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

TeleTrusT-Konferenz

Berlin, 26.06.2026

Cyber-Nation Deutschland im Lichte aktueller Entwicklungs- und Analyse-Tools

Matthias Intemann,
Bundesamt für Sicherheit in der Informationstechnik

KI-basierte Werkzeuge

- … sind nur Werkzeuge
- Helfen Software zu entwickeln, sicher zu machen, Angriffe zu detektieren und zu mitigieren
- Helfen Angriffe durchzuführen, Lücken zu finden, Social Engineering / Phishing zum Kinderspiel werden zu lassen

Präsidentin des BSI gibt Impuls

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

- Deutschland muss Cyberresillienz konkreter und operativer umsetzen
- Dazu gehört, dass KI nicht nur als Risiko zu betrachten, sondern sie selbst für Schwachstellenerkennung und Analyse zu nutzen
- Ebenso wichtig sind der Aufbau eigener KI-Fähigkeiten die zügige Umsetzung von CyberGovSecure und der Cyberdome als gemeinsamer Schutzschirm

BSI warnt

„Auswirkungen auf die Cybersicherheit von Organisationen durch die Entwicklung im Bereich Künstlicher Intelligenz“

Kritikalität: 2 / Gelb

https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262788-1032.pdf

Maßnahmenempfehlungen des BSI

- Angriffsfläche kennen und minimieren
- Patchmanagement verbessern und effizienter gestalten
- Assume Breach - Detektion und Vorfallsbearbeitung ausbauen
- Standard-Maßnahmen umsetzen
- Softwareentwicklung und Software-/System-Architekturen basierend auf modernen (nicht nur KI-)Werkzeugen mit hohem Automatisierungsanteil

ENISA empfiehlt

- Security fundamentals matter more than ever in the age of AI
- Security by design needs to be supported by adequate and engineer-grounded methodologies, tooling, development, and testing frameworks
- Urgent need for increased velocity and automation in cybersecurity rooted in 4 pillars: Vulnerability Management as Code, Incident Management as Code, Secure by Design as Code, Security Architecture as Code

Vielen Dank!