KRITIS & NIS2 – Wenn Cyberangriffe zur realen Bedrohung werden

Cyberangriffe auf kritische infrastruktur in österreich 2025

Die Studie „Cybersecurity in Österreich 2025“ von KPMG zeigt, dass Cyberangriffe zunehmend als Werkzeug geopolitischer Auseinandersetzungen eingesetzt werden. Österreich ist nicht nur betroffen, sondern auch verwundbar: Jeder 7. Cyberangriff in Österreich ist erfolgreich. Mehr als jeder 4. Angriff ist auf staatlich

Solarstrom, Router und staatlich gelenkte Hacktivisten

Cyberangriffe auf vernetzte Infrastruk-turen nehmen 2025 rasant zu

30.05.2025 · Von Thomas Joos · 5 min Lesedauer ·

Solaranlagen mit kritischen Schwachstellen, Router als Einfallstor für Botnetze und staatlich gesteuerte Hacktivisten – 2025 verschärft sich die Bedrohungslage dramatisch. Besonders vernetzte Infrastrukturen geraten ins Visier gezielter Angriffe, oft mit geopolitischer Absicht und realen Folgen für die Versorgungssicherheit.

Kritische Schwachstellen in Solaranlagen, Router-Botnetze und staatlich gelenkte Hacktivisten zeigen 2025 deutlich: Vernetzte Infrastrukturen stehen zunehmend im Fokus geopolitisch motivierter Cyberangriffe.
(Bild: © Viks_jin - stock.adobe.com)

Studie: Cyber Security in Österreich 2025

Bereits zum zehnten Mal veröffentlicht KPMG die Studie „Cybersecurity in Österreich“ gemeinsam mit dem Sicherheitsforum Digitale Wirtschaft des Kompetenzzentrum Sicheres Österreich. Die Studie bietet aktuelle Zahlen einer Umfrage, an der sich 1.391 österreichische Unternehmen beteiligt haben. Ergänzt wird die Publikation durch Analysen und ausgewählte Interviews von Expertinnen und Experten.

Informationen

Kategorie: Studien

Herausgeber / Verlag: KPMG Österreich

Ausgabedatum: 14. Mai 2025

Download: Cyber Security in Österreich 2025 - Studienbestellung

Die Ergebnisse der Studie zeigen, Cyberangriffe werden zunehmend als Werkzeug geopolitischer Auseinandersetzungen eingesetzt - Österreich ist nicht nur betroffen, sondern auch verwundbar:

- Jeder 7. Cyberangriff (14 Prozent) in Österreich ist erfolgreich.
- Mehr als jeder 4. Angriff (28 Prozent) ist auf staatlich unterstützte Akteure zurückzuführen.
- Bei jedem 3. Unternehmen (32 Prozent) waren deren Lieferanten oder Dienstleister Opfer von Cyberangriffen, die wesentliche Auswirkungen auf das eigene Unternehmen hatten.
- Jeder 1 Videon

Vorfall

Drohnen am Flughafen von Kopenhagen: Dänemarks Ministerpräsidentin Frederiksen spricht vom „bislang schwersten Anschlag auf kritische Infrastruktur“

Die dänische Ministerpräsidentin Frederiksen spricht nach der Drohnensichtung am Flughafen von Kopenhagen von einem Angriff. Es handle sich um den bislang schwersten Anschlag auf die kritische Infrastruktur des Landes, erklärte die Regierungschefin.

24.09.2025

Start › Österreich › Österreich baut Drohnenabwehr und Schutz kritischer Infrastruktur aus

Österreich baut Drohnenabwehr und Schutz kritischer Infrastruktur aus

Zuletzt aktualisiert: 29. Oktober 2025

Merkmal	KRITIS-DachG*	NIS2UmsuCG
Geltungsbereich	Kritische Infrastrukturen in Deutschland	Wichtige und besonders wichtige Einrichtungen in der gesamten EU
Ziel	Schutz lebenswichtiger Dienstleistungen	Erhöhung der Cybersicherheit & Meldepflicht bei Vorfällen
Status	In Umsetzung (DE)	Im November 2025 vom Bundestag verabschiedet
Betroffene	10 Sektoren inkl. Energie, Gesundheit, Wasser, Transport usw.	18 Sektoren inkl. öffentliche Verwaltung, Gesundheitswesen, digitale Infrastruktur
Fokus	Resilienz physischer und digitaler Systeme	Risikomanagement, Business Continuity, Incident Reporting
Aufsicht	BBK Bundesamt für Bevölkerungs- und Katastrophenschutz	BSI & Nationale Cybersicherheitsbehörden der EU-Staaten

* Das KRITIS-Dachgesetz (KRITIS-DachG) befindet sich derzeit noch im Gesetzgebungsverfahren und wurde vom Deutschen Bundestag noch nicht verabschiedet. Inhalte und Anforderungen können sich daher noch ändern.


Kritische Infrastrukturen
Gesundheit
z.B. Krankenhäuser, Rettungsdienste
Transport/ Verkehr
z.B. Flughafen-betreiber, Bahnbetreiber
Energie
z.B. Stadtwerke, Verteilnetzbetreiber
Wasser
z.B. Wasserkraft-betreiber, Klärwerk-betreiber
Staat / Verwaltung
z.B. Bundesministerien, Finanz- oder Einwohner-meldeämter (nicht verpflichtend)
Informationstechnik / Telekommunikation
z.B. Telekommunika-tionsprovider, Mobil-funkanbieter
Medien / Kultur
z.B. Rundfunk- und Fernsehanstalten (nicht verpflichtend)
Ernährung
z.B. Lebensmittel-konzerne, Lebens-mittelhändler
Finanz- / Ver-sicherungs-wesen
z.B. Banken, Versicherungen

NEUE REGELN, NEUE PFLICHTEN – NEUE CHANCEN!

