SOLUTION BRIEF

Richtlinie der Europäischen Union zur Netzwerk- und Informationssicherheit (NIS2)

Dragos kann Unternehmen aus der Europäischen Union bei der Erfüllung der Anforderungen unterstützen

Das Ziel von Dragos ist es, die Gesellschaft zu schützen, indem wir die Plattform, die Dienste und die Intelligenz zum Schutz der Betriebstechnologie (OT) und der kritischen Infrastruktur bereitstellen. Unsere Technologie unterstützt zahlreiche Standards und Vorschriften und ermöglicht unseren Kunden, Best Practices anzuwenden und Compliance-Anforderungen zu übertreffen.

Die NIS2-Richtlinie ist ein überarbeiteter Rahmen, der auf der EU-Richtlinie zur Netz- und Informationssicherheit dem ersten EU-weiten Rechtsakt zur Cybersicherheit basiert. Die Richtlinie sieht rechtliche Maßnahmen zur Verbesserung der allgemeinen Cybersicherheit in der EU vor, wobei der Schwerpunkt auf der Abwehrbereitschaft und der Zusammenarbeit in kritischen Sektoren liegt.

Die Richtlinie verpflichtet die Betreiber kritischer Dienste, geeignete Sicherheitsmaßnahmen zu ergreifen, die zuständigen nationalen Behörden über schwerwiegende Vorfälle zu informieren und die Sicherheitsrisiken in ihren Lieferketten zu verringern, indem sie die Produktqualität und die Cybersicherheitspraktiken von Lieferanten und Dienstleistern bewerten.

Das Management muss dabei eine aktive Rolle bei der Überwachung und Umsetzung übernehmen, was die Bedeutung des CISOs als Ausbilder und Ratgeber für bewährte Praktiken für leitende Angestellte stärkt. Unternehmen, die sich nicht daran halten riskieren Bußgelder, die Haftung des Managements, befristete Verbote für Manager und mehr.

Dragos bietet Überwachungstechnologie, Threat Intelligence, Incident Response und Professional Services, um Unternehmen dabei zu unterstützen, sich auf die Anforderungen der NIS2-Richtlinie vorzubereiten und diese zu erfüllen oder sogar zu übertreffen. Wir arbeiten direkt mit CISOs und anderen Führungskräften in Ihrem Unternehmen zusammen, um Sie bei der Entwicklung einer Vision, der Erstellung eines detaillierten Aktionsplans und der Erzielung konsistenter und dokumentierter Ergebnisse zu unterstützen.

Welche Sektoren fallen unter die NIS2-Richtlinie?

Gesundheitswesen

Transport

Herstellung von kritischen Produkten

(unter anderem, Pharmazeutika, Medizinische Geräte, Chemikalien)

Digitale Infrastruktur, einschließlich Rechenzentren

Raumfahrt

Lebensmittel

Post und Kurierdienste

Öffentliche Verwaltung

Wasser-versorgung

Abwasser- und Abfall-entsorgung

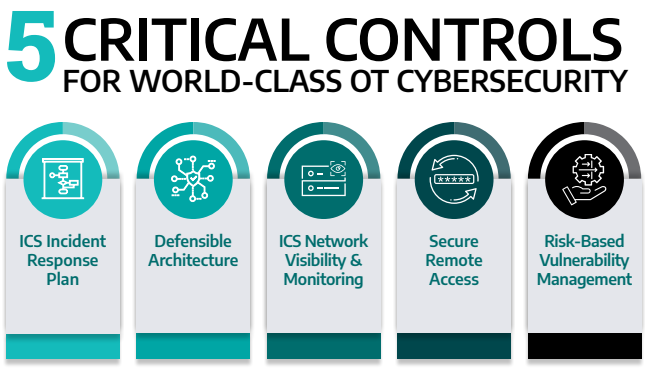
Energie

Wann tritt die NIS2-Richtlinie in Kraft?

