriffe abwenden und Schäden minimieren, um Wirtschaft und Gesellschaft vor Ausfällen und deren Folgen zu schützen.

Diese neuen Vorgaben haben nicht nur Auswirkungen auf die Betreiber kritischer Infrastrukturen an sich, sondern erstrecken sich jetzt auch auf die Industrie und erhöhen indirekt die Sicherheitsanforderungen an alle Unternehmen, die Ziel von Angriffen werden könnten.

Auf einen Blick: wie die EU Industrie und Versorger mit NIS2 zum Handeln drängt

- Verschärftes, verpflichtendes, vorsorgliches Sicherheitsmanagement und Meldepflichten bei Sicherheitsvorfällen
- NIS2 betrifft alle Unternehmen der darin definierten „kritischen“ und „wichtigen“ Sektoren, die Dienste und Produkte für Einwohner und Unternehmen in der EU anbieten – auch wenn die Anbieter selbst ihren Sitz außerhalb der EU haben, beispielsweise in den USA
- Risiken: Bußgelder bei Verstößen, je nach Sektor und Schwere des Verstoßes zwischen sieben und zehn Millionen Euro oder bis zu zwei Prozent des weltweiten Jahresumsatzes

Diese Handlungsempfehlungen richten sich an Betreiber kritischer Infrastrukturen, die ihre Sicherheitsanforderungen durch die neuen EU-Direktive erhöhen wollen, um Wirtschaft und Gesellschaft vor Ausfällen und deren Folgen zu schützen.

Hintergrund: Digitalisierung und Sicherheit in der OT

Mit der Digitalisierung und Automatisierung von Infrastruktur und Produktion steigern Unternehmen und Organisationen ihre Effizienz und schaffen neue Potenziale. Die Transformation von Informationstechnologie und operational Technologie (OT) hat sich in den zurückliegenden Jahren noch deutlich beschleunigt, nicht zuletzt durch die Pandemie.

Parallel zum Digitalisierungsgrad haben Angriffe auf Produktion und Infrastruktur in den vergangenen Jahren deutlich zugenommen. Beispiele sind die gezielte Manipulation einer Trinkwasseraufbereitung in den USA und Angriffe auf Teile des Energienetzes in Europa.

Zugleich haben Ereignisse in den vergangenen Jahren aufgezeigt, wie tiefgreifend die Auswirkungen von unterbrochenen Lieferketten und beeinträchtigter Grundversorgung sind. Die Energie- und Gesundheitsversorgung, aber auch die Produktion wichtiger Grundstoffe und Vorprodukte ist eine wesentliche Säule unserer Gesellschaft und jeder Mangel, jede Unterbrechung oder Störung kann gesamtgesellschaftliche Schäden zur Folge haben.