- Nationalrat stimmt Umsetzung der EU Richtlinie zu
- 24.09.2025 „Resilienz kritischer Einrichtungen-Gesetz“ (RKEG)
- Strafen bis zu 500.000€
- Betriebe müssen Risikoanalyse selbst vornehmen
- Ca. 600 betroffene Unternehmen in Österreich

- Erweiterte NIS2 Regelung (ab 01.10.2026):
- IT-Cyber-Sicherheitsregelungen (deutlich breiterer Geltungsbereich)
- Bisher: ca. 100 Unternehmen
- Jetzt: ca. 4000 mittelgroße Unternehmen <50 Mitarbeitende
- Inhalte unter anderem:
- „Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme“
- „Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall“
- „Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen“

NEUE REGELN, NEUE PFLICHTEN – NEUE CHANCEN!

Herausforderungen

- ❑ Zutritts- und Zugangsrisiken (KRITIS)
- ❑ Prozess- und Betriebssicherheit (KRITIS & NIS2)
- ❑ Versorgungs- und Systemverfügbarkeit (NIS2)
- ❑ Cyber- und Datensicherheit (NIS2)
- ❑ Digitale Souveränität (NIS2)
- ❑ Normenkonformität (IEC/EN 62676-4, KRITIS DachG)
- ❑ Brand- und Anlagenschutz (VDE0833-2 & EN54)
- ❑ Umwelteinflüsse & Standortbedingungen

MOBOTIX Lösungen

- ✓ Intelligente Zufahrtskontrolle
- ✓ Sicherheits-Monitoring & Anomalieerkennung
- ✓ Edge Intelligence
- ✓ Cybersecurity by Design
- ✓ Nahtlose Integration
- ✓ NDAA-Konformität & Penetrationstest-Zertifizierung
- ✓ Thermalkameras & Brandfrüherkennung
- ✓ Langlebigkeit & Serviceverfügbarkeit

Konzeption und Anforderungsprofil

Hand in Hand

Partner

- Einschätzung von KRITIS-/NIS2-Betroffenheit
- Erstellung oder Weiterentwicklung Ihrer Risikoanalyse
- Normgerechte Videoplanung nach IEC 62676-4
- Ableitung konkreter Maßnahmen
- Mindestbestand an Kameras zur Sicherstellung der Lieferfähigkeit (Dezentrales Lager)

MOBOTIX KRITIS Partner

MOBOTIX

- Bereitstellung von zugelassenen Produkten (CRA, Cyber Security – Anforderungen)
- Cactus+ Edition
- Schulungen
- Marketingunterstützung
- Mindestbestand an Kameras zur Sicherstellung der Lieferfähigkeit

MOBOTIX

KRITIS

Partner

MOBOTIX ONE

Cactus+ Edition

MOBOTIX MONE
Cactus+ Edition
Voreinstellungen

- Nur HTTPS auf Port 443 aktiv, HTTP (Port 80) abgeschaltet
- Validierbares x.509 Zertifikat in Kamera geladen
- "Benutzergruppe ""KRITIS-admin"" voreingerichtet (KRITIS Admin soll Kurator nicht öffnen dürfen)"
- Benutzergruppe "KRITIS-user" voreingerichtet
- Öffentlicher Zugriff deaktiviert
- IP-basierte Zugriffsbeschränkung voreingestellt
- Intrusion-Detection (Einbruchserkennung) aktiviert
- Aufzeichnungsverschlüsselung aktiviert
- Audio bei Aufzeichnung deaktiviert
- Digitale Signatur der Aufzeichnung aktiviert
- MQTT aktiviert (LWT aktiviert für Erkennung der Netzwerktrennung) -> erfordert Installation eines MQTT Brokers
- Zeitsynchronisation mit Zeitserver vorkonfiguriert

MOBOTIX KRITIS Partner

MOBOTIX ONE
Cactus+ Edition

Was macht‘s besonders:

- Ab Werk für kritische Infrastrukturen vorkonfiguriert
- Security by Design & Default gemäß NIS2
- Erhöhter Identitäts- und Zugriffsschutz
- Sicherheitsbestände bei Mobotix & Partner
- 1 Jahr zusätzliche Garantie*
- Cactus Sicherheits-Siegel (Sicherheitskennzeichen und Sabotageschutz)

MOBOTIX KRITIS Partner

* 6 Jahre Herstellergarantie

Schulung und Zertifizierung

User Training **(von Partnern)**

- Umgang mit Privacy-Zonen
- Alarm- und Ereignismanagement
- Statusüberwachung
- DSGVO-konforme Videonutzung
- Reporting & Dokumentation
- Export von zertifizierten Videodaten

MOBOTIX KRITIS Partner

Zertifikat: Cactus+ Spezialist **(von MOBOTIX)**

- Themenübersicht, Produktvorstellung; Einsatzgebiete
- KRITIS-DachG, IEC62676-4 Anwedungsregeln
- Installation und Konfiguration der Edition
- Passwortsicherheit und Verarbeitungsverfahren
- MQTT-Monitoring & Kameraausfall-Benachrichtigung
- Grundlagen Asymmetrischer Kryptografie & PKI
- Zertifikatsprovider, Kosten & Zertifikatsmanagement in Kameras
- Signieren von Aufzeichnungen und Echtheitsnachweis
- Zertifizierungsprüfung

Trainings
09.06.2026 und 27.10.2026

Vielen Dank

Beyond Human Vision

MOBOTIX

MOBOTIX AG
Kaiserstrasse
67722 Langmeil
Germany

+49 6302 9816-0
info@mobotix.com
www.mobotix.com