Die NIS2-Richtlinie wurde am 27. Dezember 2022 im EU-Amtsblatt veröffentlicht und trat am 16. Januar 2023 in Kraft. Die Mitgliedstaaten müssen die Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen. Jeder Mitgliedstaat wird seine eigenen spezifischen nationalen Rechtsvorschriften erlassen, um die Anforderungen der NIS2-Richtlinie zu erfüllen.

Die NIS2 zielt darauf ab, einen besser koordinierten Ansatz für das Cybersicherheitsmanagement zu entwickeln, um die Unterschiede in der Cybersicherheitsresilienz zwischen verschiedenen Sektoren zu verringern, indem mehrere Schlüsselmaßnahmen zur Beherrschung der Risiken für Netzwerk- und Informationssicherheit skizziert werden.

NIS2 und die fünf wichtigen Schritte für ICS/OT Cybersicherheit



Der Mitbegründer und CEO von Dragos, Robert M. Lee, hat zusammen mit Tim Conway, ICS Curriculum Director des SANS Institute, fünf wichtige Schritte für die ICS/OT-Cybersicherheit identifiziert. Diese Schritte können weltweit umgesetzt werden und ermöglichen Unternehmen, verschiedene Vorschriften, einschließlich der NIS2-Richtlinie, zu erfüllen oder zu übertreffen. Die fünf Schritte legen den Schwerpunkt auf Praktiken, die eine aktive Verteidigung im Gegensatz zu einem traditionellen präventionsorientierten Ansatz fördern, was gut mit dem risikobasierten Ansatz der NIS2-Richtlinie übereinstimmt.

SCHRITT	ZUSAMMENFASSUNG	ANWENDBARKEIT NIS2-RICHTLINIE
ICS Incident Response Plan	Erstellen Sie einen spezifischen Plan, der die richtigen Ansprechpartner enthält, z.B. wer über welche Fähigkeiten in denjenigen Anlage verfügt, sowie durchdachte nächste Schritte für bestimmte Szenarien für bestimmte Standorte. Identifizieren Sie verantwortliche Parteien, Benachrichtigungs- und Eskalations-richtlinien. Nutzen Sie Tabletop-Übungen, um Incident Response Pläne zu testen und zu verbessern.	Umgang mit Vorfällen (Vorbeugung, Erkennung und Reaktion) Business Continuity und Krisenmanagement
Verteidigungsfähige Architektur	OT-Sicherheitsstrategien beginnen oft mit Härtung der Umgebung - Entfernen fremder OT-Netzwerkzu-griffspunkte, Aufrechterhaltung einer starken Richtlinienkontrolle an IT/OT-Schnittstellen und die Reduzierung von Schwachstellen mit hohem Risiko. Vielleicht noch wichtiger als eine sichere Architektur sind dabei die Menschen und Prozesse, die sie erhalten. Die für die Anpassung an neue Schwachstellen und Bedrohungen erforderlichen Ressourcen und technischen Fähigkeiten sollten nicht unterschätzt werden.	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit Sicherheit der Lieferkette - einschließlich sicherheitsrelevante Aspekte der Beziehungen zwischen jeder Einrichtung und (i) ihren Lieferanten oder (ii) Dienstleistern (wie Anbietern von Daten-speicherungs- und -verarbeitung-diensten oder Anbieter von Managed Security Services)
ICS Netzwerk Sichtbarkeit und Überwachung	Man kann nicht schützen, was man nicht sehen kann. Ein erfolgreiches OT-Sicherheitskonzept enthält ein Assets-Inventor, erfasst Schwach-stellen der Assets (und Pläne zur Risikominderung), und überwacht aktiv überwacht den Datenverkehr auf potenzielle Bedrohungen. Die Sichtba-rkeit, die durch die Überwachung Ihrer Assets erreicht wird, validiert die Sich-erheitskontrollen einer verteidigungs-fähigen Architektur. Die Erkennung von Bedrohungen durch Überwachung ermöglicht Skalierbarkeit und Autom-atisierung für große und komplexe Netzwerke. Darüber hinaus erleichtert die Überwachung die Identifizierung von Schwachstellen und das Ergreifen von Maßnahmen.	Risikoanalyse und Sicherheit für Informationssysteme Sicherheit der Lieferkette - ein-schließlich sicherheitsrelevante Aspekte der Beziehungen zwischen jeder Einrichtung und (i) ihren Lieferanten oder (ii) Dienstleistern (wie Anbietern von Datenspeicherungs- und - verarbeitungdiensten oder Anbieter von Managed Security Services Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

