Webinar | 17.06.2024

Strategien und Lösungen für Systemhäuser und MSPs

Effiziente NIS-2-Compliance mit WatchGuard und ADN

adn.de

Unsere Speaker

Achim Kadar

Focus Sales Manager Security
ADN Distribution

Michael Haas

Regional Vice President,
Central Europe
WatchGuard Technologies

Agenda

1 Prognosen zu Cybercrime und die Bedeutung von IT-Security

2 Herausforderungen im Jahr 2024 & Aktuelle Bedrohungslage im Cyberraum

3 ADN NIS2-Lösungsportfolio

4 Hintergrund und Verständnis der NIS2-Richtlinien und Meldepflichten

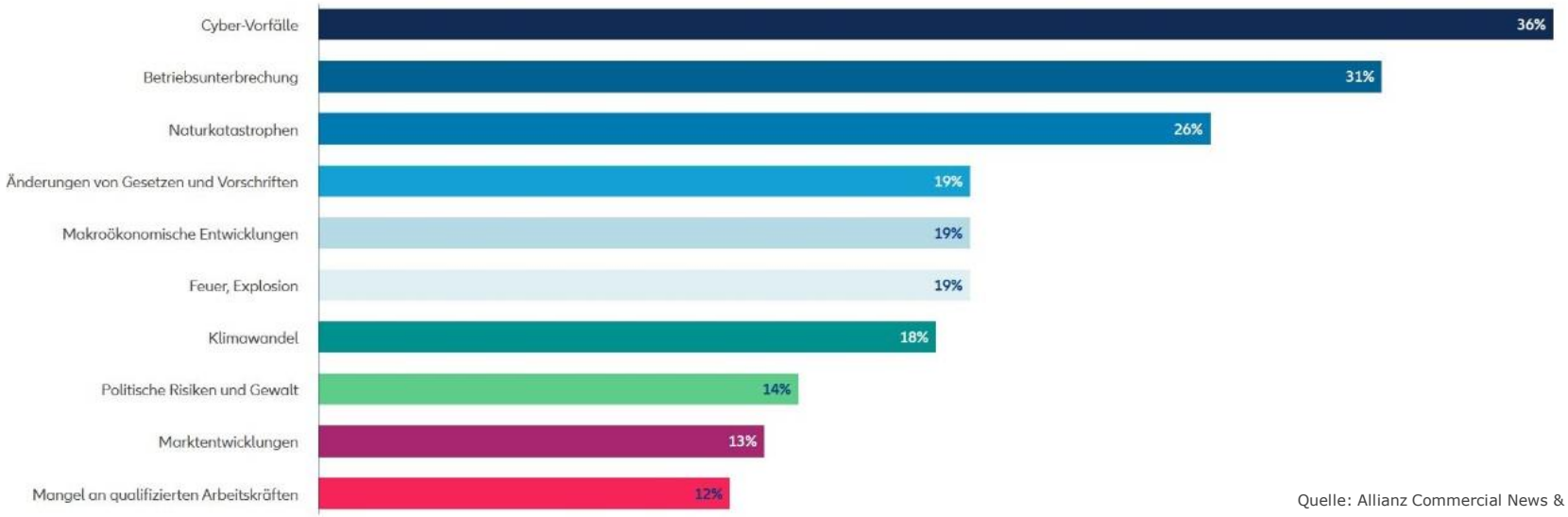
5 Wie WatchGuard Technologies die Einhaltung von NIS 2 auf EINER Plattform unterstützt

