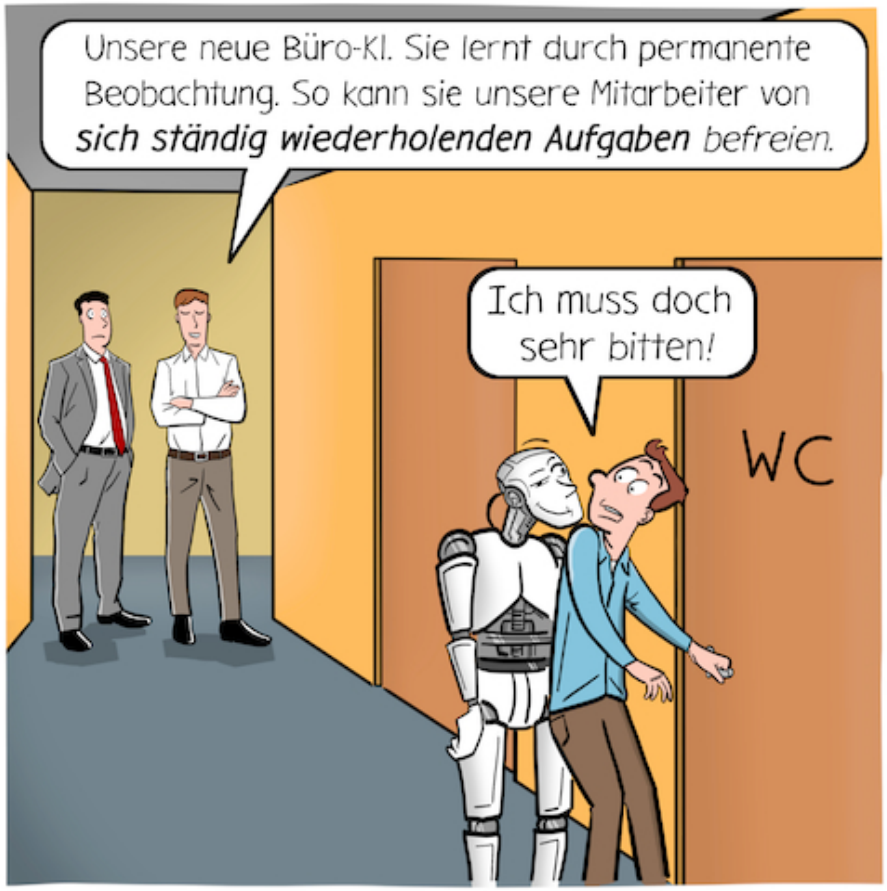
Trendthemen und interessante Dokumente

H. Lubich

lubich@acm.org

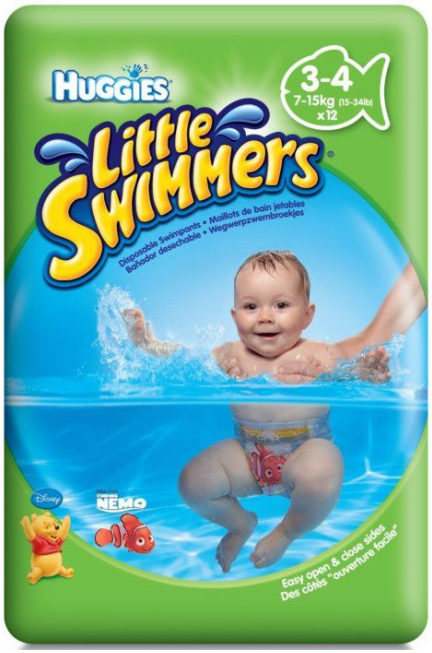
Der derzeitige Mega-Trend der IT: KI (mal wieder)



De derzeitige Mega-Trend der IT: KI (mal wieder)

- Der Weg zur heutigen KI
  - KI der 60er Jahre und «Absturz» wegen überzogener Erwartungshaltungen
  - «Wiedergeburt» als neuronale Netze und (mit viel Training) selbstlernende Systeme
  - Kombination mit autonom agierenden physischen Systemen (Robotik, Drohnen, Fahrzeuge, Produktionstechnik usw.)
  - Aktiver Wissensaustausch zwischen autonom agierenden Systemen
- Die neuen «Hintertüren» für die öffentliche Akzeptanz:
  - (Teil)-autonome Fahrzeuge
  - ChatBots mit intuitiv nutzbaren Schnittstellen / Apps
  - Bilderstellung und -bearbeitung

