"NIS2 – ist das schon Überregulierung?"

Olaf Mischkovsky,
Business Development Manager GRC & Critical Infrastructure

Rechtliche Grundlagen

EU's Cybersecurity Strategy

* Network and Information Security /// Act = unmittelbar rechtskräftig /// Directive = Umsetzung in jeweiliges nationales Gesetz notwendig

Wie sieht eine nationale Umsetzung aus?

NIS2 Umsetzungsgesetz

besonders wichtige Einrichtungen §2

- **Sektoren**: Energie, Trans… …en und Versicherun… …en, Trinkwas… …nstechnik und T… …dum …, Zentralregierung

12. „Forschungseinrichtung“ eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen; Bildungseinrichtungen gelten nicht als Forschungseinrichtungen;

§30 Risikomanagementmaßnahmen

(1) Besonders wichtige Einrichtungen und wichtige **Einrichtungen sind verpflichtet**, geeignete, **verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen**, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen auf ihre o- der andere Dienste zu verhindern oder möglichst gering zu halten.

(2) Maßnahmen nach Absatz 1 **sollen den Stand der Technik einhalten** und unter Berücksichtigung der einschlägigen **europäischen** und **internationalen Normen** sowie der Umsetzungskosten ein Sicherheitsniveau der informationstechnischen Systeme, Komponenten und Prozesse gewährleisten, das dem bestehenden Risiko angemessen ist.

(3) …

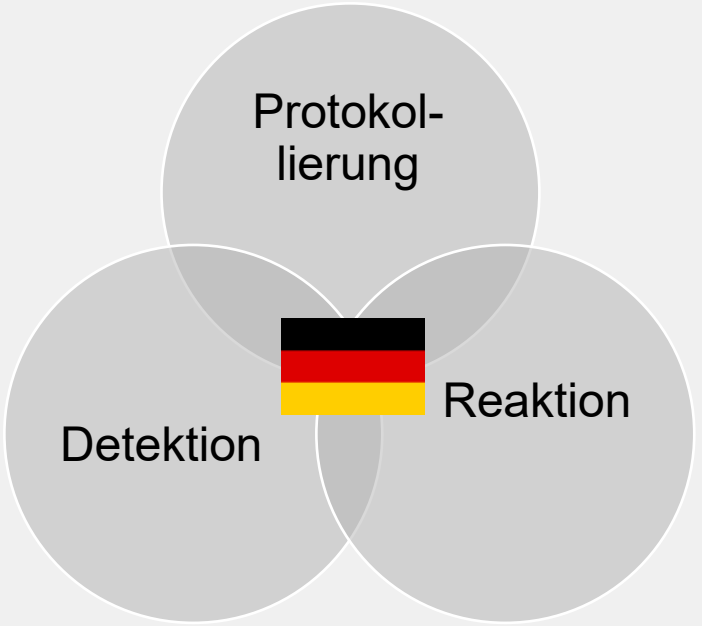
(4) Maßnahmen nach Absatz 1 **müssen auf einem gefahrenübergreifenden Ansatz beruhen**, der darauf abzielt, die informationstechnischen Systeme, Komponenten und Prozesse und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

§31 Besondere Anforderungen

an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

(1) **Für Betreiber kritischer Anlagen gelten** für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, auch **aufwändigere Maßnahmen nach § 30 als verhältnismäßig**, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht.

(2) **Betreiber kritischer Anlagen sind verpflichtet, Systeme zur Angriffserkennung einzusetzen**. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vor- zusehen. Dabei soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchti- gung der betroffenen kritischen Anlage stehen.



NIS2UmsuCG: Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen

§ 38 Absatz 1 BSIG-E

(1) **Geschäftsleitungen** besonders wichtiger Einrichtungen und wichtiger Einrichtungen **sind verpflichtet**, die von diesen Einrichtungen nach § 30 zu ergreifenden **Risikomanagementmaßnahmen umzusetzen und** ihre Umsetzung **zu überwachen**.

(2) **Geschäftsleitungen**, die ihre Pflichten nach Absatz 1 verletzen, **haften** ihrer Einrichtung für einen schuldhaft verursachten Schaden **nach den auf die Rechtsform der Einrichtung anwendbaren Regeln** des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

(3) **Geschäftsleitungen** besonders wichtiger Einrichtungen und wichtiger Einrichtungen **müssen regelmäßig an Schulungen teilnehmen**, **um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken** im Bereich der Sicherheit in der Informationstechnik **zu erlangen** sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Recap: Warum Risikobewertung wichtig ist?

Es gibt kein **einfaches Rezept** für die Absicherung der OT, da Sicherheit eine Frage des **Risikomanagements** ist.

Jede OT-Anlage stellt ein unterschiedliches Risiko für die Organisation dar, abhängig von:

- den **Bedrohungen**, denen es ausgesetzt ist,
- die **Eintrittshäufigkeiten** dieser Bedrohungen,
- die inhärenten **Schwachstellen** des Systems,
- welche **Konsequenzen** es hätte, wenn das System **kompromittiert** würde.

Jede Organisation hat ein individuellen Risikoappetit
(= Risikoakzeptanzniveau)

NIS2UmsuCG: Pflichten für Betreiber

BSI
Nachweispflicht nach § 34

Allgefahrenansatz

Organisatorische Maßnahmen

- Sicherheitsvorgaben
- Incident Management
- Business Continuity
- Sicherheit in der Lieferkette
- Sicherheit im Life-Cycle
- Bewertung der Wirksamkeit
- Schulungen
- Sicherheit des Personals

BBK
Meldepflichten nach § 32

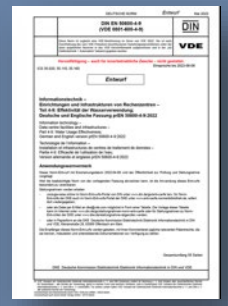
Allgefahrenansatz

Technische Maßnahmen

- Kryptografie
- Zugriffskontrolle
- Asset Management
- Multi-Faktor-Authentifizierung und kontinuierliche Auth.
- Gesicherte Kommunikation
- Gesicherte Notfallkommunikationssysteme

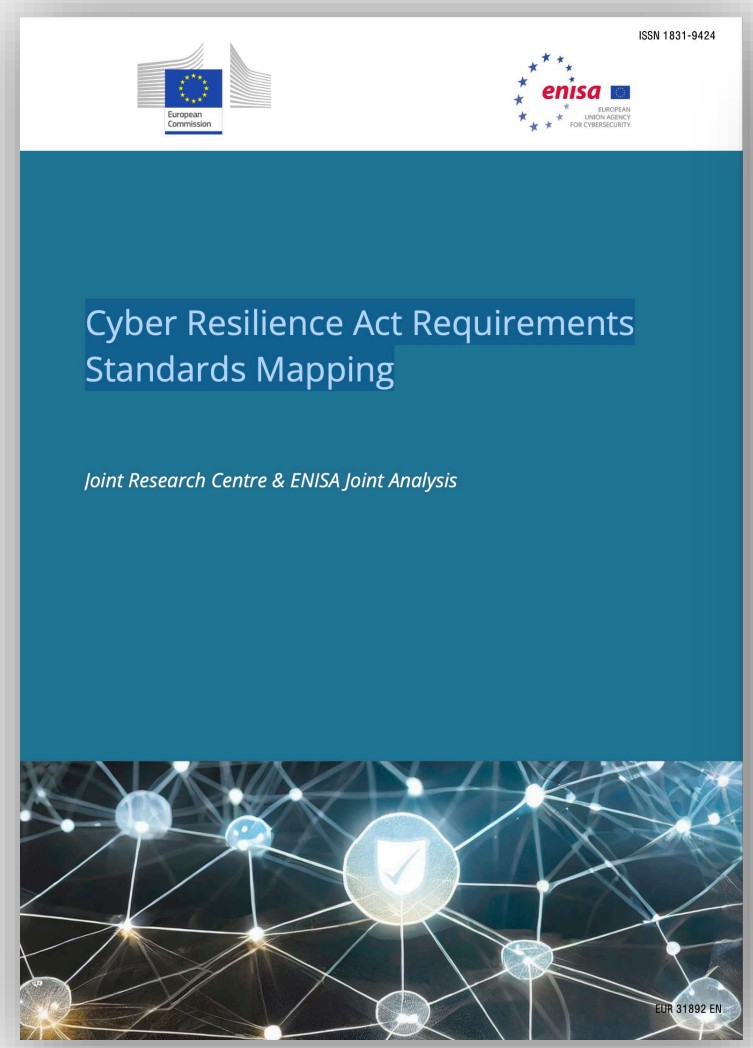
EU-Regulierung und Standardisierung

NIS RL, internationale Standards, Normen



Nationale Standards, Normen, Richtlinien

Cyber Resilience Act Requirements Standards Mapping



Security requirements relating to the properties of products with digital elements

