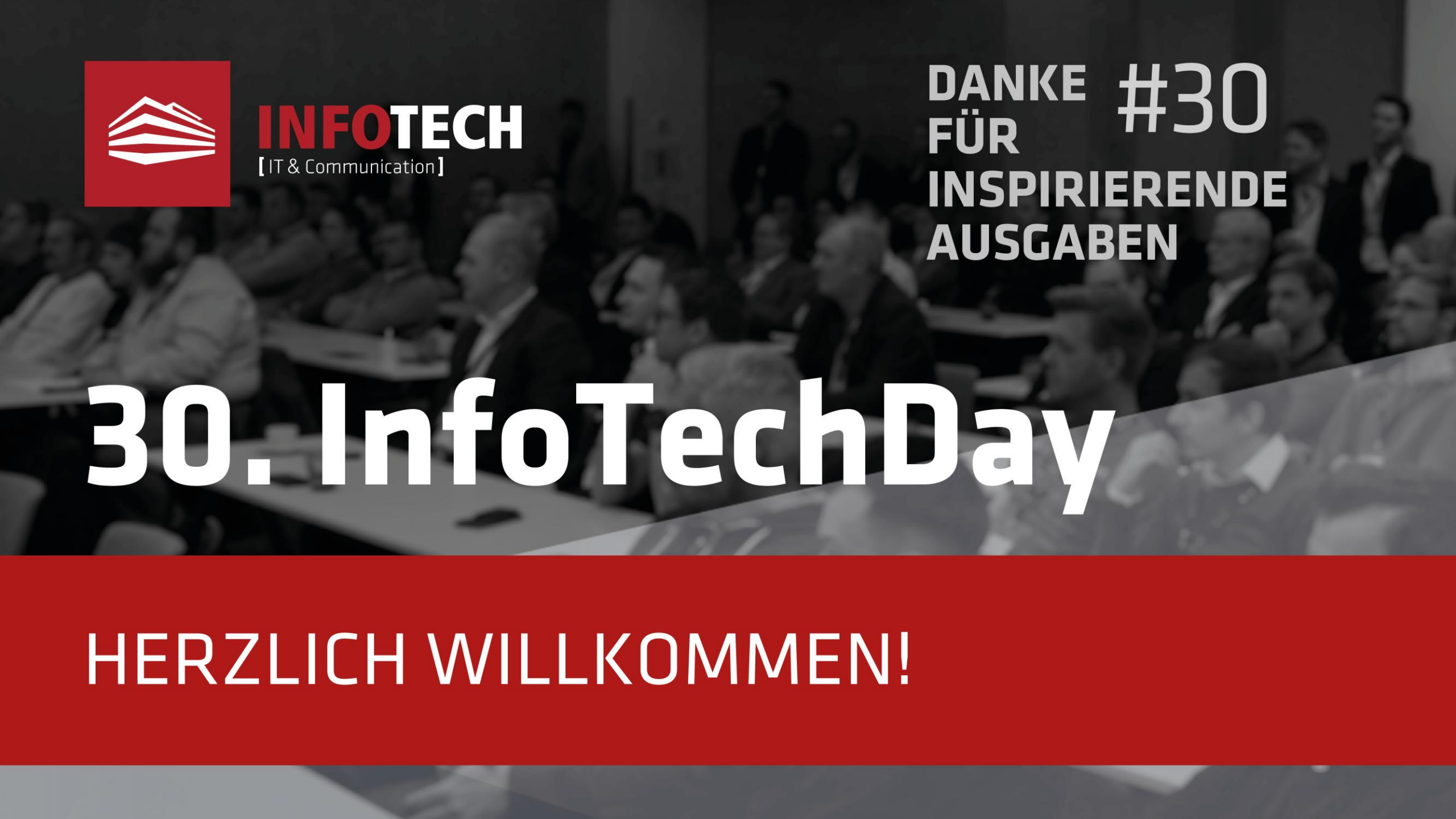

INFOTECH
[IT & Communication]
DANKE #30
FÜR
INSPIRIERENDE
AUSGABEN
30. InfoTechDay
HERZLICH WILLKOMMEN!

INFOTECH
[IT & Communication]

Digitale Verteidigung in unsicheren Zeiten

Strategien für Sicherheit und Souveränität

IHR IT-SYSTEMHAUS.

