A-SIT

Neue Möglichkeiten für die Digitale Sicherheit durch KI

Gerald Dißauer

Wieso KI für Cybersicherheit?

Wenn Maschinen sicherheitsrelevante Aufgaben im eGovernment-Bereich übernehmen, die vorher zumeist menschlicher Intelligenz vorbehalten war:

- … dann verändert KI die Art und Weise, wie wir gemeinsam Digitale Sicherheit angehen – aus immer besseren Angriffen immer schneller lernen und das Spielfeld verändern?
- … dann bietet KI der Angriffslinie und der Verteidigung innovativere, schnellere, automatisierte Werkzeuge.
- … dann hilft KI uns mit den Datenbergen umzugehen und Schlussfolgerungen, die in den Daten verborgen sind zu finden.
- … dann prägt KI die Sicherheit von Organisationen, der Gesellschaft sowie von eGovernment-Systemen (z.B. Software-Architektur, Security-Anforderungen für Wallet-Systeme, Digitale Signatursysteme).

KI und Menschen ergänzen einander

Security ist Kooperation – gemeinsam

Kompetenzen der KI als ergänzende Unterstützung

- Verteidigung stärken indem KI hilft, die technologischen Nachteile der Verteidigung aufzuholen
- Entwicklung und Betrieb von eGovernment-Systemen (z.B. Digitale Signatursysteme, EUDI-Wallet)

Zusammenarbeit zwischen Menschen und Maschinen

- KI ergänzt die Fähigkeiten der Menschen und macht Sicherheitslösungen effektiver
- Effizienterer Alltag zur kontinuierlichen Absicherung von eGovernment-Systemen

Security ist ein Teamsport und KI ist darin ein selbstlernendes Teammitglied, nur für wen?

KI - Angriffe & Verteidigung gleichzeitig?

Die Security-Dualität durch die Verwendung von KI im eGovernment - wer profitiert?

Vorteile durch die Verwendung von KI für Angriffe

- Automatisierung intelligenterer Angriffe führt zu schnellerer sowie präziserer Ausführung der Attacken
- KI-basierte Attacken sind gezielter (z.B. Ransomware-Attacken) sowie auch oft für Menschen schwer zu erkennen z.B. Social Engineering bzw. Phishing (z.B. Spear-Phishing) oder Deep Fakes

Vorteile durch die Verwendung von KI für die Verteidigung

- Früherkennung und Anomalie-Analyse erlaubt automatisches identifizieren von Angriffen und schnellere Abwehr – dadurch beschleunigte Lerneffekte durch Rückkopplung und Logfile-Analyse
- Kürzere Reaktionszeiten bei KI-gesteuerten Sicherheitslösungen und normalerweise schneller als Menschen sowie verbesserte Security Awareness-Kampagnen für Menschen

(Auch) ein Technologie-Schwerpunkt zu Künstlicher Intelligenz ist abrufbar auf:

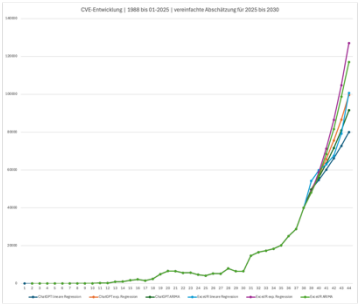
onlinesicherheit.gv.at/

Ein Beispiel aus dem Alltag

Wie könnten sich Sicherheitslücken (CVE) von 2025-2030 entwickeln? (Datenbasis: NIST NVD)

- Abschätzung drei Modelle mit KI (1) Lineare Regression, (2) Exponentielle Regression und (3) ARIMA
- Daten: NIST NVD (Basis: 1988 – 01/2025; mitte) mittels KI, Vergleich mit Excel und R (rechts)

