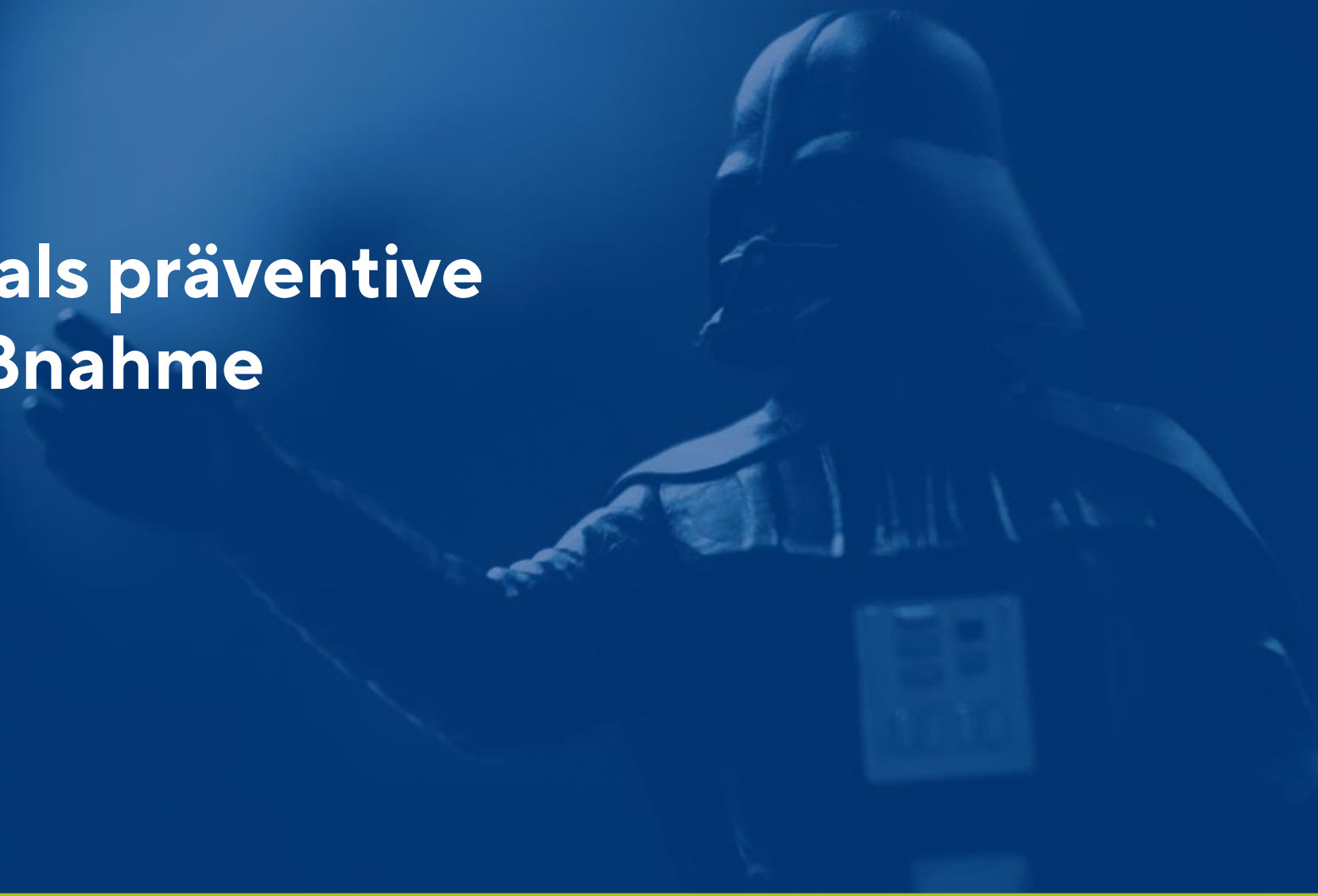
TWLKOM × FB PRO GMBH
System Hardening & Data Protection



Live Webinar

Systemhärtung als präventive IT-Security-Maßnahme

- Individuell konfiguriert
- Umfassend automatisiert
- Prozessual integriert

→ Kontinuierlich geschützt!

Ludwigshafen, 27.02.2024

Organisatorische Info

- Die Präsentation wird aufgezeichnet.
- Die Folien zum Webinar werden im Anschluss öffentlich bereitgestellt.
- Mikrofon und Kamera sind für alle Teilnehmenden deaktiviert.
- Fragen, die während des Webinars aufkommen, können im F&A Bereich gestellt werden.
- Am Ende des Webinars gibt es in der offiziellen Fragerunde die Möglichkeit, auch persönlich Fragen zu stellen. Nutzen Sie hierfür die „Hand heben“ Funktion, um sich bemerkbar zu machen.

TWL KOM × FB PRO GMBH
System Hardening & Data Protection

TWL KOM × FB PRO GMBH
System Hardening & Data Protection

Agenda

01 Wer wir sind
02 Bedrohung der Cyber Security
03 Systemhärtung als Schutzbaustein
04 TWL-KOM Full-Service-IT
05 Produkt-Demo
06 Fragen & Antworten

TWLKOM × FB PRO GMBH
System Hardening & Data Protection

01
Wer wir sind

Vorstellung – TWL-KOM

Historie

- Über 30 Jahre Vertriebserfahrung und Key Accounting in der IT-Branche

Expertise

- Datacenter und Cloud Computing
- Cloud Backup Lösungen
- Schutz vor Cyberkriminalität
- IT-Infrastrukturen und Virtualisierung

TWL-KOM

- Intelligente IT-Lösungen in den Bereichen Infrastructure as a Service, Platform as a Service bis hin zu X as a Service
- Alles aus einer Hand – nach Ihren individuellen Anforderungen
- Eigene Datacenter mit höchstmöglicher Zertifizierung

Uwe Hamann
Key Account Manager, TWL-KOM

TWL KOM × FB PRO GMBH
System Hardening & Data Protection

Vorstellung – FB Pro

Historie

- Über 20 Jahre IT-Erfahrung, u. a. Diplom-Informatiker (FH)
- IT-Compliance- & Datenschutzbeauftragter

Expertise

- Generalist im Themengebiet IT-Infrastrukturen
- Operative und regulatorische Expertise (Datenschutz und IT-Compliance)

Spezialisierung

- Fokussierung im Themengebiet „präventive IT-Sicherheit“
- Spezialisierung im Thema „Systemhärtung“ (system hardening)

FB Pro

- FB Pro bietet als einziger europäischer Anbieter „Systemhärtung“ auf Produkt-/ Lösungsbasis
- Ganzheitliche integrierte Absicherung von IT-Systemen
- Einfache Umsetzung durch ein zentrales „secure configuration management“

Florian Bröder
Founder, FB Pro

TWL KOM × FB PRO GMBH
System Hardening & Data Protection

TWLKOM × FB PRO GMBH
System Hardening & Data Protection

02
Bedrohung der Cyber Security

Wer ist der Hacker?

