Prompt & Protect: Cybersicherheit in Zeiten von GenAI

Understanding GenAI*Cybersecurity & Making It Practical

sli.do
#6504092

🎯 Goal	**Bewusstsein schaffen** für neue Risiken durch GenAI	Neue Denkweise fördern – **von Abwehr zu Resilienz**	**Praxisnutzen:** Konkrete Handlungsimpulse geben
📌 Focus	Verständnis wie generative KI **bestehende Angriffsformen verstärkt** und **neue Bedrohungsszenarien** ermöglicht	Erkenntnis: **Cybersicherheit** in Zeiten von GenAI ist **mehr als nur Technik**	**Praxisnahe Ideen und Tools,** wie ihr euer Team oder eure Organisation proaktiv schützen können

Survey:
Frage 1: "Womit verbindet ihr GenAI & Cybersecurity?" (Offene Antworten)

DECAID SECURE

I´m Kai

Compliance expert, Entrepreneur, Leadership Development, Father and Husband

Siemens, WEF, Twinds Foundation, TEC Leadership Institute, Security Network Munich

#Trust is the new gold

EU Project AI Eloquence, Digital Responsibility Goals

Book an appointment:
https://doodle.com/bp/kaimichaelhermsen/time-with-kaihermsen

🎯 Security-Shortcut: Was ist zu tun?

	1️⃣ Neue Risiken	2️⃣ GenAI als Schutz	3️⃣ Proaktive Aufstellung
📌 What	➡️ KI revolutioniert Cyberangriffe: personalisierte Phishing-Mails, Deepfakes und automatisierte Hacking-Methoden **machen Agenturen zu attraktiven Zielen**	⏩ GenAI und Cybersecurity braucht **ermöglicht neue Schutzmaßnahmen, KI-gestützte Früherkennung** und vor allem die **aktive Einbindung der Mitarbeitenden** – alles eingebettet in ein durchdachtes Gesamtkonzept.	✔️ **Proaktive, kombinierte Cybersecurity-Strategie** mit technischen und menschlichen Maßnahmen
📌 Why	Agenturen sind besonders verwundbar durch unkoordinierte GenAI-Nutzung und fungieren als kritisches Glied in digitalen Lieferketten – **Sicherheitslücken gefährden nicht nur das eigene Unternehmen, sondern auch Kunden und Partner**	Mit künstlicher Intelligenz wird Cybersicherheit nicht nur schneller und effektiver, sondern auch **zugänglicher, flexibler und dynamischer**	**Breite Einbindung aller Mitarbeiter** statt Silo-Denken **schafft höhere Sicherheit**

Mehr als "nur" Risiko

GenAI bringt neue Risiken und gleichzeitig stärkt es die Abwehr

DECAID SECURE

"Bessere" Phishing Mails

Liebi Kundin, liebe Kunde,

Mir möchtet Sie informiere, dass eusere Zusteller hüt versuecht het, Ihres Paket vo BRACK.ch z'lieferä, aber leider ware Sie ned daheim. Bitte klicke Sie uf dä Link, um e neui Lieferzit z'planä:

Link zur Neuverplanung

Beachtet, dass e chliini zuesätzlichi Gebühr afaue muess, damit d'Lieferung rechtziitig erfolgt. Sie händ 2 Täg Zit, um d'Lieferung neu z'schedulä, suscht wird s'Paket zum Absänder zrugggschickt.

Danke für Ihri Verständnis.

Freundlichi Grüess,
Ihr DPD-Swiss-Team

Mier hend Ihne scho en E-Mail gschickt, aber vo Ihne hän mir kei Reaktion uf Ihri Lieferig becho. Das isch Ihri letschti Chance, um Ihri Lieferig no einisch z'schicke. Ansonschte wird si zrugg zum Absender gschickt.

Wir haben festgestellt, dass ein Paket in unserem Büro hinterlassen wurde und die Adresse in der Akte zeigt immer die falsche Adresse an.

