



20. Mai 2026

17. Bechtle
IT-Forum
Thüringen
Steigerwald Stadion Erfurt

20
26

IT-Sicherheit von kritischen Infrastrukturen stärken



Carsten Meerpohl
Services & Security Consultant, DSB, IT-SB
KYOCERA Document Solutions Deutschland GmbH

20.05.2026

Agenda

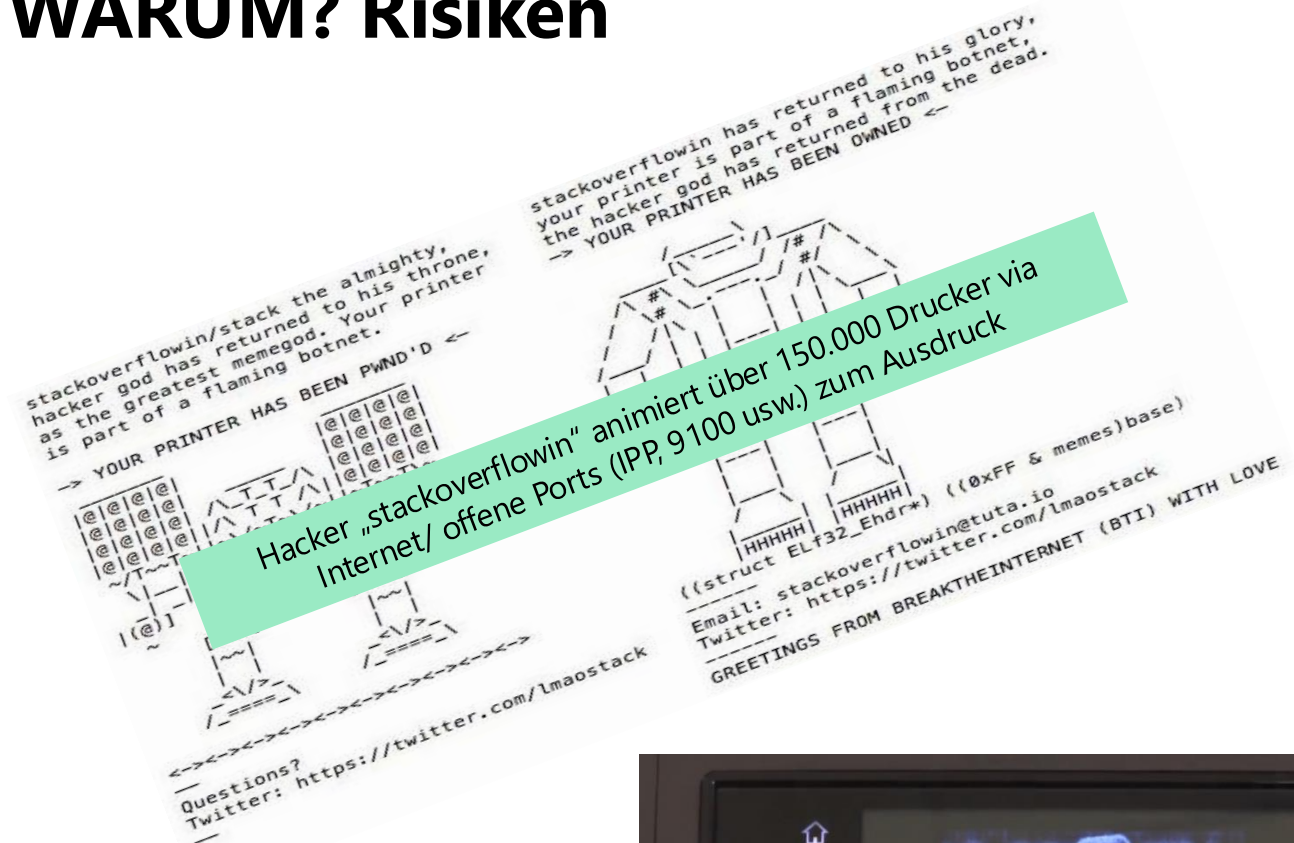
- 1. Einleitung**
- 2. NIS2, DORA, IT-SIG2.0 & Co.**
- 3. IT-Sicherheit & Datenschutz bei Druckern/ MFPs**
- 4. Sicherheitsfeatures, Checkliste**
- 5. Automatisierung**

Einleitung

Warum?
Zahlen, Daten, Fakten
Gesetze
Defizite
CRA & Co.