Motive

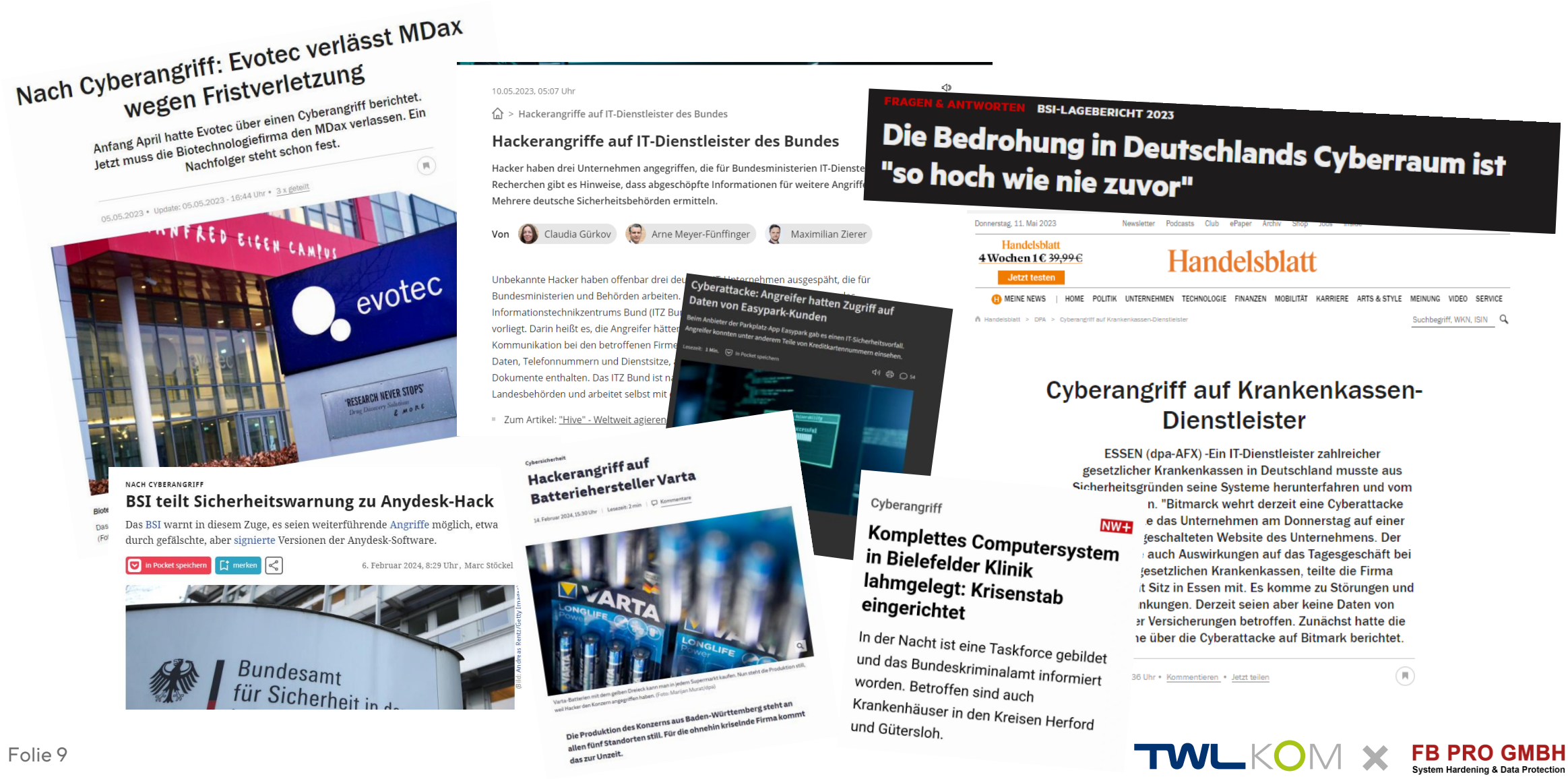
- Geld
- Datendiebstahl und Erpressung
- Aufmerksamkeit und Ansehen

Kategorisierung

- **Organisierte Unternehmen** **4 %**
  → Organisiert, zielorientiert, verdeckt
- **Technischer Angreifer** **27 %**
  → IT-Fachkraft, Programmierer
- **„Skript Kiddie“/ Amateur** **69 %**
  → Hobby, Amateur, nutzt vorgefertigte Frameworks

⟶ „Plug and Play“ Hacking

Cyberangriffe – Aktuelle Fallbeispiele



TWL KOM × FB PRO GMBH
System Hardening & Data Protection

Es kann jeden treffen!

Und dann...?

... stellen sich die folgenden Fragen

Wie gut greifen Maßnahmen?

Um Auswirkungen auf das Unternehmen zu verhindern?

Wie kann man Auswirkungen einschränken?

Auf bestimmte Bereiche/ einzelne Computer/ Services

→ **Maßnahmen im Umfeld „Erkennung und Reaktion“ reichen alleine nicht aus, um eine angemessene Informationssicherheit zu gewährleisten!**

TWLKOM × FB PRO GMBH
System Hardening & Data Protection

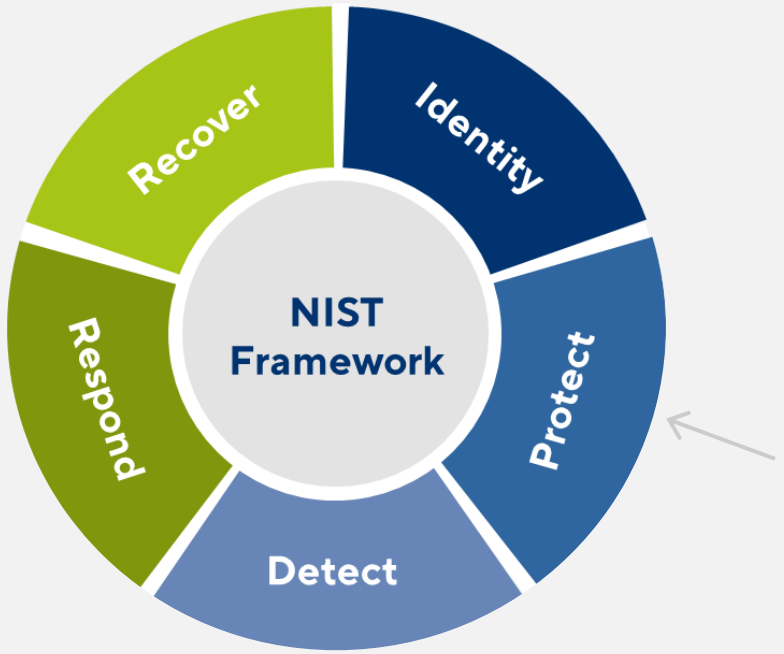
03
Systemhärtung als Schutzbaustein

Systemhärtung – Mehrwerte

Als Systemhärtung oder Härtung bezeichnet man die sichere Konfiguration von IT-Systemen.