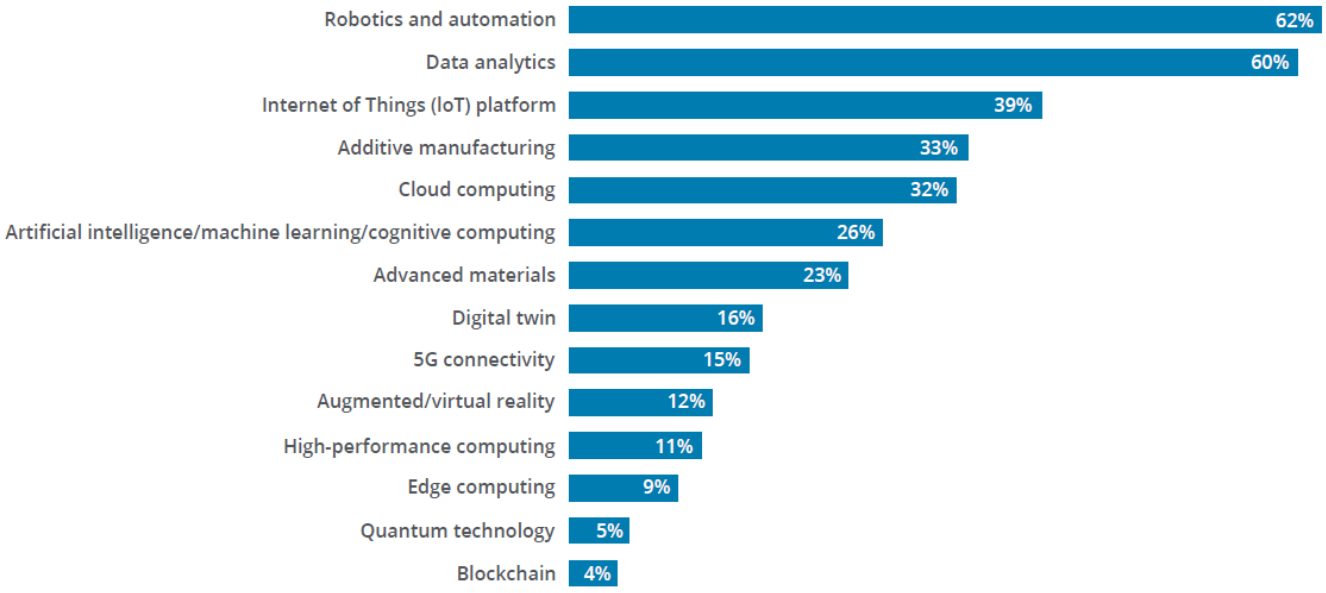
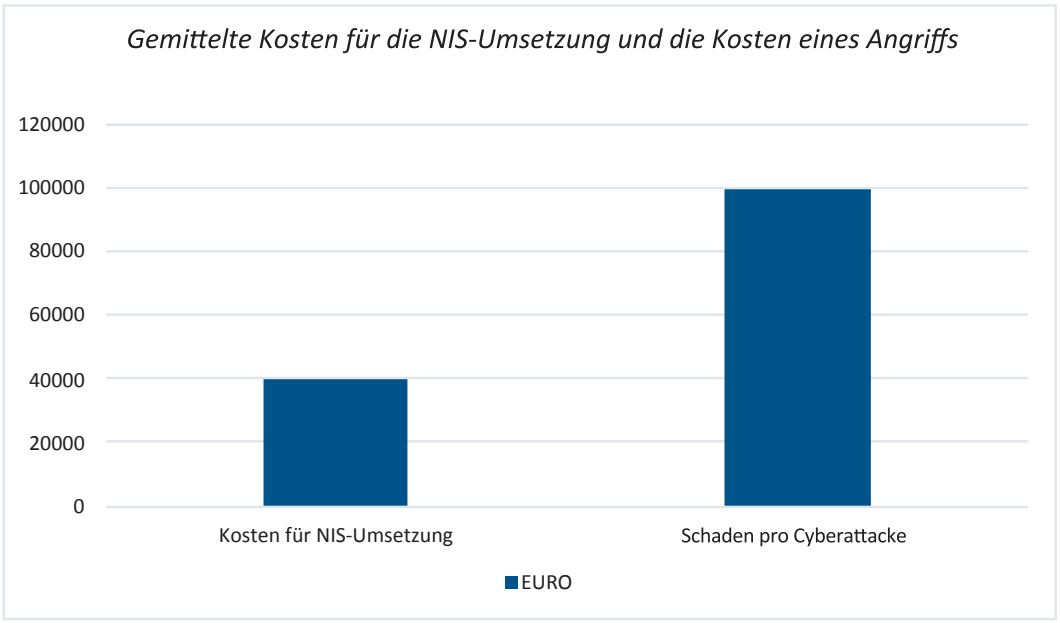


Abb. 1: Laut dem 2023 Manufacturing Industry Outlook | Deloitte US haben sich Unternehmen mit einem höheren Digitalisierungsgrad als widerstandsfähiger erwiesen. Ihre Investitionen in die Digitalisierung konzentrieren sich laut Befragung in den nächsten 12 Monaten auf eine Reihe von Technologien, um die betriebliche Effizienz zu steigern. Quelle: 2023 Deloitte manufacturing outlook survey

NIS und NIS2 – die Zeitleiste

Im Mittel gaben befragte Unternehmen 40.000 Euro für die Umsetzung der Vorgaben aus, während die „European Union Agency for Cybersecurity“ (ENISA) die Kosten eines Angriffs auf durchschnittlich 100.000 Euro schätzt. Das Sicherheitsunternehmen Sophos beziffert die Kosten eines Angriffs speziell auf produzierende Unternehmen im Report „The State of Ransomware in Manufacturing and Production 2021“ gar auf 1,5 Millionen Dollar.