ESSENTIAL CYBERSECURITY REQUIREMENTS

			On the basis of the risk assessment referred to in Article 10(2) and where applicable, products with digital elements shall:						
Standard	**Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks;**	**Products with digital elements shall be delivered without any known exploitable vulnerabilities;**	**be delivered with a secure by default configuration, including the possibility to reset the product to its original state;**	**ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication identi**	**protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant**	**protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration**	**process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended**	**protect the availability of essential functions, including the resilience against and mitigation of denial of service attack**	**minimise th availability devices or**
EN ISO/IEC 27002:2022	x		x					x	
EN ISO/IEC 27005:2022	x								
EN IEC 62443-3-2:2020	x								
EN IEC 62443-4-1:2018	x	x							
ISO/IEC 18045:2022		x							
ITU-T X.1214 (03/2018)		x							
ETSI EN 303 645 V2.1.1 (2020-06)	x	x	x	x	x	x	x	x	
ISO/IEC 18031:2011			x						
ISO/IEC 9798, Parts 1 to 6				x					
ISO/IEC 24760, Parts 1 to 3				x					
ISO/IEC 29146:2016				x					
ITU-T X.1253 (09/2011)				x					
ITU-T X.812 (11/1995)				x					
EN IEC 62443-4-2:2019				x	x	x		x	
ITU-T X.805 (10/2003)					x			x	
ISO/IEC 18033, Parts 1 to 7					x				
ITU-T X.814 (11/1995)					x				
ISO/IEC 9796, Parts 2 and 3						x			
ISO/IEC 9797, Parts 1 to 3						x			
ISO/IEC 14888, Parts 1 to 3						x			
ITU-T X.815 (11/1995)						x			
ISO/IEC 27701:2019							x		
ISO/IEC 29100:2011							x		
ETSI TS 103 485 V1.1.1 (2020-08)							x		
ISO/IEC 22237-1:2021								x	
ITU-T Y.4810 (11/2021)									
ISO/IEC TS 19249:2017									
ISO/IEC 15408-2:2022									
ISO/IEC 27001:2022									
ISO/IEC 27034-1:2011									
EN ISO/IEC 15408-3:2022									
ISO/IEC 13888-1:2020									
ISO/IEC 30111:2019									
IEC 62443-2-1:2010									
IEC 62443 Family	3-2, 4-1	4-1	[none]	4-2	4-2	4-2	[none]	4-2	
ISO 27k Family	27002,27005	[none]	27002	[none]	[none]	[none]	[none]	27002	

Vulnerability handling requirements

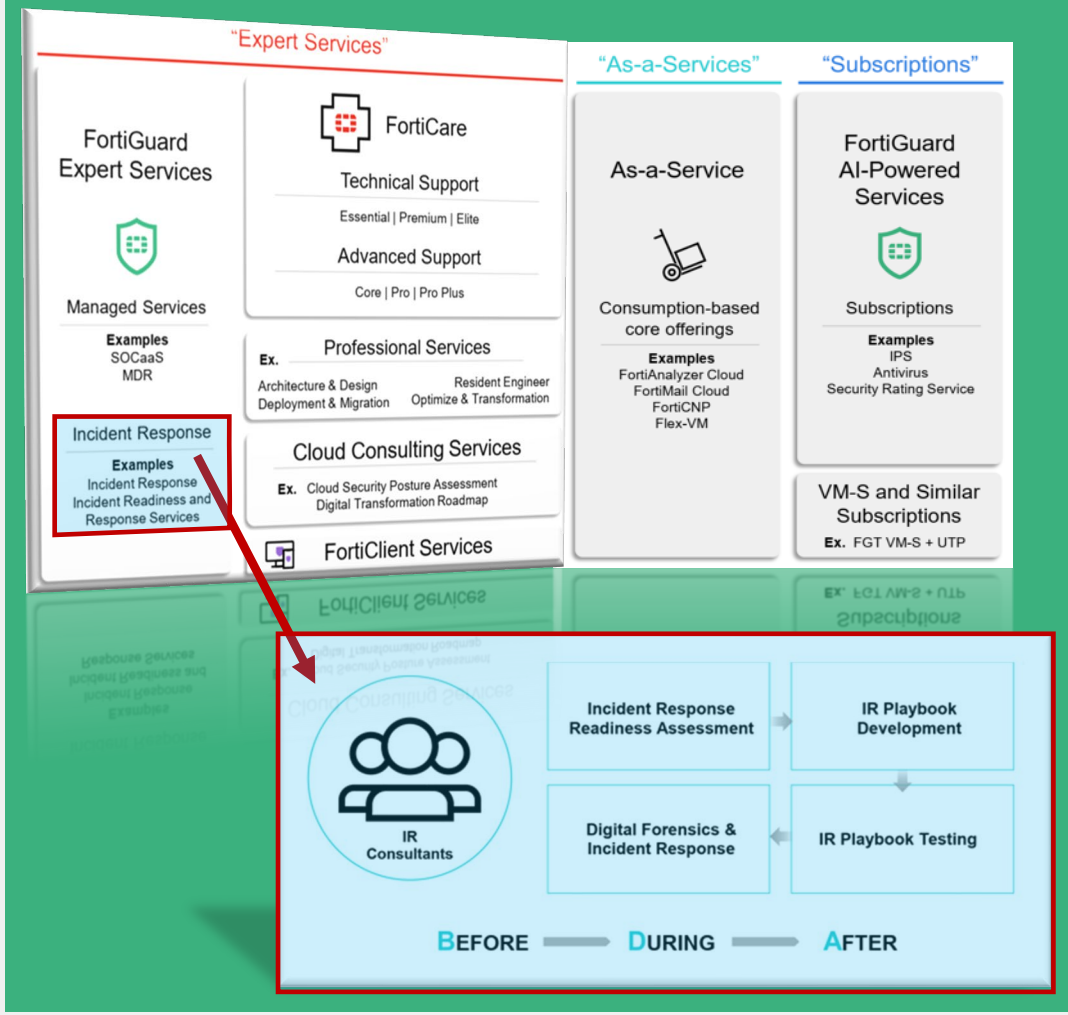
	Manufacturers of the products with digital elements shall:								
Standard	**(1) identify and document vulnerabilities and components contained in the product, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the product**	**(2) in relation to the risks posed to the products with digital elements, address and remediate vulnerabilities without delay including by providing security updates**	**(3) pply effective and regular tests and reviews of the security of the product with digital elements;**	**(4) once a security update has been made available, publically disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts**	**(5) put in place and enforce a policy on coordinated vulnerability disclosure;**	**(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of**	**(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that exploitable vulnerabilities are fixed or mitigated in a timely manner;**	**(8) ensure that, where security patches or updates are available to address identified security issues, they are disseminated without delay and free of charge, accompanied by advisory messages providing users with the relevant information, including on po**
ISO/IEC 27036, Parts 1 to 3	x							#
ISO/IEC 27001:2022		x	x					
ISO/IEC 27002:2022		x	x				x	x
EN ISO/IEC 30111:2020		x		x	x	x		x
EN ISO/IEC 29147:2020		x		x	x	x		
IEC 62443-4-1:2018		x		x			x	x
ISO/IEC TS 27034-5-1:2018			x					
ISO/IEC 27005:2022			x					
ETSI EN 303 645 V2.1.1 (2020-06)				x	x			
IEC 62443 Family	[none]	4-1	[none]	4-1	[none]	[none]	4-1	4-1
ISO 27k Family	27036	27001, 27002	27001, 27002, 27034,27005	[none]	[none]	[none]	27002	27002

Wie kommt man zu einer ganzheitlichen Umsetzung?