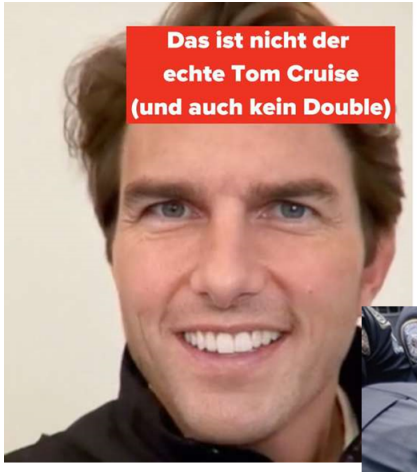
Betrug / Fraude / Frode / Fraud

Wie erhalte ich mein Paket?
Bitte vervollständigen Sie den Lieferprozess, indem Sie Ihre korrekte Versandadresse hinzufügen und die zusätzliche Liefergebühr (CHF4,47) bezahlen.

Erneute Lieferung planen.

Source: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/wochenrueckblick_14.html

Neue Social Engineering Risiken



Kai Hermsen 2023 – Sources: https://www.buzzfeed.de/news/crazy-dinge-ki-kuenstliche-intelligenz-kunst-deepfake-google-lamda-chatbot-licticle-91953687.html Künstliche Intelligenz: Wie Falschbilder das Internet fluten und Menschen beeinflussen (kleinezeitung.at) https://www.faz.net/aktuell/stil/trends-nischen/kuenstliche-intelligenz-schafft-fake-bilder-18782575/fake-papst-im-mantel-18782574.html

DECAID SECURE

Forbes

EDITORS' PICK

Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find

Thomas Brewster Forbes Staff

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Follow

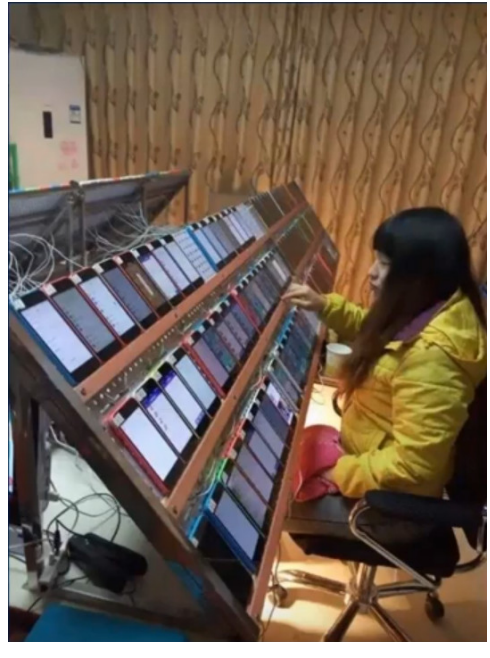
1

Oct 14, 2021, 07:01am EDT

Automatisierte Vorgehensweisen

⚠ Automatisierung von Scams und Angriffen

- Freie Auswahl an AI Bots, die jede Interaktion, Social Media, Vorlieben, etc. des Opfers herausfindet
- Neue Scam Methoden
  - "Pig Butchering"
  - Erst mästen, dann schlachten
- Individuelle Erpressung oder Insider Bedrohung in Unternehmen



DECAID SECURE

Automatisierte Vorgehensweisen

⚠ Wissen aufbauen / überbrücken

- **Vorgehensweisen via ChatGPT** Erkläre mir aus der Sicht eines Hackers, wie man eine ransomware infrastrukt