DREI JAHRE NACH INKRAFTTRETEN VON NIS HATTEN NUR VIER VON FÜNF UNTERNEHMEN DIE VORGABEN UMGESETZT.



Quellen: ENISA und Sophos

Unter NIS2 drohen bei schweren Verstößen Strafen von bis zu zehn Millionen Euro oder zwei Prozent des globalen Umsatzes des Unternehmens. Unter der bisherigen Direktive lagen Strafen für Verstöße bei lediglich 150.000 Euro. Obwohl die erste Fassung der NIS-Direktive bereits seit Jahren in Kraft ist, hatten laut ENISA, der EU-Behörde für Cybersicherheit, bis Ende 2021 nur 82 Prozent der befragten Unternehmen die NIS-Vorgaben umgesetzt.

Zwei Drittel davon mussten für die Umsetzung der Direktive zusätzliches Budget bereitstellen. **Jedes zweite Unternehmen gibt an, dass die neuen Maßnahmen seine Threat Detection verbessert haben**, ein Viertel sagt, dass sich die Recovery-Fähigkeiten dadurch verbessert haben. Das ist ein großer Fortschritt, besonders beim Thema Recovery zeigt sich hier jedoch noch Verbesserungspotenzial. Angesichts der deutlich gestiegenen Bußgelder sind Investitionen in die Cybersecurity folgendermaßen verteilt:

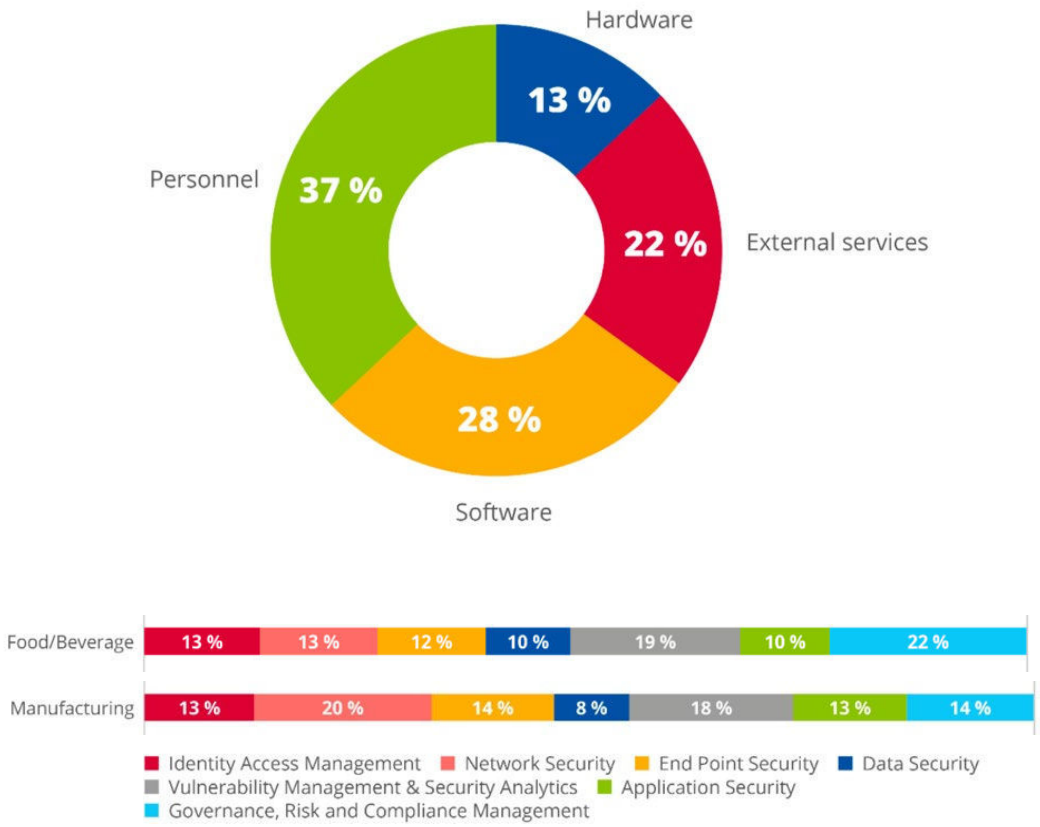


Abb. 2: Die Ausgabenverteilung und Maßnahmen für IT-Sicherheit – insgesamt und in einzelnen Industrien. Quelle: Gartner, IT Key Metrics Data 202: IT Security Measures

NIS2 – nur für KRITIS-Unternehmen?