Jahr	Lineare Regression (Prognose)	Lineare Regression (Untergrenze 95%-KI)	Lineare Regression (Obergrenze 95%-KI)	Exponentielle Regression (Prognose)	Exponentielle Regression (Untergrenze 95%-KI)	Exponentielle Regression (Obergrenze 95%-KI)	ARIMA-Modell (Prognose)	ARIMA-Modell (Untergrenze 95%-KI)	ARIMA-Modell (Obergrenze 95%-KI)
2025	49,698 CVEs	47.228 CVEs	52.168 CVEs	49.698 CVEs	47.228 CVEs	52.168 CVEs	49.698 CVEs	47.228 CVEs	52.168 CVEs
2026	54,668 CVEs	51.936 CVEs	57.399 CVEs	57.153 CVEs	54.295 CVEs	60.010 CVEs	56.053 CVEs	53.245 CVEs	58.861 CVEs
2027	60,135 CVEs	57.128 CVEs	63.141 CVEs	65.720 CVEs	62.434 CVEs	69.005 CVEs	63.350 CVEs	60.183 CVEs	66.517 CVEs
2028	66,148 CVEs	62.841 CVEs	69.455 CVEs	75.578 CVEs	71.799 CVEs	79.357 CVEs	71.583 CVEs	68.013 CVEs	75.153 CVEs
2029	72,763 CVEs	69.025 CVEs	76.500 CVEs	86.620 CVEs	82.289 CVEs	90.952 CVEs	80.957 CVEs	77.044 CVEs	84.870 CVEs
2030	80,039 CVEs	75.637 CVEs	84.440 CVEs	99.598 CVEs	94.618 CVEs	104.577 CVEs	91.535 CVEs	87.141 CVEs	95.930 CVEs



Eigene Abbildung, Datenbasis: (NIST NVD, https://nvd.nist.gov/search Letzter Zugriff: 20.1.2025)

Disclaimer:
Beispiel zu Illustrationszwecken, um eine Abschätzung der möglichen CVE-Entwicklung für eine grobe Einordnung der nächsten 5 Jahre zu erstellen. Die NIST NVD-Daten können sich ändern!

[1] CVE – Common Vulnerabilities and Exposures (Anm. zur Sammlung von Sicherheitslücken bzw. ausnutzbaren Schwachstellen)

Ein Beispiel aus dem Alltag | cont´d

KI-basierte Empfehlungen zur sicheren Konfiguration von Verteilten eGovernment-Anwendungen am Beispiel der Verwendung von TLS v1.2?

- Frage: Ist die folgende TLS-Cipher-Suite für kritische eGovernment-Anwendungen wie etwa für digitale Signatursysteme oder Wallet-Systeme empfohlen?
  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- Ergebnis der KI (am 20.1.2025): Grundsätzlich sicher für kritische Systeme aber die KI empfiehlt auch Alternativen:
  - Alternative 1: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (Vergleich: aber Legacy bis derzeit 31.12.2030 laut SOG-IS v1.3)[1]
  - Alternative 2: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (Vergleich: empfohlen laut SOG-IS v1.3)[1]
  - Alternative 3: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (Vergleich: aber Legacy bis derzeit 31.12.2030 laut SOG-IS v1.3)[1]

[1] SOG-IS Crypto Evaluation Scheme, Version 1.3, Februar 2023, abrufbar: https://sogis.eu/uk/supporting_doc_en.html [Letzter Zugriff: 20.1.2025]

Disclaimer:
Dieses bewusst gewählte Beispiel (TLSv1.2) dient dazu, um zu zeigen,
dass KI-Systeme Menschen zielgerichtet unterstützen können, um die digitale Sicherheit zu verbessern

3 absehbare Entwicklungsbereiche

Potential	Praktische Fortschritte in den nächsten Jahren im eGovernment
Fortschrittliche Verteidigung durch KI	▪ Schnellere Angriffserkennung, Muster identifizieren ohne diese verstehen zu müssen, AI-Agents ▪ Verbesserte Source Code-Analyse, optimierte Konfigurationen, gezieltere Vorbereitung, CVE-Analysen ▪ Teamsport Security – mehr denn je, KI unterstützt Menschen z.B. Guidance, Phishing-Attacken erkennen
Innovative Angriffe wegen KI	▪ Wirkungsvolle Prompt Injection Attacken (direkt vs. indirekt), Evasion Angriffe, Sensible Daten abgreifen ▪ Höherer Automatisierungsgrad, unerwünschtes Modell-Verhalten, größere Bandbreite bei Angriffsformen ▪ Schneller, neue Schwachstellen aus bestehenden Daten ableiten, die auch Herstellern nicht bekannt sind
Abschätzungen und neue Erkenntnisse	▪ Treffender pro-aktive Schutzmaßnahmen auswählen, einfachere Trendanalysen, optimierte Architektur ▪ Steigende Datenmengen quasi in Echtzeit untersuchen, etwa: Petabyte, Exabyte, Zetabyte, Yottabyte ▪ Neues Wissen das "versteckt in den Daten schlummert", etwa für gezieltere Awareness-Kampagnen
Leistungsfähige KI-Systeme einsetzen	▪ Aufholen des „1 Schritts hinter den Angreifenden" und einfangen der wachsenden Datenmenge ▪ Kombination Verteilte Systeme, mehr Rechenleistung durch neue Technologien, NoSQL-Systeme ▪ Verbesserte Software-Architektur und absichern mit aktuellen kryptografischen Verfahren (z.B. Wallet)

KI gestaltet das Spielfeld der Digitalen Sicherheit insbesondere für eGovernment-Anwendungen immer mehr und schneller als vorstellbar mit.