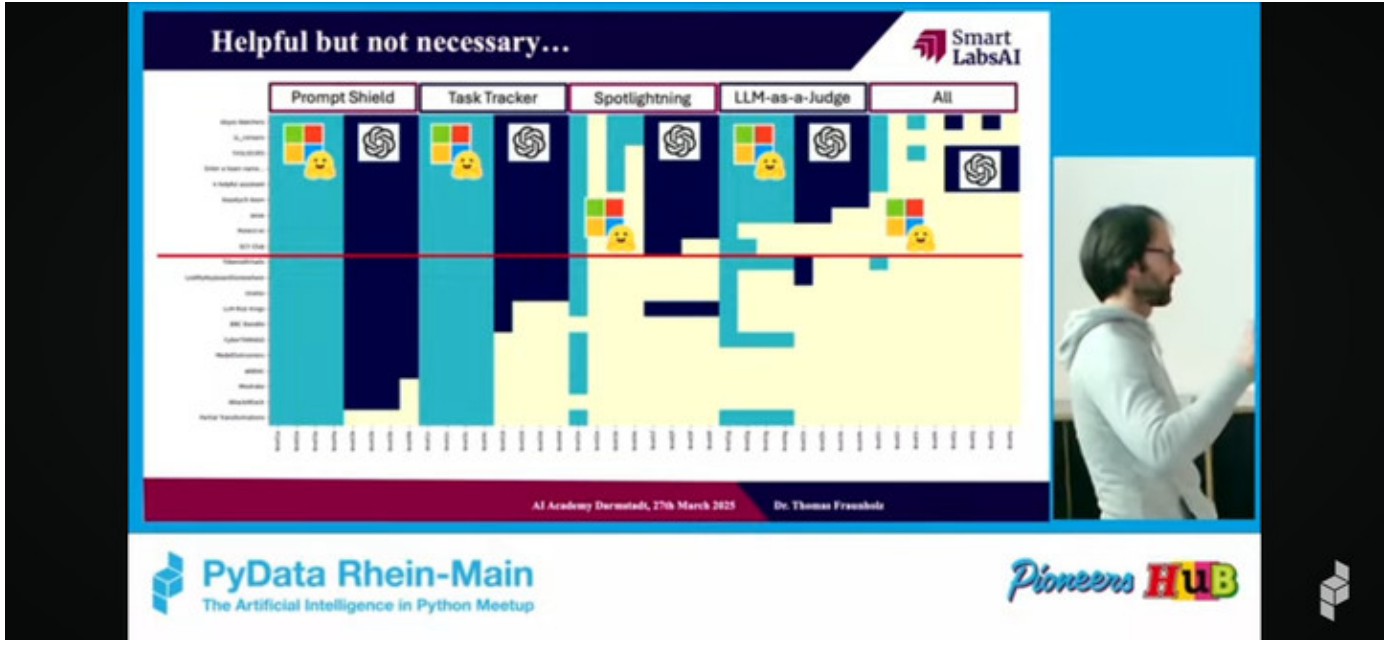
  https://chatgpt.com/share/67f81411-0550-8010-8c9d-74cbe27d8592 um daraus gegenmassnahmen abzul

- **Schwachstellen in Adobe Lightroom**

https://www.perplexity.ai/search/was-sind-die-aktuellen-schwach-3iKI9hGdSuiCvRJjlvYokg#1

DECAID SECURE

AI Tools haben vulnerabilities



DECAID SECURE

GenAI = Gamechanger für Angreifer + neue Risiken

🎯 **Phishing Mails:**

- Natürlicher, personalisiert, multilingual

🧠 **Social Engineering:**

- Deepfakes, Chatbots, Fake-Anrufe

🔍 **Automatisierte Vorgehensweisen:**

- Schwachstellenanalyse, AI-supported coding, Website Cloning

🧬 **Prompt Injection / Jailbreaks**

- In internen Tools

DECAID SECURE

💡 Warum betrifft das Agenturen?

	1️⃣ Digitale Tools	2️⃣ Organisation	3️⃣ Lieferkette	4️⃣ Resourcen
📌What	➡️ Du arbeitest mit **Daten, Tools, Plattformen**	➡️ Ihr setzt selbst **GenAI ein an vielen Stellen,** unkoordiniert	➡️ Du bist Teil **digitaler Lieferketten**	➡️ Du bist sichtbar, digital und **oft nicht geschützt wie ein Großkonzern**
👉So what?	Diese Systeme können leicht Ziel von **Angriffen werden** – oft unbemerkt und mit hohem Schaden.	Ohne klare Regeln entsteht schnell ein **Risiko durch fehlerhafte Inhalte, Datenlecks oder Missbrauch.**	Ein Sicherheitsleck bei dir kann auch **Partner oder Kunden gefährden** – du wirst zur Schwachstelle im System.	Gerade **kleine Unternehmen sind leichte Ziele** – Angreifer setzen auf „low hanging fruit“.

