STABSSTELLE CYBER-SICHERHEIT
FÜRSTENTUM LIECHTENSTEIN



Cybersicherheit in Zeiten von KI

Welchen Bedrohungen sind KMUs ausgesetzt?

22. Oktober 2026

TLP:GREEN

Cybersicherheit und Cyberbedrohung

«Cybersicherheit» bezeichnet **alle Tätigkeiten**, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von **Cyberbedrohungen** betroffene Personen **zu schützen**;

«Cyberbedrohung»: ein möglicher Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte;

TLP:GREEN

STABSSTELLE CYBER-SICHERHEIT
FÜRSTENTUM LIECHTENSTEIN

Cybersicherheit und KI



TLP:GREEN

Zeiten des Wettrüstens

Angreifer nutzen KI

- KI erhöht und beschleunigt die Chancen, Schwachstellen zu entdecken

Verteidiger nutzen KI

- Schwachstellen können schneller gepatcht werden

KI wird angegriffen

- KI hat Zugang zu privaten/vertraulichen Daten, agiert autonom (Prompt Injections)

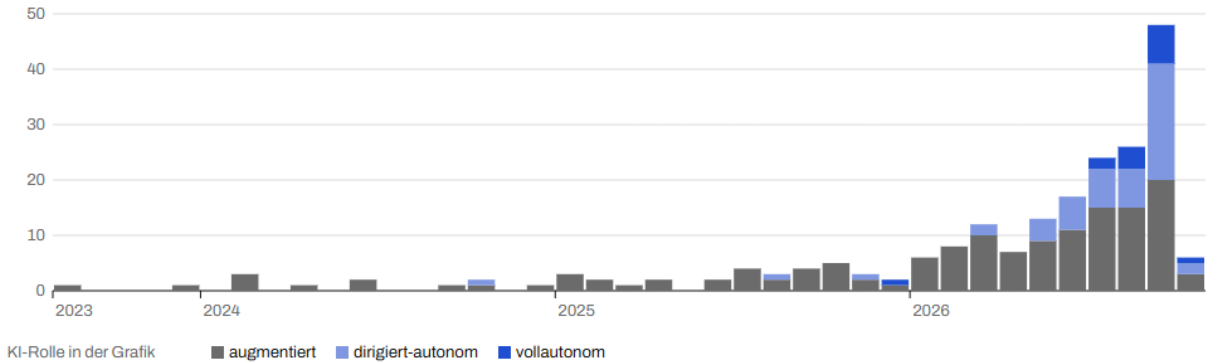
TLP:GREEN

Hackingvorfälle mit KI-Beteiligung

Reale Angriffe, die öffentlich geworden sind und bei denen nach der verlinkten Quelle ein KI-System an der Angriffskette beteiligt war. Bei augmentierten Angriffen steuert ein Mensch das Vorgehen, und die KI übernimmt einzelne Schritte, etwa die Aufklärung, das Schreiben von Code oder die Auswertung erbeuteter Daten. Dirigiert-autonom heißt, dass ein Mensch die Ziele setzt und ein Agent den Großteil der Angriffsschritte selbst ausführt. Vollautonom ist ein Angriff, wenn kein Mensch das Vorgehen gegen das Opfer angeordnet hat. **Nicht in der Liste stehen Angriffe auf KI-Systeme, Labordemonstrationen ohne belegtes Opfer, Einflusskampagnen sowie Betrug und Social Engineering, bei denen die KI nur den Köder liefert, etwa Phishingmails oder Deepfakes.** Sortiert ist sie nach dem Tag, an dem ein Fall bekannt wurde, der neueste zuerst.

Jeder Eintrag verlinkt seine Quelle und ist von einem Menschen gegengelesen; recherchiert und vorgeprüft mit KI-Agenten.