Mehrwerte

- Dauerhafte **Erhöhung** und Kontrolle des **Schutz-Niveaus**
- **Reduzierung der Wahrscheinlichkeit** eines erfolgreichen Angriffs
- **Risikominimierung** bei erfolgreichen Angriffen
- **Verlangsamung** von Schad-Software-Ausbreitung im Fall der Fälle
- **Einfache Nachweiserzeugung** für Cyber-Versicherungen, Revisoren, Auditoren
- **Generierung eines Schutz-Niveaus**, das Cyber-Versicherung überhaupt erst möglich macht (ansonsten ggfs. Ablehnung)

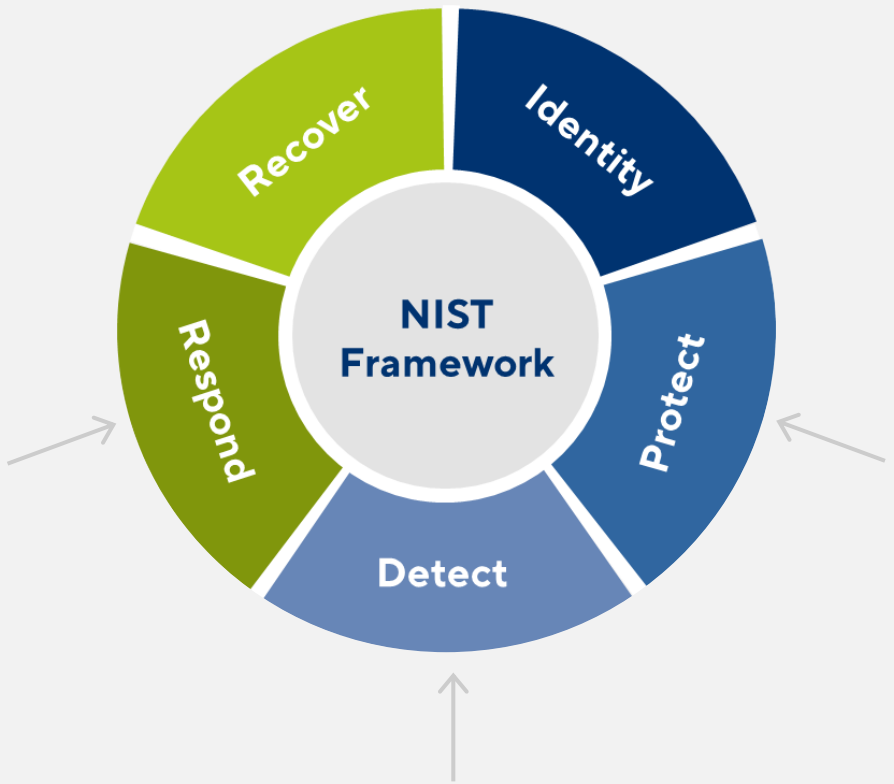


TWL KOM × FB PRO GMBH
System Hardening & Data Protection

Systemhärtung – Vergleich zu anderen Technologien

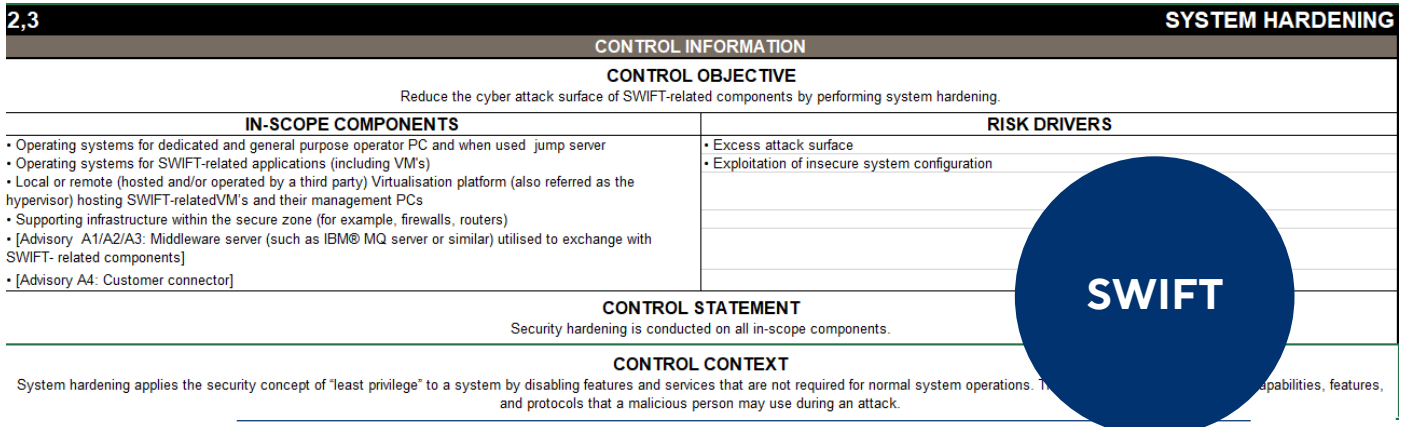
Technology	Protect	Detect	Respond
Anti-Malware solutions		X	X
Threat-Intel solutions		X	X
EDR/XDR solutions		X	X
MDR solutions		X	X
Vulnerability scanner		X	
SIEM solutions		X	X (SOC, IM process)
Compromise Assessment		X	X
Hardening	X		
Enforce Administrator	X	X	X (IM process)

→ **Was macht mehr Sinn?**
Eine offene Tür die 24/7 überwacht wird oder eine geschlossene Tür?



TWL KOM × FB PRO GMBH
System Hardening & Data Protection

Vorgaben in Security-Frameworks



2,3 SYSTEM HARDENING

CONTROL INFORMATION

CONTROL OBJECTIVE

Reduce the cyber attack surface of SWIFT-related components by performing system hardening.

