NIS2-Compliance WatchGuard Technologies

Inhalt

Inhalt

Einführung

Die Zahl der Cyberangriffe ist in den letzten Jahren sprunghaft angestiegen – einigen Schätzungen zufolge seit dem Jahr 2020 um 600 %. Dieser Anstieg ist zum Teil auf die rasche Umstellung auf Remote-Arbeit zurückzuführen, die Schwachstellen in neu digitalisierten Systemen schafft. Außerdem hat sich der Adressatenkreis von Hackerangriffen vergrößert, angefangen von Unternehmen bis hin zu Bildungseinrichtungen, und die Methoden werden immer ausgefeilter.

Dieser alarmierende Trend macht deutlich, wie dringend notwendig solide Cybersicherheitsmaßnahmen sind. Unternehmen und Organisationen müssen in Datenschutz, Mitarbeiterschulungen und aktualisierte Sicherheitssoftware investieren, um Cyberkriminellen einen Schritt voraus zu sein. Der Schutz unserer zunehmend vernetzten Welt erfordert einen proaktiven Ansatz für die Cybersicherheit.

Hintergrund zu NIS

Die 2016 umgesetzte Richtlinie für Netz- und Informationssysteme (EU) 2016/1148 (NIS) war der erste Versuch der Europäischen Union, ein einheitliches Cybersicherheitsgesetz zu schaffen. Ziel war es, ein grundlegendes Sicherheitsniveau für kritische Infrastruktursektoren wie Energie, Verkehr und Finanzen festzulegen. Mit der NIS-Richtlinie wurden die Mitgliedstaaten aufgefordert, Betreiber gesetzlich zu verpflichten, Sicherheitsvorfälle zu melden und Maßnahmen zur Bewältigung von Cybersicherheitsrisiken zu ergreifen.

Allerdings war die Richtlinie in einigen Bereichen unzulänglich. Sie deckte nicht genügend Einrichtungen ab und die Meldepflichten wurden als unzureichend angesehen. Darüber hinaus lag die Durchsetzungsbefugnis bei den einzelnen Mitgliedstaaten, was zu einer uneinheitlichen Umsetzung in der EU führte. Diese Mängel ebneten den Weg für die Einführung der strengeren Richtlinie für Netz- und Informationssysteme (EU) 2022/2555 (NIS 2) im Jahr 2022 (auch als NIS 2 bekannt).

Hintergrund zu NIS2

NIS 2 ist der Nachfolger der ursprünglichen NIS-Richtlinie (die durch NIS2 aufgehoben wurde). Die EU-Mitgliedstaaten müssen die NIS2-Richtlinie, die im Dezember 2022 vom Rat der Europäischen Union und vom Europäischen Parlament verabschiedet wurde, bis zum 17. Oktober 2024 in nationales Recht umsetzen.[1] Sie haben jedoch bis zum 17. April 2025 Zeit, die Liste der Organisationen festzulegen, die die Richtlinie einhalten müssen.

Unterschied zwischen Verordnung und Richtlinie

Eine EU-Verordnung legt direkt geltendes Recht für alle Mitgliedstaaten fest, während eine EU-Richtlinie ein Ziel festlegt, das jeder Mitgliedstaat durch seine nationalen Gesetze erreichen muss (auch als Umsetzung bezeichnet).

Mit der NIS2-Richtlinie werden die Cybersicherheitsvorschriften in der Europäischen Union erheblich verschärft. Die Richtlinie gilt für eine breitere Palette von Sektoren und umfasst kritische Sektoren wie Abfallwirtschaft, Postdienste und Hersteller kritischer Infrastrukturen.

Das Hauptziel der Richtlinie ist die Durchsetzung grundlegender Cybersicherheitsmaßnahmen in diesen Sektoren. Dazu gehören Verfahren zum Risikomanagement, Meldepflichten für Vorfälle und Sicherheitsbewertungen für Lieferketten. Außerdem soll NIS2 die EU-weite Zusammenarbeit bei Cybersicherheitsbedrohungen verbessern. Die Richtlinie sieht die Einrichtung von zuständigen Behörden, Stellen für das Cyber-Krisenmanagement, zentralen Ansprechpartnern für Cybersicherheit und Computer Security Incident Response Teams (CSIRTs) in jedem Mitgliedstaat vor und fördert den Informationsaustausch zwischen diesen Stellen.

NIS-2-Compliance verstehen

Mit der NIS2-Richtlinie werden Einrichtungen basierend auf der Kritikalität ihrer Dienstleistungen in zwei Gruppen unterteilt: „kritisch“ und „wichtig“. Einrichtungen sind in den Anhängen I und II der Richtlinie aufgeführt.

Annex I listet Sektoren auf, die als hochkritisch eingestuft werden. Hier fällt jede große Organisation, die in diesen Sektoren tätig ist, in die Kategorie

Wichtige Einrichtung	Kritische Einrichtung
Mindestens 50 Mitarbeiter	Mindestens 250 Mitarbeiter
Mindestens 10 Mio. Euro Umsatz oder 10 Mio. Euro Jahresbilanz	Mindestens 50 Mio. Euro Umsatz oder 43 Mio. Euro Jahresbilanz

Tabelle 1. Klassifizierungen von Einrichtungen nach Größe

der kritischen Einrichtungen und muss die NIS2 einhalten. Zu diesen Sektoren gehören Energie, Verkehr, Banken, Abwasser und digitale Infrastruktur. Darüber hinaus können mittelständische Unternehmen in diesen Sektoren anhand von Größenschwellenwerten (z. B. Anzahl der Mitarbeiter) als kritisch eingestuft werden.

In Annex II werden andere kritische Sektoren aufgeführt, aber Einrichtungen werden hier als „wichtig“ eingestuft. Dazu gehören Post- und Abfallwirtschaftsdienste, Hersteller kritischer Infrastrukturen und bestimmte öffentliche Verwaltungsbehörden. Anders als bei Anhang I müssen nur große oder mittlere Einrichtungen in diesen Sektoren die NIS2 einhalten.

[1] Die Niederlande kündigten im Januar 2024 an, dass sie den Termin im Oktober nicht einhalten werden, während sie Organisationen auffordern, Maßnahmen zum Schutz der geschäftlichen Kontinuität zu ergreifen.