Für wen gilt NIS2 in der Praxis? Die Definition erweitert die bisherige Fassung (NIS) von „kritischen" um „wichtigen Infrastrukturen und umfasst damit sehr viele Branchen. Bisher – unter der ersten Fassung der NIS-Direktive – konnten die EU-Mitgliedsstaaten selbst bestimmen, welche Branchen und Unternehmen sie als kritische Infrastruktur einordnen. Jetzt legt die EU allgemeingültige Sektoren und Kriterien fest.

Bedeutung der Sektoren

Die Kriterien und Sektoren ähneln denen der deutschen KRITIS-Verordnung, jetzt ist jedoch die EU-Direktive „Resilience of Critical Entities" (RCE) gültig: Die EU unterscheidet hier in der Definition zwischen „kritischen" und „wichtigen" Branchen beziehungsweise Sektoren: Elf Branchen fallen in den Bereich „kritische Infrastruktur", weitere sieben Branchen in „wichtige Infrastruktur". Dies ist mehr als bisher unter der ersten NIS-Direktive in Deutschland. Die Verordnung richtet sich an alle Branchen, in denen ein Ausfall ein Risiko für die öffentliche Sicherheit oder Gesundheit wäre oder systematische Risiken brächte. **Produzierende Unternehmen** werden jetzt zu den „Important Entities" in NIS2 gezählt, fallen damit in den Bereich „wichtige Unternehmen". Die **Herstellung von Lebensmitteln sowie industriellen und chemischen Gütern** war bisher unter der NIS-Direktive nicht erfasst, ist **von NIS2 jedoch direkt betroffen.**

Sektoren, die von NIS2 direkt betroffen sind:

Essenzielle Sektoren	**Untersektoren/Beispiele**
Abwasser und Trinkwasser	-
Banken	-
Digitale Infrastruktur	*Provider, Rechenzentren, Registrare etc.*
Energie	*Strom, Gas, Öl etc.*
Finanzen	*Handelsplätze und Co.*
Gesundheit	*Forschung, medizinische Geräte, Gesundheitsanbieter etc.*
IT-Dienstleister	*Serviceprovider, Sicherheitsanbieter etc.*
Raumfahrt	-
Transport	*Schiene, Straße etc.*
Verwaltung	*Lokale bis nationale Verwaltung*
Wichtige Sektoren	**Untersektoren/Beispiele**
Abfallentsorgung	
Chemie	
Digitale Services	*Social-Media-Anbieter, Suchmaschinen etc.*
Ernährung	
Forschung	
Industrie	*Autos, Elektrik, Computer, Maschinenbau etc.*
Post	

Abb. 3: Die Branchen der produzierenden Industrie sind von NIS2 neu erfasst und hier farblich hervorgehoben.

Größe der Unternehmen
Eine weitere Abgrenzung zieht die EU bei der Größe der Unternehmen. Mittlere (50–250 Mitarbeitende) und größere Unternehmen (> 250 MA) sind direkt betroffen. Unternehmen der digitalen Infrastruktur sind unabhängig von der Größe immer betroffen. Weitere Ausnahmen: Öffentliche Stellen und Anbieter mit grenzübergreifenden Auswirkungen fallen unter die geplante Regelung – unabhängig von der Größe. Bundes- und Länderbehörden sind jetzt ausnahmslos betroffen. Die gesetzgebenden Länder können selbst bestimmen, ob auch regionale und lokale Behörden unter die Regelung fallen sollen.

NIS2 betrifft nicht mehr nur kritische Infrastrukturen!
Chemie, Ernährung und Industrie (darunter beispielsweise Maschinenbau, Transport, Auto und Elektrik) fallen bei NIS2 unter die „wichtigen Sektoren", sind demnach direkt von der Direktive betroffen.

NIS und NIS2 wirken über die unmittelbar betroffenen Branchen hinaus. Denn einerseits setzt die Direktive Mindeststandards und Best Practices fest, an denen sich auch Unternehmen aus nicht essenziellen Branchen orientieren sollten. Nicht aus Sorge vor Compliance-Verstößen und Strafzahlungen, sondern rein pragmatisch. Beispielsweise richten sich Prämien für Versicherungen gegen Betriebsunterbrechungen oder gegen Schäden durch Cyberangriffe ebenso nach vorhandenen Schutzmaßnahmen, Schadenswahrscheinlichkeiten und vergangenen Vorfällen.