IN-SCOPE COMPONENTS	RISK DRIVERS
• Operating systems for dedicated and general purpose operator PC and when used jump server • Operating systems for SWIFT-related applications (including VM's) • Local or remote (hosted and/or operated by a third party) Virtualisation platform (also referred as the hypervisor) hosting SWIFT-relatedVM's and their management PCs • Supporting infrastructure within the secure zone (for example, firewalls, routers) • [Advisory A1/A2/A3: Middleware server (such as IBM® MQ server or similar) utilised to exchange with SWIFT- related components] • [Advisory A4: Customer connector]	• Excess attack surface • Exploitation of insecure system configuration

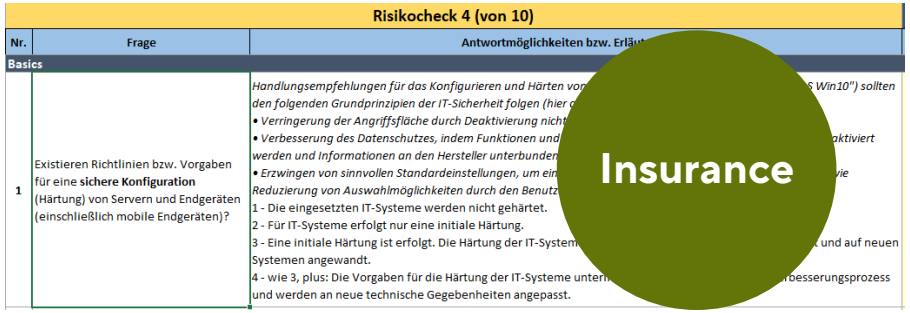
CONTROL STATEMENT

Security hardening is conducted on all in-scope components.

CONTROL CONTEXT

System hardening applies the security concept of "least privilege" to a system by disabling features and services that are not required for normal system operations. T… apabilities, features, and protocols that a malicious person may use during an attack.

SWIFT



Risikocheck 4 (von 10)

Nr.	Frage	Antwortmöglichkeiten bzw. Erlä…
Basics		
1	Existieren Richtlinien bzw. Vorgaben für eine **sichere Konfiguration** (Härtung) von Servern und Endgeräten (einschließlich mobile Endgeräten)?	*Handlungsempfehlungen für das Konfigurieren und Härten von … Win10") sollten den folgenden Grundprinzipien der IT-Sicherheit folgen (hier …* *• Verringerung der Angriffsfläche durch Deaktivierung nicht…* *• Verbesserung des Datenschutzes, indem Funktionen und … aktiviert werden und Informationen an den Hersteller unterbunden…* *• Erzwingen von sinnvollen Standardeinstellungen, um ein… wie Reduzierung von Auswahlmöglichkeiten durch den Benutz…* 1 - Die eingesetzten IT-Systeme werden nicht gehärtet. 2 - Für IT-Systeme erfolgt nur eine initiale Härtung. 3 - Eine initiale Härtung ist erfolgt. Die Härtung der IT-System… und auf neuen Systemen angewandt. 4 - wie 3, plus: Die Vorgaben für die Härtung der IT-Systeme unter… besserungsprozess und werden an neue technische Gegebenheiten angepasst.

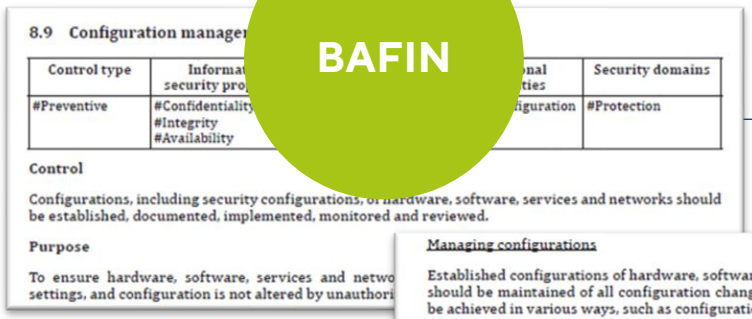
Insurance

5.2. Das Unternehmen hat auf Basis der Informationssicherheitsleitlinie und Informationssicherheitsrichtlinien angemessene, dem Stand der Technik entsprechende, operative Informationssicherheitsmaßnahmen und Prozesse zu implementieren.

Informationssicherheitsmaßnahmen und -prozesse berücksichtigen u. a.:

- Schwachstellenmanagement zur Erkennung, Bewertung, Behandlung und Dokumentation von Schwachstellen,
- Segmentierung und Kontrolle des Netzwerks (einschließlich Richtlinienkonformität der Endgeräte),
- sichere Konfiguration von IT-Systemen (Härtung),
- Verschlüsselung von Daten bei Speicherung und Übertragung gemäß Schutzbedarf,
- mehrstufigen Schutz der IT-Systeme gemäß Schutzbedarf (z. B. vor Datenverlust, Manipulation, Verfügbarkeitsangriffen oder vor nicht autorisiertem Zugriff),
- Perimeterschutz von z. B. Liegenschaften, Rechenzentren und anderen sensiblen Bereichen.

BAFIN



8.9 Configuration manage…

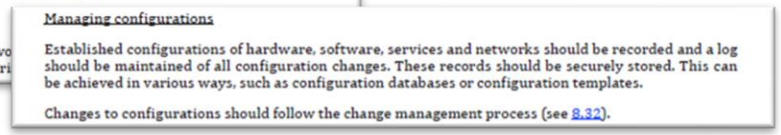
Control type	Informa… security pro…	…nal …ties	Security domains
#Preventive	#Confidentiality #Integrity #Availability	…figuration	#Protection

Control

Configurations, including security configurations, of hardware, software, services and networks should be established, documented, implemented, monitored and reviewed.

Purpose

To ensure hardware, software, services and netwo… settings, and configuration is not altered by unauthori…

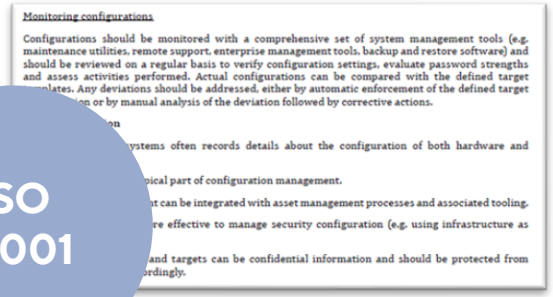


Managing configurations

Established configurations of hardware, software, services and networks should be recorded and a log should be maintained of all configuration changes. These records should be securely stored. This can be achieved in various ways, such as configuration databases or configuration templates.

Changes to configurations should follow the change management process (see 8.32).

ISO 27001



Monitoring configurations

Configurations should be monitored with a comprehensive set of system management tools (e.g. maintenance utilities, remote support, enterprise management tools, backup and restore software) and should be reviewed on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed. Actual configurations can be compared with the defined target …plates. Any deviations should be addressed, either by automatic enforcement of the defined target …or by manual analysis of the deviation followed by corrective actions.

…ystems often records details about the configuration of both hardware and …

…ical part of configuration management.

…t can be integrated with asset management processes and associated tooling.

…re effective to manage security configuration (e.g. using infrastructure as …

…and targets can be confidential information and should be protected from …rdingly.