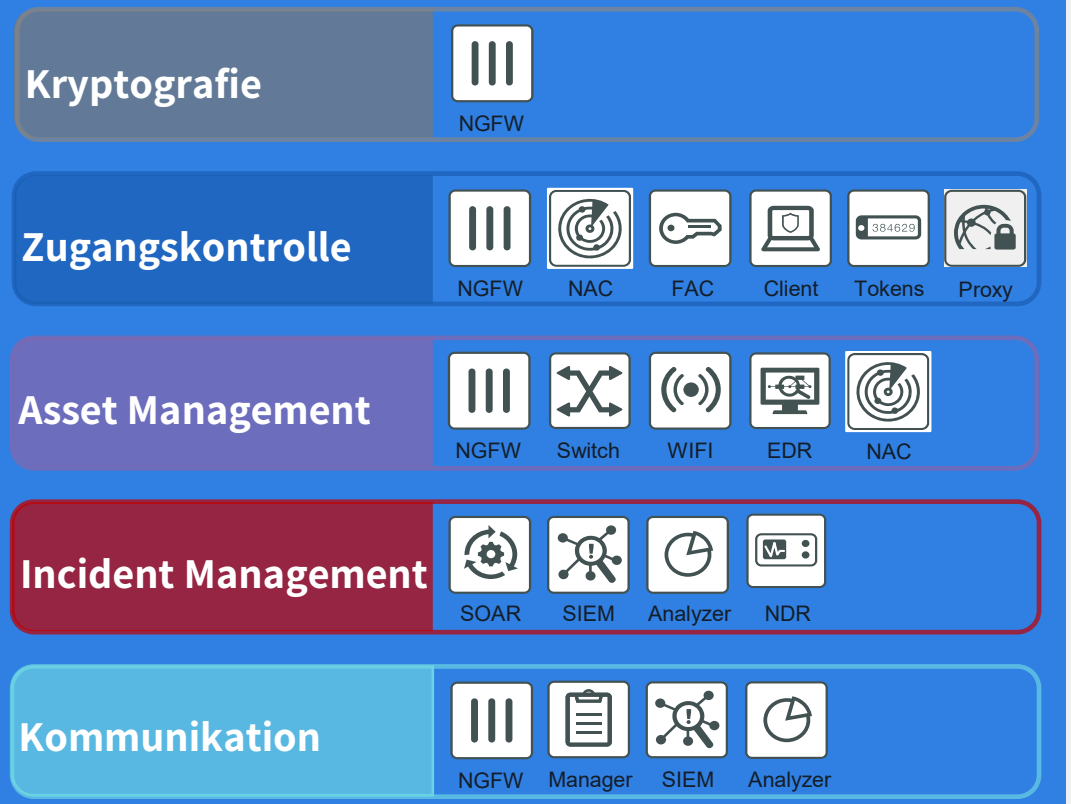
Technical & Organizational Measures (TOM´s)

Fortinet: Holistischer Lösungsansatz für NIS2UmsuCG

Organisatorische Maßnahmen



Technische Maßnahmen



NIS2UmsuCG: Anforderungen (§30 BSIG)

	Organisatorische Maßnahmen		Technische Maßnahmen
	Professional Services **	FortiGuard Services	Technical Products *
• **Sicherheitsvorgaben:** Risikoanalyse	x		
• **Incident management**	x	x	x
• **Aufrechterhaltung des Betriebs**	x		
• **Sicherheit in der Lieferkette**	x		
• **Maßnahmen im Lebenszyklus**	x		
• **Bewertung der Wirksamkeit**	x	x	x
• **Cyberhygiene und Schulungen**	x		
• **Kryptografie**			x
• **Personal**	x		
• **Zugriffskontrolle**	x		x
• **Asset Management**	x		o
• **Multi-Faktor-Authentifizierung und SSO**			x
• **Gesicherte Kommunikation**			x
• **Gesicherte Notfallkommunikationssysteme**			x

* incl. FortiCare Services with Deployment & Operational Assistance (Advanced Services)

** and / or provided by a Channel Partner

Wie identifiziere ich die richtigen Produkte?

Der Griff in FTNT´s Werkzeugkiste…

DER BAUCHLADEN

GESETZ-KONFORM

NORMEN-KONFORM

FTNT Portfolio

Fortinet Security Fabric

The industry's highest-performing integrated cybersecurity mesh platform

Product Matrix

Click on icons in this document for additional information

Fortinet Brochure
Highlighting our broad, integrated, and automated solutions, quarterly

Free Training
Fortinet is committed to training over 1 million people by 2025

FortiOS
The Heart of the Fortinet Security Fabric

Secure Networking

FortiGate
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiGate SD-WAN
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiExtender
Extend scalable and resilient LTE and LAN connectivity

FortiAP
Protected LAN Edge deployments with wireless connectivity

FortiSwitch
Deliver security, performance, and manageable access to data

Linksys HomeWRK
Secure Work-from-Home solution for remote and hybrid workers

FortiNAC
Visibility, access control and automated responses for all networked devices

FortiProxy
Enforce internet, compliance and granular application control

FortiIsolator
Maintain an "air-gap" between browser and web content

Cloud Security

FortiGate VM
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

ForitDDOS
Machine-learning quickly inspects traffic at layers 3, 4, and 7

FortiCNP
Manage risk and compliance through multi-cloud infrastructures

FortiDevSec
Continuous application security testing in CI/CD pipelines

FortiWeb
Prevent web application attacks against critical web assets

FortiADC
Application-aware intelligence for distribution of application traffic

FortiGSLB Cloud
Ensure business continuity during Unexpected network downtime

FortiMail
Secure mail getaway to protect against SPAM and virus attacks

FortiCASB
Prevent misconfigurations of SaaS applications and meet compliance

Zero Trust Access

FortiSASE
Enforce dynamic network access control and network segmentation

ZTNA Agent
Remote access, application access, and risk reduction

FortiAuthenticator
Identify users wherever they are and enforce strong authentication

FortiToken
One-time password application with push notification

FortiClient Fabric Agent
IPSec and SSL VPN tunnel, endpoint telemetry and more

FortiConnect
Simplified guest access, BYOD, and policy management

FortiGuard Threat Intelligence

Powered by FortiGuard Labs

Fabric Management Center: NOC

FortiManager
Centralized management of your Fortinet security infrastructure

FortiGate Cloud
Saas w/ zero touch deployment, configuration, and management

FortiMonitor
Analysis tool to provide NOC and SOC monitoring capabilities

FortiAIOps
Network inspection to rapidly analyze, enable, and correlate

FortiExtender Cloud
Deploy, manage and customize LTE internet access

FNDN
Exclusive developer community for access to advanced tools & scripts

Open Ecosystem

The industry's most extensive ecosystem of integrated solutions

Fabric Connectors
Fortinet-developed

DevOp Tools & Script
Fortinet & community-driven

Fabric API Integration
Partner-led

Extended Ecosystem
Threat sharing w/ tech vendors

Fabric Management Center: SOC

FortiDeceptor
Discover active attackers inside with decoy assets

FortiNDR
Accelerate mitigation of evolving threats and threat investigation

FortiEDR
Automated protection and orchestrated incident response

FortiSandbox / FortiAI
Secure virtual runtime environment to expose unknown threats

FortiAnalyzer
Correlation, reporting, and log management in Security Fabric

FortiSIEM
Integrated security, performance, and availability monitoring

FortiSOAR
Automated security operations, analytics, and response

FortiTester
Network performance testing and breach attack simulation (BAS)

SOC-as-a-Service
Continuous awareness and control of events, alerts, and threats

Incident Response Service
Digital forensic analysis, response, containment, and guidance

Support & Mitigation Services

FortiCare Essentials*
15% of hardware, FG-80 & below

FortiCare Premium*
20% of hardware

FortiCare Elite**
25% of hardware

FortiConverter
25% of hardware

* FortiCare Premium is formerly 24x7 Support. Lower support price for Switches and APs

** Response time for High Priority tickets. Available for ForiGate, FortiManager, FortiAnalyzer, FortiSwitch, and FortiAP

Communication and Surveillance

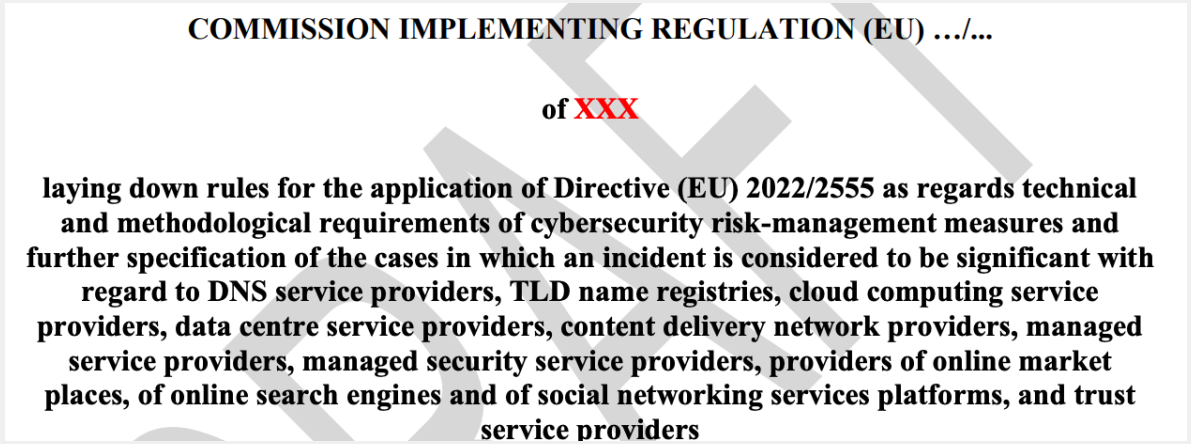
FortiFone
Application-centric, scalable, and Secure SD-WAN with NGFW