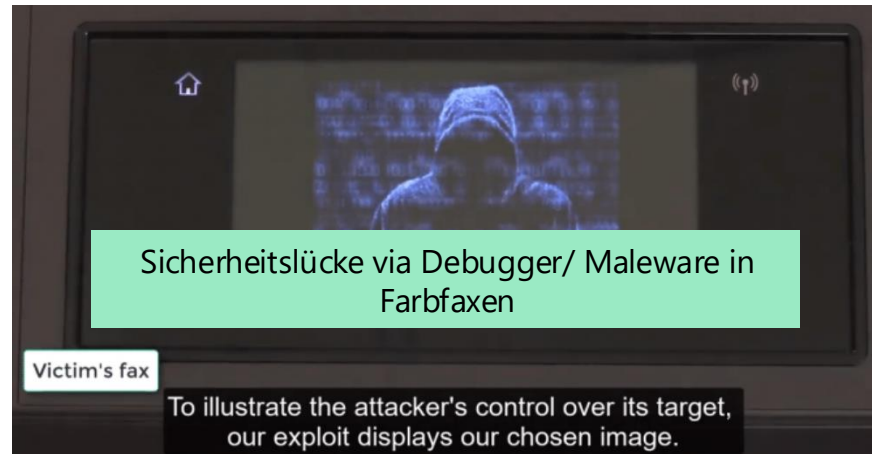
WARUM? Risiken



Hacker „stackoverflowin“ animiert über 150.000 Drucker via Internet/ offene Ports (IPP, 9100 usw.) zum Ausdruck



CPU Sicherheitslücken „Meltdown“ und „Spectre“ erfordern Firmware-Updates



Sicherheitslücke via Debugger/ Maleware in Farbfaxen

RUHR UNIVERSITÄT BOCHUM **RUB**

Printers / Printer Languages	Attack Categories		Print Job Manipulation		Information Disclosure				# Printer Vulnerabilities
	Attacks	PS	content overlay	content replacement	memory access	file system access	print job capture	credential disclosure	
9. Brother MFC-L8400CDN									9
10. Lexmark X264dn									9
11. Lexmark E360dn									10
12. Lexmark C736dn									10
13. Dell 5130cdn									6
14. Dell 1720n									11

PRET-Tool by RUB Bochum – Testen auch Sie die Möglichkeit von DoS und Co

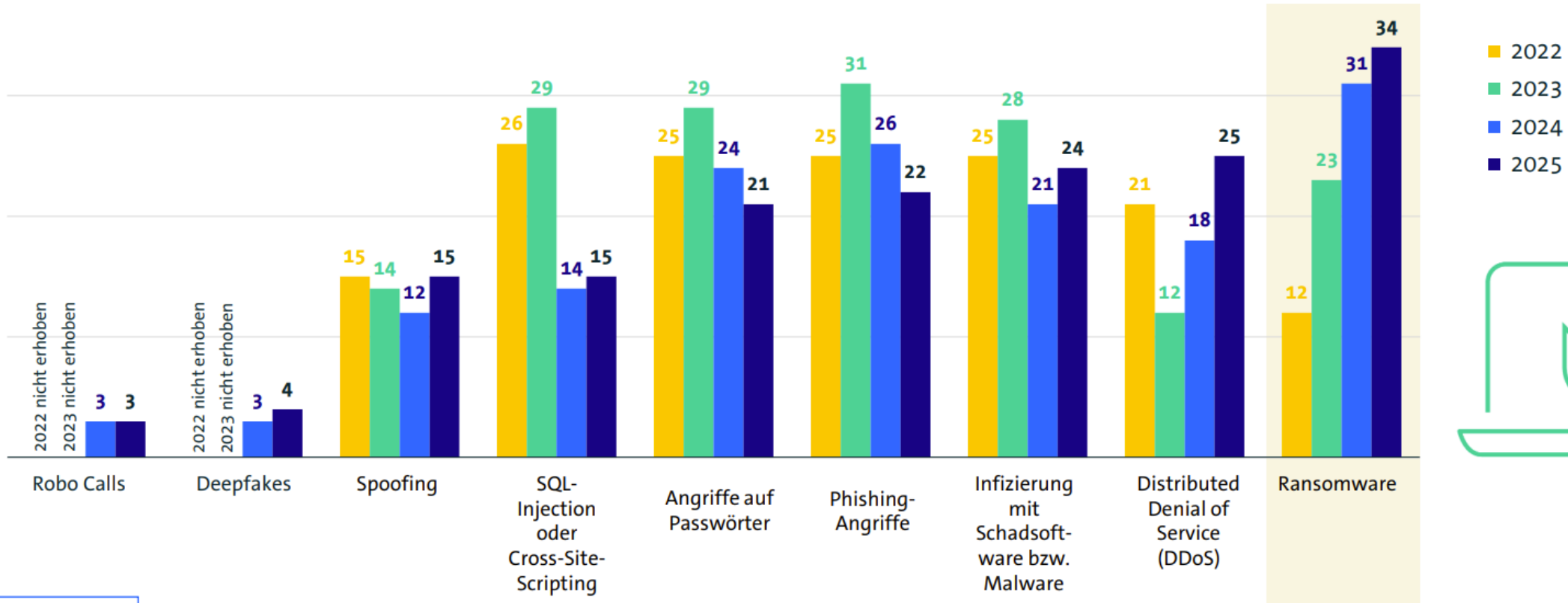
289 Milliarden Euro Schaden für die deutsche Wirtschaft