Michael Eder
Martin Mallinger

Aktuelles Lagebild

INFOTECH
[IT & Communication]

- Weil jede Präsentation ein KI-generiertes Bild benötigt

Quelle: ChatGPT / KI generiert

Aktuelles Lagebild

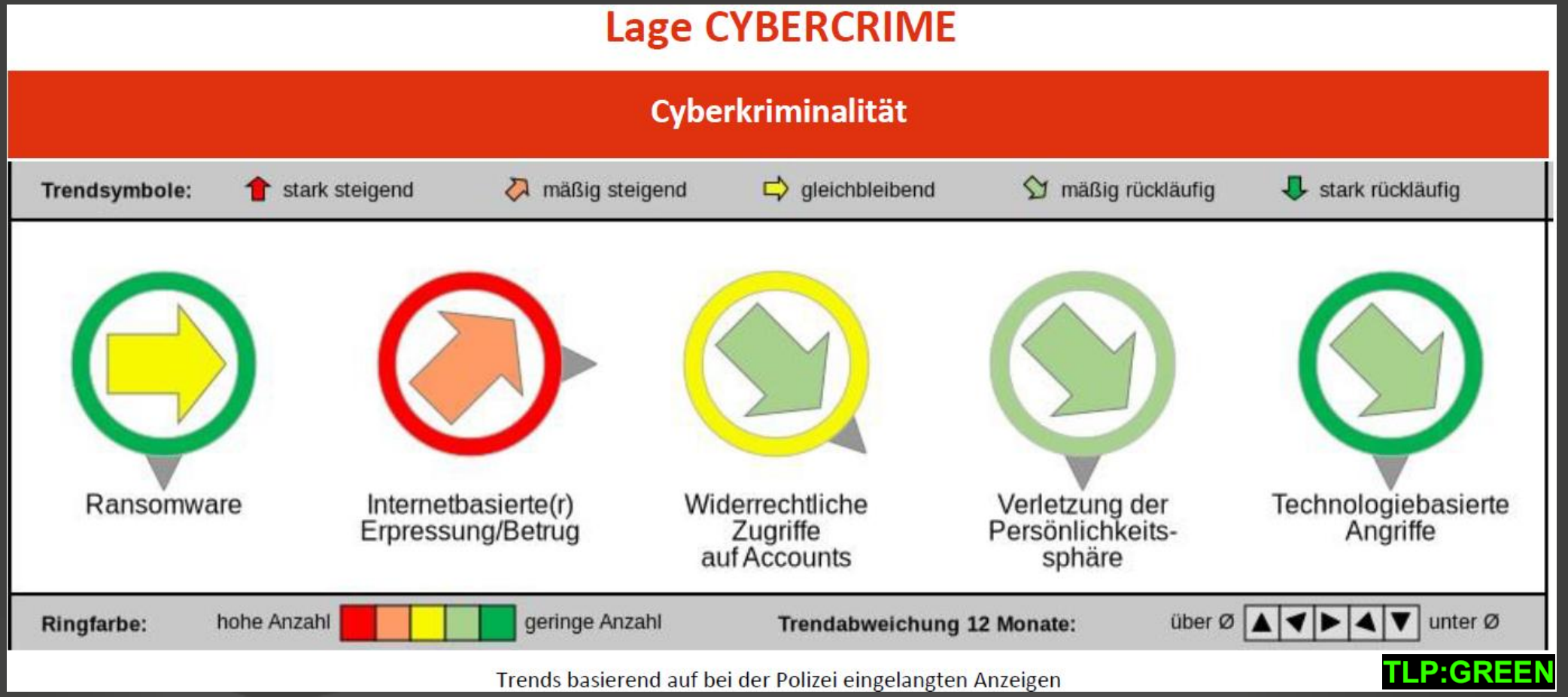
INFOTECH
【IT & Communication】

Was i

Quelle: Copilot / KI generiert

Aktuelles Lagebild

INFOTECH
[IT & Communication]