FortiVoice
Extend scalable and resilient LTE and LAN connectivity

FortiCamera
NGFW w/ SOC acceleration and industry-leading secure SD-WAN

FortiRecorder
Protected LAN Edge deployments with wireless connectivity

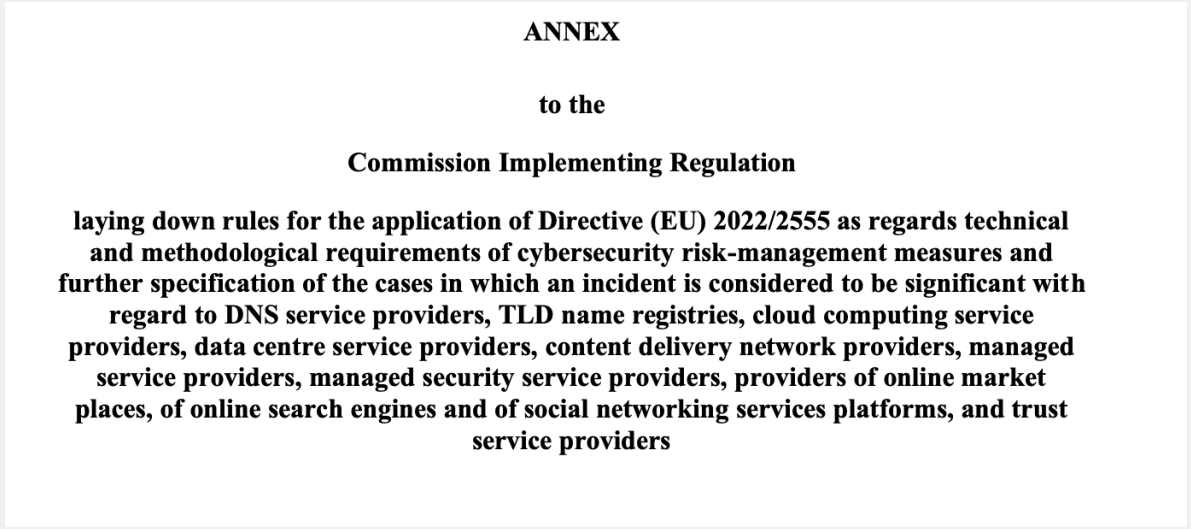
nach Art. 23 Abs. 11 der NIS-2-RL - Durchführungsrechtsakte



COMMISSION IMPLEMENTING REGULATION (EU) …/...

of XXX

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers



ANNEX

to the

Commission Implementing Regulation

laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers

2.1 Risk management framework

2.3 . Independent review of information and network security

3.2 Monitoring and logging

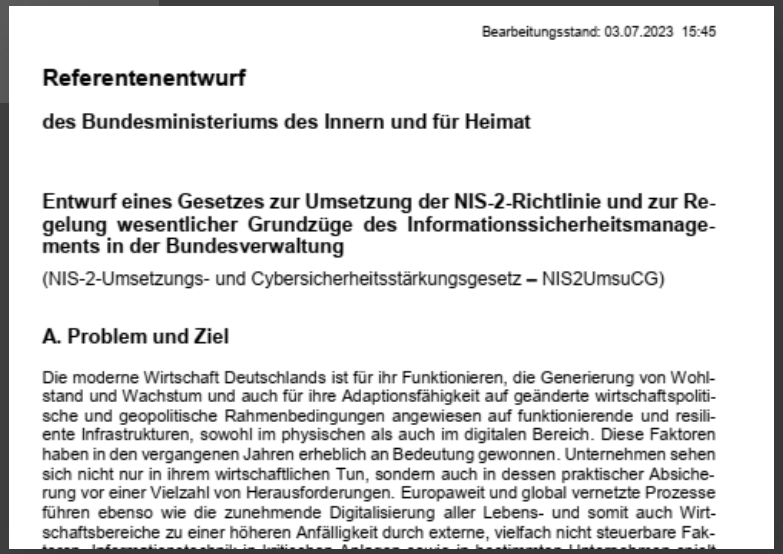
6.7 Network security

6.8 Network segmentation

6.9 Protection against malicious and unauthorised software

Wie kommt man nun zu einer ganzheitlichen Umsetzung?

Beispiel „DE Gesetz-konform“: KRITIS Kunde folgt NIS2UmsuCG



Bearbeitungsstand: 03.07.2023 15:45

Referentenentwurf

des Bundesministeriums des Innern und für Heimat

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

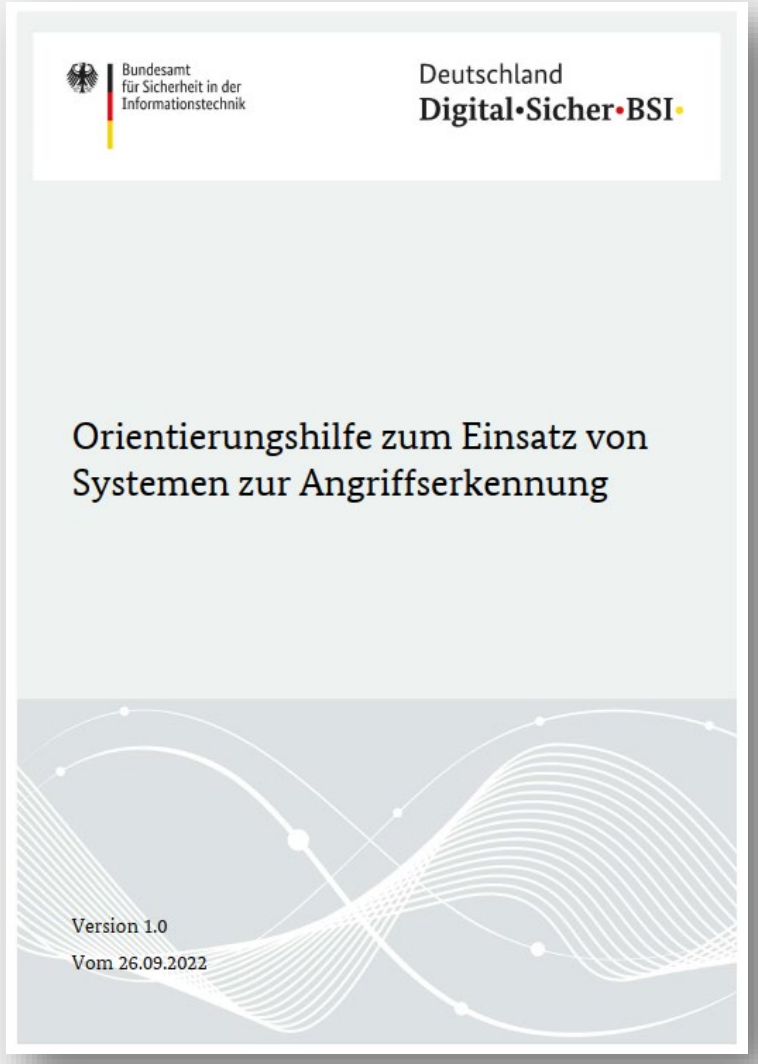
(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)

A. Problem und Ziel

Die moderne Wirtschaft Deutschlands ist für ihr Funktionieren, die Generierung von Wohlstand und Wachstum und auch für ihre Adaptionsfähigkeit auf geänderte wirtschaftspolitische und geopolitische Rahmenbedingungen angewiesen auf funktionierende und resiliente Infrastrukturen, sowohl im physischen als auch im digitalen Bereich. Diese Faktoren haben in den vergangenen Jahren erheblich an Bedeutung gewonnen. Unternehmen sehen sich nicht nur in ihrem wirtschaftlichen Tun, sondern auch in dessen praktischer Absicherung vor einer Vielzahl von Herausforderungen. Europaweit und global vernetzte Prozesse führen ebenso wie die zunehmende Digitalisierung aller Lebens- und somit auch Wirtschaftsbereiche zu einer höheren Anfälligkeit durch externe, vielfach nicht steuerbare Fak-