Annex IAnnex I („wichtig“ UND „kritisch“)	Annex IAnnex II (NUR „wichtig“)
Energiewirtschaft: Strom, Fernwärme und -kälte, Öl, Gas, Wasserstoff	Post und Kurierdienste
Transport: Luftfahrt, Schienenverkehr, Schifffahrt, Straße	Abfallwirtschaft
Bankwesen	Herstellung, Produktion und Vertrieb von Chemikalien
Finanzmarktinfrastrukturen	Herstellung, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheit	Produktion: Medizinische Geräte, Computer/elektronische/optische Produkte, elektrische Ausrüstung, Maschinen, Kraftfahrzeuge, Anhänger, Sattelanhänger
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschung
Digitale Infrastruktur	
Verwaltung von Diensten der Informations- und Kommunikationstechnologie	
Öffentliche Verwaltung	
Raumfahrt	

Tabelle 2. Sektoren und Teilsektoren für jeden Anhang

Multinationale Organisationen, die in der EU tätig sind und kritische Dienste anbieten, müssen die NIS2 einhalten. Sehen Sie in Annex Iund Annex II der Richtlinie nach, ob Ihr Sektor unter kritische oder wichtige Einrichtungen fällt. Vergessen Sie nicht, dass die Compliance-Anforderungen je nach Mitgliedstaat unterschiedlich sein können. Informieren Sie sich daher über die jeweiligen lokalen Vorschriften, die Sie in jedem EU-Land, in dem Sie tätig sind, befolgen müssen.

NIS2-Compliance und Service Provider

In Anhang 1 der NIS2-Richtlinie wird das IKT-Servicemanagement, das Managed Service Provider (MSPs) und Managed Security Service Provider (MSSPs) umfasst, als hochkritischer Sektor eingestuft. Dies bedeutet, dass MSPs und MSSPs unter NIS2 strengeren Cybersicherheitsanforderungen unterliegen.

Diese strengeren Anforderungen sehen vor, dass MSPs/MSSPs geeignete technische, betriebliche und organisatorische Maßnahmen zur Bewältigung von Cybersicherheitsrisiken implementieren müssen. Dazu zählen die Prävention von Vorfällen, die Minimierung von Auswirkungen und die Meldung an Behörden. Angesichts des verstärkten Fokus auf die Sicherheit der Lieferketten müssen darüber hinaus Unternehmen, die in Annex I aufgeführt sind und MSPs/MSSPs einsetzen, möglicherweise die Cybersicherheitspraktiken ihrer Anbieter im Rahmen des Anbieterrisikomanagements bewerten.

Grundlegende Cybersicherheitsmaßnahmen

Die NIS2-Richtlinie schreibt für „kritische“ und „wichtige“ Einrichtungen in verschiedenen Sektoren grundlegende Cybersicherheitsmaßnahmen vor. Im Zentrum dieser Maßnahmen steht ein Risikomanagement-Ansatz, der Unternehmen dazu verpflichtet, regelmäßige Risikobewertungen durchzuführen, technische und organisatorische Sicherheitsvorkehrungen (wie Firewalls und Zugangskontrollen) zu treffen und Verfahren zur Erkennung, Meldung und Reaktion auf Sicherheitsvorfälle einzurichten.

Gemäß der NIS2-Richtlinie müssen die EU-Mitgliedstaaten sicherstellen, dass „kritische“ und „wichtige“ Einrichtungen geeignete Cybersicherheitsmaßnahmen ergreifen. Diese Maßnahmen sollten auf die jeweiligen Risiken der Netz- und Informationssysteme des Unternehmens zugeschnitten sein. Dazu gehören Maßnahmen, um Vorfälle zu verhindern, ihre Auswirkungen auf Serviceempfänger und andere Services zu minimieren und letztendlich ein Sicherheitsniveau aufrechtzuerhalten, das den potenziellen Risiken entspricht.

Faktoren wie technologische Fortschritte, relevante europäische und internationale Sicherheitsstandards und Implementierungskosten sollten bei der Festlegung der geeigneten Maßnahmen berücksichtigt werden. Darüber hinaus sollte die Verhältnismäßigkeit dieser Maßnahmen auf der Grundlage der Größe des Unternehmens, der Wahrscheinlichkeit und Schwere potenzieller Vorfälle (einschließlich gesellschaftlicher und wirtschaftlicher Auswirkungen) und der allgemeinen Gefährdung des Unternehmens durch Cyberbedrohungen bewertet werden. Zu den in der NIS2-Richtlinie beschriebenen grundlegenden Maßnahmen gehören:

- Richtlinien für Risikoanalysen und die Sicherheit von Informationssystemen
- Bewältigung von Vorfällen
- Ein Plan zur Aufrechterhaltung des Betriebs, der Backup-Management, Disaster Recovery und Krisenmanagement umfasst
- Sicherheit der Lieferkette, einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Service Providern
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
- Konzepte und Verfahren für den Einsatz von Kryptografie und ggf. Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen

Die Kernanforderungen der NIS2 folgen für „kritische“ und „wichtige“ Einrichtungen den gleichen Grundsätzen. Aufgrund der Kritikalität ihrer Dienste könnten die Anforderungen an „kritische Einrichtungen“ allerdings detaillierter und strenger sein und die Meldepflichten könnten umfangreicher ausfallen.

Meldepflichten

Mit der NIS2 wurden die Anforderungen an die Meldung von Vorfällen im Vergleich zur vorherigen NIS-Richtlinie verschärft. Diese Anforderungen gelten sowohl für „kritische“ als auch für „wichtige“ Einrichtungen:

- **Frühzeitige Warnung:** Nach der Identifizierung eines signifikanten Vorfalls müssen Einrichtungen der zuständigen Behörde innerhalb von 24 Stunden einen „Frühwarnbericht“ vorlegen. Dieser Bericht sollte eine vorläufige Bewertung der Art des Vorfalls und seiner möglichen Auswirkungen enthalten.
- **Meldung über Vorfall:** Nach der Frühwarnung muss innerhalb von 72 Stunden eine detailliertere Meldung über den Vorfall eingereicht werden. Dieser Bericht sollte Details wie Zeitpunkt und Art des Vorfalls, betroffene Systeme und Daten sowie die ergriffenen Maßnahmen zur Minderung der Auswirkungen enthalten.
- **Abschlussbericht:** Spätestens einen Monat nach der ersten Meldung muss ein Abschlussbericht mit einer umfassenden Analyse des Vorfalls, der Grundursache, der gewonnenen Erkenntnisse und der durchgeführten Korrekturmaßnahmen vorgelegt werden.