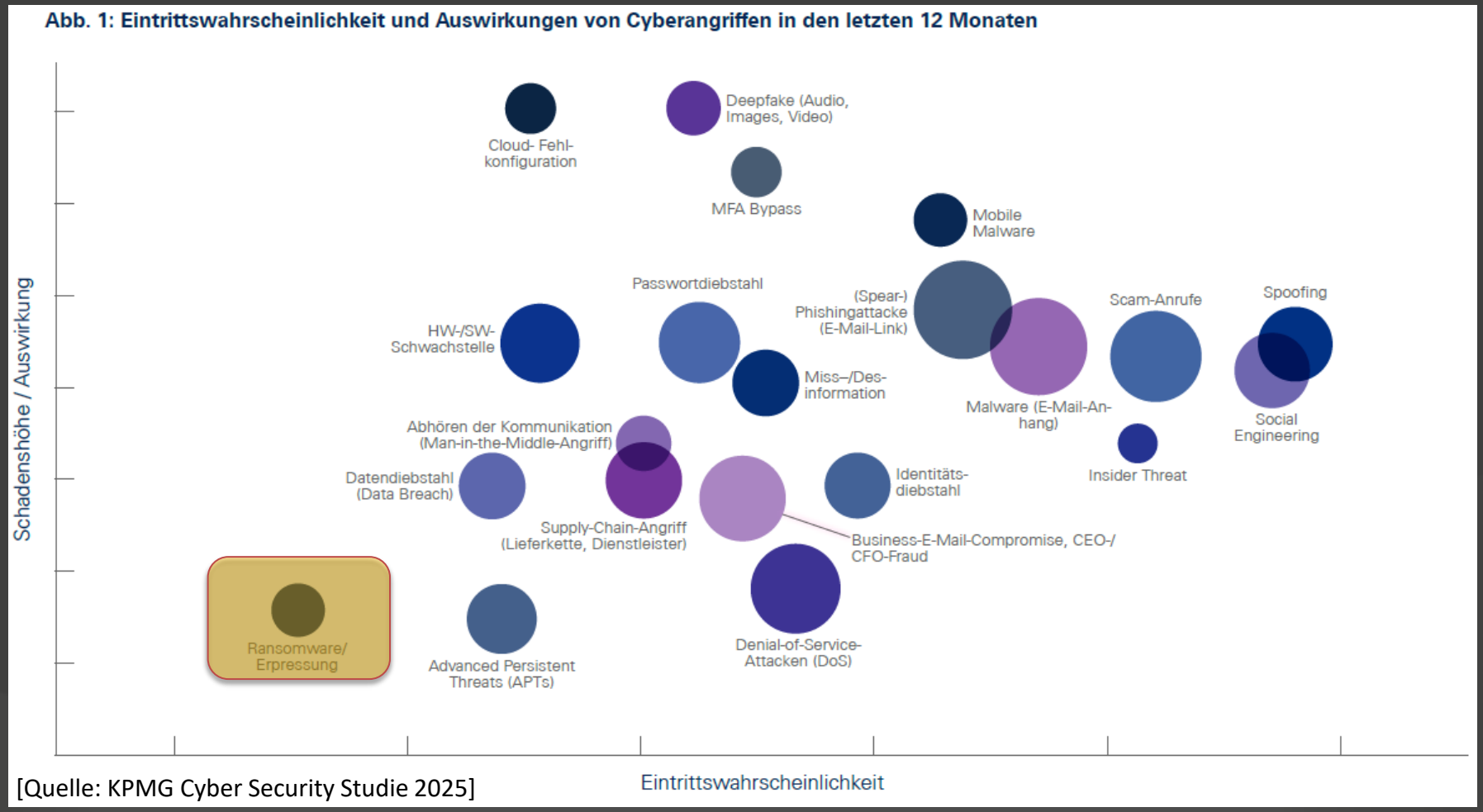


[Quelle: IKDOK OpKoord Lagebild 09/2025]

Aktuelles Lagebild

INFOTECH
[IT & Communication]

Abb. 1: Eintrittswahrscheinlichkeit und Auswirkungen von Cyberangriffen in den letzten 12 Monaten

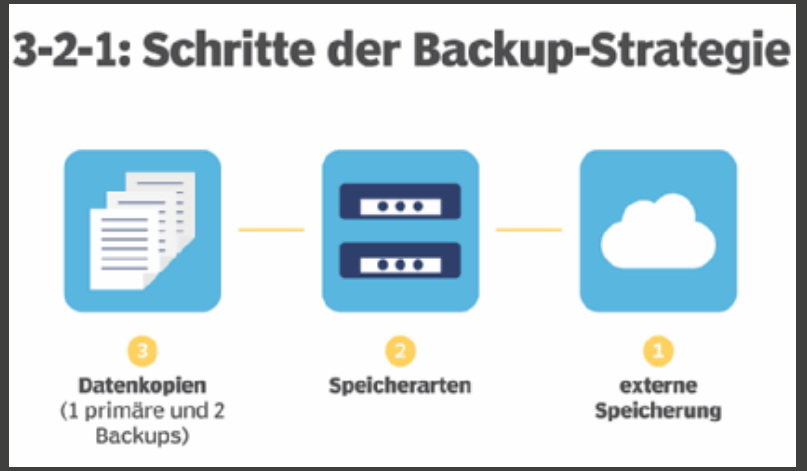


[Quelle: KPMG Cyber Security Studie 2025]

Backup als organisatorisches Thema

INFOTECH
[IT & Communication]

- **Durchführung der Backups + Job Kontrolle**
  - Verteilung der Backups auf mehrere Standorte
  - Tägliche Kontrolle der Jobs durch Alerts
  - Wöchentliche Kontrolle durch einen Admin