SiSyPHuS Win10: Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10

Bundesamt für Sicherheit in der Informationstechnik

BSI

Vorgaben in Security-Frameworks: CIS, BSI, TeleTrusT

CIS Center for Internet Security®

CIS Sub-Control
CIS Control Title

		1	2	3
CIS Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers				
5.1	Establish Secure Configurations	●	●	●
5.2	Maintain Secure Images		●	●
5.3	Securely Store Master Images		●	●
5.4	Deploy System Configuration Management Tools		●	●
5.5	Implement Automated Configuration Monitoring Systems		●	●

04 Secure Configuration of Enterprise Assets and Software

4.1	Establish and Maintain a Secure Configuration Process	●	●	●
4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure	●	●	●
4.3	Configure Automatic Session Locking on Enterprise Assets	●	●	●
4.4	Implement and Manage a Firewall on Servers	●	●	●
4.5	Implement and Manage a Firewall on End-User Devices	●	●	●
4.6	Securely Manage Enterprise Assets and Software	●	●	●
4.7	Manage Default Accounts on Enterprise Assets and Software	●	●	●
4.8	Uninstall or Disable Unnecessary Services on Enterprise Assets and Software		●	●
4.9	Configure Trusted DNS Servers on Enterprise Assets		●	●
4.10	Enforce Automatic Device Lockout on Portable End-User Devices		●	●
4.11	Enforce Remote Wipe Capability on Portable End-User Devices		●	●
4.12	Separate Enterprise Workspaces on Mobile End-User Devices			●

Bundesamt für Sicherheit in der Informationstechnik

SYS.1.1.A11 Festlegung einer Sicherheitsrichtlinie für Server (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an Server in einer separaten Sicherheitsrichtlinie konkretisiert werden. Diese Richtlinie SOLLTE allen Administratoren und anderen Personen, die an der Beschaffung und dem Betrieb der Server beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft und die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

SYS.1.1.A6 Deaktivierung nicht benötigter Dienste (B)

Alle nicht benötigten Dienste und Anwendungen MÜSSEN deaktiviert oder deinstalliert werden, vor allem Netzdienste. Auch alle nicht benötigten Funktionen in der Firmware MÜSSEN deaktiviert werden. Auf Servern SOLLTE der Speicherplatz für die einzelnen Benutzer, aber auch für Anwendungen, geeignet beschränkt werden.

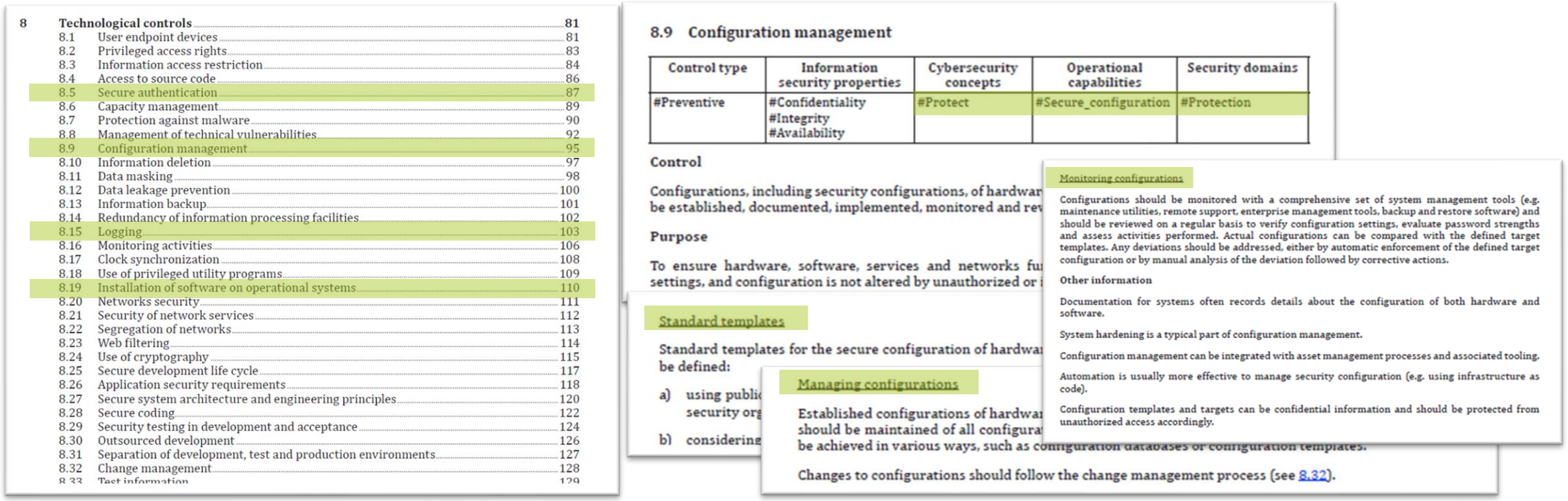
SYS.1.2.2.A3 Sichere Konfiguration von Windows Server 2019 (B)

Mehrere wesentliche Funktionen bzw. Rollen SOLLTEN NICHT durch einen einzigen Server erfüllt, sondern geeignet aufgeteilt werden. Vor Inbetriebnahme SOLLTE das System grundlegend gehärtet werden. Alle sicherheitsrelevanten Einstellungen SOLLTEN bedarfsgerecht konfiguriert, getestet und regelmäßig überprüft werden. Dafür SOLLTEN Sicherheitsrichtlinien, unter Berücksichtigung der Empfehlungen des Betriebssystemherstellers und des voreingestellten Standardverhaltens, konfiguriert werden, sofern das Standardverhalten nicht anderen Anforderungen aus dem IT-Grundschutz oder der Institution widerspricht. Die Entscheidungen SOLLTEN dokumentiert und begründet werden. Sicherheitsrichtlinien SOLLTEN in jedem Fall gesetzt werden, auch dann, wenn das voreingestellte Standardverhalten dadurch nicht verändert wird.

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

3.2.10	Layer 2 encryption
3.2.11	Cloud-based data exchange
3.2.12	Data storage in the cloud
3.2.13	Use of mobile voice and data services
3.2.14	Communication through instant messenger
3.2.15	Mobile Device Management
3.2.16	Router security
3.2.17	Network monitoring using Intrusion Detectio
3.2.18	Web traffic protection
3.2.19	Web application protection
3.2.20	Remote network access/ remote maintenan
3.2.21	Server hardening
3.2.22	Endpoint Detection & Response Platform
3.2.23	Using internet with web isolation
3.2.24	Attack detection and analysis (SIEM)
3.2.25	Confidential computing
3.2.26	Sandboxing for malicious code analysis
3.2.27	Cyber threat intelligence
3.2.28	Securing administrative IT systems
3.2.29	Monitoring of Directory Services and Identity