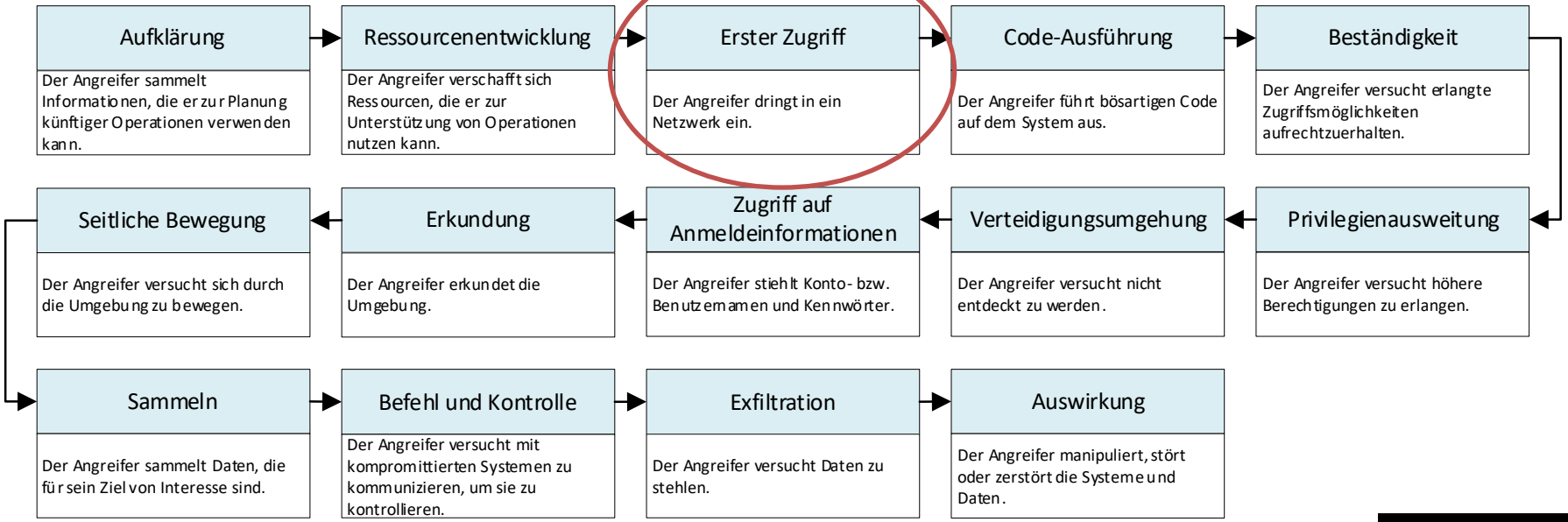
Stand 07.10.2026, 210 Vorfälle. RSS



https://www.ully.com/ki-hacking-vorfaelle/

TLP:GREEN

Cyber Kill Chain oder Attack Lifecycle *(dt. Angriffslebenszyklus)*



TLP:GREEN

Cyber Kill Chain – Einsatz KI (1)



https://cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access?hl=en

TLP:GREEN

Cyber Kill Chain – Einsatz KI (2)

Zusammenfassung GTIG vom 11. Mai 2026

- Schwachstellenerkennung und Exploit-Generierung
- KI-verstärkte Entwicklung für Verteidigungsumgehung
- Autonome Malware-Operationen
- Lieferkettenangriffe

TLP:GREEN

Cyber Kill Chain – Einsatz KI (3)



https://cloud.google.com/blog/topics/threat-intelligence/from-prompting-to-autonomy-the-evolution-of-adversarial-ai?hl=en

TLP:GREEN

Cyber Kill Chain – Einsatz KI (4)

Zusammenfassung GTIG vom 8. September 2026

- Erweiterung der Risiken in der Software-Lieferkette
- Verschiebung hin zu agentischer KI und Automatisierung
- Mehrstufige Lebenszyklus-Erweiterung
- Illegale Kontenbeschaffung & LLMJacking