Zudem sorgt ein steigendes Schutzniveau in den regulierten kritischen Branchen potenziell dafür, dass Angreifer zunehmend auf andere Sektoren ausweichen könnten, die vermeintlich schlechter geschützt und somit leichtere Ziele sind. **Laut der europäischen ENISA hat bislang nur jedes zweite Unternehmen eine Cyberversicherung.**

Was Unternehmen umsetzen müssen

Die konkreten Vorgaben von NIS2 verlangen von Anbietern kritischer Infrastrukturen effektive Cybersicherheitsmaßnahmen, beispielsweise im Rahmen des Risikomanagements. In der Direktive wird besonders deutlich, dass Unternehmen vor allem strukturelle Maßnahmen ergreifen sollen: Sie sollten Risiken bewerten, Regeln aufstellen und auf dieser Basis die Umsetzung vollziehen oder Lösungen implementieren. Hier wird von der Politik eine gelebte Sicherheitskultur verlangt, statt bestimmte Sicherheitsmechanismen vorzuschreiben. Denn Lösungen allein helfen nur bedingt: In ihrer Studie zur NIS-Umsetzung hat die Sicherheitsagentur ENISA beispielsweise festgestellt, dass in Unternehmen die Wirkung des reinen Vorhandenseins von Sicherheitslösungen über- und die tatsächliche Effektivität dieser Lösungen als Variable unterschätzt wird.

JEDES ZWEITE UNTERNEHMEN GIBT AN, DASS DIE NEUEN (NIS-) MASSNAHMEN SEINE THREAT DETECTION VERBESSERT HABEN.

Risikomanagement und Incident Response in der OT

Die Direktive beschäftigt sich mit einigen Aspekten und Maßnahmen der Cybersecurity und fokussiert sich dabei vor allem auf zwei Aspekte: Risikomanagement und Incident Response. Für Verantwortliche in der OT sind diese beiden Aspekte der Cybersecurity ebenfalls besonders relevant. Beim Risikomanagement geht es darum, Schwachstellen und potenzielle Angriffspunkte zu identifizieren, bevor andere es tun. Auch die Abschätzung potenzieller Folgen gehört mit zum Risikomanagement.

Abb. 4: Die ersten Schritte, um NIS2-Konformität zu erreichen.

Was Unternehmen in die Praxis bringen müssen

NIS2 zwingt jetzt auch Unternehmen der produzierenden Industrie jenseits des bisherigen KRITIS-Einflussbereichs dazu, hinreichende Regeln, Prozesse und Strukturen zu implementieren, um systematisch mit potenziellen Sicherheitsrisiken umgehen zu können. Hier finden Sie eine Übersicht über die grundsätzlich notwendigen Ebenen der Maßnahmen.

Führung

Die Leitung hat die Verantwortung, Regeln und Prozesse festzulegen sowie die Effektivität der Maßnahmen zu überprüfen. Cybersicherheit ist heute auch für nicht regulierte Branchen geschäftskritisch.

Risikomanagement

Unternehmen müssen Risiken identifizieren, verstehen und bewerten.
Dabei hilft beispielsweise das Handbuch „Management von Cyber-Risiken", Anhang B.

Asset-Management

Alle Komponenten, die nötig sind, um elementare Dienste zu betreiben, müssen erfasst werden. Das beginnt beim Personal und führt über alle Geräte und Systeme bis hin zu den kritischen Daten.

Training und Personal

Personal für Cybersecurity einstellen, Mitarbeitende schulen, Sicherheit in der Personalbeschaffung.

Schutzmaßnahmen implementieren

Sicherheitsprozesse nach ISO 27001/IEC 62443 aufbauen, beispielsweise nach den Vorgaben der IT-Grundschutz-Profile.
Lösungen für Monitoring, Abwehr und Instant Recovery implementieren, um Ausfälle zu vermeiden bzw. zu minimieren.

Incident Management

Vorfälle müssen vermieden, erkannt und professionell behandelt werden.

Verschlüsselung

Kommunikation, Daten und Systeme sollten kryptografisch gesichert werden.