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2025)	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	73,3	54,5	35,0
Kosten für Rechtsstreitigkeiten	53,0	53,1	29,8
Kosten für Ermittlungen und Ersatzmaßnahmen	37,0	32,2	25,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	30,6	39,2	15,3
Datenschutzrechtliche Maßnahmen, z.B. durch Behörden	23,8	27,2	12,4
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	23,1	11,2	21,5
Patentrechtsverletzungen, auch vor Anmeldung	16,0	14,8	10,4
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	15,9	20,2	35,3
Erpressung mit gestohlenen Daten	15,6	13,4	16,1
Geldabfluss durch Betrugsversuche	0,9	0,8	3,9
Sonstige Schäden	0	0	1,1
Gesamtschaden pro Jahr	289,2	266,6	205,9

Ransomware verursacht am häufigsten Schäden

Welche der folgenden Arten von Cyberangriffen haben innerhalb der letzten 12 Monate in Ihrem Unternehmen einen Schaden verursacht?



in Prozent

DEFIZITE BEI DER CYBERSICHERHEIT IN KRITISCHEN SEKTOREN

Unvollständige Risikoanalyse und unzureichende Sicherheitsmaßnahmen

Mängel im Identitäts- und Zugangsmanagement

Schwächen bei der Erkennung und Meldung von Sicherheitsvorfällen

Defizite bei der Reaktion auf Cyberangriffe

Probleme bei der Umsetzung von Resilienzmaßnahmen

Unvollständige IT-Assetübersichten und Sicherheitsarchitektur

Schwachstellen in der physischen und digitalen Sicherheitsarchitektur

Fehlende Cyber-Abwehrmechanismen

Defizite bei Notfall- und Krisenmanagementplänen

Probleme bei der Erfüllung gesetzlicher Vorschriften

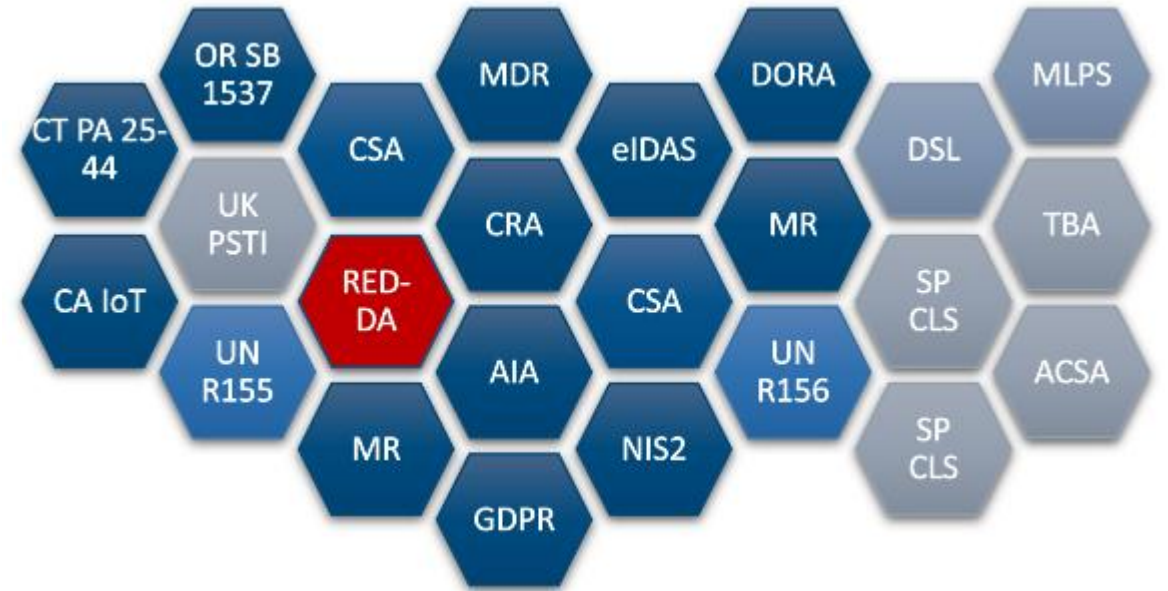
European Cyber Resilience Act (CRA)