TLP:GREEN

STABSSTELLE CYBER-SICHERHEIT
FÜRSTENTUM LIECHTENSTEIN

KMU - Angriffsvektoren



TLP:GREEN

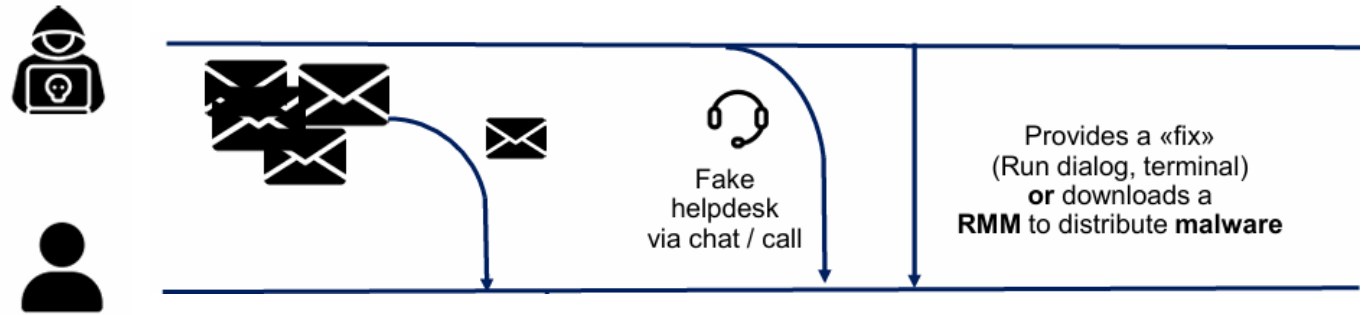
Angriffsvektoren

- Phishing und Social Engineering (Faktor Mensch)
  - Perfekte Grammatik und Stil
  - Hochgradige Personalisierung (Spear-Phishing)
  - Deepfakes (Audio/Video)
- Schwache, gestohlene oder wiederverwendete Passwörter
- Veraltete oder nicht gewartete Software mit (bekannten) Sicherheitslücken
- Fehlkonfigurationen, mangelnde Cyberhygiene-Massnahmen
- Verbreitung von Malware via Lieferketten z.B. JavaScript (npm-Pakete)

TLP:GREEN

Angriffsvektor MS Teams als Einfallstor - Beispiel

1. Mail bombing Opfer erhält hunderte E-Mails;
2. Fake IT-Helpdesk bietet Unterstützung an (externer MS tenant);
3. Malware Installation durch ClickFix (Infektionsmethode) oder via Remote Management Tools.



TLP:GREEN

Angriffsvektor Deepfakes



https://www.srf.ch/sendungen/kassensturz-espresso/kassensturz/online-betrug-deepfakes-und-stimmenklone-locken-opfer-in-die-betrugsfalle

TLP:GREEN

Angriffsvektor Deepfakes - Beispiel

Veröffentlicht am 27. Januar 2026

Woche 4: «Dringende Überweisung» – CEO-Betrug bleibt ein Dauerbrenner für KMU

Der sogenannte CEO-Betrug gehört nach wie vor zu den am meisten dem BACS gemeldeten Betrugsmethoden und hat im vergangenen Jahr verglichen mit 2024 von 719 auf 971 Fälle zugenommen. Auch in der vergangenen Woche gingen beim BACS erneut Meldungen ein, die zeigen, dass die Täter ihre Masche stetig verfeinern. Sie setzen nicht mehr ausschliesslich auf gefälschte E-Mails, sondern auch gezielt auf psychologische Manipulation und künstliche Intelligenz. Wie Sie die subtilen Warnsignale im Arbeitsalltag erkennen, beleuchtet der aktuelle Wochenrückblick.

https://www.bacs.admin.ch/de/26w4-de

TLP:GREEN

Angriffsvektor Deepfakes - Beispiel

Sicherheitsdepartement › Kantonspolizei › Medienmitteilungen › Kanton Schwyz

Kanton Schwyz: Unbekannte erlangen mit CEO-Fraud-Masche Millionen-Betrag

19. Januar 2026

Die Täterschaft nahm telefonisch Kontakt mit dem Inhaber des geschädigten Unternehmens auf und gab sich glaubhaft als bekannter Geschäftspartner aus. Dabei kam eine mithilfe künstlicher Intelligenz manipulierte Stimme zum Einsatz. Durch diese Täuschung gelang es den Tätern, das

https://www.sz.ch/verwaltung/sicherheitsdepartement/kantonspolizei/medienmitteilungen/detailseite.html/8756-8758-8802-9496-9613-10011-12161/news/24495

TLP:GREEN

Angriffsvektor schwache Passwörter – Beispiel (1)

Unbekannte greifen auf dänisches Personenregister zu

Unbekannte haben in Dänemark Zugriff auf die Daten von rund 8,8 Millionen Menschen erhalten. Das Ausmaß ist unklar – ein klassischer Cyberangriff war es nicht.