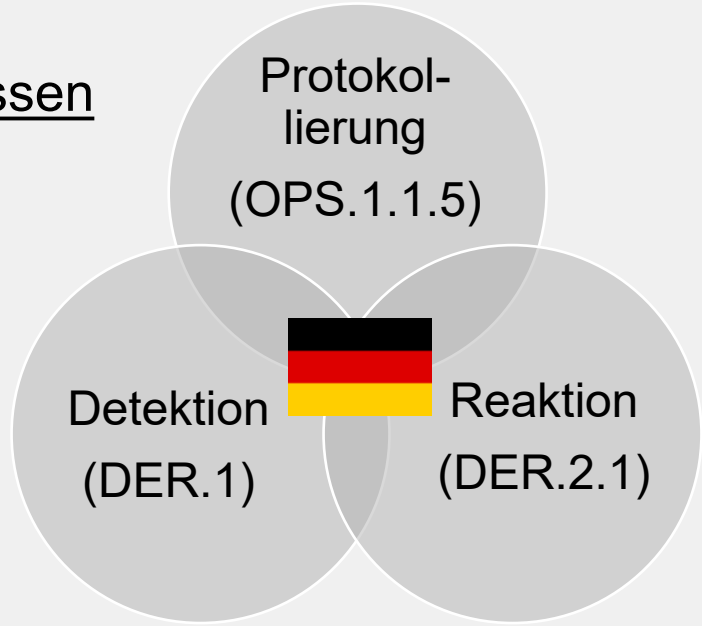
BSI: Orientierungshilfe Angriffserkennung

Umsetzungshilfe des alten § 8a Absatz, aktuell als §31 übernommen in NIS2UmsuCG



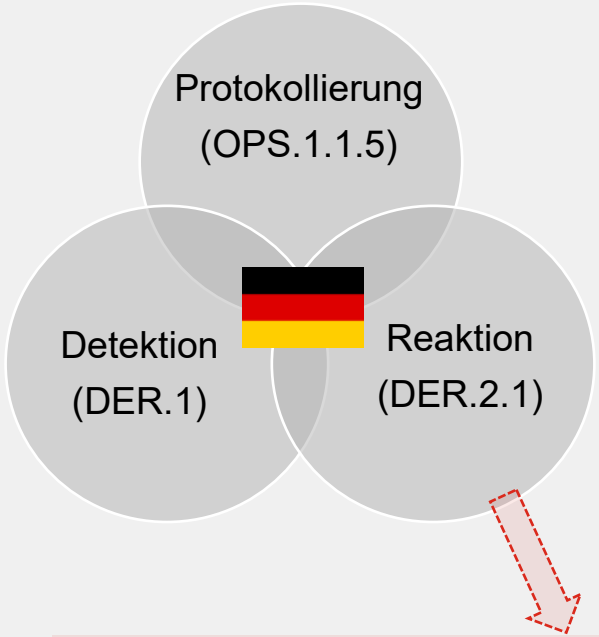
Weiterführende Orientierung:

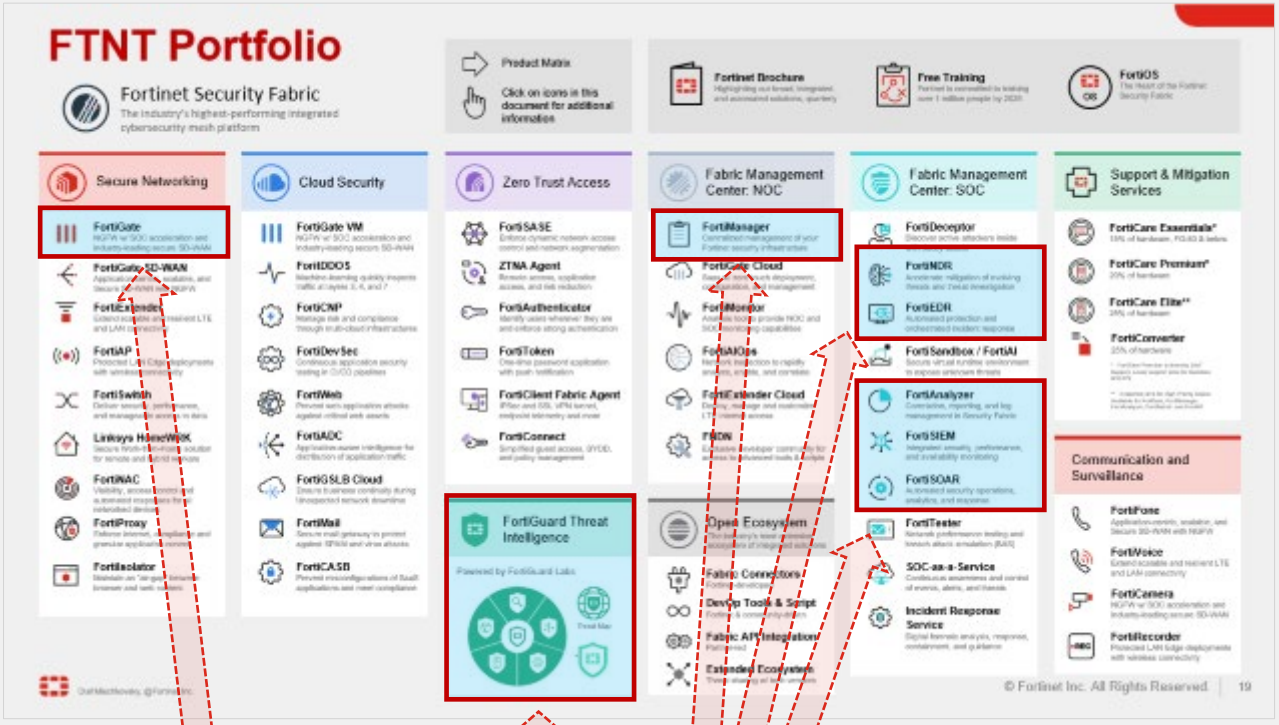
- OPS.1.1.4: Schutz vor Schadprogrammen
- OPS.1.1.5: Protokollierung
- NET.1.2: Netzmanagement
- NET.3.2: Firewall
- DER.1: Detektion von sicherheitsrelevanten Ereignissen
- DER.2.1: Behandlung von Sicherheitsvorfällen



Fortinet Umsetzung „Angriffserkennung“

Produkte zur Umsetzung § 31 (alt § 8a) BSIG





Risiko-basiert

Die zur Angriffserkennung eingesetzten Systeme **SOLLTEN automatisiert Maßnahmen zur Vermeidung und Beseitigung von angriffsbedingten Störungen** ergreifen können, ….

Dabei **MUSS gewährleistet sein, dass ausschließlich automatisiert ergriffene Maßnahmen nicht zu einer relevanten Beeinträchtigung der kritischen Dienstleistung des Betreibers führen können**.

- Single Pane Management
- Threat Intelligence
- Interoperability

Secure Networking

NET.1.2: Netzmanagement, NET.3.2: Firewall

Ruggedized Design
Fan-less and use of robust components ensure reliable operation in harsh industrial environments.

Consolidated Security Architecture
FortiGate running FortiOS consolidated security offers better protection and lower cost of ownership than multiple point products.

Ease of Management
Allows rapid provision and deployment, monitoring of device and threat status while providing actionable reports.

FortiGate Rugged Series

FGR-70F
DIN-rail mounted, SoC4-powered, security and VPN gateway

FGR-70F 3G/4G
DIN-rail mounted, SoC-4-powered, security and VPN gateway with embedded 3G/4G/LTE

FGR-60F
SoC4-powered, security and VPN gateway

FGR-60F 3G/4G
SoC-4-powered, security and VPN gateway with embedded 3G/4G/LTE

FortiGate Features

- Security (IPS, FW, OT traffic monitor)
- Encryption (GRE, VXLAN, IPSEC)
- Connectivity (Proxy, VLANs, IPv6.)
- Advance features (SD-WAN)
- Central authentication (LDAP, RADIUS)
- IPS Service (Virtual Patching)
- Industrial Security Service for OT
- IoT Detection Service
- Antivirus, Anti-malware, Bonet, CDR, Virus Outbreak Protection & Sandbox services
- URL, Web, Video DNS Content Filtering
- Wi-Fi
- IPSEC VPN & SSL VPN
- SSL Inspection
- Packet capture triggered by IPS
- Virtual Domains (VDOM)
- Transparent or Proxy

FortiSwitch, FortiAP & FortiDeceptor Rugged

FSR-112D-POE
Fan-less passive cooling with DIN-rail or wall-mountable. Power over Ethernet capable including PoE+. Redundant power input terminals. Mean time between failure greater than 25 years.