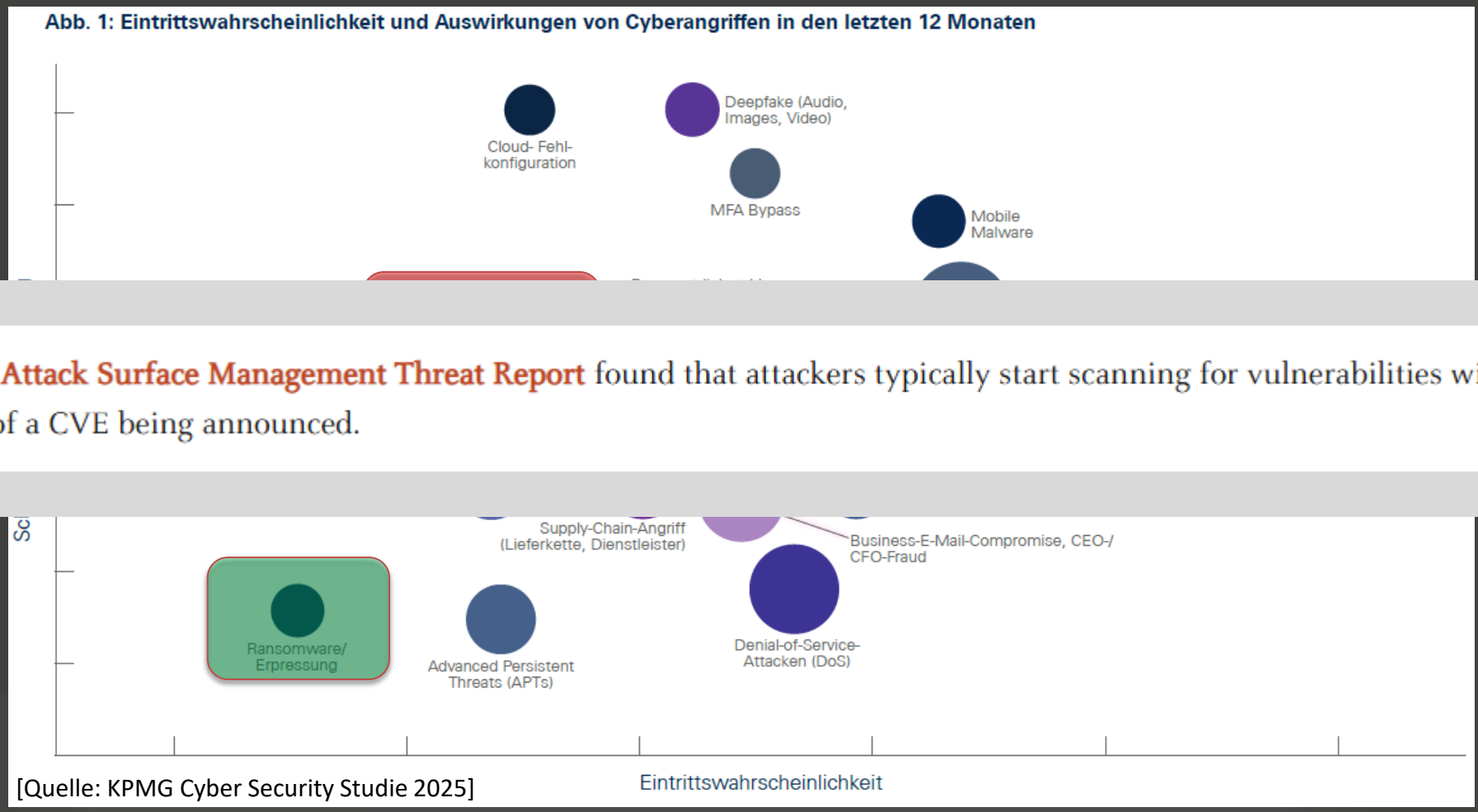


- **Restoretests**
  - Testen der Restores kompletter VMs
  - Restoretests sollten einmal im Quartal durchgeführt werden
  - Desaster Recovery Tests sollten einmal im Jahr durchgeführt werden

Aktuelles Lagebild

INFOTECH
[IT & Communication]

Abb. 1: Eintrittswahrscheinlichkeit und Auswirkungen von Cyberangriffen in den letzten 12 Monaten



[Quelle: KPMG Cyber Security Studie 2025]

W

The 2021 Attack Surface Management Threat Report found that attackers typically start scanning for vulnerabilities within 15 minutes of a CVE being announced.

n?

Patching

INFOTECH
[IT & Communication]

- A
  - V

Affected Software	Age
Microsoft Edge Chromium-based (+ 4...	12 d
Oracle Firefox (+ 169 more)	2 ye
Mozilla Firefox (+ 28 more)	3 mo
Microsoft Teams	2 ye
Microsoft Teams	2 ye
Ubuntu Webp (+ 69 more)	2 ye
Microsoft Edge Chromium-based (+ 4...	7 da
Microsoft Edge Chromium-based (+ 4...	7 da
Microsoft Windows Server 2012 R2 (+...	3 mo
Oracle Log4j (+ 77 more)	4 ye

CVE-2022-23302

Open vulnerability page Report inaccuracy

Vulnerability details | **Exposed devices** | Affected software

Export 4 items Search

Name	OS platform	Last seen	Criticality level	Update availab...
[redacted]	Windows Server 20...	Sep 29, 2025 5:47 AM	High	Available
[redacted]	Windows 11	Sep 29, 2025 10:11 AM		Available
[redacted]	Windows 11	Sep 29, 2025 2:35 PM		Available
[redacted]	Windows Server 20...	Sep 29, 2025 5:41 AM		Available