Über die Benachrichtigung der zuständigen Behörde in ihrem Mitgliedstaat hinaus können Unternehmen auch verpflichtet werden, andere Mitgliedstaaten, ihre Kunden und die Öffentlichkeit zu informieren.

Für NIS2-Compliance zuständige Behörde

In erster Linie sind die einzelnen EU-Mitgliedstaaten für die Durchsetzung verantwortlich. Jeder Mitgliedstaat benennt eine „zuständige Behörde“, die für die Überwachung der Einhaltung der Vorschriften in seinem Gebiet oder vertikalen Markt zuständig ist. Je nach Struktur des Mitgliedstaats können diese Behörden nationale Cybersicherheitsbehörden, branchenbezogene Regulierungsbehörden oder eine Kombination davon sein. Sie führen Inspektionen durch, untersuchen gemeldete Vorfälle und sind befugt, Sanktionen bei Nichteinhaltung zu verhängen.

Auch wenn die Durchsetzung auf der Ebene der Mitgliedstaaten erfolgt, fördert NIS2 die Zusammenarbeit in der EU. Jeder Mitgliedstaat richtet eine zentrale Anlaufstelle für die Kommunikation mit anderen Behörden ein. Dies erleichtert den Austausch von Informationen über Cyberbedrohungen, Best Practices und koordinierte Reaktionen auf große Cybervorfälle. Darüber hinaus überwacht die Europäische Kommission die allgemeine Umsetzung und Wirksamkeit von NIS2 in der EU. Sie kann Vertragsverletzungsverfahren gegen Mitgliedstaaten einleiten, die die Richtlinie nicht angemessen durchsetzen.

Kritische Einrichtungen	Wichtige Einrichtungen
Inspektionen vor Ort und externe Aufsicht, einschließlich Stichprobenkontrollen durch geschultes Fachpersonal	Inspektionen vor Ort und externe Ex-post-Aufsicht durch geschultes Fachpersonal
Regelmäßige und gezielte Sicherheitsaudits, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden	Gezielte Sicherheitsaudits, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden
Ad-hoc-Audits, auch wenn dies aufgrund eines bedeutenden Vorfalls oder eines Verstoßes gegen diese Richtlinie durch die kritische Einrichtung gerechtfertigt ist	–
Sicherheitsscans auf der Grundlage objektiver, diskriminierungsfreier, fairer und transparenter Risikobewertungskriterien, falls erforderlich in Zusammenarbeit mit der betroffenen Einrichtung	Sicherheitsscans auf der Grundlage objektiver, diskriminierungsfreier, fairer und transparenter Risikobewertungskriterien, falls erforderlich in Zusammenarbeit mit der betroffenen Einrichtung
Anforderungen von Informationen, die zur Bewertung der von der betreffenden Einrichtung ergriffenen Maßnahmen zum Cybersicherheitsrisikomanagement erforderlich sind, einschließlich dokumentierter Cybersicherheitsrichtlinien sowie der Einhaltung der Verpflichtung zur Übermittlung von Informationen an die zuständigen Behörden	Anforderungen von Informationen, die zur Bewertung der von der betreffenden Einrichtung ergriffenen Maßnahmen zum Cybersicherheitsrisikomanagement erforderlich sind, einschließlich dokumentierter Cybersicherheitsrichtlinien sowie der Einhaltung der Verpflichtung zur Übermittlung von Informationen an die zuständigen Behörden
Anforderungen des Zugriffs auf Daten, Dokumente und Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind	Anforderungen des Zugriffs auf Daten, Dokumente und Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind
Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. von Ergebnissen von Sicherheitsprüfungen, die von einem qualifizierten Prüfer durchgeführt wurden, und der entsprechenden zugrunde liegenden Nachweise	Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. von Ergebnissen von Sicherheitsprüfungen, die von einem qualifizierten Prüfer durchgeführt wurden, und der entsprechenden zugrunde liegenden Nachweise

Tabelle 3. Aufsichts- und Durchsetzungsmaßnahmen

Strafen bei Verstößen gegen NIS2

NIS2 verhängt hohe Strafen für die Nichteinhaltung, wobei der Schweregrad von der Klassifizierung des Unternehmens (als „kritisch“ bzw. „wichtig“) und dem Mitgliedstaat, der die Richtlinie durchsetzt, abhängt. Dies sind Höchststrafen und die tatsächlich verhängte Strafe wird von der zuständigen Behörde in jedem EU-Mitgliedstaat auf der Grundlage der Schwere des Verstoßes festgelegt.

Es ist wichtig zu beachten, dass finanzielle Sanktionen nicht die einzige Folge eines Verstoßes sind. Die Nichteinhaltung der Richtlinie kann auch einen erheblichen Imageschaden zur Folge haben. Daher müssen „kritische“ und „wichtige“ Einrichtungen die Richtlinie ernst nehmen und die erforderlichen Cybersicherheitsmaßnahmen ergreifen.

Kritische Einrichtungen	Wichtige Einrichtungen
Geldstrafe, die 10 Mio. Euro oder 2 % des weltweiten Umsatzes der Einrichtung im Vorjahr beträgt, je nachdem, welcher Betrag höher ist	Geldstrafe, die 7 Mio. Euro oder 1,4 % des weltweiten Umsatzes der Einrichtung im Vorjahr beträgt, je nachdem, welcher Betrag höher ist
Offenlegung der Verstöße	Offenlegung der Verstöße
Aussetzung oder Einschränkung des Betriebs	Einschränkung des Betriebs
Haftung der Geschäftsführung bis zur Ebene des CEO	

Tabelle 4. Verwaltungsstrafen

NIS2 und Sicherheits-Frameworks

ISO 27001 ist eine weltweit anerkannte Norm, die die Anforderungen für die Einrichtung, Implementierung, Wartung und kontinuierliche Verbesserung eines Informations- und Sicherheitsmanagementsystems (ISMS) festlegt. Eine ISO 27001-Zertifizierung ist zwar keine Garantie für die Einhaltung der NIS2-Richtlinie, weist jedoch eine hohe Informationssicherheit nach und kann Unternehmen dabei helfen, viele NIS2-Anforderungen zu erfüllen. Unternehmen, die der NIS2 unterliegen, können ISO 27001 als Roadmap zur Erreichung der Compliance nutzen.