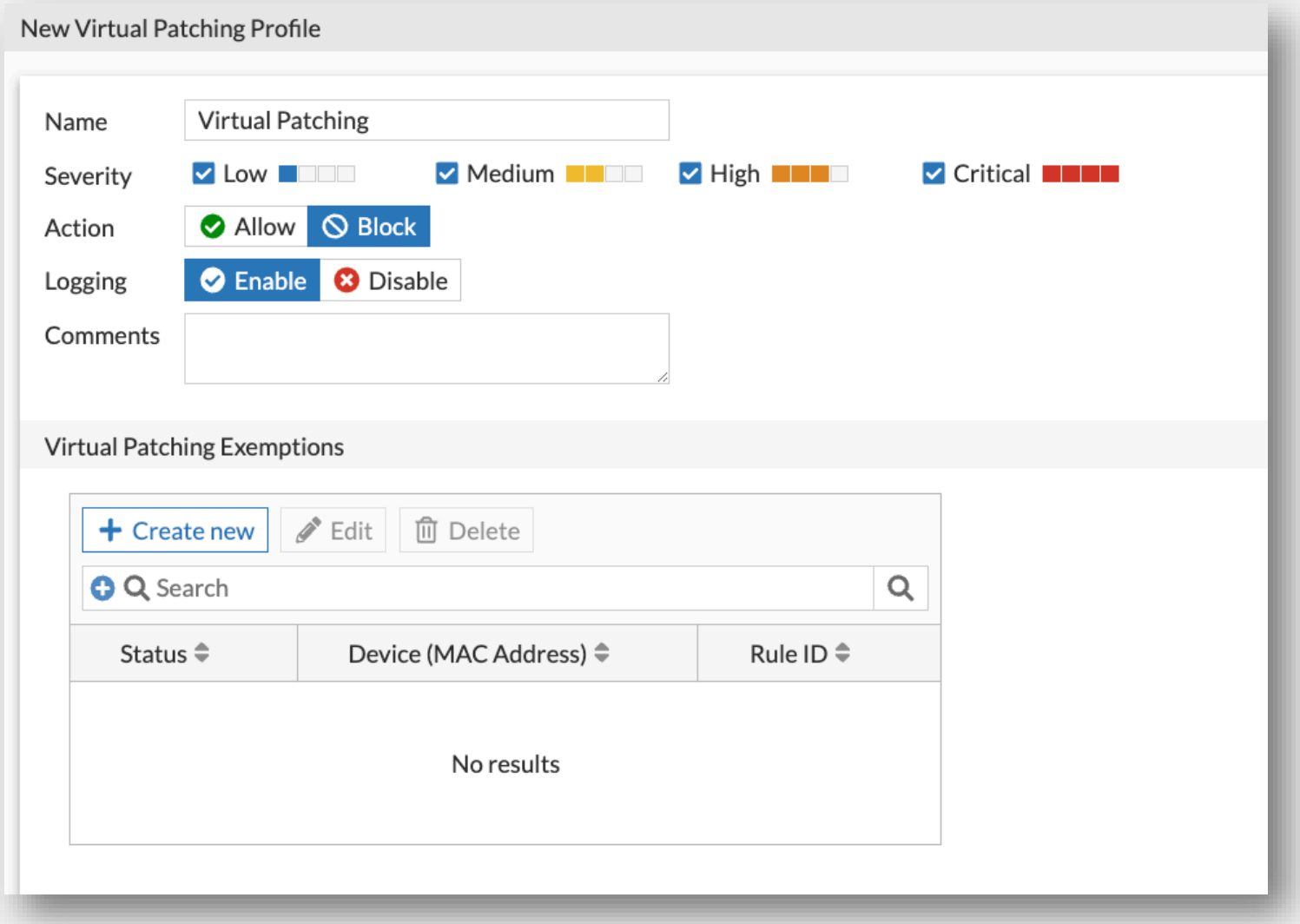
FortiDeceptor Rugged 100G
Fan-less desktop form factor. AC or DC powered. 6 x 1GbE RJ-45 ports. 1TB SSD storage.

FortiAP Rugged 234F & FortiAP Rugged 432F
External Antennas
IP67, Indoor/Outdoor Use
PoE Powered
Wall- and pole-mountable
Wi-Fi Alliance Certified

Virtual Patching

OPS.1.1.3 Patch- und Änderungsmanagement

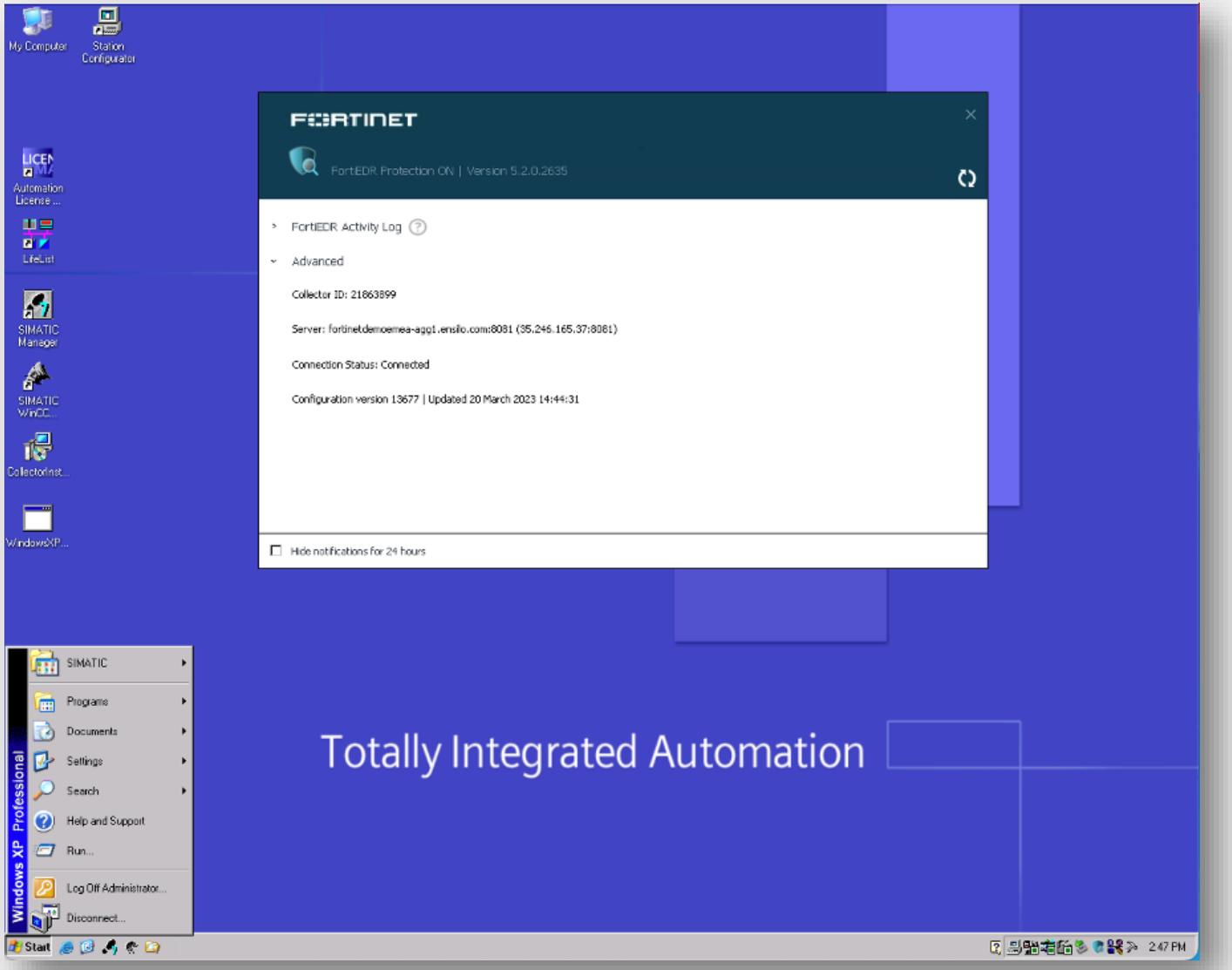
- Patchmanagement virtuell auf Netzwerkebene oder lokal auf den Systemen
- Entzerrung des Patch-Prozesses bzw. Bereitstellung von Patches für nicht-patchbare Systeme



