



53. Action Group Informationssicherheit & Cybersecurity:

Darknet Monitoring & Attack Surface Reduktion – einfach erklärt

29. Jänner 2026, CMG Online Event

Zur Person



Ing. Andreas Schuster

Leiter CMG Themenpanel
Informationssicherheit & Cybersecurity

andreas.schuster@cmg-ae.at

Mobil +43 678 1216943

LinkedIn: [linkedin.com/in/andreas-schuster-infosec/](https://www.linkedin.com/in/andreas-schuster-infosec/)

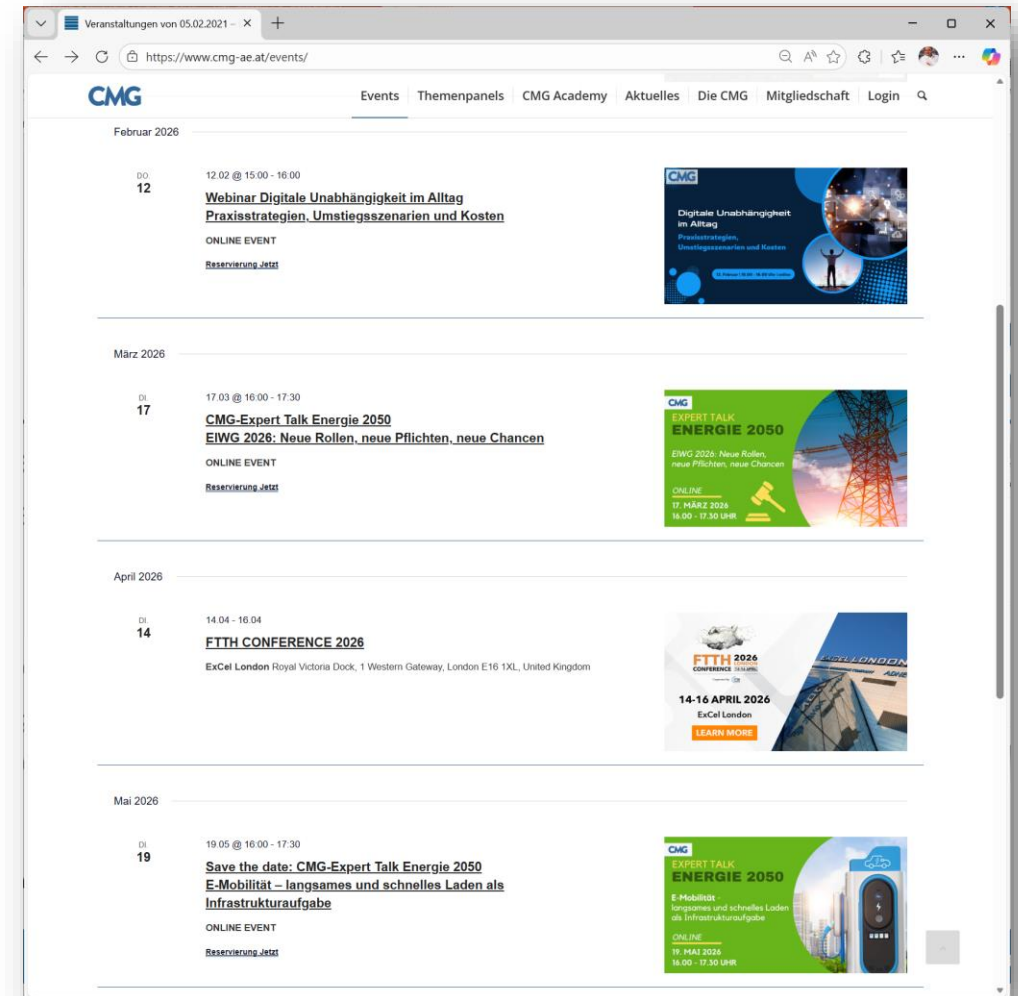
CMG-AE – wer sind wir?

- Gemeinnütziger Verein (seit mehr als 25 Jahren)
- Bieten eine Plattform zur offenen (anbieterunabhängigen) Diskussion von Themen im technologischen Umfeld
- Wir organisieren Symposien, Tagungen & Spotlights
- In Arbeitsgruppen (Themenpanels) werden konkrete Themen diskutiert
- Wir bieten Einzelmitgliedschaften und Firmenmitgliedschaften

CMG-AE – was tun wir?