Vorgaben in Security-Frameworks: ISO 27001:2022



8 Technological controls 81
8.1 User endpoint devices 81
8.2 Privileged access rights 83
8.3 Information access restriction 84
8.4 Access to source code 86
8.5 Secure authentication 87
8.6 Capacity management 89
8.7 Protection against malware 90
8.8 Management of technical vulnerabilities 92
8.9 Configuration management 95
8.10 Information deletion 97
8.11 Data masking 98
8.12 Data leakage prevention 100
8.13 Information backup 101
8.14 Redundancy of information processing facilities 102
8.15 Logging 103
8.16 Monitoring activities 106
8.17 Clock synchronization 108
8.18 Use of privileged utility programs 109
8.19 Installation of software on operational systems 110
8.20 Networks security 111
8.21 Security of network services 112
8.22 Segregation of networks 113
8.23 Web filtering 114
8.24 Use of cryptography 115
8.25 Secure development life cycle 117
8.26 Application security requirements 118
8.27 Secure system architecture and engineering principles 120
8.28 Secure coding 122
8.29 Security testing in development and acceptance 124
8.30 Outsourced development 126
8.31 Separation of development, test and production environments 127
8.32 Change management 128
8.33 Test information 129

8.9 Configuration management

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Secure_configuration	#Protection

Control

Configurations, including security configurations, of hardwar
be established, documented, implemented, monitored and rev

Purpose

To ensure hardware, software, services and networks fu
settings, and configuration is not altered by unauthorized or i

Standard templates

Standard templates for the secure configuration of hardwa
be defined:

a) using publi
security org

b) considering

Managing configurations

Established configurations of hardwa
should be maintained of all configura
be achieved in various ways, such as configuration databases or configuration templates.

Changes to configurations should follow the change management process (see 8.32).

Monitoring configurations

Configurations should be monitored with a comprehensive set of system management tools (e.g. maintenance utilities, remote support, enterprise management tools, backup and restore software) and should be reviewed on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed. Actual configurations can be compared with the defined target templates. Any deviations should be addressed, either by automatic enforcement of the defined target configuration or by manual analysis of the deviation followed by corrective actions.

Other information

Documentation for systems often records details about the configuration of both hardware and software.

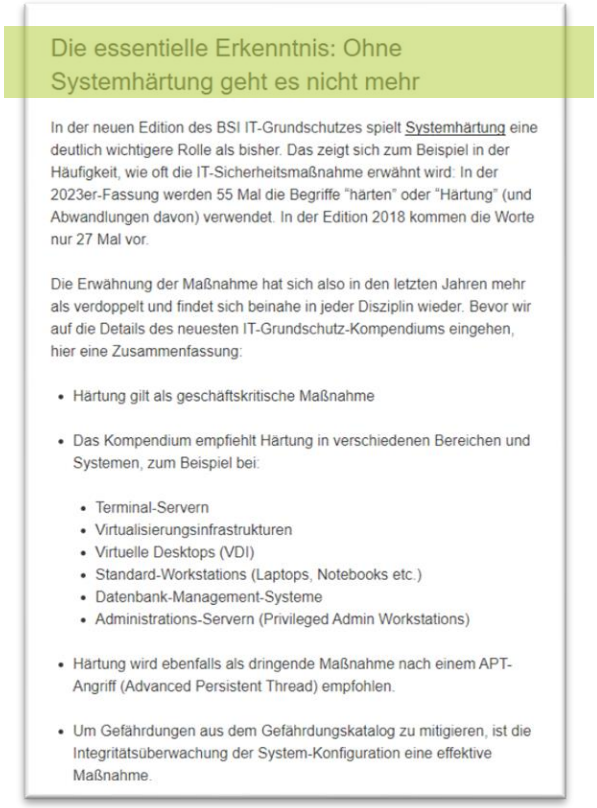
System hardening is a typical part of configuration management.

Configuration management can be integrated with asset management processes and associated tooling.

Automation is usually more effective to manage security configuration (e.g. using infrastructure as code).

Configuration templates and targets can be confidential information and should be protected from unauthorized access accordingly.

Vorgaben in Security-Frameworks: BSI IT-Grundschutz

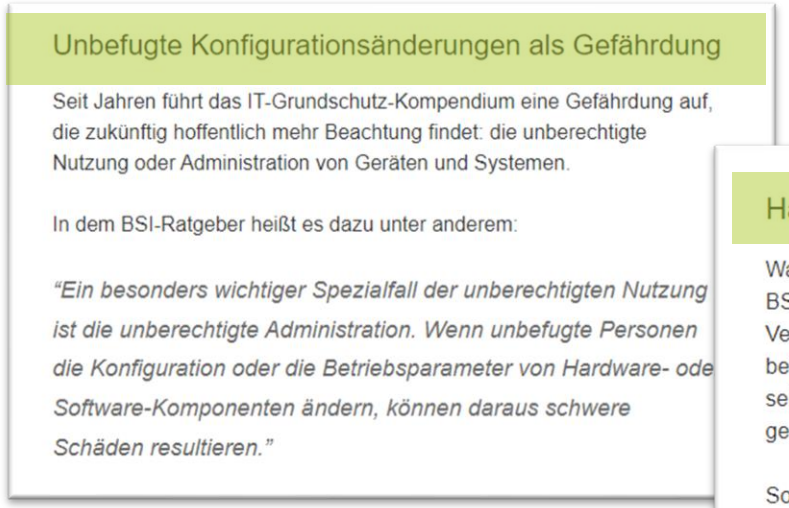


Die essentielle Erkenntnis: Ohne Systemhärtung geht es nicht mehr

In der neuen Edition des BSI IT-Grundschutzes spielt Systemhärtung eine deutlich wichtigere Rolle als bisher. Das zeigt sich zum Beispiel in der Häufigkeit, wie oft die IT-Sicherheitsmaßnahme erwähnt wird: In der 2023er-Fassung werden 55 Mal die Begriffe "härten" oder "Härtung" (und Abwandlungen davon) verwendet. In der Edition 2018 kommen die Worte nur 27 Mal vor.

Die Erwähnung der Maßnahme hat sich also in den letzten Jahren mehr als verdoppelt und findet sich beinahe in jeder Disziplin wieder. Bevor wir auf die Details des neuesten IT-Grundschutz-Kompendiums eingehen, hier eine Zusammenfassung:

- Härtung gilt als geschäftskritische Maßnahme
- Das Kompendium empfiehlt Härtung in verschiedenen Bereichen und Systemen, zum Beispiel bei:
  - Terminal-Servern
  - Virtualisierungsinfrastrukturen
  - Virtuelle Desktops (VDI)
  - Standard-Workstations (Laptops, Notebooks etc.)
  - Datenbank-Management-Systeme
  - Administrations-Servern (Privileged Admin Workstations)
- Härtung wird ebenfalls als dringende Maßnahme nach einem APT-Angriff (Advanced Persistent Thread) empfohlen.
- Um Gefährdungen aus dem Gefährdungskatalog zu mitigieren, ist die Integritätsüberwachung der System-Konfiguration eine effektive Maßnahme.