Allianz

Top 10 Geschäftsrisiken weltweit in 2024

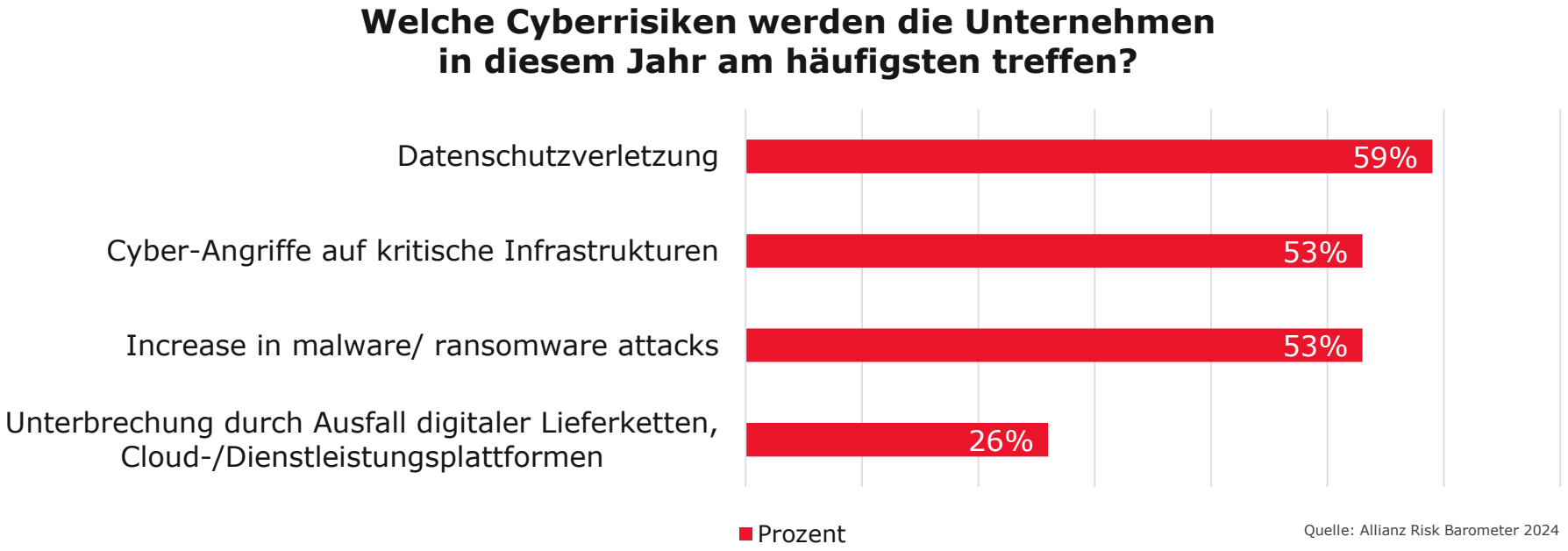
Allianz Risk Barometer 2024

Basierend auf den Antworten von 3,069 Risikomanagement-Experten aus 92 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



Quelle: Allianz Commercial News & Insight

Prognose



Quelle: Allianz Risk Barometer 2024

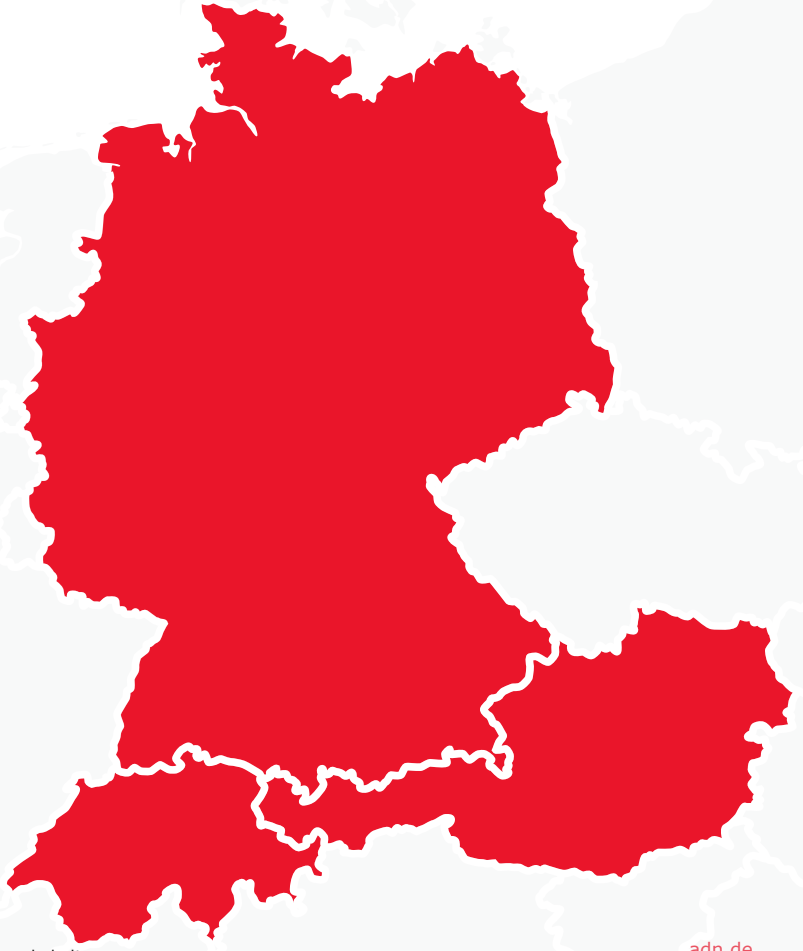
Unsere Herausforderungen 2024

Unsere Lage der IT-Sicherheit in Deutschland

Cyberangriffe auf Unternehmen

MALWARE

Die Anzahl neuer Schadprogramm-Varianten hat in einem Jahr um rund 116,6 Millionen Zugenommen.