- Digitale Souveränität
- Energie 2050
- Informationssicherheit & Cybersecurity
- Business Continuity
- LEAN-Management
- Glasfaser (Action Group Gigabit Fiber Access – AGGFA)

www.cmg-ae.at/events



Informationssicherheit & Cybersecurity

The background of the central graphic is a close-up, high-angle shot of a complex electronic circuit board. The board is densely packed with components, and its surface is highlighted with a warm, golden light. Overlaid on this background is a large, metallic shield with a prominent keyhole in the center, symbolizing protection and security.

www.cmg-ae.at

**Darknet Monitoring &
Attack Surface Reduktion -
einfach erklärt**

**53. Action Group
Informationssicherheit & Cybersecurity**

**29. Jänner 2026
15.00 - 17.00 Uhr Online**

INFORMATIONSSICHERHEIT &
CYBERSECURITY 

Darknet Monitoring in der ISO 27001



→ ISO 27001 → Annex A (2 von 93 Controls)

		The organization shall establish and maintain contact with relevant authorities.
5.6	Contact with special interest groups	Control The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
5.7	Threat intelligence	Control Information relating to information security threats shall be collected and analysed to produce threat intelligence.
5.8	Information security in project management	Control

Threat Intelligence (auf Deutsch oft Bedrohungsinformationen oder Bedrohungsaufklärung) bezeichnet das systematische Sammeln, Analysieren und Nutzen von Informationen über Cyberbedrohungen, um Angriffe frühzeitig zu erkennen, zu verhindern oder besser darauf zu reagieren.

Kurz gesagt: 👉 Man versucht zu verstehen, wer angreift, wie, warum und womit.

Attack Surface Reduction in der ISO 27001



Cheat Sheet ISO 27001:2022

A5.1 InfoSec-Richtlinien	A5.2 InfoSec Verantwortlichkeiten	A5.3 Aufgabentrennung	A5.4 Verantwortung der Leitung	A5.5 Kontakt mit Behörden	A5.6 Kontakt mit Interessensgruppen	A5.7 Informationen zur Bedrohungslage	A5.8 InfoSec im Projektmanagement	A5.9 Inventar der Informationen / Assets	A5.10 Zulässiger Gebrauch von Assets
A5.11 Rückgabe von Werten	A5.12 Klassifizierung von Informationen	A5.13 Kennzeichnung von Informationen	A5.14 Informationsübermittlung	A5.15 Zugangssteuerung	A5.16 Identitätsmanagement	A5.17 Authentisierungsinformationen	A5.18 Zugangsrechte	A5.19 InfoSec bei Lieferanten	A5.20 Lieferantenvereinbarungen
A5.21 InfoSec in der Lieferkette	A5.22 Überwachung Lieferantenleistungen	A5.23 InfoSec bei Cloud-Diensten	A5.24 Management Sicherheitsvorfälle	A5.25 Bewertung Sicherheitsereignisse	A5.26 Reaktion auf Sicherheitsvorfälle	A5.27 Erkenntnisse aus Sicherheitsvorfällen	A5.28 Sammeln von Beweismaterial	A5.29 InfoSec bei Störungen	A5.30 Geschäfts-Kontinuität
A5.31 Compliance	A5.32 Geistiges Eigentum	A5.33 Schutz von Aufzeichnungen	A5.34 DSGVO - Datenschutz	A5.35 Überprüfung d. Informationssicherheit	A5.36 Einhaltung von Richtlinien	A5.37 Dokumentierte Betriebsabläufe			
A6.1 Bewerber Sicherheitsüberprüfung	A6.2 InfoSec in Arbeitsverträgen	A6.3 Security Awareness	A6.4 Maßregelungsprozess	A6.5 Beendigung von Beschäftigung	A6.6 Vertraulichkeitsvereinbarungen	A6.7 Remote-Arbeit	A6.8 Meldung von InfoSec Ereignissen		
A7.1 Physischer Sicherheitsperimeter	A7.2 Physischer Zutritt	A7.3 Sichern von Standorten	A7.4 Phys. Sicherheitsüberwachung	A7.5 Schutz vor Umweltbedrohungen	A7.6 Arbeiten in Sicherheitsbereichen	A7.7 Arbeitsplatzsicherheit (Sperrung)	A7.8 Schutz von Geräten/Betriebsmittel	A7.9 Werte außerhalb der Räumlichkeiten	A7.10 Speichermedien
A7.11 Versorgungseinrichtungen	A7.12 Sicherheit der Verkabelung	A7.13 Instandhaltung von Geräten	A7.14 Sichere Entsorgung						
A8.1 Benutzer Endgeräte	A8.2 Privilegierte Zugangsrechte	A8.3 Informationszugangsbeschränkung	A8.4 Zugriff auf den Quellcode	A8.5 Sichere Authentisierung	A8.6 Kapazitätssteuerung	A8.7 Schutz gegen Schadsoftware	A8.8 Technische Schwachstellen	A8.9 Konfigurationsmanagement	A8.10 Löschung von Informationen
A8.11 Datenmaskierung	A8.12 Verhinderung von Datenlecks (DLP)	A8.13 Sicherung von Informationen	A8.14 Redundanzen	A8.15 Protokollierung	A8.16 Überwachung von Aktivitäten	A8.17 Uhrensynchronisation	A8.18 Privilegierte Hilfsprogramme	A8.19 Installation von Software	A8.20 Netzwerksicherheit
A8.21 Sicherheit von Netzdiensten	A8.22 Trennung von Netzwerken	A8.23 Webfilterung	A8.24 Verwendung von Kryptographie	A8.25 Lebenszyklus sicherer Entwicklung	A8.26 Anforderung an Anwendungssicherheit	A8.27 Sichere Entwicklungsgrundsätze	A8.28 Sichere Codierung	A8.29 Sicherheitsprüfung b. Entwicklung	A8.30 Ausgegliederte Entwicklung
A8.31 Trennung von Entwicklung/Test/Prod.	A8.32 Änderungssteuerung	A8.33 Testdaten	A8.34 Schutz der IT während Tests						