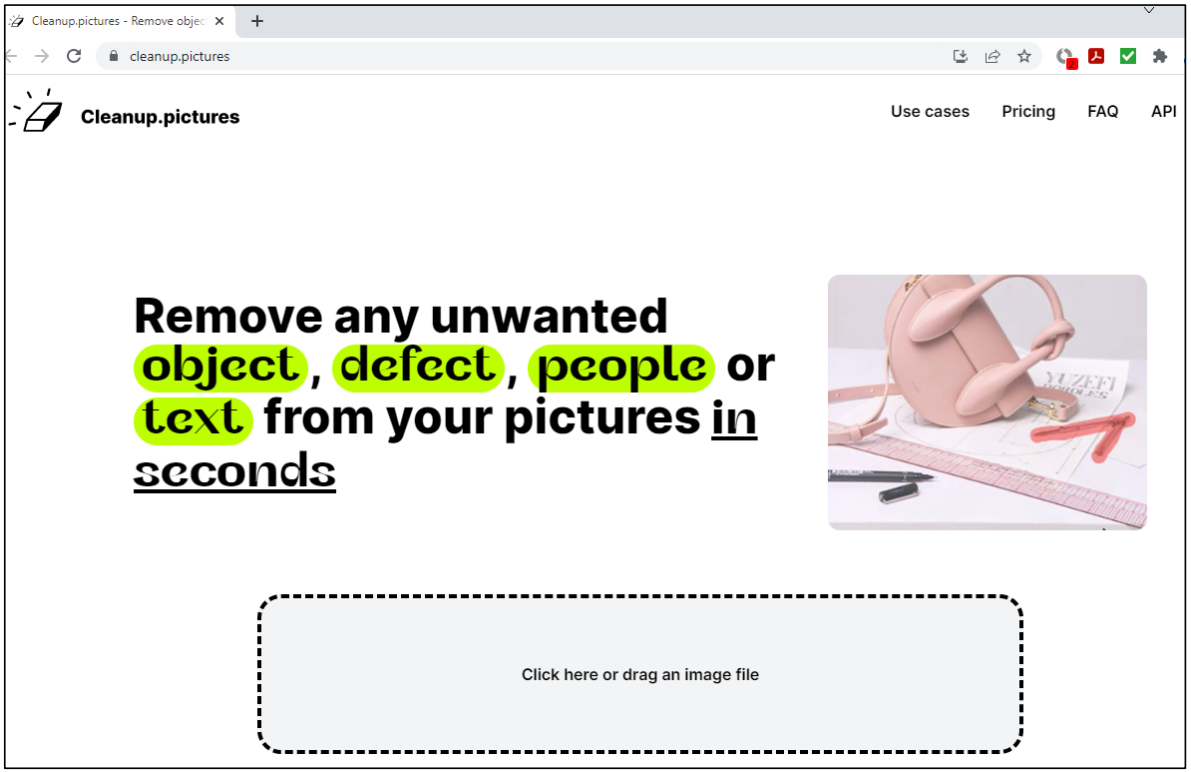
Beispiel 1



Der «alte» Weg: Man beauftragt einen Adobe Photoshop Spezialisten und hofft, dass es keine Blamage wird

Der «neue» Weg»: man beauftragt einen KI Software-Dienst (Midjourney, Microsoft Bing Image Creator etc.)

