Cybersecurity im Zeitalter der Künstlichen Intelligenz

#DigitalSecuritySolutions

Eviden Austria GmbH
Birgit Kattnig

EVIDEN Österreich - Kurzvorstellung

Unternehmen Standorte Mitarbeitende & wichtige Fakten

#1 Digitaler Service Provider in Österreich

200 m€ Umsatz pro Jahr

~500 aktive Kunden

3 Tochtergesellschaften

2 Globale Produkte (critical communications, Space)

~1.000 Mitarbeitende

~20 Trainees & Lehrlinge

~40 Werkstudierende

7 Standorte

SEC Consult

consensium

amsbg

Inhalt und Agenda

1. KI-Anwendungen in der öffentlichen Verwaltung
2. Cyber Security trifft KI: Ein Überblick
3. Aktuelle Cyber-Bedrohungen
4. Verantwortungsvolle und sichere KI-Implementierung

Inhalt und Agenda

EVIDEN

KI-Anwendungen in der öffentlichen Verwaltung

Eine zunehmende Entwicklung und aktueller Trend

KI-Anwendungen können helfen schneller, effizienter und serviceorientierter im Sinne der Bürger und Bürgerinnen Bedürfnisse zu bearbeiten.

- **Chatbot** für Standardanfragen von Kunden, Bürgerinnen und Bürger
- Abarbeiten von **Standard** – **Anträgen** wie Förderungen
- **Aufbereitung** von Daten aus verschiedenen Quellen und generieren von Informationen zu **komplexen Themen** wie juristische Recherchen, Arbeitsrecht, etc.

EVIDEN

Was Führungskräfte denken ...

94%

der Führungskräfte möchten dass KI-Lösungen vor der **Implementierung abgesichert** sind, doch nur 24% der GenAI Projekte werden Cybersecurity innerhalb der nächsten sechs Monate berücksichtigen .

Wie werden Cybersicherheitsmaß-nahmen für GenAI umgesetzt und Datenschutz gewährleistet?

84%

der Führungskräfte planen, **generative KI-Cybersicherheitslösungen** gegenüber konventionellen Cybersicherheitslösungen zu priorisieren.

Wie kann GenAI eingesetzt werden um die Cybersicherheit zu verbessern?

85%

der Sicherheitsexperten führten den **Anstieg der Angriffe** im vergangenen Jahr auf böswillige Akteure zurück **, die generative KI einsetzen.**

Wie verteidigt man sich gegen KI unterstützte Cyberangriffe?

Unterschiedliche Studien zeigen ähnliche Ergebnisse, auch wenn der Prozentwert verschieden ist.

Inhalt und Agenda

Cyber Security trifft KI: Ein Überblick

Robuste und sicher Implementierung

- **Beraten:** Kunde kennt Risiken
- **Design:** Robuste KI-Lösungen
- **Implementieren:** Bekannte Sicherheitskonzepte berücksichtigen
- **Betreiben:** Kontinuierliche Überwachung

Cybersicherheitsmaßnahmen

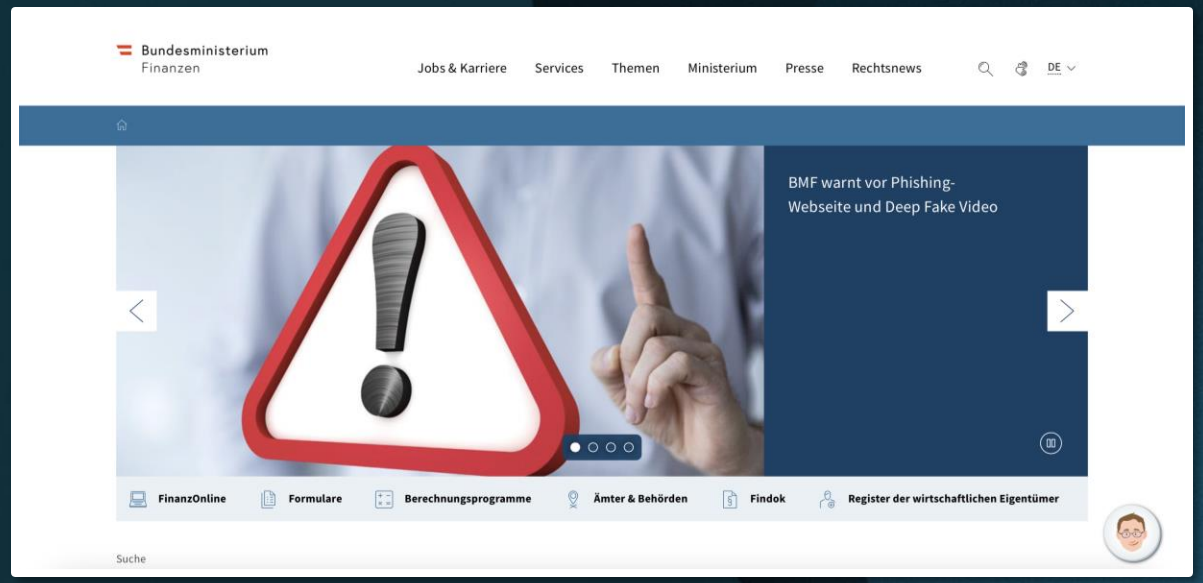
- **Verbessern:** KI-Technologien nutzen, um bestehende Sicherheitsmaßnahmen zu stärken