Patching

INFOTECH
[IT & Communication]

- **Patch Management**
  - Betriebssysteme, Applikationen und Firmwarestände sollen rechtzeitig und wenn möglich automatisiert gepatched werden
  - Auslagerung der Tätigkeit an externe Firmen (IT Care)
  - Patch My PC

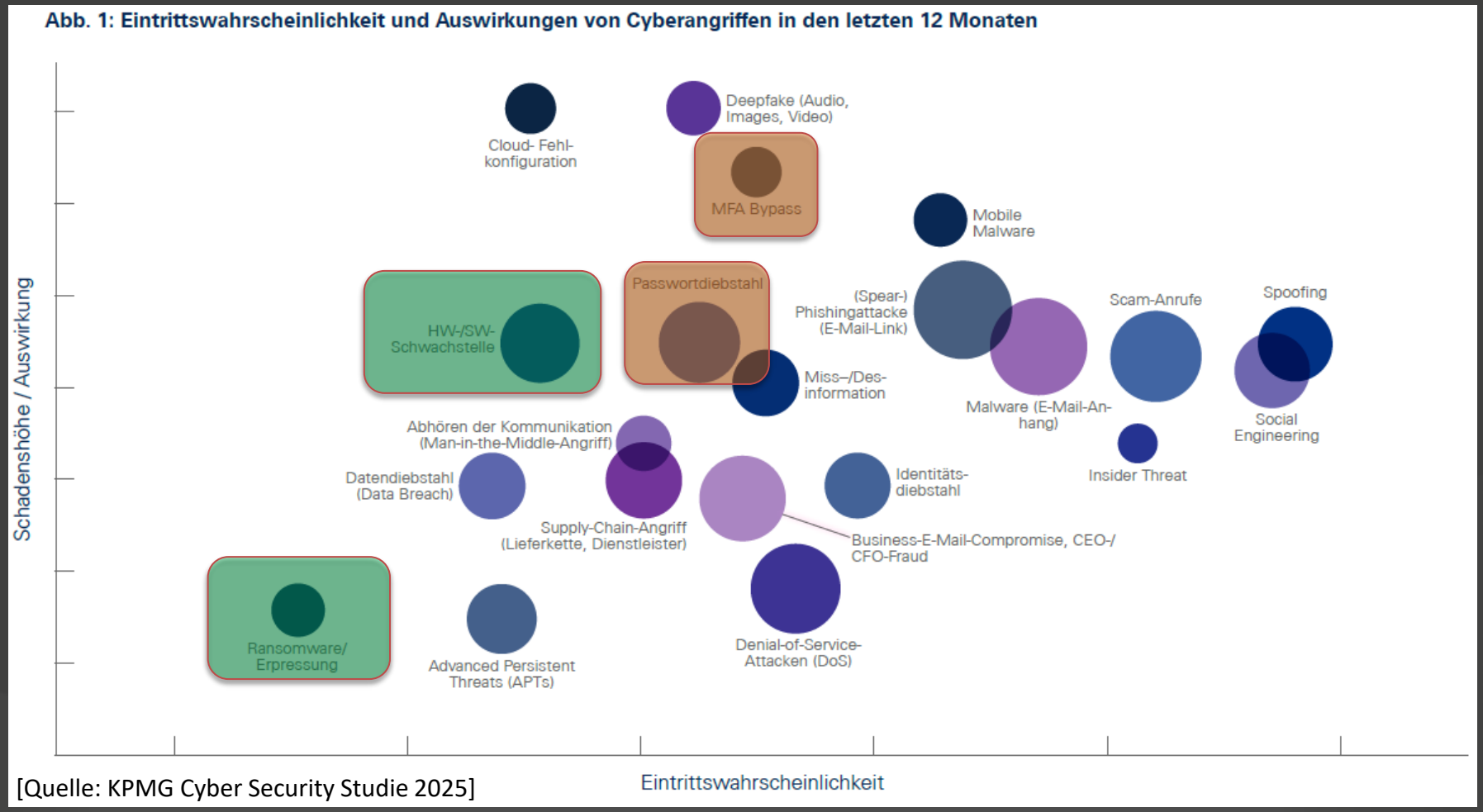
Update for Google Chrome 140.0.7339.128 (x64)	Windows	Windows app (Win32)	140.0.7339.128
Update for Cisco Secure Client AnyConnect VPN 5.1.8.105	Windows	Windows app (Win32)	5.1.8.105