• Europäische Union (EU)

- (EU) 2022/30 RED Delegated Act (**RED-DA**)
- (EU) 2019/881 Cybersecurity Act (**CSA**) incl. CSA2 proposal (2026)
- (EU) 2024/1183 European Digital Identity Framework (**eIDAS**)
- (EU) 2022/2554 Digital Operational Resilience Act (**DORA**)
- (EU) 2016/679 General Data Protection Regulation (**GDPR**)
- (EU) 2024/1689 Artificial Intelligence Act (**AIA**)
- (EU) 2023/1230 Machinery Regulation (**MR**)
- (EU) 2017/745 Medical Device Regulation (**MDR**)
- (EU) 2022/2555 Network Infrastructure Security (**NIS2**)

• Weltweit (Non-EU)

- UK Product Security and Telecoms Infrastructure Act (**UK PSTI**)
- UNECE Vehicle Cybersecurity (**UNECE 155/156**)
- US States IoT Security Laws (**CA IoT, OR SB 1537, CT PA 25-44**)
- CN Multi-Level Protection (MLPS) & Data Security Law (**DSL**)
- Australian Cybersecurity Act (**ACSA**)
- Singapore Cybersecurity Labeling Scheme (**CLS**)
- Japan Telecommunications Business Act IoT Amendments (**TBA**)



NIS2, DORA, IT-SIG2.0, BSI & Co.

Warum?
Zahlen, Daten, Fakten



Gesetzliche Anforderungen: Überblick

EU-DSGVO & BDSG: Datenschutz, Nachvollziehbarkeit und Rechenschaftspflicht

IT-SiG 2.0 & NIS2: Gesetzliche Grundlage für Betreiber kritischer Infrastrukturen und EU-weite Vorgaben für Cybersicherheitsanforderungen in Unternehmen und öffentlichen Einrichtungen

DORA: EU-Regulierung zur digitalen operativen Resilienz im Finanzsektor

BSI IT-Grundschutz: Deutsches Standard- und Methodenset für Informationssicherheits-Managementssysteme (ISMS)



GDPR

GENERAL DATA PROTECTION REGULATION

Gesetzliche Anforderungen: Überblick

EU-DSGVO & BDSG: Erfordern Datenschutz-Management, Dokumentation, Risikobewertungen, technische & organisatorische Maßnahmen (TOMs).

IT-SiG 2.0 & NIS2: Erweiterter Anwendungsbereich (18 Sektoren), verschärfte Sanktionen, Verpflichtung zu Angriffserkennungssystemen & Resilienztests.

DORA: Regelt einheitliche Anforderungen an ICT-Risiken, Berichterstattung, Drittanbieter-Risiken und Resilienz im Finanzsektor.

BSI IT-Grundschutz: Ganzheitlicher Ansatz (technisch, personell, organisatorisch, infrastrukturell) für Unternehmen in Deutschland.



NETZWERKSPEZIFISCHE ARTIKEL DER REGULIERUNGEN

Erkennung & Reaktion auf Bedrohungen in Echtzeit:

- NIS2 Art. 21
- DORA Art. 5
- KRITIS/BSI IT-Sicherheitsgesetz §8a

Zero Trust Architektur für Netzwerksicherheit:

- NIS2 Art. 20
- DORA Art. 6
- SzA nach BSI

Kontinuierliches Monitoring & Logging für Transparenz:

- NIS2 Art. 22
- DORA Art. 11
- KRITIS-Anforderung

Regelmässige digitale Resilienztest, inkl. TLPT:

- DORA Art. 11

NIS2-RL: ANWENDUNGSBEREICHE

Neuer erweiterter Anwendungsbereich der NIS2-RL:

Die NIS2-RL weitet den bisherigen Anwendungsbereich deutlich aus und erstreckt sich nun auf 18 Sektoren, sowohl im öffentlichen als auch im privaten Bereich. Durch die umfassendere Definition des Anwendungsbereichs obliegt die Festlegung relevanter Sektoren nicht mehr den Mitgliedstaaten, die Schwellenwerte der deutschen BSI-Kritisverordnung dürften daher bald Geschichte sein.