Quelle: BSI – Bundesamt für Sicherheit in der Informationstechnik
bsi.bund.de

Unsere Lage der IT-Sicherheit in Deutschland

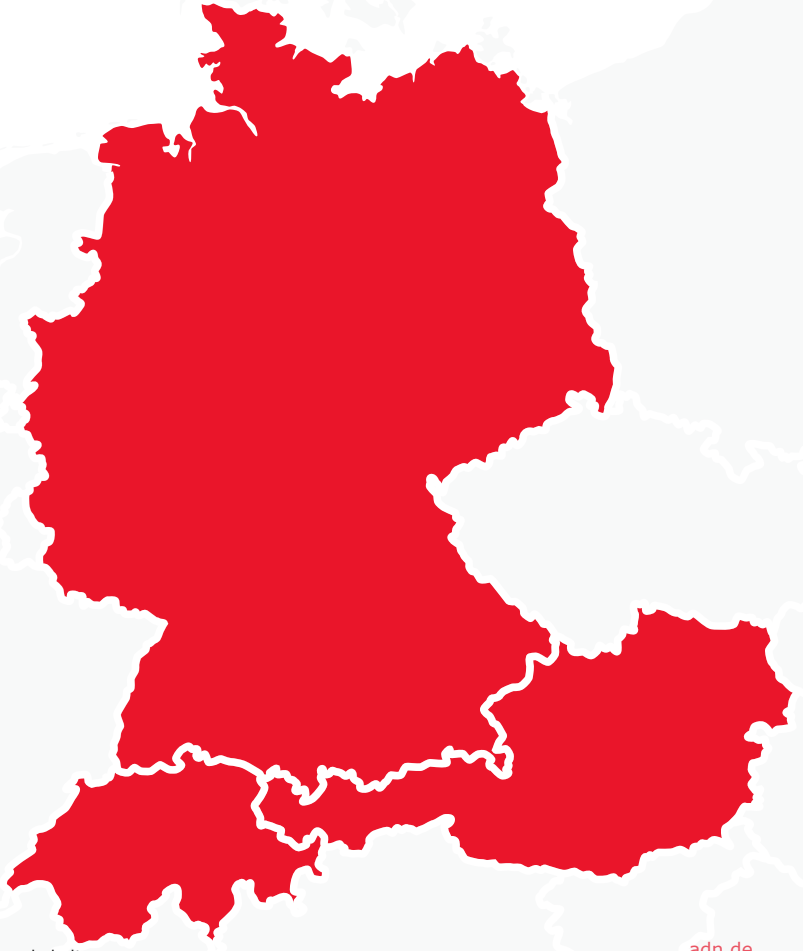
Cyberangriffe auf Unternehmen

RANSOMWARE

ist weiterhin die größte Bedrohung.

Schlimmste Folge:

Hoher Leidensdruck beim geschädigten Unternehmen durch direkte Auswirkung im Betrieb.



Quelle: BSI – Bundesamt für Sicherheit in der Informationstechnik
bsi.bund.de

Unsere Lage der IT-Sicherheit in Deutschland

Wie sieht die Cybersecurity im KMU-Markt aus?

- „Mein Unternehmen ist für Angreifer doch uninteressant."
- Mein Router hat schon Sicherheitsfunktionen integriert, das reicht!"
- „Das Budget möchte ich an dieser Stelle nicht aufbringen."
- „Dafür habe ich keine Mitarbeiter."
- „Dafür finde ich keine Mitarbeiter."