Name	Object type	Quality	Feature	Quality deferral
Windows Autopatch	Autopatch group	Running	Running	Mixed
Windows Autopatch Update Policy - Default - Test	Update rings f...	Running	Running	0 days
Windows Autopatch Update Policy - Default - Ring1	Update rings f...	Running	Running	1 days
Windows Autopatch Update Policy - Default - Ring2	Update rings f...	Running	Running	6 days
Windows Autopatch Update Policy - Default - Ring3	Update rings f...	Running	Running	9 days
Windows Autopatch Update Policy - Default - Last	Update rings f...	Running	Running	11 days

Aktuelles Lagebild

INFOTECH
[IT & Communication]

Abb. 1: Eintrittswahrscheinlichkeit und Auswirkungen von Cyberangriffen in den letzten 12 Monaten



[Quelle: KPMG Cyber Security Studie 2025]

(Un)sichere Passwörter …

INFOTECH
[IT & Communication]

- „… das weiß doch mittlerweile eh jeder“

- Passwörter müssen
    - Komplex sein (Ziffern, Buchstaben, Sonderzeichen, möglichst lange)
    - Sollen nicht wiederverwendet werden
    - Sollen sicher gespeichert werden (Browser?)
        - Login von privaten Geräten!?

(Un)sichere Passwörter ...

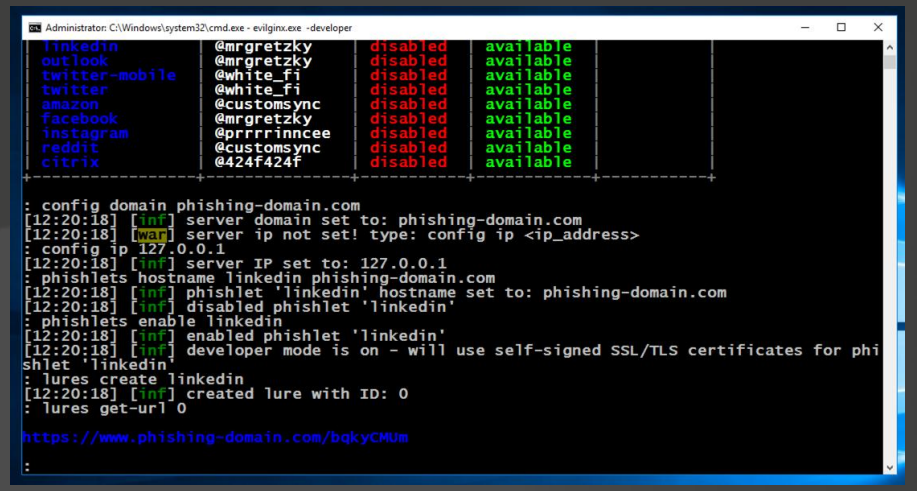
INFOTECH
[IT & Communication]

- Die Lösung: Kein Passwort ist sicher
    - Passwordless Authentication
        - Windows Hello (for Business)
        - Yubikeys
        - Authenticator Apps
- Wer setzt passwortlose Authentifizierung im Unternehmen ein?
- MFA ist weiterhin Pflicht!

Passwörter / Phishing

INFOTECH
[IT & Communication]