NIS1-RL/BSI-KRITISVERORDNUNG	NIS2-RL
Energie	Energie
Wasser	Trinkwasser, Abwasser
Ernährung	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Informationstechnik und Telekommunikation	Digitale Infrastruktur
Gesundheit	Gesundheitswesen
Finanz- und Versicherungswesen	Bankwesen, Finanzmarktinfrastrukturen
Transport/Verkehr	Verkehr, Weltraum (teilweise), Post- und Kurierdienste,
Entsorgung	Abfallbewirtschaftung
	Verwaltung von IKT-Diensten (B2B)
	Öffentliche Verwaltung
	Produktion, Herstellung und Handel mit chemischen Stoffen
	Verarbeitendes Gewerbe/Herstellung von Waren
	Anbieter digitaler Dienste
	Forschung

NIS2-RL: WESENTLICHE UND WICHTIGE EINRICHTUNGEN

Wesentliche und wichtige Einrichtungen:

Der Anwendungsbereich der NIS2-RL erstreckt sich im Grundsatz nur auf Einrichtungen, die folgende Schwellenwerte überschreiten: Mindestens 50 Beschäftigte oder über 10 Mio. EUR Jahresumsatz bzw. Jahresbilanzsumme. In bestimmten Fällen (z.B. bei Anbietern von öffentlich zugänglichen elektronischen Kommunikationsdiensten) greift die NIS2-Richtlinie auch unabhängig von der Größe.

Ihre Verpflichtungen knüpft die NIS2-RL überwiegend an die Klassifizierung eines Betreibers als „wesentliche“ oder „wichtige“ Einrichtung.

WESENTLICHE EINRICHTUNG	WICHTIGE EINRICHTUNG
<p>Sektor in Anhang I + mind. 250 Beschäftigte oder über 50 Mio. EUR Jahresumsatz bzw. über 43 Mio. EUR Jahresbilanzsumme</p>	<p>Sektoren in Anhang I u. II + mind. 50 Beschäftigte oder über 10 Mio. EUR Jahresumsatz bzw. Jahresbilanzsumme (soweit nicht bereits wesentliche Einrichtungen)</p>
<p>bestimmte Sonderfälle, z.B. Zentralregierung, DNS-Diensteanbieter oder staatliche Einstufung als wesentliche Einrichtung</p>	<p>bestimmte größenunabhängige Sonderfälle, z.B. staatliche Einstufung als wichtige Einrichtung</p>

NIS2-RL SANKTIONEN BEI VERSTÖßEN

Sanktionen bei Verstößen:

Die NIS2-RL erlegt den EU-Mitgliedstaaten die Pflicht auf, Bußgeldtatbestände für Verstöße gegen Art. 21 (Risikomanagementmaßnahmen, s.o.) und Art. 23 NIS2-RL (Berichtspflichten über erhebliche Sicherheitsvorfälle) zu schaffen. Gleichzeitig legt die NIS2-RL bereits einen Mindestwert für die obere Grenze des Bußgeldrahmens fest:

WESENTLICHE EINRICHTUNGEN	WICHTIGE EINRICHTUNGEN
Geldbuße bis zu: 10 Mio. EUR oder 2 % des gesamten weltweiten Vorjahresumsatzes des Unternehmens, dem die Einrichtung angehört	Geldbuße bis zu: 7 Mio. EUR oder 1,4 % des gesamten weltweiten Vorjahresumsatzes des Unternehmens, dem die Einrichtung angehört

NIS2-RL: ERGREIFEN GEEIGNETER MAßNAHMEN

Policies:

Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme

Incident Management:

Bewältigung von Sicherheitsvorfällen

Schulungen:

grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit

Supply Chain:

Sicherheit der Lieferkette einschl. sicherheitsbezogener Aspekte zwischen den einzelnen Einrichtungen und ihren Anbietern

Weitere organisatorische Maßnahmen:

Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen

Business Continuity:

Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement

Einkauf:

Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschl. Mgmt. und Offenlegung von Schwachstellen

Verschlüsselung:

Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung

Effektivität:

Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit

Weitere technische Maßnahmen:

Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung, gesicherte Kommunikation, gesicherte Notfallkommunikationssysteme

DORA: ANWENDUNGSBEREICHE

Digital Operational Resilience Act

Die DORA-Verordnung gilt für alle wesentlichen Finanzmarktteilnehmer innerhalb des Binnenmarkts der Europäischen Union, einschließlich Banken, Versicherungsunternehmen, Investmentfirmen und Zahlungsdienstleister.

Des Weiteren beinhaltet DORA Maßnahmen für relevante Drittanbieter von Informations- und Kommunikationstechnologie-Dienstleistungen (IKT-Dienstleister) innerhalb und außerhalb der EU, die kritische Dienste für den EU-Finanzmarkt bereitstellen.