Deutscher Traditionshersteller ist insolvent: Hacker-Angriff war der Grund

12.01.2023 06:19 | Von: TOBIAS STADLER

Bedrohungslage

Umfassende IT-Security Lösungen

ADN Lösungsportfolio

Endpoint Security	**Network Security / Firewalls**	**Identity Security & Management**	**E-Mail Security**
Information Protection (Data Loss Prevention)	**Schwachstellen-management**	**Cloud Security**	**Threat Intelligence & SIEM**
Sicherheitsbewusstsein & Schulung	**Cloud-Plattform**	**Backup & Recovery / Data Protection**	

Sichern Sie sich Ihre persönliche NIS-2-Portfolio-Beratung!

security@adn.de

Hintergrund und Verständnis der NIS 2 Richtlinien und Meldepflichten

NIS 2 Übersicht

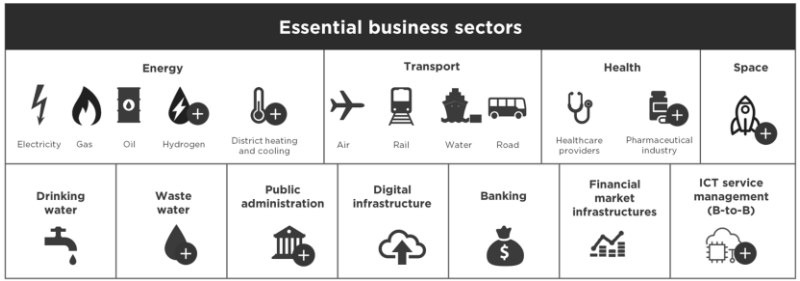
NIS	NIS 2
30 Arten von Entitäten	67 Arten von Entitäten
Betreiber wesentlicher Dienste und Anbieter digitaler Dienste	Umfasst einige KMU und Lieferketten
Sicherheitsanforderungen und Meldung von Vorfällen	Regelmäßige Audits, Anforderungen an die Meldung von Vorfällen, Risikomanagement über mehrere Bereiche hinweg
Von jedem EU-Mitgliedstaat festgelegte Sanktionen	Bußgelder, Aussetzung von Zertifizierungen, Verantwortung des Managements
Schaffung einer Kooperationsgruppe und Computer Security Incident Response Teams (CSIRT) zur Erleichterung des Informationsaustauschs	Schaffung eines Cyber Crisis Liaison Organization Network (EU-CyCLONe)

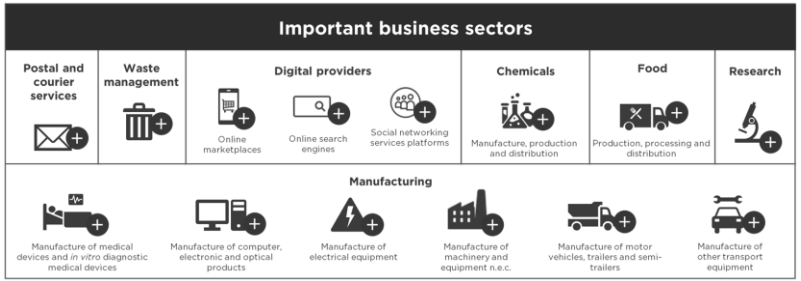
- ✓ Richtlinie über Maßnahmen für ein höheres Cybersicherheitsniveau in der Europäischen Union (EU)
- ✓ Ersetzt die bisherige NIS-Richtlinie
- ✓ Führt strengere Anforderungen für Organisationen ein, die in der EU tätig sind
- ✓ Zielt darauf ab, die Cybersicherheit in Einrichtungen in kritischen Sektoren zu verbessern
- ✓ Betrifft ca 30.000 Institutionen und Unternehmen in Deutschland
- ✓ Betrifft grundsätzlich nur Unternehmen mit mehr als 50 Beschäftigten oder 10 mio Euro Umsatz

Wer muss NIS 2 einhalten?

- Ein breiteres Spektrum an Unternehmen und Sektoren
- Wesentliche Einrichtungen
  - Großunternehmen, öffentliche Verwaltung, Kritis
- Wichtige Einrichtungen
  - Mittelgroße Unternehmen und Einrichtungen

