A COMPANION OF

digitalswitzerland

DigitalBern

Digital Hack: «Cybersecurity im Wandel – wie KI die Spielregeln verändert»

Key Takeaways

1. Cybersecurity im Wandel – wie KI Risiken und Schutzmechanismen verändert

Prof. Dr. Endre Bangerter, Co-Leiter Institut ICE, BFH

„Als Thesen zu verstehen (sie können sich als falsch herausstellen)":

- **Beide Seiten profitieren – aber das Gleichgewicht ist offen:** Am Beispiel der 0-Day-Schwachstellen haben wir gesehen: sowohl Angriff als auch Verteidigung können von KI profitieren. Natürlich ist man um das Gleichgewicht besorgt – vor allem, wenn die Angreiferseite bevorteilt wird. In welche Richtung es langfristig geht, ist aber nicht klar.
- **Ein neues Niveau – kein neues Spiel:** Cyber bleibt ein Katz-und-Maus-Spiel zwischen Menschen. KI macht beide Seiten schneller, billiger und leistungsfähiger, aber sie kippt das Gleichgewicht wohl nicht fundamental. Temporäre Vorteile sind möglich – etwa für den, der zuerst Zugriff auf das stärkste Modell hat.
- **Die Arbeit in der Cybersecurity verändert sich fundamental:** Auch wenn das Spiel gleich bleibt, ändern sich die Werkzeuge, die Geschwindigkeit und die Rollen. Aufgaben, die bisher rare Spezialisten brauchten (z. B. Reverse Engineering, 0-Day-Suche), werden automatisierbar. Wer in diesem Feld arbeitet – oder Cybersecurity einkauft – muss sich auf massiv veränderte Vorgehensweisen einstellen.

2. Der Einfluss von KI auf Cybersecurity in der Praxis – die Sicht des Dienstleisters

Christoph Wyss, CEO, Wagner AG

- **KI beschleunigt die Cyberwelt. Angreifer & Abwehr.**
- **Nutze führende Abwehrtechnologien mit KI und Menschen.**
- **IT-Basics sind Pflicht (gehärtete PC, Enterprise Level EDR/MDR, MFA / phishing resistant MFA, uvm. frage KI).**

3. Digitale Kommunikation im KI-Zeitalter – neue Risiken für Datensicherheit und Compliance

Renato Stalder, CEO, ePost

- **Digitale Kommunikation ist heute ein Risiko-Thema – nicht nur ein Effizienz-Thema:** Viele Unternehmen nutzen weiterhin E-Mail, Portale oder Messenger für geschäftsrelevante Kommunikation. Diese Kanäle sind jedoch oft nicht ausreichend sicher, nicht nachvollziehbar oder nicht verbindlich – und damit kritisch im Kontext von Datenschutz und Compliance.
- **Verbindlichkeit wird zum entscheidenden Faktor:** Geschäftskommunikation braucht mehr als Geschwindigkeit: Sie muss nachweisbar, rechtssicher und vertrauenswürdig sein. Der digitale Brief zeigt, wie sich die Vorteile der digitalen Welt (Tempo, Automatisierung) mit der Verbindlichkeit des klassischen Briefs kombinieren lassen.
- **Die Zukunft ist hybrid – und automatisiert:** Unternehmen müssen sich nicht mehr zwischen digital und physisch entscheiden: Moderne Kommunikationslösungen ermöglichen eine automatische Zustellung je nach Empfängerpräferenz – digital oder physisch. Das reduziert Komplexität und stellt sicher, dass Inhalte immer ankommen.

Ihre nächsten Schritte

- **Kommunikationsrisiken identifizieren:** Wo fliessen heute sensible oder rechtlich relevante Informationen? Prüfen Sie E-Mail, Portale und manuelle Prozesse auf Schwachstellen und definieren Sie klare Standards für kritische Kommunikation.
- Auf sichere, hybride Lösungen setzen: Digitale und physische Zustellung lassen sich intelligent kombinieren, ohne Medienbruch und mit voller Nachweisbarkeit. **Mehr erfahren oder Beratung anfordern.**
- Interesse an einer Vertiefung der Inhalte? Die Wagner AG zeigt Ihnen gerne auf, wie sie Sie in Sachen Cybersecurity, dem sicheren Einsatz von KI sowie weiteren IT-Themen – vom flexiblen Arbeitsplatz bis zum Premium IT-Support – unterstützen kann. **Kurztermin buchen**
- **Grundsätzlich empfiehlt es sich, auf eine solide IT-Security-Hygiene zu achten**. Darüber hinaus lohnt es sich für jedes Unternehmen, KI zumindest einmal auszuprobieren, nicht zwingend im IT-Security-Kontext, sondern ganz allgemein im Betrieb, um mögliche Effizienzgewinne zu entdecken.
- **KI sicher und regelkonform einsetzen:** Wer KI im Unternehmen einsetzt, muss auch die Sicherheits- und Governance-Anforderungen im Blick haben. Unser Partner EY zeigt, wie Sie KI-Modelle absichern, regulatorische Anforderungen einhalten und klare Verantwortlichkeiten etablieren. **Hier mehr erfahren**