DORA: WESENTLICHE NEUERUNGEN

**Spezifische Fokussierung auf den
Finanzsektor**

**Verbindliche Berichtspflichten und
Resilienztests**

Managementverantwortung

**Harmonisierung der Anforderungen
auf EU-Ebene:**

Regulierung kritischer Drittdienstleister

Überwachung und Compliance:

BSI IT-Grundschutz

IT-Grundschutz-Kompendium – Werkzeug für Informationssicherheit

Edition 2023

IT-Grundschutz-Kompendium (Edition 2023)

Das IT-Grundschutz-Kompendium Edition 2023 ist seit dem 1. Februar 2023 verfügbar und löst damit die Edition 2022 ab.

Download: [↓ Gesamt-PDF des IT-Grundschutz-Kompendiums \(Edition 2023\)](#)

BAUSTEIN SYS.4.1

DRUCKER, KOPIERER UND MULTIFUNKTIONSGERÄTE

Basis-Anforderungen

SYS.4.1.A1 Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten (B)

SYS.4.1.A2 Geeignete Aufstellung und Zugriff auf Drucker, Kopierer und Multifunktionsgeräte (B)

SYS.4.1.A22 Ordnungsgemäße Entsorgung ausgedruckter Dokumente (B)

Standard-Anforderungen

SYS.4.1.A4 Erstellung einer Sicherheitsrichtlinie für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten (S)

SYS.4.1.A5 Erstellung von Nutzungsrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten (S)

[Informationssicherheitsbeauftragte (ISB)]

SYS.4.1.A7 Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte (S)

SYS.4.1.A11 Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten (S)

SYS.4.1.A15 Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (S)

SYS.4.1.A17 Schutz von Nutz- und Metadaten (S)

SYS.4.1.A18 Konfiguration von Druckern, Kopierern und Multifunktionsgeräten (S)

Anforderungen bei erhöhtem Schutzbedarf

SYS.4.1.A14 Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten (H)

SYS.4.1.A16 Verringerung von Ausfallzeiten bei Druckern, Kopierern und Multifunktionsgeräten (H)

SYS.4.1.A20 Erweiterter Schutz von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (H)

SYS.4.1.A21 Erweiterte Absicherung von Druckern, Kopierern und Multifunktionsgeräten (H)

IT-Sicherheit & Datenschutz bei Druckern/ MFPs

Differenzierung
Datenschutz
IT-Sicherheit/ Informationssicherheit



Differenzierung

IT Sicherheit/ Informationssicherheit:

- Beschäftigt sich mit der „Sicherheit“ Ihres Unternehmens
- Sie wollen Ihr Unternehmen schützen vor „Angreifern“
- In der Regel durch technische und organisatorische Maßnahmen, z.B. Firewall, Sicherheitseinstellungen, Schlösser, Authentifizierung usw.

Datenschutz:

- Beschäftigt sich mit dem Schutz „personenbezogener Daten“
- Ihr Unternehmen ist also der „Angreifer“
- Hauptsächlich durch Compliance, Richtlinien, definierte Prozesse, Verzeichnis der Verfahren, Risikobewertung und o.g. IT Sicherheit

DATENSCHUTZ – EIN INTEGRATIVES ZIEL



**Netzwerk-
sicherheit**
Schutz der
Daten im Netzwerk

**Geräte-
sicherheit**
Schutz der
Daten im Drucker

**Benutzer-
sicherheit**
Schutz der
Ausdrucke

**Dokumenten-
sicherheit**
Schutz der
Dokumente

SICHERHEIT NETZWERK

- Schützen Sie Ihre Daten, die über das Netzwerk übertragen werden.
- Kommunikationskanäle schützen
 - SNMPv3, IPSec, TLS/SSL
- Authentifizierungsprotokolle
 - IEEE802.1x, SMTP, POP before SMTP
- Protokolle/ Ports prüfen/ schützen
- Firewall-Schutz?

Netzwerk-
sicherheit



SICHERHEIT NETZWERK

Schützen Sie Ihre Druckjobs vor externen Zugriffen und Angriffen.

- Nutzungsbeschränkungen einrichten
 - Schnittstellen/ Bedienfeld sperren, logische Sperre bei USB-Speicher
- Standard Passwörter ändern
 - CommandCenter, Maintenance Menü
- Benutzerauthentifizierung verwenden
 - Lokale-/ Netzwerk- (NTLM/ Kerberos) Authentifizierung

Geräte-
sicherheit



SICHERHEIT BENUTZER

➤ Schützen Sie Ihre Ausdrücke vor unbefugten Personen.