- Der entsprechende Sektor hat eine höhere Priorität

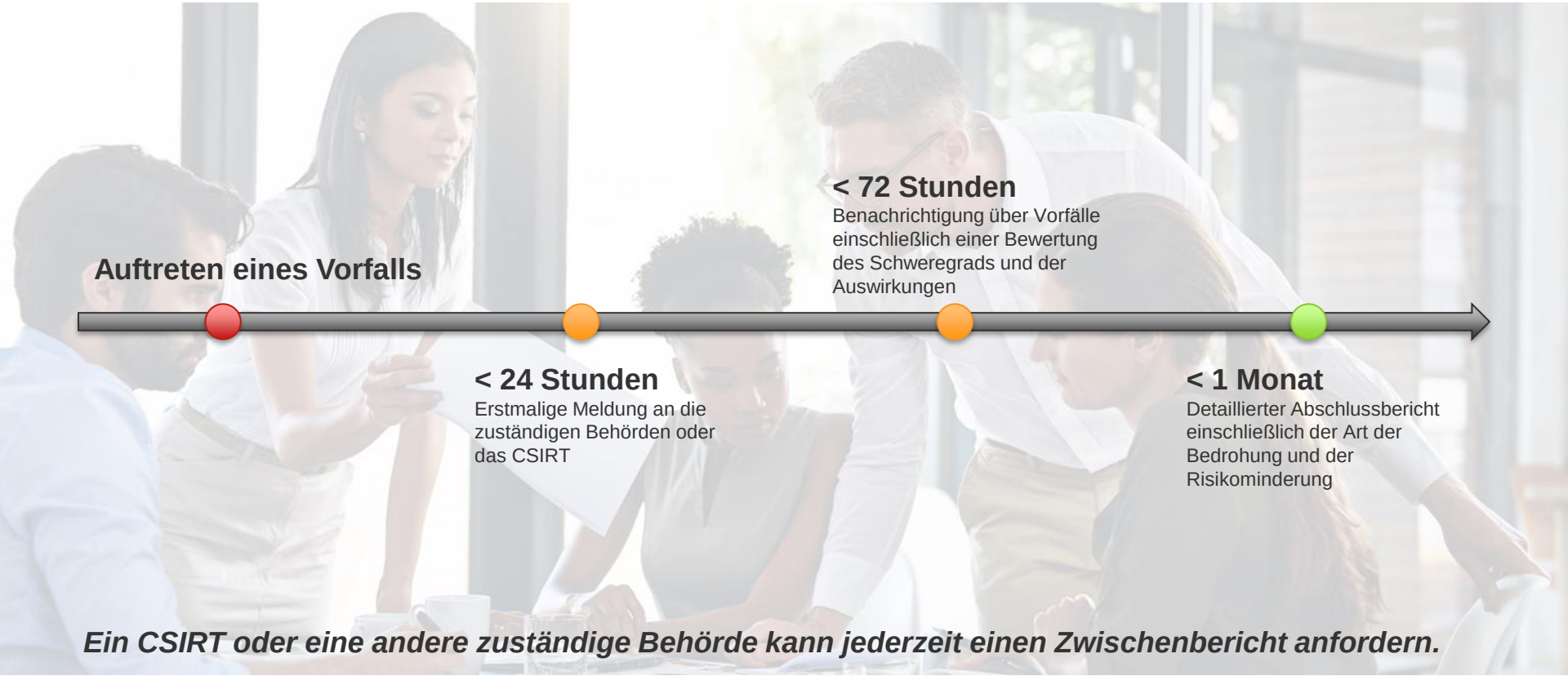




Was sind die wichtigsten Anforderungen von NIS 2?

- **Risikomanagement**
- **Meldung von Vorfällen**
- **Sicherheit in der Lieferkette**
- **Cybersicherheitsmaßnahmen**
- **Governance und Rechenschaftspflicht**

Berichtspflichten



Ein CSIRT oder eine andere zuständige Behörde kann jederzeit einen Zwischenbericht anfordern.

Die Frist für die Einhaltung rückt näher

- 16. Januar 2023
  - NIS 2 von der EU genehmigt
- 17. Oktober 2024
  - Frist für die Mitgliedstaaten zur Umsetzung der Richtlinie in nationales Recht
- 17. April 2025
  - Frist für die Mitgliedstaaten zur Erstellung einer Liste der wesentlichen und wichtigen Einrichtungen

Organisationen, die in der EU tätig sind, müssen konform sein, um Strafen zu vermeiden

Einhaltung von NIS 2 auf EINER Plattform

WatchGuard-Lösungen für NIS 2

	Authpoint	Endpoint Security	Firebox	MDR	Orion	Advanced Reporting Tool	Patch Management	WatchGuard Cloud	ThreatSync	Data Control	Full Encryption
Risk analysis and information system security policies		✓		✓		✓	✓		✓	✓	✓
Incident handling		✓	✓	✓	✓	✓	✓		✓	✓	✓
Business continuity, including recovery and management		✓		✓	✓		✓	✓			
Supply chain security		✓		✓	✓			✓			
Security maintenance and vulnerability handling		✓	✓	✓			✓		✓		
Assessing cybersecurity risk management measures		✓					✓	✓			
Basic cyber hygiene practices		✓		✓		✓	✓				✓
Using cryptography and encryption			✓	✓	✓			✓			✓
Access control and asset management		✓	✓					✓			
Multi-factor authentication	✓		✓								