SCHRITT	ZUSAMMENFASSUNG	ANWENDBARKEIT NIS2-RICHTLINIE
Sicherer Fernzugriff	Ein sicherer Fernzugriff ist entscheidend für OT-Umgebungen. Eine wichtige Methode, Multi-Faktor-Authentifizierung (MFA) ist ein seltener Fall einer klassischen IT-Kontrolle, die auf OT angewendet werden kann. Implementieren Sie MFA in allen Ihren Systemen, um eine zusätzliche Sicherheitsebene für eine relativ geringe Investition zu schaffen. Wo MFA nicht möglich ist, sollten alternative Kontrollen wie Jump-Hosts mit gezielter Überwachung eingesetzt werden. Der Schwerpunkt sollte hierbei auf den Verbindungen in und aus dem OT-Netz und nicht auf den Verbindungen innerhalb des Netzes liegen.	Die Verwendung von Kryptographie und Verschlüsselung
Risikobasiertes Schwachstellen-management	Die eigenen Schwachstellen zu kennen – und einen Plan zu haben, wie man mit ihnen umgeht - ist eine wesentliche Komponente für einer verteidigungsfähigen Architektur. Über 1200 OT-spezifische Schwach-stellen wurden im vergangenen Jahr veröffentlicht, die meisten von ihnen mit unvollständigen oder fehlerhaften Informationen. Während es relativ einfach ist, ein IT-System wie den Laptop eines Mitarbeiters zu patchen, ist das Herunterfahren einer Anlage mit enormen Kosten verbunden. Ein effektives OT Schwachstellen-management-Programm erfordert das rechtzeitige Erkennen der wichtigsten Schwachstellen, die sich auf die Umgebung auswirken, mit korrekten Informationen und Risikobewertungen sowie alternativen Minderungsstrategien, um die Gefährdung zu minimieren und gleichzeitig den Betrieb aufrechtzuerhalten.	Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen Sicherheit der Lieferkette - einschließlich sicherheitsrelevante Aspekte der Beziehungen zwischen jeder Einrichtung und (i) ihren Lief-eranten oder (ii) Dienstleistern (wie Anbietern von Datenspeicherungs- und -verarbeitungdiensten oder Anbieter von Managed Security Services)

Dragos Lösungen zu den spezifischen NIS2-Anforderungen

Die folgende Tabelle zeigt die Zuordnung der Dragos Lösungen zu den spezifischen NIS2-Anforderungen

NIS2 RICHTLINIE, KAPITEL IV, ARTIKEL 21	BESCHREIBUNG	DRAGOS ANGEBOT
a	Risikoanalyse und Sicherheit für Informationssysteme	• Dragos Industrial Cyber Risk Management (ICRM) • Tabletop Exercises • OT Cybersecurity Assessment
b	Incident Handling (Vorbeugung, Erkennung und Reaktion)	• Dragos Platform • OT Watch • Dragos WorldView Threat Intelligence • Incident Response/Rapid Response Retainer
c	Business Continuity und Krisenmanagement	• Incident Response/Rapid Response Retainer • OT Cybersecurity Assessment • Dragos ICS-OT Cybersecurity Training
d	Sicherheit der Lieferkette - einschließlich sicherheitsrelevante Aspekte der Beziehungen zwischen jeder Einrichtung und (i) ihren Lieferanten oder (ii) Dienstleistern (wie Anbietern von Datenspeicherungs- und - verarbeitungsdiensten oder Anbieter von Managed Security Services)	• Dragos Platform • Dragos Industrial Cyber Risk Management (ICRM) • Dragos WorldView Threat Intelligence • ICS Network Vulnerability Assessment
e	Sicherheitsmaßnahmen in Netzwerken und Informationssystemen – Erwerb, Entwicklung und Wartung von Netz- und Informations-systemen, einschließlich Management und Offenlegung von Schwachstellen	• Dragos Platform • OT Watch • OT Cybersecurity Assessment • Dragos WorldView Threat Intelligence • Dragos Neighborhood Keeper • ICS Penetration Testing