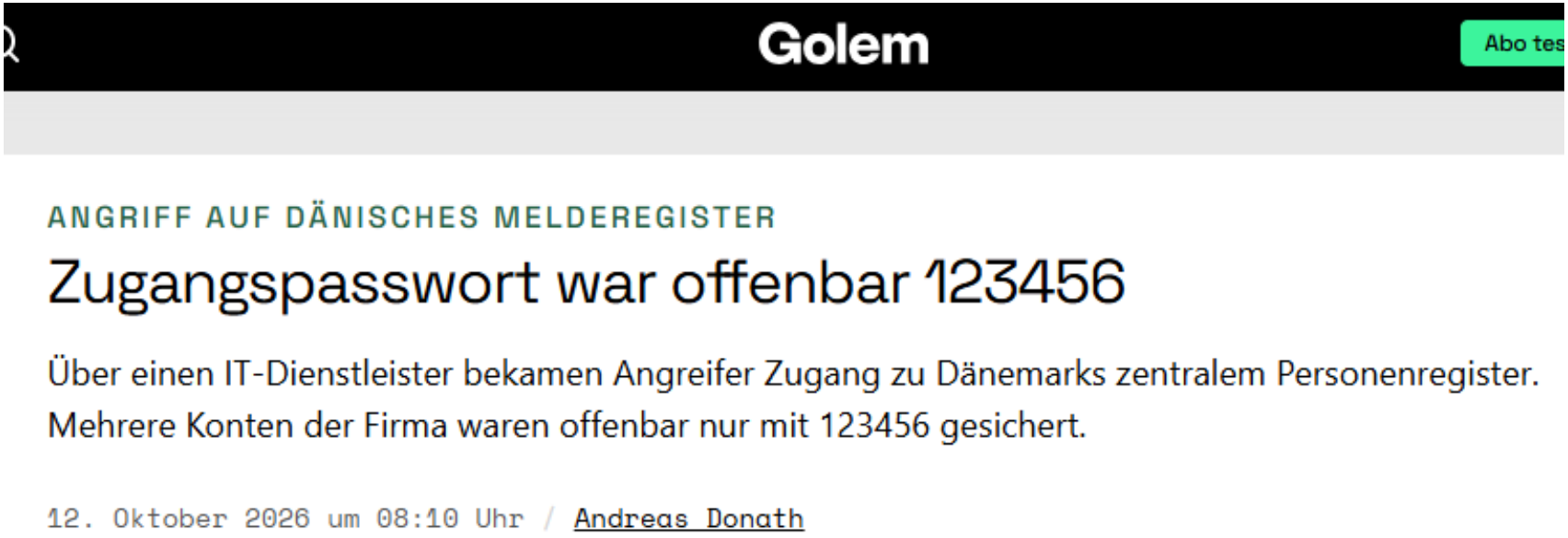
05.10.2026, 12:52 Uhr Lesezeit: 1 Min.

Von dpa

https://www.heise.de/news/Daenemark-Illegaler-Zugriff-auf-Millionen-Datensaetze-11476119.html

TLP:GREEN

Angriffsvektor schwache Passwörter – Beispiel (2)



Golem

Abo tes

ANGRIFF AUF DÄNISCHES MELDEREGISTER

Zugangspasswort war offenbar 123456

Über einen IT-Dienstleister bekamen Angreifer Zugang zu Dänemarks zentralem Personenregister. Mehrere Konten der Firma waren offenbar nur mit 123456 gesichert.

12. Oktober 2026 um 08:10 Uhr / Andreas Donath

TLP:GREEN

Angriffsvektor Veraltete oder nicht gewartete Software mit (bekannten) Sicherheitslücken (1)



Alert!

Exchange-Sicherheitslücke: 85 Prozent der On-Prem-Server in Deutschland anfällig

Ein Proof-of-Concept-Exploit für eine hochriskante Exchange-Lücke ist öffentlich. 85 Prozent der On-Premises-Server sind anfällig.