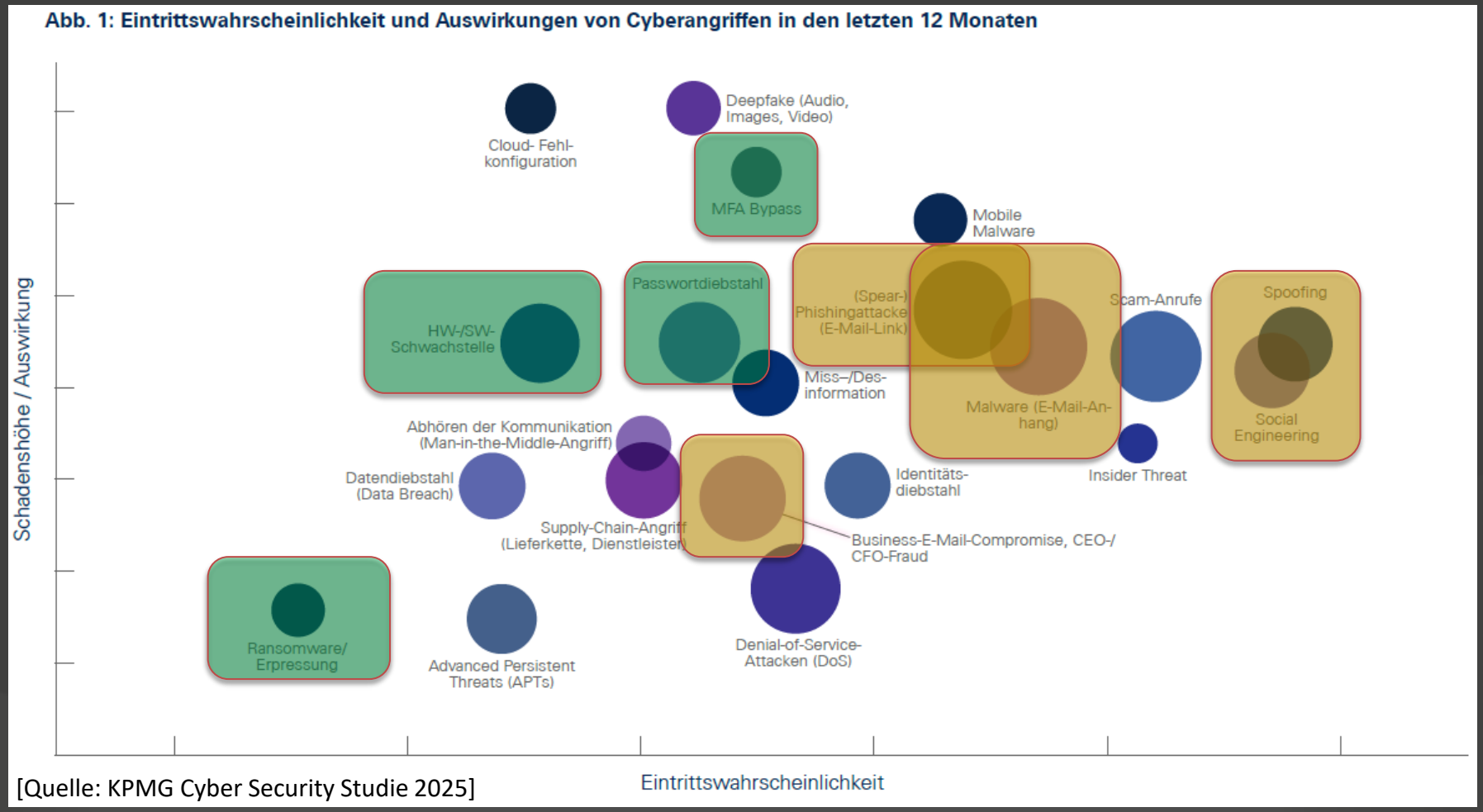
- **Phishing von MFA-Token**
  - Schwache MFA-Methoden wie SMS, Telefon oder E-Mail vermeiden
  - Phishing Resistent MFA verwenden
  - Verbesserten Schutz durch Conditional Access Policies
- **Awareness schaffen bei den Mitarbeitern**



Aktuelles Lagebild

INFOTECH
[IT & Communication]

Abb. 1: Eintrittswahrscheinlichkeit und Auswirkungen von Cyberangriffen in den letzten 12 Monaten

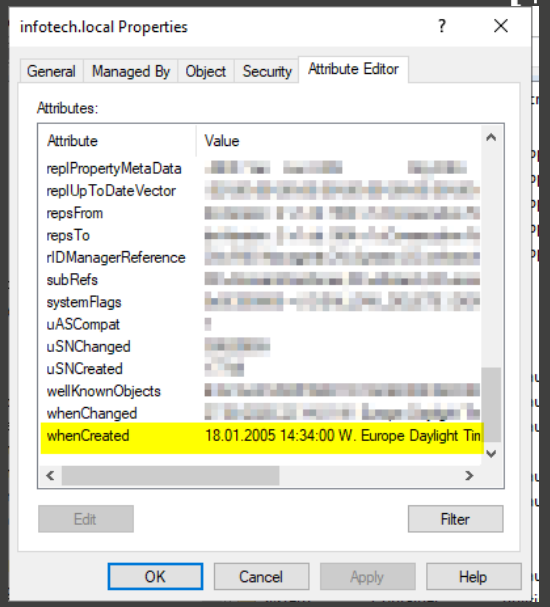


[Quelle: KPMG Cyber Security Studie 2025]

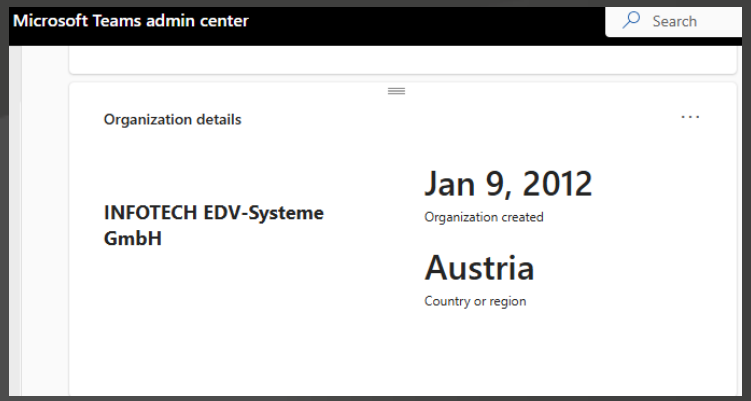
AD/M365 Hygiene/Hardening

INFOTECH
[IT & Communication]

- **Wer betreibt ein Active Directory?**
  - Wann wurde dieses installiert?
  - Wann fand die letzte Überprüfung der Konfiguration statt?