Endpoint Detection & Response

OPS.1.1.4: Schutz vor Schadprogrammen

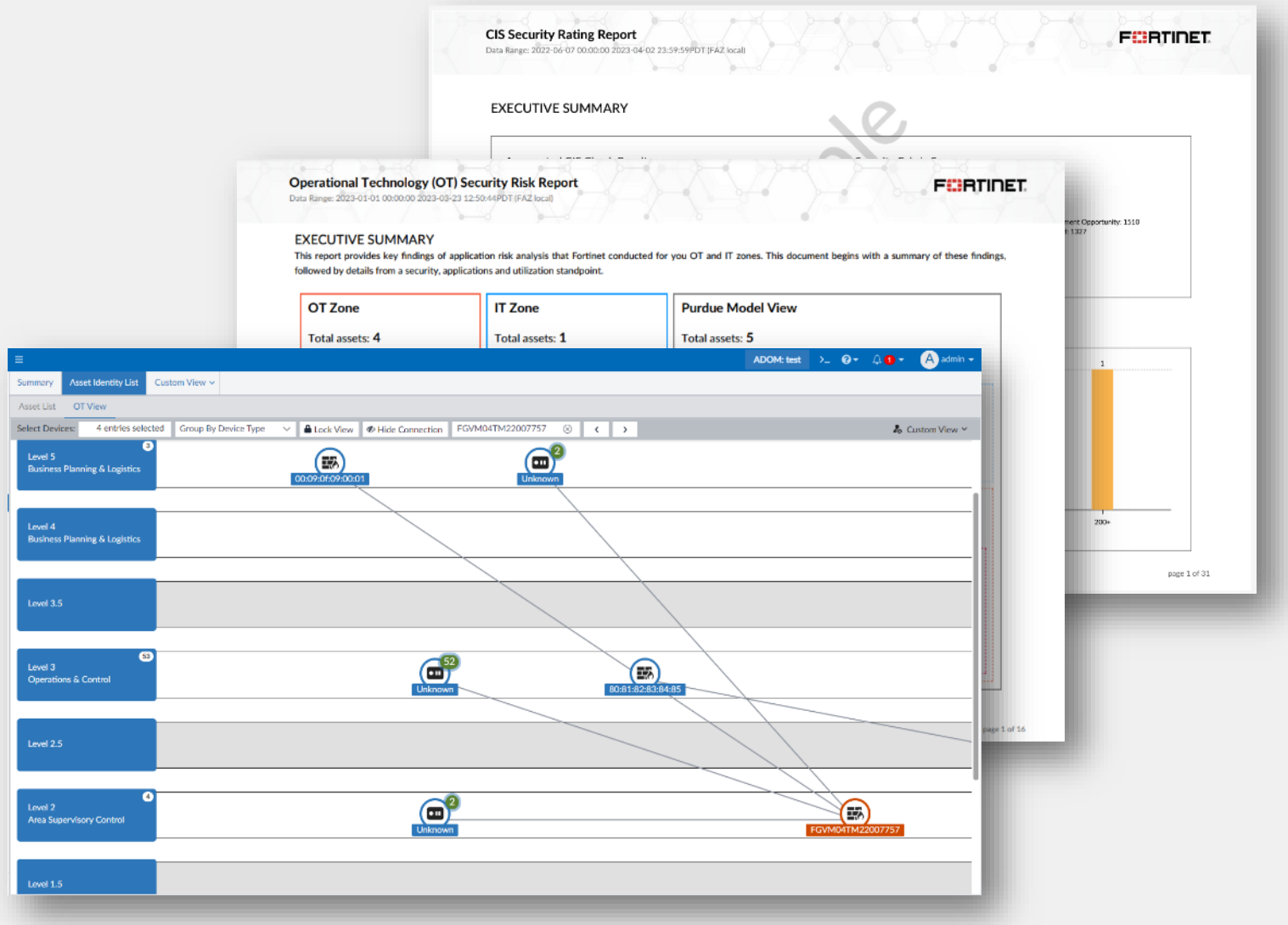
- Full feature set for legacy & up-to-date OS
- Full support for collector
- Low footprint / resource requirement (< 1% CPU, 60MB memory, 20MB Disk usage)
- No reboot needed for installation



Logging & Monitoring

OPS.1.1.5: Protokollierung

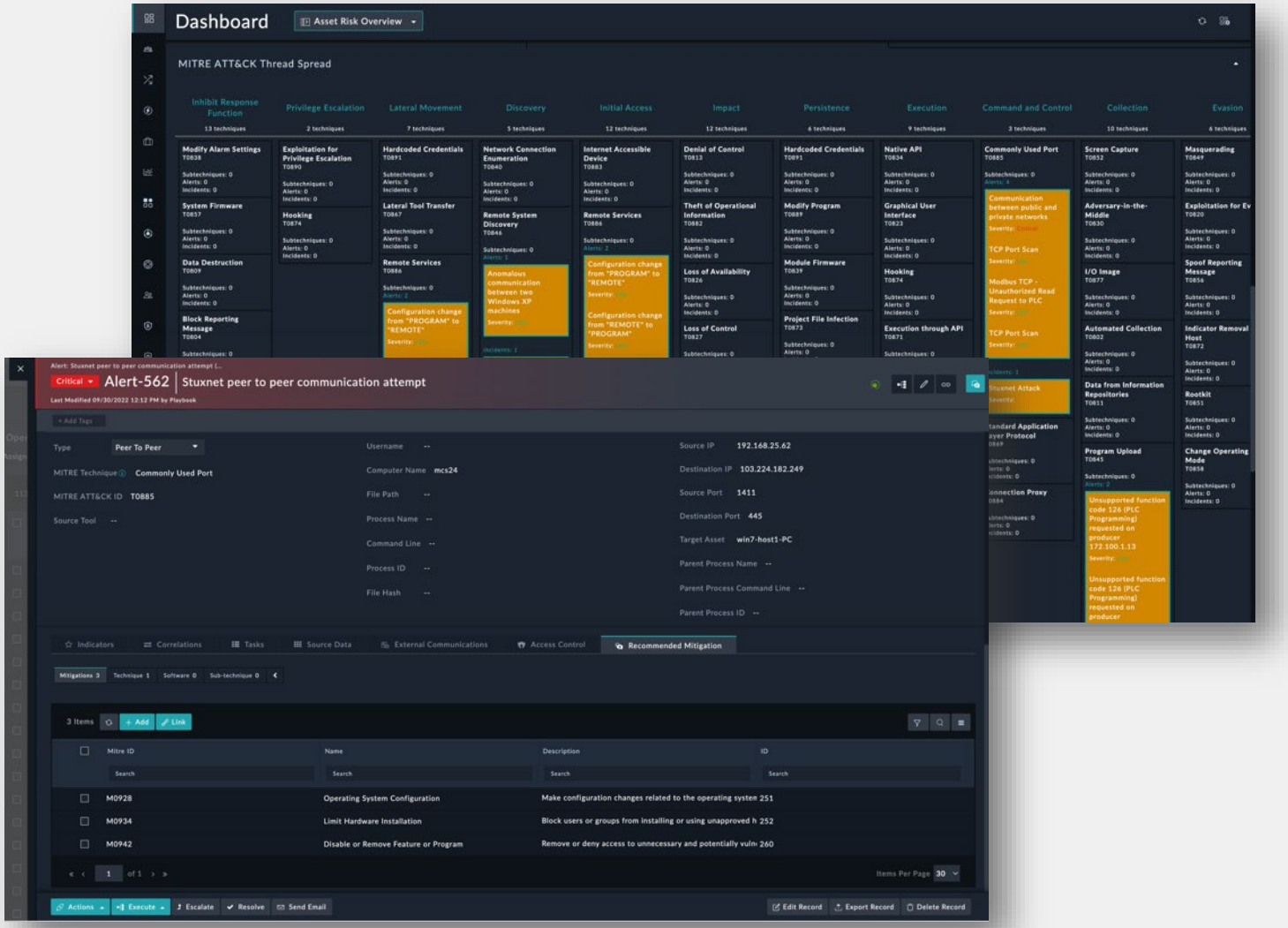
- OT-Dashboards
- Automatisierte Asset-Erkennung und -Klassifizierung
- Berichte zu OT-Risiken und Kommunikationsbeziehungen
- Compliance-Berichte zu NERC CIP, NIST, IEC 62443-3-3…
- MITRE ATT&CK for ICS



(Automatisierte) Alarmbehandlung

DER.2.1: Behandlung von Sicherheitsvorfällen

- Matching von Vorfällen auf das MITRE ATT&CK for Industrial Control Systems Framework
- Empfohlene Maßnahmen direkt aus dem CVE oder anhand der erkannten MITRE Technik
- „Playbooks“ können vordefiniert werden, um Maßnahmen vorab festzulegen