31.08.2026, 08:01 Uhr Lesezeit: 2 Min. | Security

Von Dirk Knop

https://www.heise.de/news/Exchange-Sicherheitsluecke-85-Prozent-der-On-Prem-Server-in-Deutschland-anfaellig-11434785.html

TLP:GREEN

Angriffsvektor Veraltete oder nicht gewartete Software mit (bekannten) Sicherheitslücken (2)

Herausforderungen durch Einsatz von KI auf Seite der Angreifer

- drastischen Verkürzung des Zeitfensters zwischen **Entdeckung, Exploit-Entwicklung und Angriff**
- Höhere Skalierung von Angriffen
- Schwierige Priorisierung

-> Das **Patchmanagement** entwickelt sich von einer regelmässigen IT-Betriebsaufgabe zu einer **zeitkritischen Massnahme des Risikomanagements**.

TLP:GREEN

STABSSTELLE CYBER-SICHERHEIT
FÜRSTENTUM LIECHTENSTEIN

KMU - Verteidigungsmassnahmen



TLP:GREEN

Wie können sich KMUs verteidigen? (1)

- Verantwortlich für die Cybersicherheit ist die Unternehmensleitung!
- Kenntnis über die verwendeten Netz- und Informationssysteme
- Regelmässige Datensicherungen / Backups
- Wartung der Soft- und Hardware
- Sicherheit der Mailkonten
- Sensibilisierung der Mitarbeitenden
- Einsatz von KI in der Verteidigung

TLP:GREEN

Wie können sich KMUs verteidigen? (2)

KI Agenten – Security Cheat Sheet (Best Practices)

- Tool Security & Least Privilege
- Input Validation & Prompt Injection Defense
- Memory & Context Security
- Human-in-the-Loop Controls
- Output Validation & Guardrails
- …

https://cheatsheetseries.owasp.org/cheatsheets/AI_Agent_Security_Cheat_Sheet.html

TLP:GREEN

STABSSTELLE CYBER-SICHERHEIT
FÜRSTENTUM LIECHTENSTEIN

KMUs profitieren von…



TLP:GREEN

Was passiert gerade?

- Massnahmen- und Umsetzungsplan zur Nationalen Cybersicherheitsstrategie
- Ein Schwerpunkt liegt auf den KMUs

KMU-Förderschecks 2026

Die sogenannten Digitalschecks[1] unterstützen KMUs, mit einer mindestens drei Jahren währenden wirtschaftlichen Tätigkeit, bei der digitalen Transformation. **Cybersicherheit ist ein wesentlicher Bestandteil der Digitalisierung**. Unter bestimmten Voraussetzungen sind auch Projekte in den Bereichen der (Cyber-)Sicherheit förderungswürdig.

[1]https://www.llv.li/de/landesverwaltung/amt-fuer-volkswirtschaft/standortfoerderung/foerderinstrumente/digitalscheck

TLP:GREEN

Dienste CSIRT.LI

- Warn- und Informationsdienst (WID)
  - Registrierung über team@csirt.li
  - 68 Warnungen und Informationen im Jahr 2025
  - 72 Warnungen und Informationen im Jahr 2026 (Stand 14.10.26)
  - ca. 185 Empfänger in Unternehmen und Behörden bekommen Warnmeldungen
- Spezifische Schwachstellenhinweise (SSH)
- **Empfehlung**: Newsbeitrag «Auswirkungen neuer KI-Modelle zur autonomen Entdeckung und Ausnutzung von Schwachstellen»

https://csirt.li/

TLP:GREEN

Zusammenfassung

- Wettrüsten – Angreifer und Verteidiger verwenden KI
- **Geschwindigkeit** ist der bestimmende Faktor
- Zentrale Massnahmen zur Vorbeugung ist die **Sensibilisierung** sowie die Umsetzung klassischer **Cyberhygiene-Massnahmen**.
- Services der Stabsstelle Cyber-Sicherheit für KMUs
  - WID – Anmeldung unter team@csirt.li

TLP:GREEN

Vielen Dank für Ihre Aufmerksamkeit

Stabsstelle Cyber-Sicherheit

Pflugstrasse 16
9490 Vaduz
www.scs.llv.li
info.scs@llv.li

TLP:GREEN