NIS2 RICHTLINIE, KAPITEL IV, ARTIKEL 21	BESCHREIBUNG	DRAGOS ANGEBOT
f	Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit	• Dragos Industrial Cyber Risk Management (ICRM) • OT Cybersecurity Assessment • ICS Penetration Testing • Maturity Assessment
g	Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;	• Dragos Platform • OT Cybersecurity Assessment, inklusive Architecture Review und Penetration Testing

Beschreibungen der Dragos Angebote

Dragos Industrial Cyber Risk Management (ICRM)

Die Dragos Richtlinien für industrielles Cyber-Risikomanagement fassen Best Practices, Frameworks und Standards in einem Prozess zusammen, der sowohl für Neueinsteiger als auch für erfahrene Risikomanager zugänglich ist.

Tabletop Exercises

Die Dragos Dienstleistung Tabletop Exercise (TTX) ist eine schrittweise Methode, die zeigt, wie ein realistischer Angriff in Ihrer spezifischen ICS-Umgebung durchgeführt werden kann - basierend auf den Hauptrisiken Ihres Unternehmens. Dragos TTXs beinhalten die Zusammenarbeit aller Beteiligten, einschließlich der Informationstechnologie (IT) und der Sicherheitsteams für industrielle Kontrollsysteme (ICS), um interne Kommunikationsstrategien zu stärken und Beziehungen zu entwickeln.

OT Cybersecurity Assessment

Das OT Cybersecurity Assessment umfasst eine vollständige Programmüberprüfung, eine Kronjuwelenanalyse, eine Topologieüberprüfung, eine Überprüfung von Standards und Vorschriften, die Suche nach Anzeichen einer Kompromittierung, die Identifizierung von Bedrohungen, eine Bestandsaufnahme der Assets, eine Bewertung der Netzwerkanfälligkeit und eine Schwachstellenbewertung.

Dragos Platform

Die Dragos Platform ist eine Cyber-Sicherheitstechnologie für industrielle Kontrollsysteme (ICS), die einen unvergleichlichen Einblick in Ihre ICS/OT-Assets und -Kommunikation bietet. Sie zeigt Bedrohungen durch intelligente Analysen schnell auf, identifiziert und priorisiert Schwachstellen und bietet Best-Practice-Playbooks, um Teams bei der Untersuchung und Reaktion auf Bedrohungen zu unterstützen, bevor diese erheblichen betrieblichen Auswirkungen haben.

OT Watch

Mit Dragos OT Watch werden unsere ICS-Cybersicherheitsexperten Teil Ihres Teams und führen mit der Dragos Platform eine Triage der schwerwiegendsten Meldungen und proaktive Bedrohungssuche durch, um sicherzustellen, dass Bedrohungen nicht übersehen werden. Unser Expertenteam von Analysten sucht proaktiv nach Bedrohungen in Ihrer ICS-Umgebung und informiert Sie über die Ergebnisse, wobei die neuesten Bedrohungsdaten exklusiv für Dragos-Kunden verwendet werden. In Zusammenarbeit mit Ihrem Team führen wir eine Triage der schwerwiegendsten Meldungen durch und untersuche diese, um die Belastung Ihrer internen Ressourcen zu reduzieren.