Zulieferer

Auch die Lieferkette und deren potenzielle Sicherheitsrisiken müssen gemäß der Direktive erfasst, bewertet und gesteuert werden.

Umsetzung mit Hilfe eines Daten- und OT-Endpoint-Managements

Wichtige Unternehmen sind angehalten, Ausfälle zu verhindern und im Ernstfall deren Dauer zu minimieren. Dazu benötigen sie eine effektive Lösung für ihre Daten- und Backup-Strategie und müssen ihre Endpoints zunächst vollständig erfassen.

1. Unternehmen müssen einerseits alle Assets in der Produktion katalogisieren und beobachten, das **Asset-Management**. Jede SPS-Steuerung, jede Komponente der Automatisierung und jede Maschine sollten digital erfasst und überwacht werden. Dies ist die Grundlage für jeden folgenden Schritt.
2. Im zweiten Schritt gehört die **Versionierung** aller Softwarestände und -änderungen (Change Management) zu jeder Sicherheitsstrategie. Wer hat welche Änderung vorgenommen? Zugleich ist dies die Grundlage dafür, nach einem Fehler oder einem Angriff den zuletzt funktionierenden Stand (Recovery) wiederherzustellen.
3. Die **Zugriffssteuerung** legt fest, wer welche Daten ändern darf.
4. Das **Monitoring** aller erfassten Anlagen macht Änderungen und Abweichungen vom Sollzustand transparent und ermöglicht es erst, auf Vorfälle zu reagieren.
5. Die **Backup-Strategie** bestimmt, welche Daten wo und wie lange redundant vorgehalten werden, um jederzeit auf eine sichere Kopie aller Produktionsprogramme und Softwarestände zugreifen zu können.

Mit diesen Ansätzen schaffen sich produzierende Unternehmen die Grundvoraussetzungen für alle rechtlichen Anforderungen aus NIS, KRITIS und weiteren Sicherheitsgesetzen. Nur wer seine Produktion digital erfasst sowie überwacht und seine Daten systematisch sichert, kann die aktuellen Vorgaben erfüllen und seine Prozesse auch auf zukünftige, strengere Anforderungen adaptieren.

Wie octoplant Ihre Produktion absichert

Mit octoplant, der modularen Lösung für Endpoint- und Datenmanagement in der Produktion, können Unternehmen Automatisierungsgeräte in der Produktion vor Risiken und kostspieligen Produktionsausfällen schützen. Anwender sind stets auf dem neuesten Stand der Technik und können damit Compliance-Anforderungen umsetzen. octoplant ist modular am Anwendernutzen ausgerichtet:

Threat Protection
Mit octoplant überwachen Unternehmen ihre Assets und werden automatisch über Schwachstellen und Risiken informiert. Ein individueller Risiko-Score für jedes Asset zeigt potenzielle Gefahren. Weitere präventive Maßnahmen wie die Erkennung von Änderungen und Schwachstellen unterstützen aktiv dabei, Ausfälle zu vermeiden. Somit ist octoplant ein wichtiger Teil der Sicherheitsarchitektur in der Produktion.

Safeguarding Assets
In komplexen Produktionsumgebungen kann die Versionierung zahlreicher unterschiedlicher Projekte und deren jeweiliger Änderungen nicht nur zu einer aufwändigen, sondern zu einer kritischen Aufgabe werden. Versionsverwaltung und automatische Backups aller Versionen und Änderungen sorgen dafür, dass immer die korrekte Version läuft. Unterschiede zwischen Datenständen lassen sich grafisch und tabellarisch darstellen. Die automatisierte Datensicherung spart Zeit, reduziert Fehler und erhöht die Zuverlässigkeit für die Programmierung und Konfiguration der Geräte.

Device Management
Heterogene Steuerungen und inkompatible Herstellerlösungen bremsen die vernetzte Automatisierung und können effektive Sicherheitslösungen erschweren. octoplant bindet alle gängigen IoT Devices ein, verwaltet und überwacht herstellerübergreifend alle Konfigurationsdaten und schlüsselt auf, wer, wann welche Änderungen vorgenommen hat. Dies macht octoplant zur idealen Plattform für OT-Datenmanagement.