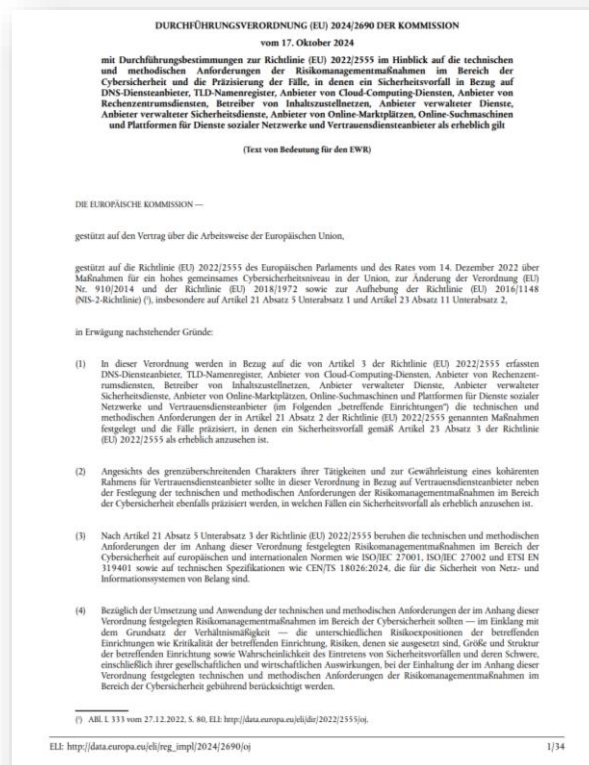
NIS-2: Darknet Monitoring & Attack Surface Reduction



Durchführungsverordnung
2024/2690 für NIS-2*



ENISA TECHNICAL IMPLEMENTATION
GUIDANCE June 2025 V1.0*



Seite 104, 6.10.3:
“Ensure comprehensive documentation of identified vulnerabilities, the associated risk assessments and any mitigation plans developed.”

*) aktuell nur gewisse Branchen verpflichtet

Erfahrungsaustausch mit Michael KARL



- ❖ Attack Surface Management (ASM)
- ❖ Darknet Monitoring
- ❖ Zusammenspiel von ASM & Darknet Monitoring
- ❖ Einblicke in seine tägliche Arbeit und Use Cases aus Unternehmen



Michael KARL



blacklens.io

a service by © snopSEC GmbH

Erkenntnisse aus der Action Group



1. Cyberhygiene vermindert das Risiko Cyberattacken
2. Durch Phishing-resistente MFA reduziert sich die Gefahr von Passwortdiebstahl, nicht jedoch die des Session Diebstahls
3. Kurze Session-Token Zeiten z.B. 8h reduzieren die Gefahr, dass Session-Token im Darknet verkauft werden
4. Bei größeren Unternehmen sollte man frühzeitig einen Reaktionsprozess für den Umgang mit Darknet-Findings und resultierenden Passwort-Resets definieren
5. Bevor Unternehmen sich einen Darknet Monitoring Anbieter suchen, bitte unbedingt überlegen, welche Assets man hat und welche Erwartungen man den den Anbieter stellt
6. Viele Darknet Monitoring Anbieter können ihre Versprechen (vollständige Überwachung) nicht einhalten
7. Schwachstellenscannen benötigt ein Enterprise Feed – Lösungen, die rein auf Open-Source basieren hinken bei der Erkennung von CVE oft deutlich nach
8. Attack Surface Management (ASM) ist heute deutlich mehr als reines Vulnerability Management, z.B. Account Taker, Session Stealer, Hinweise und Rückschlüsse auf aktuelle Vorfälle