➤ Nutzer-Authentifizierung sichert Zugriff durch autorisierte Benutzer

➤ Kein Einscannen oder Versenden von Dokumenten durch Unberechtigte

➤ Vertraulicher Druck durch Print & Follow Funktionalität

Benutzer-
sicherheit



SICHERHEIT DOKUMENTE

- Schützen Sie vertrauliche Dokumente
 - Sicherer Druck durch Authentifizierung
 - E-MPS Auftragspeicher nutzen
 - Privater Druck & Boxen
 - Sicherheitswasserzeichen & Textstempel

Dokumenten-
sicherheit



Sicherheitsfeatures

Standard Sicherheitsfeatures
Checkliste sichere Konfiguration



STANDARDS IN KYOCERA GERÄTEN

KYOCERA STANDARD HARDWARE SICHERHEIT

- Abwehr DoS Angriffe
- Gehärtetes Linux Derivat
- Signierte und zertifizierte Firmware
- SIEM Support
- Trusted Plattform Module (TPM)
- Secure Boot
- Run-time-Integrity Check
- SCEP Support/ OCSP/ CRL (Zertifikatsverteilung)
- Verschlüsseln/Löschen/Überschreiben
- IP-Filter, Command Center
- Manuelle und automatische Löschprozesse (Data-Security-Kit onboard)
- Common Criteria Zertifizierung (ISO 15408)
- EAL Level Konformität und Validierung (IEEE 2600.x)
- Allowlistening
- S/MIME (Secure / Multipurpose Internet Mail Extensions)
- Individuelle Passwörter (CCRX, Device Admin, MM)

TPM, RTIC & Secure Boot

Data Security Kit Standard
(DSK)

- Löschung DoD 5220.22-M (E) -
- Verschlüsselung mit AES-256Bit
- ISO/IEC 15408 Common Criteria EAL2
- IEEE 2600.2

Trusted Platform Module
(TPM)

- Speichert verschlüsselt Infos über verwendete Hardware und Software
- Basis für SIEM und RTIC & Secure Boot
- Verwaltet Verschlüsselungs-Keys

Run Time Integrity Check
(RTIC)

- Prüft Validität der Firmware im Betrieb an Hand der digitalen Signatur
- meldet Fehler/ System wird angehalten

Secure Boot

- Prüft Validität der Firmware beim Start an Hand der digitalen Signatur
- meldet Fehler/ Start wird unterbrochen

Security Information and Event
Management (SIEM)



CHECKLISTE "SICHERE KONFIGURATION"

- **Datum/Uhrzeit** einstellen – besser Zeitserver eintragen
- **Standard Passwörter** (Admin/Admin, Maintenance Mode Code usw.) ändern
- **Authentifizierung** (Lokale- oder Netzwerk-) aktivieren – besser Print & Follow einsetzen
- **Rücksetztimer** Bedienfeld setzen, Zeitspanne für automatisches Löschen setzen
- **Unsichere Protokolle** deaktivieren, nur sichere Protokolle nutzen
- **SSL** aktivieren und auf Protokolle anwenden, nur aktuelle TLS-Versionen, Verschlüsselungen und Hashs nutzen
- **DSK** aktivieren/ registrieren und konfigurieren
- **LDAP** anbinden/ nutzen, keine lokalen Adressbücher verwenden
- **Protokolle** Anzeige Status/Protokolle anzeigen konfigurieren
- **Zertifikate** nutzen (CA/ SCEP usw.)
- **Flotten-Management** nutzen zur Sicherstellung "Versorgung der Geräte mit Verbrauchsmaterial"
- **Flotten-Management** nutzen für Remote Services (Firmware Updates, Einstellungen usw.)



Automatisierung

Security Consulting
AKI PrinTaurus Security Suite

27.05.2026



Nutzung von Sicherheitstools

Professionelle Tools unterstützen die technische Umsetzung – aber: Sie entfalten nur mit Beratung ihr volles Potenzial. Beispielhafte Tools:

- **AKI PrinTaurus Security Suite**
- **HP Security Manager**
- **TA Cockpit Red**
- **u.v.m.**

Einfaches Deployment ohne strategische Beratung reicht nicht – Planung, Integration und Betrieb sind Schlüsselemente.