Wenn wir mehr über NIS 2 und die nationalen Gesetze der EU-Mitgliedstaaten erfahren, wird sich dies wahrscheinlich ändern

WatchGuard-Lösungen und Richtlinienanforderungen

	Authpoint
Risk analysis and information system security policies	
Incident handling	
Business continuity, including recovery and management	
Supply chain security	
Security maintenance and vulnerability handling	
Assessing cybersecurity risk management measures	
Basic cyber hygiene practices	
Using cryptography and encryption	
Access control and asset management	
Multi-factor authentication	✓

Angewandte Technologien

- Multi-Factor Authentication (MFA)
- Mehrere Authentifizierungsmethoden
- Einzigartige Telefon-DNA
- Cloud-Based Management
- Skalierbarkeit für Unternehmen jeder Größe

WatchGuard-Lösungen und Richtlinienanforderungen

	Endpoint Security
Risk analysis and information system security policies	✓
Incident handling	✓
Business continuity, including recovery and management	✓
Supply chain security	✓
Security maintenance and vulnerability handling	✓
Assessing cybersecurity risk management measures	✓
Basic cyber hygiene practices	✓
Using cryptography and encryption	
Access control and asset management	✓
Multi-factor authentication	

Angewandte Technologien

- Multi-Layered Threat Protection
- Next-Gen Anti-Virus
- Endpoint Detection and Response (EDR)
- Application Control
- Device Control
- Web Content Filtering
- Centralized Management

WatchGuard-Lösungen und Richtlinienanforderungen

	Firebox
Risk analysis and information system security policies	
Incident handling	✓
Business continuity, including recovery and management	
Supply chain security	
Security maintenance and vulnerability handling	✓
Assessing cybersecurity risk management measures	
Basic cyber hygiene practices	
Using cryptography and encryption	✓
Access control and asset management	✓
Multi-factor authentication	✓

Angewandte Technologien

- Unified Threat Management (UTM)
- Skalierbarkeit für unterschiedliche Anforderungen
- Zentralisiertes Management
- Mehrschichtige Security

WatchGuard-Lösungen und Richtlinienanforderungen

	MDR
Risk analysis and information system security policies	✓
Incident handling	✓
Business continuity, including recovery and management	✓
Supply chain security	✓
Security maintenance and vulnerability handling	✓
Assessing cybersecurity risk management measures	
Basic cyber hygiene practices	✓
Using cryptography and encryption	✓
Access control and asset management	
Multi-factor authentication	

Angewandte Technologien

- 24/7 Threat Detection and Response
- ErweiterteS Sicherheitsteam
- Unterstützt durch Sicherheitsanalysen und KI
- Verbesserte Sicherheitslage für Anwender

WatchGuard-Lösungen und Richtlinienanforderungen

	Patch Management
Risk analysis and information system security policies	✓
Incident handling	✓
Business continuity, including recovery and management	✓
Supply chain security	
Security maintenance and vulnerability handling	✓
Assessing cybersecurity risk management measures	✓
Basic cyber hygiene practices	✓
Using cryptography and encryption	
Access control and asset management	
Multi-factor authentication	

Angewandte Technologien

- Schwachstellenerkennung und Patch-Management
- Unterstützung gängiger OS Plattformen
- Automatisierte Patch-Bereitstellung (Optional)
- Zentralisiertes Management

Die nächsten Schritte

1. **Beurteilen Sie Ihre Situation**
2. **Führen Sie eine Lückenanalyse durch**
3. **Entwickeln Sie einen Compliance-Plan**

Zusätzliche Ressourcen

- WatchGuard NIS 2 White Paper
- Die Europäische Kommission - https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- European Union Agency for Cybersecurity - https://www.enisa.europa.eu/
- Nationale Cybersicherheitsbehörde - jeder EU-Mitgliedstaat hat seine eigene

Ihre Fragen – unsere Antworten

Sprechen Sie uns an

Kontaktdaten

Achim Kadar

E achim.kadar@adn.de
T +49 2327 9912-452

Michael Haas

E Michael.Haas@watchguard.com
T +49 (170) 7727415