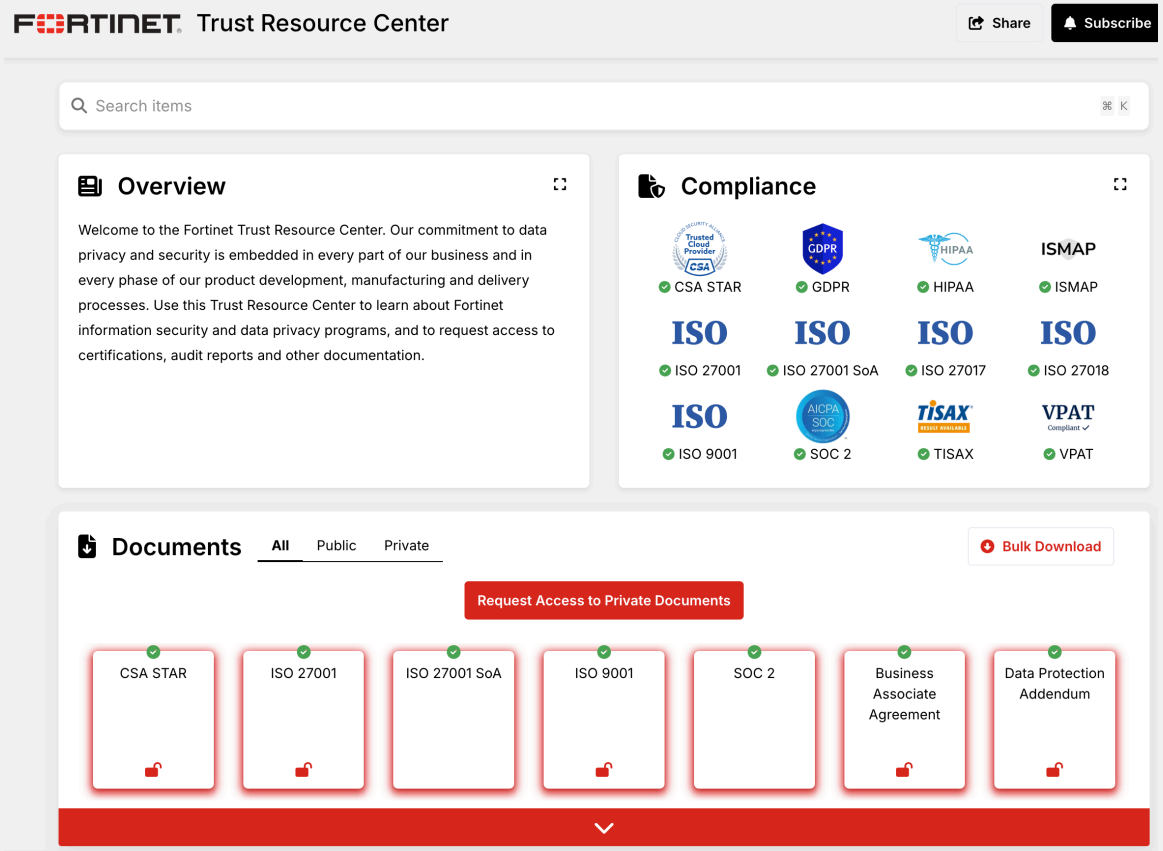
Incident Readiness Services

Unterstützung unserer Kunden

Die Fortinet Trust Webpage

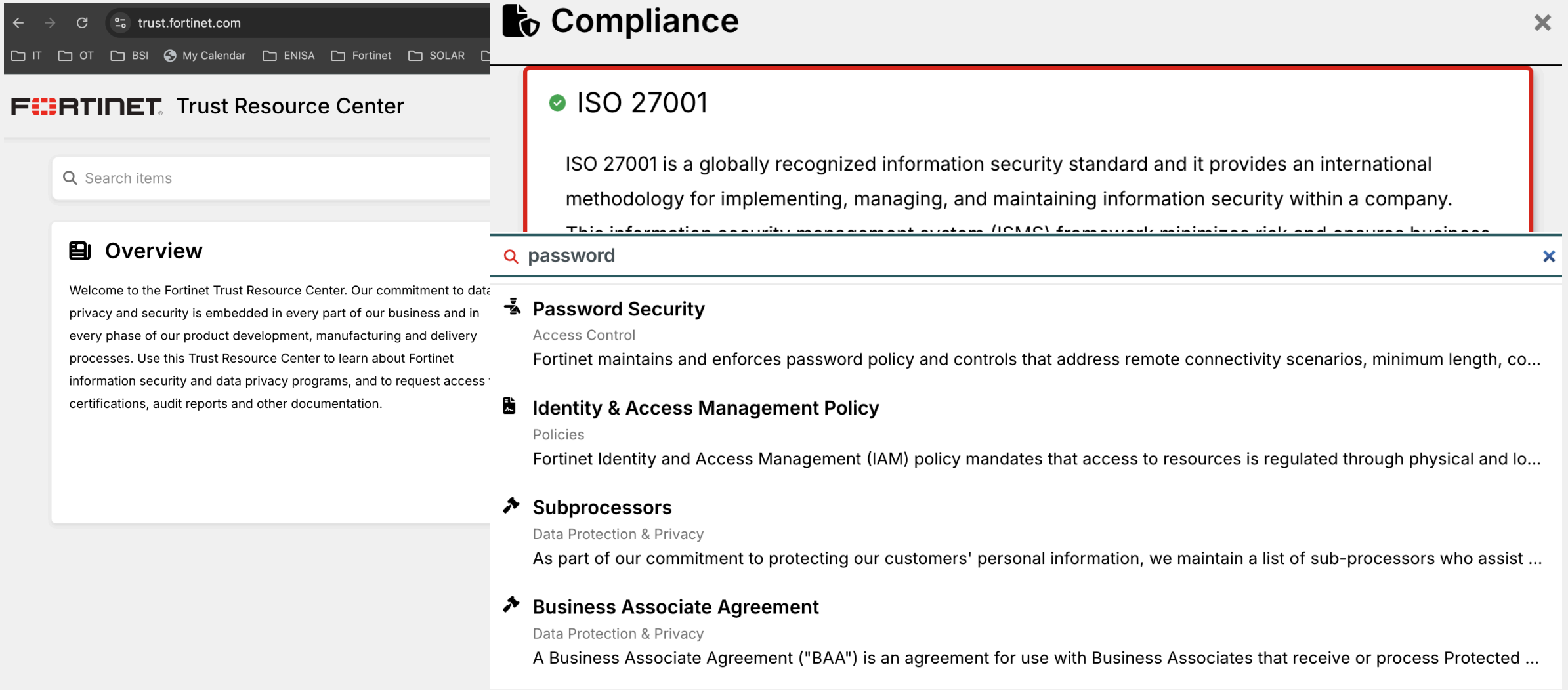
Erster Anlaufpunkt zu allen Compliance Themen

- Die Anzahl zu Compliance relevanter Inhalte ist dramatisch gestiegen
- Regularien wie DSGVO, DORA, NIS2, CRA erfordern Nachweise
- z.B. Darstellung einer sicheren Lieferkette (NIS2 und CRA)
- die Trust Website trust.fortinet.com beantwortet 95% aller Kundenanfragen



The Fortinet trust webpage

Erster Anlaufpunkt zu allen Compliance Themen



Der Sustainable Report

What is sustainability reporting?

Sustainability reporting refers to the disclosure of non-financial information that is relevant to all stakeholders of a company or other organization. The disclosure of reports can be voluntary, desired or mandatory.

With the help of a sustainability report, an organization communicates its positive or negative impact on the environment, society and corporate governance (ESG) as well as its progress

Source: https://envoria.com/de/sustainability-reporting#:~:text=Unter%20Nachhaltigkeitsberichterstattung%20bzw.,freiwillig%2C%20erw%C3%BCnscht%20oder%20obligatorisch%20sein.

https://www.fortinet.com/corporate/about-us/corporate-social-responsibility/sustainability-report

- Today, reporting is seen as proof of integrity, transparency and a sense of responsibility
- Means of demonstrating a company's commitment to sustainable growth
- the disclosure of their sustainability and ESG strategies
- confirmed by the TÜV Süd

Olaf Mischkovsky

Business Development Manager

E: omischkovsky@fortinet.com
M: +49 172 3649284

Fortinet GmbH
Feldbergstraße 35
60323 Frankfurt a.M.
Germany

Oliver Dahmen

Named Account Manager Research

0160 2066586

odahmen@fortinet.com

UNSERE VISION

Eine digitale Welt ermöglichen, der man immer vertrauen kann