Dragos WorldView Threat Intelligence

Dragos WorldView Industrial Threat Intelligence liefert umsetzbare Informationen und Empfehlungen zu Bedrohungen für OT-Umgebungen. Es bietet Sicherheitsteams einen detaillierten Einblick die Taktiken, Techniken und Verfahren (TTPs) hochentwickelter Angreifer, die weltweit auf industrielle Netzwerke abzielen. So kann sich Ihr Unternehmen besser auf mögliche Angriffe vorbereiten, diese erkennen und darauf reagieren.

Incident Response/Rapid Response Retainer

OT-spezifische Reaktionspläne sind für industrielle Umgebungen unerlässlich. Die möglichen Auswirkungen eines Cyber-Angriffs können je nach Sichtbarkeit, Reaktionsfähigkeit und Sicherheitslage Ihres Unternehmens variieren. Deshalb ist ein spezifischer ICS/OT-Reaktionsplan, der Ihre Bedürfnisse berücksichtigt, entscheidend, um Vorfälle schnell zu erkennen, zu untersuchen und darauf zu reagieren. Als Eckpfeiler Ihres ICS/OT-Cybersicherheitsprogramms gewährleistet ein ICS-spezifischer Incident Response Retainer eine schnelle Reaktion und sichere Wiederherstellung.

Dragos ICS-OT Cybersecurity Training

Das Training schafft ein besseres gemeinsames Verständnis der Terminologien, des Zwecks, der Sicherheitsziele und der Technologien, die in OT-Umgebungen und Sicherheitsprogrammen verwendet werden. Die Schulung der Mitarbeiter in Grundlagen der Cybersicherheit ist ein wichtiger Teil der Business Continuity - Cybersicherheit geht alle an, und die Mitarbeitenden stehen an vorderster Front, wenn es darum geht, Probleme zu erkennen und zu entschärfen.

ICS Network Vulnerability Assessment

Ein ICS Network Vulnerability Assessment hilft Ihrem Oranisation, Lücken im Netzwerkschutz zu schließen, indem die aktuellen Schutz-, Erkennungs- und Reaktionsfähigkeiten Ihrer Umgebung bewertet werden.

Dragos Neighborhood Keeper

Neighborhood Keeper ist eine Lösung für die kollektive Verteidigung und die Sichtbarkeit in der Community, die durch den Austausch von aggregierten und anonymisierten Informationen über Bedrohungen und Schwachstellen über Sektoren und geografische Regionen hinweg eine effektivere industrielle Cyberabwehr ermöglicht. Durch die Teilnahme wird die Verteidigungsfähigkeit jeder Organisation gestärkt, was sie alleine nicht erreichen könnte.

ICS Penetration Testing

ICS Penetration Testing verhindert schwerwiegende Sicherheitsverletzungen, indem Taktiken, Techniken und Verfahren (TTP) von Angreifern aus der realen Welt verwendet werden. Penetrationstests identifizieren Geräte, die Zugang zu kritischen ICS-Anlagen ermöglichen könnten, und zeigen, wie sich Angreifer in ICS-Umgebungen bewegen können.

Maturity Assessment

Unser branchenführendes Professional Services-Team kann Sie bei der Bewertung und Weiterentwicklung Ihres OT-Cybersicherheitsprogramms mit einer Bewertung nach dem Cybersecurity Capability Maturity Model (C2M2) unterstützen. Das C2M2 wurde vom U.S. Department of Energy entwickelt und bietet eine strukturierte Methode zur Bewertung von Cybersicherheitsfähigkeiten anhand eine abgestuften Reifegradskala, die Unternehmen dabei hilft, ihre aktuellen Cybersicherheits-fähigkeiten besser zu verstehen und ihre Sicherheitslage zu verbessern.