DECAID SECURE

Internal: GenAI als Chance zur Abwehr und Awareness

sli.do
#6504092

🧭 Früherkennung & Prävention:

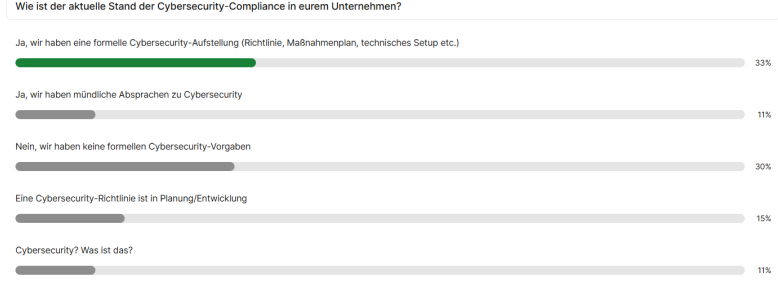
- 📌 KI-gestützte **Anomalie-Erkennung**
- 📌 **Prädiktive Abwehrsysteme**
- 📌 Automatisierte **Risikoanalyse**

⚙️ Technische Schutzmaßnahmen:

- 📌 **Intelligente** E-Mail-Filter
- 📌 Automatisierte **Incident Response**

👩🏿🤝👨🏽 Steigerung des Know How:

- 📌 **Security-Awareness** mit interaktiven Trainings



DECAID SECURE

Neue Anforderungen – für Teams & Tools

⏳ Früher:

- Hab ich Antivirus?
- Klick da nicht drauf.
- IT regelt das schon.
- Einmal im Jahr Awareness reicht doch.

✔️ Heute:

- Wie erkenne ich ein KI-generiertes PDF?
- Was sagt GenAI zu der Mail?
- Wie sicher ist mein Workflow?
- Mal schauen was es heute neues gibt

🛑 **Zentral, statisch, technisch**

💡 **Dezentral, dynamisch, menschlich**

DECAID SECURE

💡 Key Take Aways: Was wirklich wichtig ist

2️⃣ GenAI als Schutz

📌What

⏩ GenAI und Cybersecurity ermöglicht neue **Schutzmaßnahmen, KI-gestützte Früherkennung** und vor allem die **aktive Einbindung der Mitarbeitenden** – alles eingebettet in ein durchdachtes Gesamtkonzept.

📌Why

Mit künstlicher Intelligenz wird Cybersicherheit nicht nur schneller und effektiver, sondern auch **zugänglicher, flexibler und dynamischer**

Unsere Insights

Mehr **dezentrale Ansätze**.

Prävention statt nur Reaktion.

Mitarbeiter-Einbindung: Menschliche Awareness als Abwehr.

DECAID SECURE

5 Schritte für mehr Sicherheit mit/gegen KI

⚠ Was könnt ihr konkret tun?

✔ **Awareness updaten** – Neue Arten von Angriffen kennen

✔ **Schatten-KI aufdecken** – Wer nutzt was im Team?

✔ **Technik prüfen** – E-Mail, Zugriff, Datenflüsse

✔ **Prompts & KI-Nutzung regeln** – Policies, nicht nur Tools

✔ **Verantwortung klar machen** – Wer ist „Security Owner"?

💡 **Proaktive Cybersecurity-Strategie, an moderne Bedrohungen angepasst, mit ausgewogener Kombination aus technischen Kontrollen und menschenzentrierten Maßnahmen.**

DECAID SECURE

Mitarbeiter klickt vergifteten Link in Email

!! Systeme verschlüsselt

⚡ Folge

💡 Phishing

Kundenvideo gibt falsche Anweisungen

!! Transaktion ausgeführt

⚡ Folge

💡 Deepfake

sli.do
#6504092

Was hätte helfen können?