Instant Recovery
In einem Notfall sorgt Instant Recovery dafür, dass alle notwendigen Programme und Daten in kürzester Zeit auf dem zuletzt aktuellen Stand wiederhergestellt werden. Somit ermöglicht es octoplant, einzelne Geräte oder die gesamte Produktionsanlage jederzeit valide wiederherstellen zu können. Ausfälle und Störungen werden so minimiert, Fehler und Manipulationen rückgängig gemacht.

Compliance einhalten
Um Prozesse im Alltag rechtssicher gestalten zu können, bietet octoplant eine integrierte Dokumentation für Compliance-konforme Abläufe und Compliance Management. Alle Produktionsabläufe sind hier im Falle eines Audits lückenlos nachverfolgbar.

ANWENDUNGSFÄLLE IN DER PRODUKTION & WASSERVERSORGUNG

Anwendungsfall Wasserversorgung

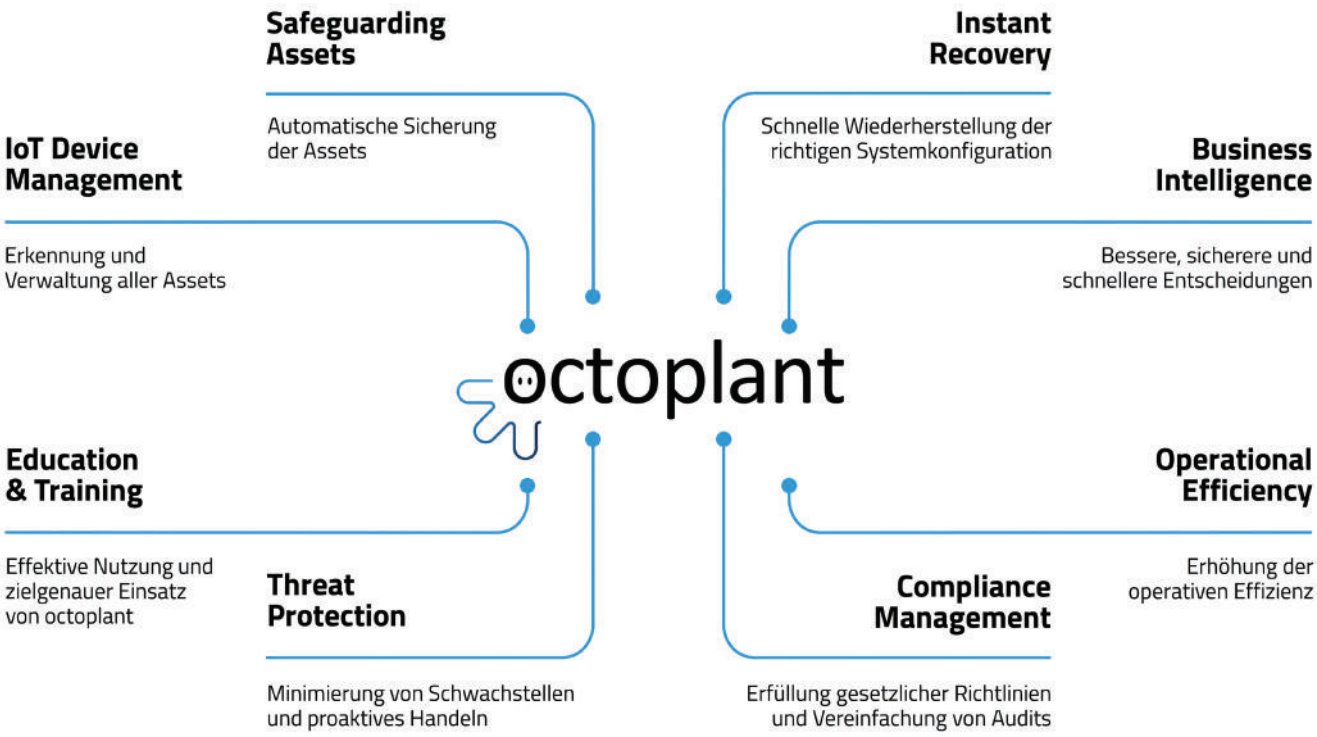
Die Wasserwirtschaft zählt zu den essenziellen Versorgungsleistungen und unterliegt deshalb der KRITIS-Verordnung und jetzt zusätzlich auch der NIS2-Direktive. Der Wasserversorger Canal de Isabel II ist der zentrale Wasserversorger in der Region Madrid. Die 600 Messstationen und 250.000 Messvariablen aller Wasserwerke des Versorgers sollten zu einem einheitlichen Überwachungssystem konsolidiert werden. Auf dieser Plattform werden Statusinformationen der Stationen, der Prozesse und der Geräte visuell in Echtzeit abgebildet. Das Daten- und Endpoint-Management von AUVESY-MDT dient in diesem Systemverbund als Absicherung und verwaltet Backups und die Wiederherstellung früherer Versionen dieser überwachten Geräte.