WatchGuard hat die ISO/IEC 27001:2013-Zertifizierung für sein ISMS erhalten. Der Umfang der Zertifizierung beschränkt sich auf das ISMS der WatchGuard-Infrastruktur für die Konfiguration, Verwaltung, Unterstützung und Bereitstellung der WatchGuard ID, AuthPoint-Multifaktor-Authentifizierung, Endpoint- und WatchGuard-Cloud-Anwendungen und -Dienste, die Firebox-Firewalls und WLAN in der WatchGuard Cloud unterstützen.

Neben ISO 27001 untersuchen die EU-Mitgliedstaaten andere Frameworks wie NIST CSF und CIS Controls. Es wird erwartet, dass die Umsetzung dieser Frameworks als ausreichender Nachweis dafür angesehen wird, dass geeignete Sicherheitsmaßnahmen ergriffen wurden. Auch hier ist es wichtig, die lokalen Vorschriften für die EU-Mitgliedstaaten, in denen Sie tätig sind, zu prüfen.

So unterstützt WatchGuard Technologies NIS2-Compliance

Die Unified Security Platform von WatchGuard kann die Einhaltung der NIS2-Vorschriften optimieren, indem sie eine einzige Plattform für die Verwaltung verschiedener Sicherheitsdienste bietet, einschließlich Intrusion Prevention, Endpoint Protection und Multifaktor-Authentifizierung. Diese Konsolidierung vereinfacht die Berichterstattung, Bedrohungserkennung und die allgemeine Sicherheitslage und erleichtert es Unternehmen, die strengen Cybersicherheitsanforderungen der Richtlinie zu erfüllen.

Anforderungen der NIS2-Richtlinie	WatchGuard-Lösung	So wird die Anforderung erfüllt
Richtlinien für Risikoanalysen und die Sicherheit von Informations-systemen	Unified Security Platform® von WatchGuard	WatchGuard empfiehlt die Implementierung eines Systems oder Rahmens für Informations- und Sicherheitsmanagement wie ISO27001 oder CIS Critical Security Controls, um die Cybersicherheit eines Unternehmens bestmöglich zu verwalten. In unserer Unified Security Platform bieten wir Produkte, die die Implementierung von Kontrollen und die Bewältigung von Cybersicherheitsrisikobereichen erleichtern.
	ThreatSync (XDR) von WatchGuard	ThreatSync nutzt eine zentrale Plattform, um Cyberbedrohungen im gesamten WatchGuard-Netzwerk und in den Endpoint-Sicherheitsprodukten aufzudecken, zu priorisieren und schnell darauf zu reagieren.

Anforderungen der NIS2-Richtlinie	WatchGuard-Lösung	So wird die Anforderung erfüllt
Richtlinien für Risikoanalysen und die Sicherheit von Informations-systemen	WatchGuard ThreatSync+ NDR	ThreatSync+ NDR hilft bei der Risikoanalyse, indem es detaillierte Einblicke in die Schwachstellen und potenziellen Bedrohungen Ihres Netzwerks bietet. Sie können Sicherheitsmaßnahmen priorisieren, indem Sie die Angriffsfläche Ihres Netzwerks verstehen und Bereiche mit hohem Risiko identifizieren. Die NDR-Lösung umfasst zudem ISO 27001- und NIST CSF-Sicherheitsrichtlinien, die die Risikoanalyse unterstützen. Die Lösung generiert umfassende Berichte, die als Grundlage für Verbesserungen der Informationssystem-Sicherheitsrichtlinien Ihrer Organisation verwendet werden können. Dieser datengesteuerte Ansatz stellt sicher, dass Ihre Richtlinien mit aktuellen Bedrohungen und regulatorischen Anforderungen übereinstimmen.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	Das Risiko-Dashboard in EPP, EDR, EPDR und Advanced EPDR zeigt die Sicherheitsrisikostufe an, die Computern in Ihrem Netzwerk zugewiesen wurde. Der Software- und Hardwarebestand liefert Informationen zu nicht autorisierter Software und Versionen, die an den Endpoints installiert sind. Device Control regelt das Verhalten, wenn Wechsel- oder Massenspeichergeräte mit den Endpoints verbunden sind, und autorisiert oder blockiert diese. Advanced EPDR ermöglicht es Ihnen, die Ausführung von Systemanwendungen, die normalerweise von Bedrohungen verwendet werden, wie PowerShell, der Linux-Shell und der Windows-CMD-Shell zu überwachen oder zu verweigern. WatchGuard Clouds Endpoint Manager und WatchGuard Endpoint Security-Plug-Ins und -Integrationen für beliebte RMM-Anwendungen (ConnectWise, Kaseya, N-able, NinjaOne usw.) ermöglichen es Partnern, die Sicherheitsrichtlinien mehrerer Kundenkonten zu verwalten.
	WatchGuard Patch Management	Ermöglicht die Einrichtung von Richtlinien für das Schwachstellenmanagement und die Durchführung automatisierter Schwachstellenscans
	WatchGuard Full Encryption	Ermöglicht die Einrichtung von Datenschutzrichtlinien durch vollständige Festplattenverschlüsselung
	WatchGuard Advanced Reporting Tool	Das Application Control-Dashboard zeigt Details zu Anwendungen an, die im Netzwerk installiert und ausgeführt werden, einschließlich legitimer Software, die möglicherweise böswillig verwendet wird. Es hilft, unerwünschte, nicht autorisierte, nicht lizenzierte oder anfällige Anwendungen und solche zu identifizieren, die übermäßige Bandbreite verbrauchen oder für Skripte, Fernzugriff oder Systemtools verwendet werden. Auf der Registerkarte für anfällige Anwendungen werden vernetzte Anwendungen mit bekannten Schwachstellen hervorgehoben. Auf der Registerkarte Anwendungen mit hohem Bandbreitenverbrauch werden Programme mit hohem Datentransfervolumen aufgeführt. Das Monitoring von skriptbasierten Anwendungen wie PowerShell, Linux-Shell, Windows-CMD-Shell, Remotezugriffs-Anwendungen oder unerwünschten kostenlosen Anwendungen ist wichtig, um deren Nutzungsmuster zu verstehen und potenzielle Bedrohungen zu mindern.