Verteidigung gegen Cyberangriffe mit KI

- **Verteidigen**: KI-Technologien nutzen, um bestehende Sicherheitsmaßnahmen zu stärken

Inhalt und Agenda

Aktuelles



BMF warnt vor Phishing-Webseite und Deep Fake Video

Internetbetrüger versuchen mit Hilfe einer gefälschten Webseite im Stil von Bundesschatz.at und einem Deep Fake Video an persönliche Daten von Bürgerinnen und Bürgern zu gelangen.

Ministerium warnt vor betrügerischer Webseite im Stil von bundesschatz.at

Eindringliche Betrugswarnung des Finanzministeriums: Internetbetrüger versuchen derzeit, mit Hilfe einer gefälschten Webseite im Stil von bundesschatz.at und einem „Deep Fake Video“ von Finanzminister Brunner an persönliche Daten zu gelangen.

Inhalt und Agenda

1 KI-Anwendungen in der öffentlichen Verwaltung

2 Cyber Security trifft KI: Ein Überblick

3 Aktuelle Cyber-Bedrohungen

4 **Verantwortungsvolle und sichere KI-Implementierung**

Verantwortungsvoll KI-Anwendungen Implementieren

Governance

Ethische KI

Entwickeln Sie Strategien, Innovationen und sorgen Sie für einen ethischen Umgang mit KI

Governance

Etablieren Sie Governance und Kontrolle für Ihre Daten- und KI-Lösungen

Management und Betrieb

Effizientes Verwalten und Betreiben Ihrer Daten und KI-Lösungen

Transparenz und Voreingenommenheit

Erklärbare KI, Übersetzungen, Inklusivität, Fairness und Voreingenommenheits-erkennung

Sicherheit

Datenschutz, Sicherheit, feindliche Angriffe, Stabilität und Robustheit

Kultur, Arbeitsweise und Akzeptanz

EVIDEN

Gestalten Sie Ihre KI-Strategie auf sicheren Grundlagen

„Bei GenAI geht es nicht nur um die Nutzung neuer Technologien, auch viele der bestehenden Sicherheitskontrollen können äußerst nützlich sein“

GenAI Spezifisch Risiken

Neue Risiken für sensible Daten

Erweiterte Bestimmungen

Weitere Bedrohungen und Schwachstellen

Erweiterung des Portfolios

Gen AI, Automatisierung, Analytik, Data Lake, Threat Intel, KI-Modelle, Edge Computing, HPC

Zugriffs-konzepte

Künstliche Intelligenz

KI-gestützte Cyber-Resilienz

Menschliche Intelligenz

Gefahr Erkennung, Antwort, & Erholung

Daten-sicherheit

Cloud Anwendung Sicherheit

CERT, Modern Security Operations Center (MSOC), Vulnerability Labs, Innovationszentren

Anwendung & Infrastruktur Risiken

Sicherheitsberatung, Sicherheitsintegration und Managed Security Services

Bestehende Cybersecurity -Portfolio

EVIDEN

AI Act: EU-Verordnung zur KI

Wann? Wer?

- Am 13.März 2024 durch das Europäische Parlament verabschiedet
- 2026 Inkrafttreten
- Wichtig für Anbieter und Betreiber von KI-Systemen

Klassifizierung

- **Unbedenklich**: Geringes Risiko, minimale Vorschriften
- **Risiko**: Bestimmte Anforderungen an Transparenz und Datenmanagement
- **Hochrisiko**: Strengere Anforderungen, muss vor Markeinführung geprüft werden
- **Verboten**: Praktiken, die als unakzeptabel gelten (z.B. Social Scoring)

Was wird verboten?

- Biometrische und sensible Kategorien
- Auslesen von Gesichtsbildern
- Erfassung von Emotionen
- Social Scoring
- Anwendungen, die manipulieren oder Schwächen gezielt ausnutzen

EVIDEN

Danke!

Birgit Kattnig