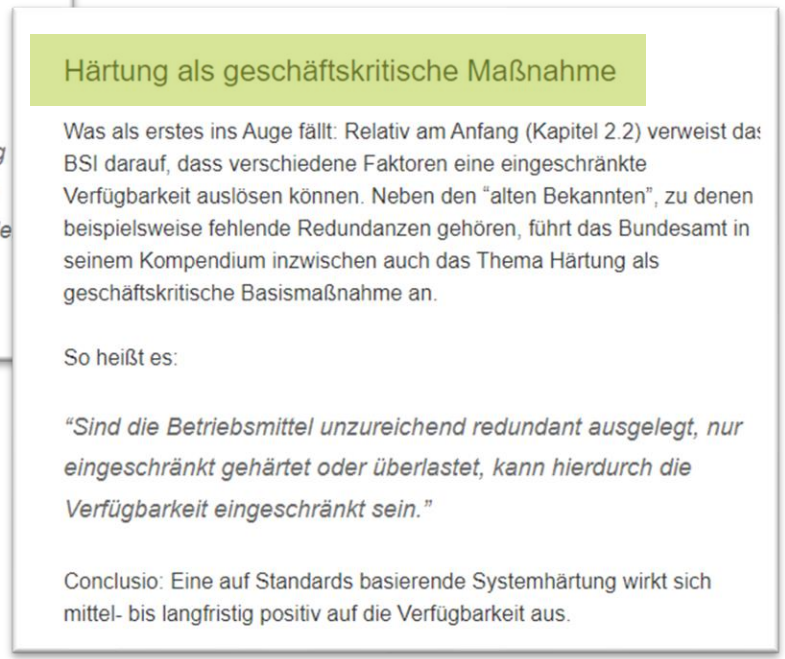


Unbefugte Konfigurationsänderungen als Gefährdung

Seit Jahren führt das IT-Grundschutz-Kompendium eine Gefährdung auf, die zukünftig hoffentlich mehr Beachtung findet: die unberechtigte Nutzung oder Administration von Geräten und Systemen.

In dem BSI-Ratgeber heißt es dazu unter anderem:

"Ein besonders wichtiger Spezialfall der unberechtigten Nutzung ist die unberechtigte Administration. Wenn unbefugte Personen die Konfiguration oder die Betriebsparameter von Hardware- ode Software-Komponenten ändern, können daraus schwere Schäden resultieren."



Härtung als geschäftskritische Maßnahme

Was als erstes ins Auge fällt: Relativ am Anfang (Kapitel 2.2) verweist das BSI darauf, dass verschiedene Faktoren eine eingeschränkte Verfügbarkeit auslösen können. Neben den "alten Bekannten", zu denen beispielsweise fehlende Redundanzen gehören, führt das Bundesamt in seinem Kompendium inzwischen auch das Thema Härtung als geschäftskritische Basismaßnahme an.

So heißt es:

"Sind die Betriebsmittel unzureichend redundant ausgelegt, nur eingeschränkt gehärtet oder überlastet, kann hierdurch die Verfügbarkeit eingeschränkt sein."

Conclusio: Eine auf Standards basierende Systemhärtung wirkt sich mittel- bis langfristig positiv auf die Verfügbarkeit aus.

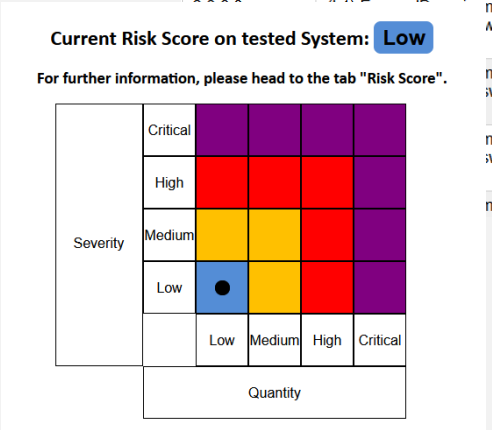
BSI IT-Grundschutz 2023: Was das aktuelle Kompendium zum Thema "Systemhärtung" empfiehlt - FB Pro GmbH (fb-pro.com)

Systemhärtung – Standardisiert

Beispiele für „Fehler“ und Konfigurationspunkte:

- Warum sind die XBOX-Dienste an?
- Warum kann jeder Anwender Drucker-Treiber installieren?
- Warum sind alte Protokolle (SMBv1, RC4, etc.) angeschaltet?
- Warum werden nur „Basisdinge“ protokolliert (Forensik?)
- Passworteinstellungen? Multifaktor-Authentisierung?
- Braucht man Bluetooth und die Kamera überall?
- Müssen Server vom Office-Rechner aus administriert werden?

Id	Task	Message	Status
1.1.6	(L1) Ensure 'Relax minimum password length limits' is set to 'Enabled'	Compliant	True
2.3.1.2	(L1) Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'	Compliant	True
2.3.1.4	(L1) Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'	Compliant	True
2.3.2.1	(L1) Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'	Compliant	True
2.3.2.2	(L1) Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	Compliant	True
2.3.4.1	(L1) Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators and Interactive Users'	Compliant	True
2.3.4.2	(L2) Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'	Compliant	True
2.3.6.1	(L1) Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'	Compliant	True
2.3.6.2	(L1) Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'	Compliant	True
	nember: Digitally sign when possible)' is set to	Compliant	True
	nember: Disable sword changes' is set to	Compliant	True
	nember: Maximum sword age' is set to '30 or	Compliant	True
	nember: Require strong	Compliant	True