Die Lebensrealität und Entscheidungen zur Digitalen Sicherheit der Gesellschaft werden von KI mitgeprägt. Wissen erneuert sich in immer kürzeren Abständen.

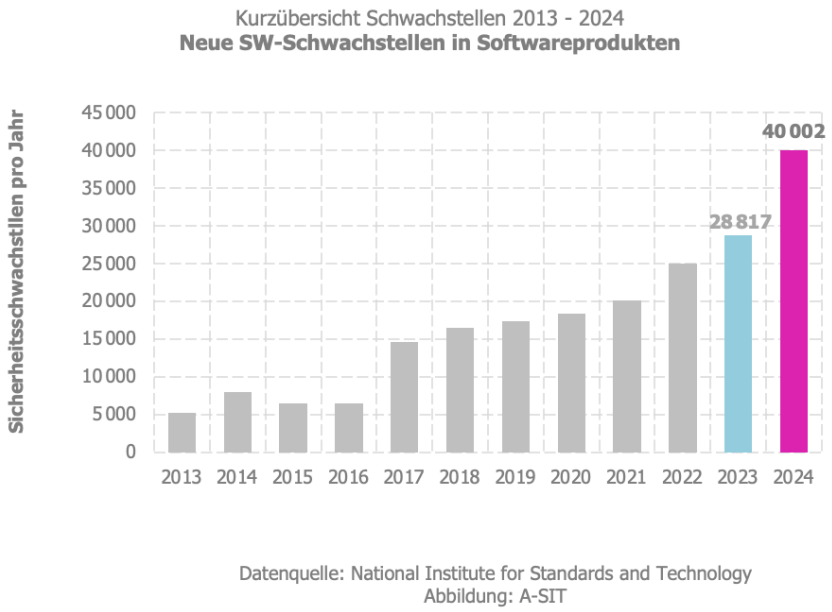
Durch Nutzung der KI kann die Verteidigung den Rückstand auf die Angriffslinie verringern und die Zukunftsfähigkeit von Organisationen und Systemen stärken.

a-sit.at/

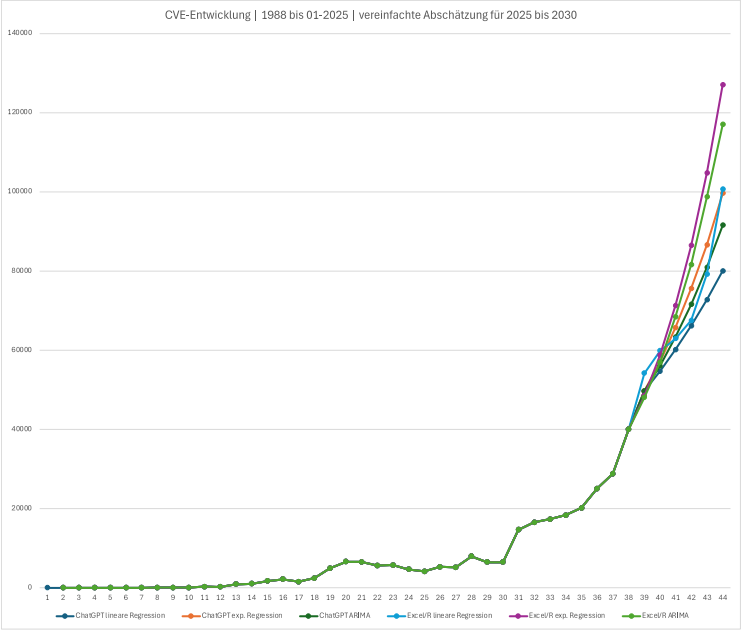
a-sit.at/

Ein Beispiel aus dem Alltag - Vergrößert

Größere Darstellung der beiden Abbildungen CVE-Entwicklung (2013 bis 2024 – links; und 1988 bis 2030 – rechts)



Eigene Abbildung, Datenbasis: (NIST NVD, Letzter Zugriff: 20.1.2025)



Eigene Abbildung, Datenbasis: (NIST NVD, Letzter Zugriff: 20.1.2025)