Canal de Isabel II, Spanien

Anwendungsfall in der Produktion

Nanostone: keramische Membranfilter für die Wasseraufbereitung, mit automatisierter Produktion in Deutschland – zunehmend automatisiert. Die Produkte werden für Entsalzung, Industrie und die öffentliche Wasserversorgung eingesetzt. Die Produktion dieser Keramikfilter ist besonders kritisch. Nanostone setzt in der Produktion zahlreiche unterschiedliche Siemens-PLCs für die verschiedenen Produktionsprozesse ein. Roboter, CNC-Maschinen, Laser und Transport in der Fertigung. AUVESY-MDT wird seit 2018 für Zugangskontrolle und Versionierung eingesetzt. Das Daten- und Endpoint-Management verwaltet die Dateiversionen, macht Änderungen transparent und sichert die Produktion. Zugriff haben die interne C&I-Automatisierung und Instandhaltung sowie ein externer Dienstleister. Das Unternehmen kann somit alle Versions- und Rezepturänderungen nachvollziehen. Alle Dokumentationsunterlagen befinden sich in einem eigenen Ordner als zentraler Anlaufstelle für die aktuelle Dokumentation. Die Implementierung von AUVESY-MDT lief „überraschend" schnell und reibungslos.

Nanostone Water GmbH, Deutschland



Fazit: sichere, rechtskonforme Produktion mit octoplant

octoplant ermöglicht es Verantwortlichen im Unternehmen, mit einer zentralisierten Standardlösung die gesamte Produktion zu überwachen und zu steuern. Damit werden alle Assets und Devices – über alle Hersteller hinweg – zentral verwaltet. Zentrales Device Monitoring sorgt für Überblick, Safeguarding der Assets durch Backups und die Versionierung erzeugt ein vollständiges Datenabbild der Produktionsanlage. Zugleich bringt Instant Recovery von Softwareversionen und Programmdaten im Notfall alle Daten wieder auf den richtigen Stand. Und: Durch proaktive Schwachstellen-, Änderungs- und Risikoerkennung schützt octoplant Produktionsabläufe vor Angriffen und vermeidet Schäden und Produktionsausfälle.

MEHR ALS 2.800 KUNDEN SETZEN BEI IHRER INSTANDHALTUNG UND PRODUKTIONS-VERWALTUNG BEREITS AUF DIE LÖSUNGEN VON AUVESY-MDT.

Informieren Sie sich jetzt über die kostenlose Testversion!

Hier klicken: octoplant Web-Demo

*https://auvesy-mdt.com/de/live-web-demo

AUVESY-MDT

AUVESY-MDT ist der weltweite Markt- und Technologieführer für Versionierungs- und Backuplösungen in der industriellen Automatisierung. Mit seiner Softwareplattform octoplant sichert das Unternehmen die Automatisierung von Produktionsprozessen durch ein starkes End-Point-Management ab, in dem es die Änderungen an Konfigurationen, Programmierungen und Projektständen in der Fertigung konsequent erfasst und überwacht. So können Stillstandzeiten minimiert, die Effizienz sowie Qualitäts- und Sicherheitsstandards erhöht sowie Kosten und Ressourcen eingespart werden. Als modulare Lösung, lässt sich octoplant herstellerunabhängig mit unterschiedlichen Automatisierungstechnologien und Geräten verknüpfen.

AUVESY-MDT entstand 2022 aus dem Zusammenschluss der beiden etablierten Marktführer AUVESY GmbH und MDT Software Inc. Der Hauptsitz ist in Landau in der Pfalz, weitere Standorte befinden sich in den USA und in China. Das Unternehmen arbeitet mit mehr als 100 Partnern auf allen Kontinenten zusammen und betreut über 2.800 Kunden weltweit.

Novotek

Novotek Switzerland AG

Glutz-Blotzheim-Strasse 3
CH-4500 Solothurn
+41 58 255 32 32
info@novotek.ch