Beispiel 2: Bilder bearbeiten (in der Cloud!)



https://cleanup.pictures/

KI im Kontext Cyber-Sicherheit

- Angreifer: bessere Deep Fakes (Bilder, Videos, Sprache), gezielte authentische Fake News oder Data Poisoning zur Meinungsbeeinflussung, authentische Gesprächsführung mit Opfern, Erkenntnisse aus der Auswertung von Anfragen, Erstellung authentischer Phishing-Mails und Malware, sehr adaptive Angriffe auf Sicherheitssysteme und auf kommerziell interessante Anwendungen (z.B. Sportwetten, Online-Casinos) usw.
- Verteidiger: Erkennung von Fakes, Erkennung komplexer, bisher nicht erkannter Muster in grossen Datenmengen (Logs usw.), Automatisierung von Analysen
- Beide Seiten: hoher Aufwand für Training und effektiven Einsatz, Spezialwissen, Umgang mit Fehlern und «false positives»
- KI gegen KI: (noch) nicht direkt, aber zu erwarten (Chatbot Angreifer sucht Informationen zu Opfer vs. Chatbot im Honeypot sucht Informationen zu Angreifer oder «KI-Firewall» vs. «KI-Attack-Roboter»)
- Regulatorische Massnahmen (Moratorium, Labelling, Ethik-Vorgaben usw.) greifen vermutlich nicht

Interessante Dokumente

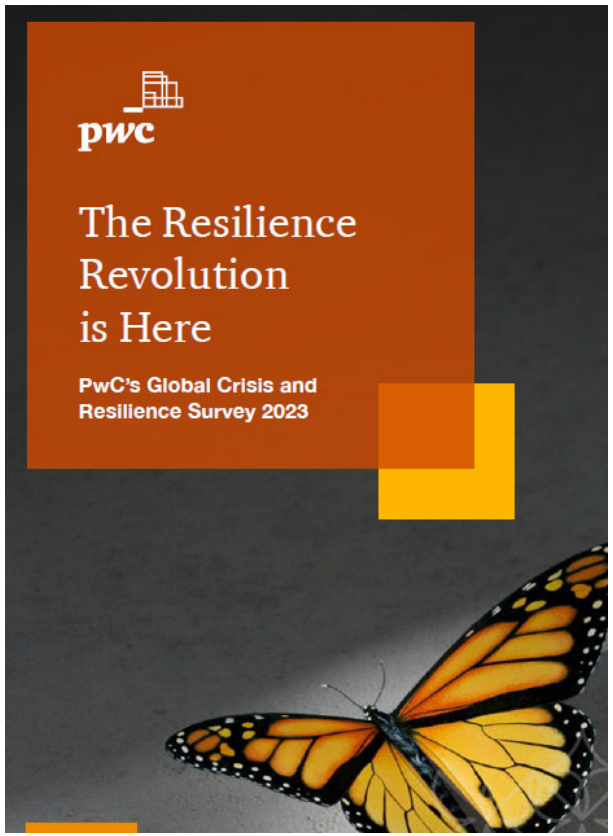
Nationale Cyberstrategie ab 2023

- Erarbeitung unter stärkerem Einbezug diverser Fachexperten und Anspruchsgruppen
- Geltung ab 2023, kein fixes «Ablaufdatum» mehr, Steuerung und Updates durch Bund, Kantone, Wirtschaft und Hochschulen
- Koordination mit umgebenden Dokumenten: Strategie Digitale Schweiz, Nationale Strategie zum Schutz kritischer Infrastrukturen (SKI), Bericht des BR über die Sicherheitspolitik der Schweiz, Gesamtkonzeption Cyber der Schweizer Armee, Strategie Digitalaussenpolitik usw.
- 3 Bundeszuständigkeiten: Cybersicherheit, Cyberdefence, Cyberstrafverfolgung

Bericht diverser Cybersicherheitsgehörden zu «Security by Design and Default»

Table of Contents

PwC Global Crisis ad Resilience Survey 2023



Besides the pandemic, what are organisations concerned about in the next two years?

01 **Cyberattack**

02 **Supply chain disruption**

03 **Employee retention and recruitment**

It is with these insights in mind, and amid the current state of constant disruption, that we believe all organisations should be asking these key questions to rethink their approach to resilience:

The survey data revealed three key takeaways:

Integration

An integrated resilience programme is essential – and if you aren't developing a strategy to move in that direction, you are falling behind.

Leadership

Thriving in permacrisis requires a senior leader, executive sponsorship and upskilled teams.

Operational Resilience

Leading organisations are adopting an operational resilience (OpRes) approach and leveraging technology to enable a panoramic view of their risk and resilience landscape.

CYBERSICHERHEIT