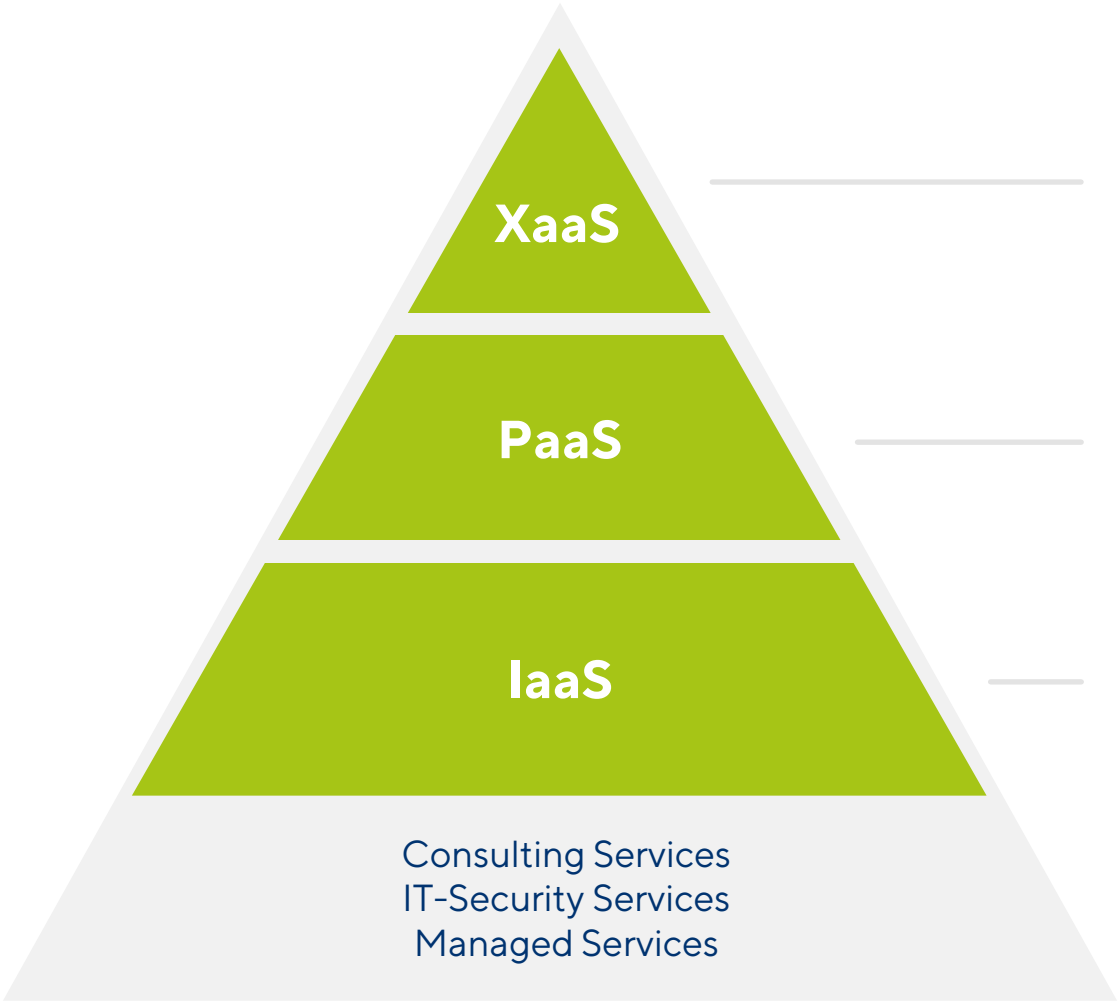


TWL KOM × FB PRO GMBH
System Hardening & Data Protection

TWL KOM × FB PRO GMBH
System Hardening & Data Protection

04
TWL-KOM Full-Service-IT

Unsere Full-Service-IT im Überblick



X as a Service
- Corporate IT Services
- User Help Desk Services

Platform as a Service
- Cloud Services
- Web & Hosting Services
- Backup Services

Infrastructure as a Service
- Datacenter Services
- WAN/LAN Services
- Business Internet Services

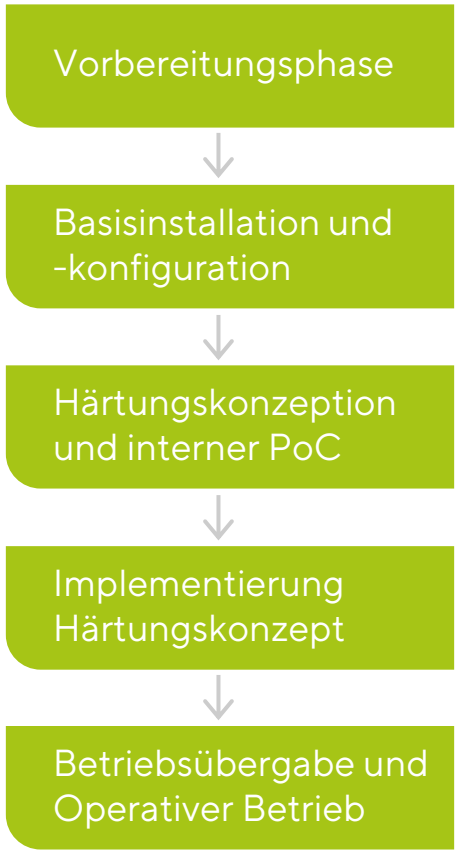
TWL KOM × FB PRO GMBH System Hardening & Data Protection

Cyber Security Solutions

- Security Architecture & Design
- Perimetersecurity
- System Hardening
- Patch Management
- Vulnerability Management
- E-Mail Security
- Mobile Device Management
- Awareness

Rollout durch TWL-KOM

TWL-KOM begleitet die 5 Rollout-Phasen



Vorteile

- Enge Zusammenarbeit zwischen Hersteller und Consulting
- Hochgradige Kompetenz im Projektgeschäft
- Erfahrungswerte im Bereich Systemhärtung
- Effiziente und saubere Integration in Ihre Umgebung

TWL KOM × FB PRO GMBH
System Hardening & Data Protection

Systemhardening-as-a-Service

Sicherheit

- Hardening als Maßnahme des BSI IT-Grundschutz
- Vorbereitend auf die Anforderungen von NIS II
- Unterstützungsleistungen bei Zertifizierungen

Vorteile

- Enge Zusammenarbeit mit dem Hersteller
- IT-Mitarbeiter des Kunden werden entlastet
- Erhebung und Verarbeitung KPI
- Lifecycle und kontinuierliche Optimierung (KVP)
- Synergien mit weiteren Managed Services
- Compliance und Rechtssicherheit

TWLKOM × FB PRO GMBH
System Hardening & Data Protection

05
Produkt-Demo

Produkt-Demo

TWLKOM × FB PRO GMBH
System Hardening & Data Protection

Sprechen Sie uns an, wenn Sie...

- sich auf ein **externes Audit (Nachweispflicht)** vorbereiten wollen/müssen.
- die **Angriffsfläche Ihrer IT-Systeme maximal reduzieren** wollen.
- **regulatorische Anforderungen** erfüllen müssen.
- ihr **Haftungsrisiko minimieren**, bzw. reduzieren wollen.
- umfänglich ein **Business Continuity Management planen** (z. B. NIS 2).
- **Schwachstellen** nicht verwaltet, sondern **verringert werden sollen.**
- **nach einem Cyber-Angriff** noch laufende Systeme **maximal absichern** wollen.
- ihre **Cyber-Versicherung** behalten/abschließen wollen.

TWLKOM × FB PRO GMBH
System Hardening & Data Protection

06
Fragen & Antworten

TWL KOM × FB PRO GMBH
System Hardening & Data Protection

Vielen Dank!

→ **Kontinuierlich geschützt durch Systemhärtung!**

TWL-KOM GmbH

Donnersbergweg 4

67059 Ludwigshafen

Telefon: 0621 669005 880

E-Mail: vertrieb@twl-kom.de

www.twl-kom.de