AKI PrinTaurus Security Suite

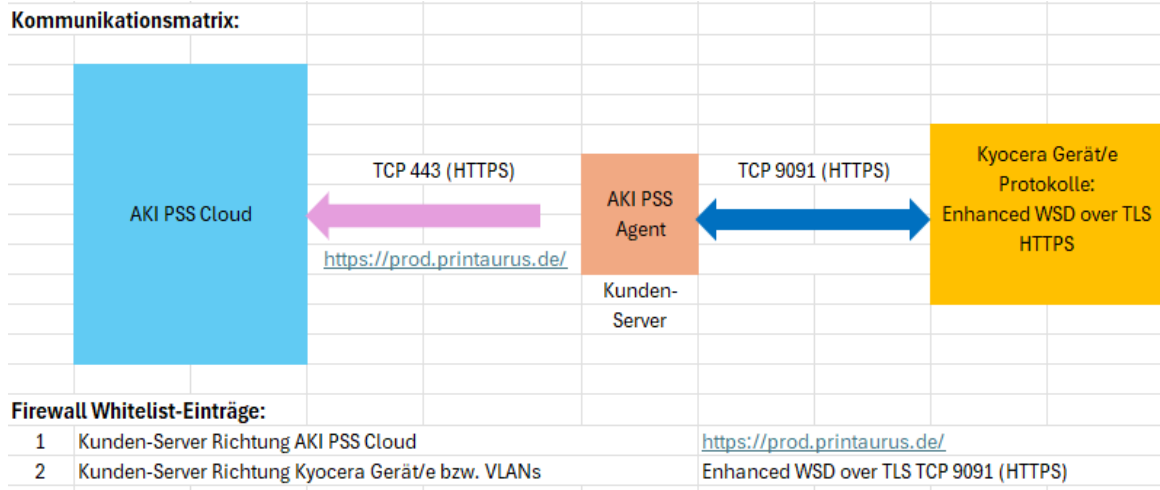
- **Definition von Richtlinien für die Sicherheitseinstellungen der Drucksysteme**
- **Die sicherheitsrelevanten Einstellungen der Drucksysteme werden in vorgegebenen Intervallen überprüft und automatisch berichtigt**
- **Dashboard zur Übersicht über den Sicherheitsstatus der Drucksysteme**
- **Erstellung von Reports über die Prüfung und Korrektur der Einstellungen**



PrinTaurus Security Suite

Druckinfrastruktur auf höchstem Sicherheitsniveau

Security im Daily Business



Printaurus Cloud - Carsten seine Firma

NETZWERKSCANS: 3 | GEFUNDENE GERÄTE: 75 | KONFORME GERÄTE: 2 | WARNUNGEN: 10 | UNSICHERE GERÄTE: 63

Netzwerkscans

Gesellschaft	Name	Benutzername	Start-Adresse	End-Adresse	Template	Letzter Scan	Gefundene Geräte	Konforme Geräte
Carsten seine Firma								
Carsten seine Firma	CsF Scan 1	Admin	172.17.233.1	172.17.233.255	CsF Vorlage 1	15.03.2026 23:05:43	76	1
Carsten seine Firma	Testscan auf 172.17.233.20	Admin	172.17.233.20	172.17.233.20	CsF Vorlage 1	15.03.2026 23:55:05	1	—
Carsten seine Firma	Testscan auf 172.17.233.78	Admin	172.17.233.78	172.17.233.78	CsF Vorlage 1	15.03.2026 23:55:08	1	1

Buttons: + Neu, Bearbeiten, Löschen, Filter löschen | Page: 1 | 100 Zeilen pro Seite | Zeilen 1 - 3 von 3

Cloud-Version: Mandantenfähige Lösung zur Verwaltung der Sicherheitseinstellungen der Drucksysteme über das Internet.

On-Premises-Version: Lokale Installation zur Verwaltung der Sicherheitseinstellungen der Drucksysteme im Unternehmensnetzwerk. (Verfügbar ab Q2/2026)

Security Consulting

In einer digitalisierten Wirtschaft wird IT-Sicherheit zum zentralen Erfolgsfaktor.

Unternehmen investieren verstärkt in Sicherheitslösungen – jedoch ist die technische Implementierung ohne strategisches Security Consulting oft ineffektiv oder sogar riskant.

Security Consulting verbindet Technik, Compliance und Strategie – und schafft dadurch wirtschaftlichen Mehrwert.



KYOCERA Document Solutions Deutschland GmbH
Otto-Hahn-Straße 12
40670 Meerbusch

Carsten Meerpohl
Services Consultant/ DSB

Telefon: +49(0)160/95138933
Carsten.Meerpohl@dde.kyocera.com

<https://www.kyoceradocumentsolutions.de/>
<https://kyocera.blog/>



<https://smart.kyoceradocumentsolutions.de/>