Anforderungen der NIS2-Richtlinie	WatchGuard-Lösung	So wird die Anforderung erfüllt
Richtlinien für Risikoanalysen und die Sicherheit von Informations-systemen	WatchGuard MDR	Wöchentliche Berichte zum Sicherheitsstatus enthalten wichtige Informationen zum Endpoint-Risiko basierend auf Schutzstatus und -konfiguration, Erkennungen und Sicherheitspatches, die noch nicht installiert wurden. Im Rahmen des Service-Onboarding bewertet das WatchGuard MDR-Team die Angriffsfläche an den Endpoints, um die Sicherheit zu erhöhen und die allgemeine Resilienz gegenüber Cyberbedrohungen sofort zu verbessern.
Bewältigung von Vorfällen, einschließlich Prävention, Erkennung, Reaktion, Wiederherstellung und Meldung	Firebox von WatchGuard	Fireboxes überwachen kontinuierlich Bedrohungen, die von böswilligen Personen oder einfach nur von Mitarbeitern verursacht werden können, die versehentlich auf einen Weblink klicken. Die Sicherheitsdienste können Bedrohungen erkennen, automatische Abhilfemaßnahmen implementieren und die Vorfallsdaten an ThreatSync senden, um den Vorfall auf der gesamten WatchGuard-Plattform zu korrelieren.
	ThreatSync (XDR) von WatchGuard	ThreatSync bietet eine konsolidierte Ansicht aller Erkennungen im gesamten WatchGuard-Portfolio in einem einzigen Sicherheitsbetriebssystem, mit dem Incident Responder den gesamten Vorfallsreaktionszyklus in einem einzigen Fenster bearbeiten und sich wiederholende Abhilfemaßnahmen automatisieren können.
	WatchGuard ThreatSync+ NDR	ThreatSync+ NDR nutzt eine fortschrittliche KI-Engine, um potenzielle Angriffe auf Bedrohungsoberflächen Ihres Netzwerks zu erkennen und darauf zu reagieren. Die Lösung hilft Ihnen, Sicherheitsvorfälle von Anfang bis Ende zu verwalten. Wenn ein Angriff innerhalb der Netzwerkumgebung auftritt, wird er schnell erkannt und ermöglicht eine sofortige und effektive Reaktion, um Schäden vorzubeugen. Und schließlich stellt es detaillierte Vorfallsberichte bereit und hilft Ihnen so, Ihre Sicherheit für die Zukunft zu verbessern.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	Integrieren Sie innovative Technologien wie Anti-Exploit im Speicher, kontextbezogene Erkennungen, Erkennung von bösartigem Datenverkehr und Managed Services (Zero-Trust Application Services und der Threat Hunting Service), um die Prävention, Erkennung und Behebung von Bedrohungen über alle Endpoints hinweg zu automatisieren. Der Zero-Trust Application Service ist ein einzigartiger automatisierter Managed Security Service, der 100 % der laufenden Prozesse auf Endpoints klassifiziert und sicherstellt, dass nur sichere Anwendungen ausgeführt werden. Er nutzt KI/maschinelles Lernen und Deep Learning, um die automatische Klassifizierung unbekannter Prozesse zu verbessern. Endpoint Access Enforcement (EAE) verweigert eingehende Verbindungen zu Endpoints von ungeschützten Endpoints.
	WatchGuard Patch Management	Automatisiert das Patch-Management für das Betriebssystem und Anwendungen. Es deckt den gesamten Patch-Management-Zyklus ab, einschließlich der automatischen Suche nach verfügbaren Patches, Behebung und Überwachung.

Anforderungen der NIS2-Richtlinie	WatchGuard-Lösung	So wird die Anforderung erfüllt
Bewältigung von Vorfällen, einschließlich Prävention, Erkennung, Reaktion, Wiederherstellung und Meldung	WatchGuard Full Encryption	Verhindert durch Festplattenverschlüsselung, dass unbefugte Anwender auf vertrauliche Daten zugreifen.
	WatchGuard Advanced Reporting Tool	Das WatchGuard Advanced Reporting Tool bietet 365-Tage-Telemetrie mit Transparenz darüber, was auf den Maschinen von welchen Anwendern und über welche Verbindungen ausgeführt wird. Es ermöglicht die Identifizierung ungewöhnlicher und nicht richtlinienkonformer Ausführungen und Verhaltensweisen.
	WatchGuard MDR	Ein qualifiziertes WatchGuard-Team aus Cyber-Sicherheitsexperten schützt die Endpoints von Kunden rund um die Uhr mit Sicherheitsüberwachung, Threat Hunting, Angriffsabwehr, -erkennung und -eindämmung. WatchGuard MDR liefert automatisch regelmäßige Dienstaktivitäts- und Sicherheitsstatusberichte, die dazu beitragen, die Angriffsfläche an den Endpoints und in Office 365 zu reduzieren. Im Falle eines Cyberangriffs benachrichtigt das Team WatchGuard Partner unverzüglich und stellt auch einen Vorfallsbericht, sowie Konzepte für den Eindämmungs- und Behebungsprozess zur Verfügung, um Bedrohungen sofort zu stoppen und zu beheben. Die Eindämmung kann an das MDR delegiert werden, das betroffene Endpoints automatisch über Ablaufpläne isoliert.
	WatchGuard Orion	Es ermöglicht Service Providern, Indikatoren für Angriffe und Kompromittierung zu erkennen, zu priorisieren und zu untersuchen, indem Sicherheitsanalysen automatisch auf die angereicherte 365-Tage-Telemetriedaten angewendet werden, die aus der Überwachung der Endpoint-Aktivitäten gesammelt wurden, und diese Taktiken und Techniken des Mitre ATT&CK-Frameworks zuordnet. Das Störfallmanagement erleichtert die Zusammenarbeit zwischen Analysten, Respondern und Huntern bei der Untersuchung und Korrelation verdächtiger Aktivitäten im Zusammenhang mit Bedrohungen, die von anderen Kontrollen übersehen wurden. Die Eindämmungs- und Behebungstools wie Endpoint-Isolation, Neustart, Prozess- und Service-Management, Dateiübertragung und Befehlszeilenoperationen durch Fernzugriff auf Endpoints ermöglichen eine schnelle Reaktion auf und Wiederherstellung von Bedrohungen an den Endpoints. Orion APIs erleichtern die Integration mit anderen Systemen für einen optimierten Betrieb.
	WatchGuard Data Control	Mit WatchGuard Data Control wissen Sie Bescheid, ob auf kompromittierten Endpoints gehostete Dateien personenbezogene Daten oder kritische Geschäftsinformationen enthalten.