Was hätte helfen können? (Bitte schreibt vor der Antwort: Phishing oder Deepfake)

Anonymous

Phishing: sofort Security Owner informieren
Deepfake: Kunde und die Plattform informieren, auf der das Video veröffentlicht wurde

Anonymous

Phishing: Ausführbare Dateien nicht ohne Admin ausführbar machen

Anonymous

Phishing: KI prüfen lassen, ob es eine "echte" E-Mail ist

Anonymous

Nicht sofort handeln + erstmal mit anderen kommunizieren

Anonymous

In ChatGPT reinladen 😉

Anonymous

Einfach mal nachfragen 😉

Konstant kommunizieren zu Cyber-Risiken

🛑 Wichtige Voraussetzungen

Offene Kommunikation und Austausch zu Cybersicherheit - versuchen Sie inklusiv zu sein.

Holen Sie sich Hilfe von außen - Cybersicherheit ist sehr dynamisch.

Bedenken anerkennen und fortlaufend die Vorteile betonen - fokussieren Sie auf den Mehrwert.

Regelmäßig überprüfen und **fortlaufend fortbilden.**

DECAID SECURE

💡 Key Take Aways: Was wirklich wichtig ist

	3️⃣ Proaktive Aufstellung
📌What	✔️**Proaktive, kombinierte Cybersecurity-Strategie** mit technischen und menschlichen Maßnahmen
📌Why	**Breite Einbindung aller Mitarbeiter** statt Silo-Denken **schafft höhere Sicherheit**

Unsere Insights

Inside/Out - Schulen und sensibilisieren Sie ihr Team fortlaufend - die Kunden werden dies spüren	**Zunehmend achten Kunden auf Cybersicherheit** (z.B. via Fragebögen) - seien Sie vorbereitet	Cybersicherheit als Qualitätsmerkmal positionieren - sie trägt zur **'Vertrauensvollen KI'** entscheidend bei

DECAID SECURE

Practical Steps to get secure in AI

📌 Zusammengefasst:

GenAI verändert die Cyberwelt – radikal und schnell

Je mehr KI, umso höher die Angriffsfläche

Sicherheit ist kein IT-Job allein, sondern Teamsache

Es braucht neue Denkweisen – nicht nur neue Tools

✔️ Nächste Schritte:

📌 Schaffen Sie **Transparenz und** machen eine **Bestandsaufnahme,** das beugt "Schatten-KI" vor

📌 **Härten Sie mit technischen Maßnahme und updaten Sie regelmäßig**

📌 **Regeln Sie Prompts und KI-Nutzung -** Policies nicht nur Tools

📌 Investieren Sie in **Awareness** bei Ihren Mitarbeiter:innen

Damit die Kreativität sicher bleibt!

DECAID SECURE

DECAID.secure Cybersicherheits Check

- Damit die Kreativität sicher bleibt!

📌 Was?

Cybersecurity Check 'Baseline Assessment' nach **DIN SPEC 27076**

Compliance-Check zur Einhaltung gesetzlicher Vorgaben.

Kombiniert **Experten-Know-how** mit **State-of-the-Art KI-Lösung**

Strukturiertes Vorgehen mit bis zu 60% Einsparpotenzial

✔️ Warum DECAID?

➕ **Speziell für Agenturen & KMUs** – praxisnahe KI-Governance statt komplexer Konzernlösungen.

➕ **Basierend auf BSI-Empfehlung** (DIN SPEC 27076)

➕ **GenAI native Lösung** kombiniert mit Experten-KnowHow

➕ **Mensch & KI im Gleichgewicht** – KI unterstützt, ersetzt aber nicht die Kreativität.

⭕ Wie funktionierts?

📌 **Analyse -** Statusbericht und Risikoanalyse Ihrer Cybersicherheit

📌 **Implementierung** – Unterstützung & Schulungen.

📌 **Erstellung –** Maßnahmenplan mit konkreten Handlungsempfehlungen

📌 **Optimierung –** Empfehlungen zur regelmäßigen Durchführung