Nächste Schritte: Anpassung der OT-Cybersicherheitsstrategie an den NIS2 Anforderungen

Dragos empfiehlt, mit der Unternehmensleitung und dem Management zusammenzuarbeiten, um alle Beteiligten in die Diskussion über die NIS2-Konformität einzubeziehen. Wenn Sie diese Schritte jetzt unternehmen, wird Ihr Unternehmen in der Lage sein, Programme und Verfahren zu entwickeln, die der Richtlinie entsprechen, wenn sie in Ihrem Land in Kraft tritt.

SCHRITT 1	**Sensibilisierung der obersten Führungsebene für das Risikomanagement im Bereich der Cybersicherheit, die NIS2 Anforderungen und die möglichen Auswirkungen einer Beibehaltung des Status quo.**
SCHRITT 2	**Zusammenarbeit mit internen Teams zur Überprüfung der in der NIS2-Richtlinie beschriebenen Maßnahmen zum Management von Cybersicherheitsrisiken. Bestimmen Sie den aktuellen Reifegrad Ihres Unternehmens in Bezug auf jedes Mandat.**

SCHRITT 3	**Denken Sie zuerst an die Reaktion auf einen Vorfall und die dazugehörige Berichterstattung. Haben Sie eine Vereinbarung über einen Response Retainer getroffen? Verfügen Sie über einen vollständig ausgearbeiteten, vereinbarten und geübten Notfallplan? Wissen Sie, was den Prozess der Reaktion auf einen Vorfall auslöst? Verfügt Ihr Unternehmen über einen Business Continuity- und Krisenmanagementplan, der alle Bereiche Ihres Unternehmens umfasst? Sollten Sie eine dieser Fragen verneinen müssen, empfehlen wir eine Zusammenarbeit mit Dragos, um Ihr Incident-Response-Programm vollständig zu entwickeln und in Ihre Prozesse zu integrieren.**
SCHRITT 4	**Bewerten Sie die Sicherheit Ihrer Lieferkette. Erstellen Sie eine Liste aller Assets, die zu Ihrer Umgebung gehören (Die Nutzung von Technologien wie der Dragos Platform kann diesen Prozess erheblich vereinfachen) - jeder dieser Assets-Anbieter ist Teil Ihrer Lieferkette. Welche Softwarelösungen werden in Ihrem Prozess verwendet? Auch dieser Anbieter sind Teil Ihrer Lieferkette. Das Gleiche gilt auch für die Hardware und Software auf Unternehmensebene, da sie mit den Netzwerken Ihrer Werke und anderen Betrieben verbunden ist. Alle diese Anbieter müssen bewertet werden. Dragos kann Fremdzugriffe von Drittanbietern identifizieren, Richtlinien und Kontrollen zur Verwaltung dieser Verbindungen überprüfen und Änderungen an Technologien, Richtlinien und Verfahren empfehlen, um diese Zugänge sicherer zu gestalten.**
SCHRITT 5	**Erstellen Sie eine umfassende Roadmap für die Cybersicherheit von OT-Systemen, die den aktuellen Reifegrad in den wichtigsten Bereichen enthält und zeitgebundene Pläne für Verbesserungen und Optimierungen aufzeigt. Um Fortschritte konsequent messen zu können, empfiehlt es sich, einen langfristigen Ausblick auf die Cyberbereitschaft zu erstellen. Dabei sollten Sie von der Einführung neuer Technologien bis zur Personalentwicklung alle Aspekte berücksichtigen.**

Über Dragos, Inc.

Dragos, Inc. hat es sich zum Ziel gesetzt, die Gesellschaft vor denjenigen zu schützen, die versuchen, die industrielle Infrastruktur zu stören, auf die wir tagtäglich angewiesen sind. Dragos ist ein Privatunternehmen mit Hauptsitz in der Region Washington, D.C., und regionalen Niederlassungen auf der ganzen Welt, darunter in Kanada, Australien, Neuseeland, Europa und Nahost.

Kontaktieren Sie uns heute, um mehr über unser Technologie-, Dienstleistungs- und Threat Intelligence-Angebote zu erfahren oder besuchen Sie **dragos.com**.

Demo Anfrage | Schicken Sie uns eine Email