Anforderungen der NIS2-Richtlinie	WatchGuard-Lösung	So wird die Anforderung erfüllt
Ein Plan zur Aufrechterhaltung des Betriebs, der Backup-Management, Disaster Recovery und Krisenmanagement umfasst	WatchGuard Cloud	WatchGuard Cloud ermöglicht Backups kritischer Sicherheitsinfrastrukturkonfigurationen wie von Fireboxes und WatchGuard Access Points. Durch Integrationen mit Remote-Monitoring- und Management-Tools können Endpoints schnell isoliert, bereinigt und ggf. neu bereitgestellt werden.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	Schattenkopien können alle 24 Stunden erstellt werden, um ein kompromittiertes System wieder in seinen vorherigen Zustand zu versetzen. Mit der Advanced EPDR (R16) Forensic and Investigation Console können Sie die betroffenen Assets für die Wiederherstellungs- und Benachrichtigungsphasen ermitteln.
	WatchGuard Patch Management	Die enge Integration des Patch-Managements in die gleiche Management-Konsole ermöglicht die Korrelation von Bedrohungserkennungen mit Endpoint-Schwachstellen. Dies ermögicht ein sofortiges Patchen, um die Ausnutzung zu verhindern und die Ausbreitung von Bedrohungen über Endpoints hinweg zu mindern.
	WatchGuard MDR	Ermöglicht Business Continuity Management mit 24/7-Erkennung und Zusammenarbeit mit unseren MSPs bei der Reaktion auf Sicherheitsvorfälle über Endpoints und Microsoft 365 hinweg und nutzt ein erfahrenes Cybersicherheitsteam, KI und fortschrittliche Technologien von WatchGuard SOC.
	WatchGuard Orion	Ermöglicht Ihnen, verdächtige Aktivitäten automatisch zu identifizieren, Indikatoren für Angriffe zu priorisieren und durch angereicherte 365-Tage-Telemetriedaten schnell nach potenziellen Bedrohungen auf Ihren Endpoints und Servern zu suchen. Mit der Forensic and Investigation Console und dem Incident Case Management können Analysten die betroffenen Assets, die Ursache der Sicherheitsverletzung und die verwendeten TTPs untersuchen. Diese kritischen Informationen helfen bei der Wiederherstellung, bei Entscheidungen zur Verbesserung der Sicherheitslage und in Benachrichtigungsphasen.
Sicherheit der Lieferkette, einschließlich sicherheits-bezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Service Providern	WatchGuard Cloud	Mit WatchGuard Cloud können Sie Executive Summarys und Konfigurationsberichte erstellen, mit denen Sie auf Anfrage Sicherheitskontrollen für Auditoren und andere Einrichtungen in der Lieferkette dokumentieren können.
	WatchGuard ThreatSync+ NDR	Digitale Lieferketten hängen von vernetzten Netzwerken und der Kommunikation zwischen Lieferkettenpartnern ab. ThreatSync+ NDR überwacht ständig die Netzwerkkommunikation innerhalb und über Netzwerkgrenzen hinweg, identifiziert und meldet Risiken und Schwachstellen und hält gleichzeitig nach potenziellen Bedrohungen Ausschau. Die Lösung bietet Risikoberichte für Lieferketten, die externe Risikoprüfer verwenden können, um die Cybersicherheitspraktiken jedes Mitglieds zu bewerten.

Anforderungen der NIS2-Richtlinie	WatchGuard-Lösung	So wird die Anforderung erfüllt
Sicherheit der Lieferkette, einschließlich sicherheits-bezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Service Providern	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	WatchGuard Endpoint Security geht über herkömmliche Antivirenprogramme hinaus und bietet eine umfassende Erkennung, Anti-Exploit und Verhaltensüberwachung, um versteckte Bedrohungen, auch von Drittanbietern, zu stoppen. Der Zero-Trust Application Service und der Threat Hunting Service stärken die Abwehr fortgeschrittener Angriffe weiter.
	WatchGuard MDR	WatchGuard SOC Threat Hunter und Analysten arbeiten rund um die Uhr daran, potenzielle Bedrohungen und Vorfälle in der Lieferkette proaktiv zu suchen, zu validieren und zu untersuchen, abnormes Anwendungsverhalten zu korrelieren und Richtlinien für die Reaktion für unsere Partner bereitzustellen.
	WatchGuard Orion	Es ermöglicht Service Providern, ihre eigenen Hunting-Regeln zu erstellen, proaktiv nach potenziellen Bedrohungen und Vorfällen in der Lieferkette zu suchen, diese zu validieren und zu untersuchen.
Sicherheits-maßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informations-systemen, einschließlich Management und Offenlegung von Schwachstellen	Firebox von WatchGuard	Die Firebox von WatchGuard bietet mehrschichtigen Netzwerkschutz, vereinfachte Updates mit WatchGuard Cloud, verschlüsseltes Management mit Multifaktor-Authentifizierung (MFA), sicheren Fernzugriff mit MFA und Network Access Enforcement (NAE) über Firebox VPN sowie Intrusion Detection/Prevention (IDS/IPS) mit Traffic-Segmentierungsfunktionen.
	ThreatSync (XDR) von WatchGuard	ThreatSync von WatchGuard ist ein Cloud-basierter Dienst, der Daten von Ihren WatchGuard-Netzwerkgeräten und Endpoint-Sicherheitsprodukten analysiert. Durch die Kombination dieser Informationen werden potenzielle Sicherheitsbedrohungen in Ihrem gesamten Netzwerk erkannt und priorisiert, sodass Sie schneller und effektiver darauf reagieren können.
	WatchGuard ThreatSync+ NDR	Die ThreatSync+ NDR-Lösung stärkt die Sicherheit von Netzwerk- und Informationssystemen, indem sie erweiterte Funktionen zur Erkennung und Abwehr von Bedrohungen bereitstellt, einschließlich der Erkennung und Reaktion auf Schwachstellen. Sie nutzt KI und maschinelles Lernen, um netzwerkbasierte Bedrohungen zu identifizieren und zu bekämpfen, das Risiko von Sicherheitsverstöße zu reduzieren und die Auswirkungen von Vorfällen zu minimieren. Dies hilft Organisationen dabei, die Sicherheit ihrer Systeme und Daten während ihres gesamten Lebenszyklus zu gewährleisten.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	WatchGuard Endpoint Security-Lösungen stoppen fortgeschrittene Cyberangriffe auf Informationssysteme.