- **Wer verwendet M365 Services?**
  - Wann wurde der Tenant angelegt?
  - Wann fand die letzte Überprüfung der Konfiguration statt?



AD/M365 Hygiene/Hardening

INFOTECH
[IT & Communication]

- **Review der Umgebung**
  - Toolunterstützte ist Stand Erhebung (MS Defender, Inside Agent, PingCastle,...)

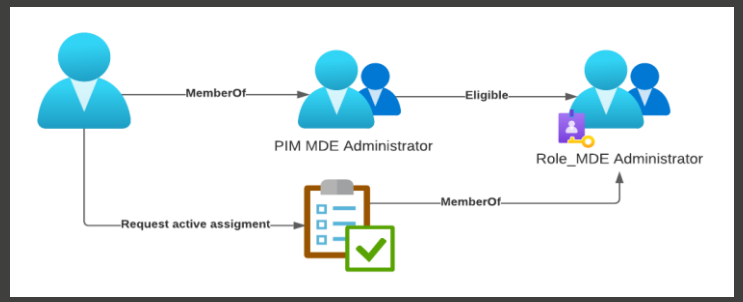
Recommended action	Score impact	Points achieved	Status
Block execution of potentially obfuscated scripts	+0.76%	8.48/9	To address
Block Office applications from injecting code into other processes	+0.76%	8.48/9	To address

Severity	Name	Policy Description	Checked At	Standard	CIS	Action
Critical	Ensure all member users are 'MFA capable'	Microsoft defines Multifactor authentication capable as being registered and enabled for a strong authentication The following checks are performed: 1.	17 September 2025 at 07:09	Not Compliant	5.2.3.4	
High	Security Default State	Security defaults in Microsoft Entra ID make it easier to be secure and help protect the organization.	17 September 2025 at 07:08	Compliant		
High	Guest User Access Restrictions	Microsoft Entra ID, part of Microsoft Entra, allows you to restrict what external guest users can see in their organization in Microsoft Entra ID.	17 September 2025 at 07:08	Compliant	5.1.6.2	
High	Guest Invitation Policy	The Guest Invitation Policy in Microsoft Entra ID controls whether guest users can invite other external users to the organization.	17 September 2025 at 07:08	Compliant		

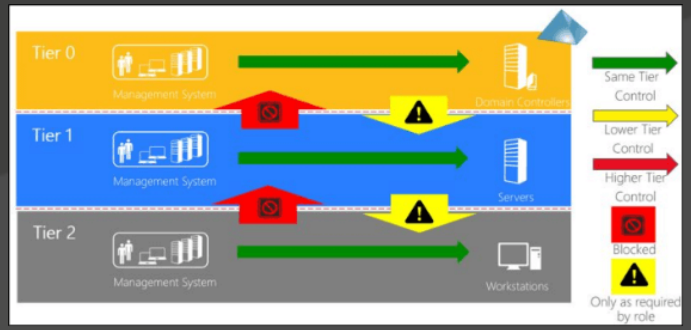
AD/M365 Hygiene/Hardening

INFOTECH
[IT & Communication]

- **Usermanagement und Application Management**
  - Least Privilege Konzept einführen (Users, Guests, Applikationen)
  - Just in Time Access einführen



  - Tiering Konzept einführen
    - Unterteilung der Tätigkeiten und User in verschiedene Ebenen



AD/M365 Hygiene/Hardening

INFOTECH
[IT & Communication]

- **Legacy Protokolle deaktivieren**
  - Veraltete Protokolle sollen durch aktuelle sichere ersetzt werden
    - SMB v1/v2 durch SMB v3
    - NTLM durch Kerberos
    - ....
  - Hohes Sicherheitsrisiko
  - Kompatibilitätsprobleme mit aktuellen Betriebssystemen

Digitale Verteidigung in unsicheren Zeiten – Strategien für Sicherheit und Souveränität

INFOTECH
[IT & Communication]

Quelle: Copilot / KI generiert

Ihr Systemhaus.

Digitale Souveränität

INFOTECH
[IT & Communication]

- **Digitale Souveränität**
  - Selbstbestimmtes Handeln
  - Volle Hoheit über eigene Daten
  - Unabhängigkeit von einzelnen Anbietern

- **Gedankenexperiment:**
  - Keine Mails
  - Keine Telefonie
  - Keine Daten

Digitale Souveränitat

INFOTECH
[IT & Communication]

- **Backup für Cloud Produkte**
  - 3. Anbieter verwenden
  - Alle verwendeten Produkte sollen ein Backup haben (Exchange Online, SharePoint, Azure VMs, AWS VMs...)

- **Verwendung regionaler Lösungen**
  - Verwendung regionaler Cloud Anbieter
  - Gesetzliche Vorgaben, bzgl. Datenschutz

INFOTECH
[IT & Communication]

Fragen oder Diskussion?

INFOTECH

[IT & Communication]

Ihr Systemhaus.