Anforderungen der NIS2-Richtlinie	WatchGuard-Lösung	So wird die Anforderung erfüllt
Sicherheits-maßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informations-systemen, einschließlich Management und Offenlegung von Schwachstellen	WatchGuard Patch Management	WatchGuard Endpoint-Produkte können verwendet werden, um Schwachstellen und EOL-Software zu entdecken. Das Patch-Management-Modul reduziert Cybersicherheitsrisiken, indem es die Funktionen für den gesamten Patch-Management-Zyklus bereitstellt. Es ermöglicht Administratoren, bedarfsgesteuerte und geplante Aufgaben zu erstellen, um Patches an verwaltete Geräte zu übertragen. Der Patch-Katalog wird aktualisiert, wenn neue Schwachstellen entdeckt und angekündigt werden.
	WatchGuard MDR	Der Managed Detection and Response (MDR)-Dienst überwacht Informationssysteme von einem 24x7 Security Operations Center (SOC) aus, das von Cybersicherheitsexperten betrieben wird. Wöchentliche Berichte zum Sicherheitsstatus enthalten wichtige Informationen zum Endpoint-Risiko basierend auf Schutzstatus und -konfiguration, Erkennungen und Sicherheitspatches, die noch nicht installiert wurden.
Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagement-maßnahmen im Bereich der Cybersicherheit	WatchGuard Cloud	WatchGuard Cloud bietet umfassende Transparenz und Berichterstattung über Abweichungen in der Konfiguration der Cybersicherheitsprodukte. Beispiel: Ein Richtlinienverwendungsbericht für die Firewall, der nicht verwendete Richtlinien anzeigt.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	Alle WatchGuard Endpoint Security-Produkte ermöglichen es Ihnen, Konfigurationen und Richtlinien festzulegen, um die Angriffsfläche zu reduzieren. Die Dashboards überwachen Sicherheitsrisiken am Endpoint, Erkennungen und andere kritische Aspekte vor und nach der Anwendung von Maßnahmen des Sicherheitsrisikomanagements und ermöglichen die Bewertung ihrer Wirksamkeit.
Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit	WatchGuard Patch Management	Patch-Management-Dashboards überwachen Sicherheitslücken mit einem anzuwendenden Patch und bewerten die Patch-Management-Richtlinien und -Verfahren.

Anforderungen der NIS2-Richtlinie	WatchGuard-Lösung	So wird die Anforderung erfüllt
Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	Alle WatchGuard Endpoints Security-Lösungen umfassen Technologien und Richtlinien zur Reduzierung der Angriffsfläche an den Endpoints, wie z. B. die Erkennung von und Benachrichtigung über nicht verwaltete Endpoints, Schutzprobleme, nicht verbundene Endpoints an der Cloud-Management-Konsole, Anti-Tampering-Technologien und viele andere Mechanismen, die die Anwendung grundlegender Verfahren zur Cyberhygiene erleichtern.
	WatchGuard Patch Management	WatchGuard Patch Management ermöglicht die Identifizierung ausstehender Sicherheitspatches zur Behebung von Schwachstellen und die Identifizierung von an den Endpoints installierter EOL-Software, wodurch einige der grundlegendsten Verfahren zur Cyberhygiene unterstützt werden.
	WatchGuard Full Encryption	WatchGuard Full Encryption erleichtert die Verwaltung der Datenverschlüsselung im Ruhezustand als grundlegende Maßnahme für den Datenschutz.
	WatchGuard Advanced Reporting Tool	Das WatchGuard Advanced Reporting Tool hilft dabei, den Missbrauch von Anwendungen zu erkennen, einschließlich unproduktiver, sehr bandbreitenintensiver und Living-of-Land (LotL)-Techniken, Anwender, die an der Ausführung und Enthüllung von Verbindungen zu nicht gewünschten Ländern beteiligt sind, und ermöglicht so IT-Hygiene. Um dies zu kontrollieren, können Verfahren zur IT-Hygiene implementiert werden.
	WatchGuard MDR	Wöchentliche Zustandsberichte decken gefährdete Endpoints auf und empfehlen die Implementierung von Verfahren zur Cyberhygiene.
	DNSWatch	Obwohl WatchGuard keine Schulungssuite für Cybersicherheit anbietet, zeigt das DNSWatch-Produkt Anwendern im Browser ein Phishing-Schulungsvideo an, wenn es einen Phishing-Versuch blockiert.

Anforderungen der NIS2-Richtlinie	WatchGuard-Lösung	So wird die Anforderung erfüllt
Konzepte und Verfahren für den Einsatz von Kryptografie und ggf. Verschlüsselung	Firebox von WatchGuard	Die Fireboxes von WatchGuard ermöglichen Administratoren Flexibilität bei der Erstellung von Richtlinien, um die sicherste Bereitstellung mit umfassender Transparenz von Netzwerkereignissen zu ermöglichen. Zusammen mit den Sicherheitsrichtlinien bietet die Firebox die neuesten FIPS-Verschlüsselungsmethoden für Datenverkehr, der während der Übertragung verschlüsselt werden muss. Fireboxes mit IKEv2 Pre-Logon mit VPN-Unterstützung, kombiniert mit MFA.
	WatchGuard Cloud	Die gesamte Verwaltung der Produkte von WatchGuard Cloud erfolgt über eine sichere, verschlüsselte Kommunikation.
	WatchGuard Full Encryption	WatchGuard Full Encryption verhindert unbefugten Zugriff und Datensicherheitsverletzungen, indem es eine vollständige Festplattenverschlüsselung für Windows- und macOS-Geräte bereitstellt. Alle Wiederherstellungsschlüssel werden auf unserer Cloud-basierten Plattform sicher gespeichert.
	WatchGuard MDR	WatchGuard SOC-Analysten überwachen die Nutzung der Verschlüsselungsbibliothek, um Versuche von Ransomware-Cyberangriffen so schnell wie möglich zu erkennen.
	WatchGuard Orion	WatchGuard Orion überwacht, wenn potenzielle Bedrohungsakteure Verschlüsselungsbibliotheken aufrufen, ordnet diese Aktivität entsprechenden Mitre& ATT CK-Techniken zu und informiert Sicherheitsanalysten. So können sie untersuchen, ob die verdächtige Aktivität mit Ransomware oder einem anderen potenziellen Cyberangriff zusammenhängt.
Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen	WatchGuard Cloud	WatchGuard Cloud vereinfacht die Bestandsverwaltung durch eine zentrale Konsole zur Verfolgung und Verwaltung aller Ihrer WatchGuard-Geräte, einschließlich Firewalls, Endpoints und Access Points. So erhalten Sie einen klaren Überblick über Ihre Netzwerksicherheit, sodass Sie Lizenzen effizient zuweisen und auf Bedrohungen reagieren können.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	Für das Bestandsmanagement bieten die WatchGuard Endpoint Security-Lösungen eine Inventarisierungsfunktion für Hardware über alle verwalteten Geräte hinweg und mit Details pro Gerät: CPU, RAM, Speicher, TPM, BIOS-Informationen, Systemtyp, virtuell oder physisch, Betriebssystemdetails, private und öffentliche IP und MAC-Adressen. Der gerätespezifische Softwarebestand enthält Angaben wie Name, Herausgeber, Version usw. Die Network Access Enforcement (NAE)-Funktion für WatchGuard-Fireboxes und WLAN-Zugriffspunkte stellt sicher, dass nur geschützte Endpoints eine Verbindung zum Netzwerk herstellen können. Diese Funktion blockiert den Netzwerkzugriff von Geräten, auf denen keine WatchGuard Endpoint Security Solutions mit der entsprechenden Konfiguration ausgeführt werden.

Tabelle 5. WatchGuard-Lösungen für NIS2

Anforderungen der NIS2-Richtlinie	WatchGuard-Lösung	So wird die Anforderung erfüllt
Multifaktor-Authentifizierung oder kontinuierliche Authentifizierungs-lösungen, gesicherte Sprach-, Video- und Textkommunikation sowie gesicherte Notfall-kommunikations-systeme innerhalb des Unternehmens, falls zutreffend.	AuthPoint von WatchGuard	WatchGuard AuthPoint bietet Multifaktor-Authentifizierung (MFA) für ein großes Ökosystem von Drittanbieteranwendungen. Anwender können sich direkt von ihrem eigenen Mobiltelefon oder mit einem optionalen Hardware-Token authentifizieren. AuthPoint unterstützt Push-Benachrichtigungen, QR-Code-Frage und -Antwort sowie OTP (Einmalpasswort) als zweiten Faktor. Das mobile Token ist an das vom Anwender verwendete Mobiltelefon gebunden und kann nicht auf ein anderes Telefon kopiert oder geklont werden. MFA kann für den VPN-Zugriff konfiguriert werden, indem AuthPoint einfach in WatchGuard Cloud integriert wird. AuthPoint MFA erstreckt sich über RESTful-APIs auf benutzerdefinierte Anwendungen. AuthPoint bietet auch eine Benutzerübernahme, um die Zugriffskontrolle für Service Provider zu vereinfachen, indem es ihnen ermöglicht, den Ressourcenzugriff bei Ausscheiden von Mitarbeitern des Service Providers einfach zu widerrufen.
	Firebox von WatchGuard	Die Fireboxes von WatchGuard bieten viele Optionen, um sichere verschlüsselte VPN-Tunnel zwischen Standorten oder VPN-Zugriff von Remote-Anwendern (mobilen Anwendern) auf Unternehmensdaten zu konfigurieren, wobei die neuesten Standards der IKEv2-Kryptographie verwendet werden.

Fazit

Auch wenn die Grundzüge der NIS2 in der gesamten EU einheitlich sind, erfordert die Einhaltung der Vorschriften Flexibilität, da die jeweiligen Mitgliedstaaten die Richtlinien selbst umsetzen müssen. WatchGuard Technologies ist weiterhin bestrebt, mit diesen sich verändernden Vorschriften Schritt zu halten. Wir werden weiterhin informative Ressourcen zur Verfügung stellen und sicherstellen, dass sich unsere Sicherheitslösungen an die sich ständig verändernde NIS2-Landschaft anpassen, sodass Ihr Unternehmen die Compliance zuverlässig steuern kann.

Referenzlinks

- NIS2-Richtlinie 2022/2555(wählen Sie Ihre Sprache in HTML oder PDF)
- Europäische Kommission: Seite zur NIS2-Richtlinie
- Leitlinien der Europäischen Kommission – Anwendung der NIS2-Richtlinie Artikel 4 Absätze 1 und 2
- Leitlinien der Europäischen Kommission – Anwendung der NIS2-Richtlinie Artikel 3 Absatz 4
- Agentur der Europäischen Union für Cybersicherheit (ENISA): Seite zur NIS-Richtlinie
- Weitere Informationen zu WatchGuard-Produkten

Informationen zu WatchGuard

WatchGuard® Technologies, Inc. gehört zu den führenden Anbietern im Bereich Cyber-Sicherheit. Unsere Unified Security Platform® ist speziell auf Managed Service Provider ausgelegt, damit sie erstklassige Sicherheit bieten können, die die Skalierbarkeit und Schnelligkeit ihres Unternehmens erhöht und gleichzeitig die betriebliche Effizienz verbessert. Über 17.000 Vertriebspartner und Dienstleister im Bereich Sicherheit verlassen sich auf die prämierten Produkte und Services des Unternehmens, die die Bereiche Netzwerksicherheit und -informationen, fortschrittlicher Endpoint-Schutz, Multifaktor-Authentifizierung sowie sicheres WLAN umfassen, und sorgen somit für den Schutz von mehr als 250.000 Kunden. Gemeinsam bieten diese Bereiche die fünf entscheidenden Elemente einer Sicherheitsplattform: umfassende Sicherheit, kollektive Intelligenz, Transparenz und Kontrolle, operative Ausrichtung und Automatisierung. Neben der Zentrale in Seattle im US-Bundesstaat Washington unterhält das Unternehmen Niederlassungen in Nordamerika, Lateinamerika und Europa sowie im asiatisch-pazifischen Raum. Weitere Informationen finden Sie unter WatchGuard.de.