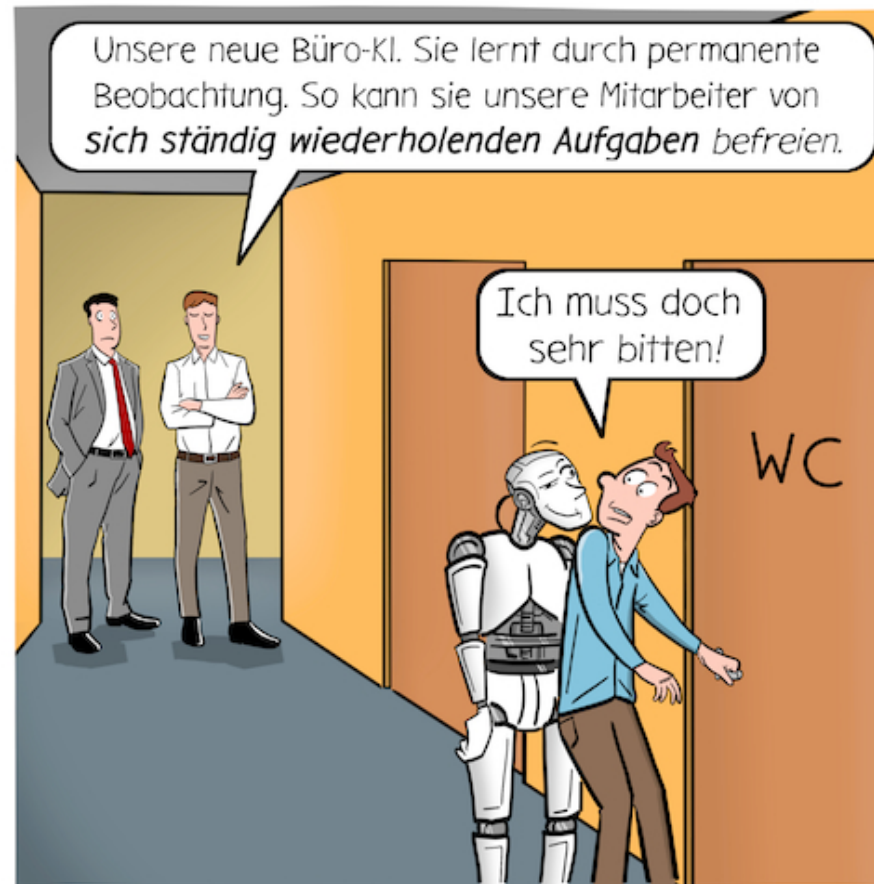


Trendthemen und interessante Dokumente

H. Lubich

lubich@acm.org

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



Der 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

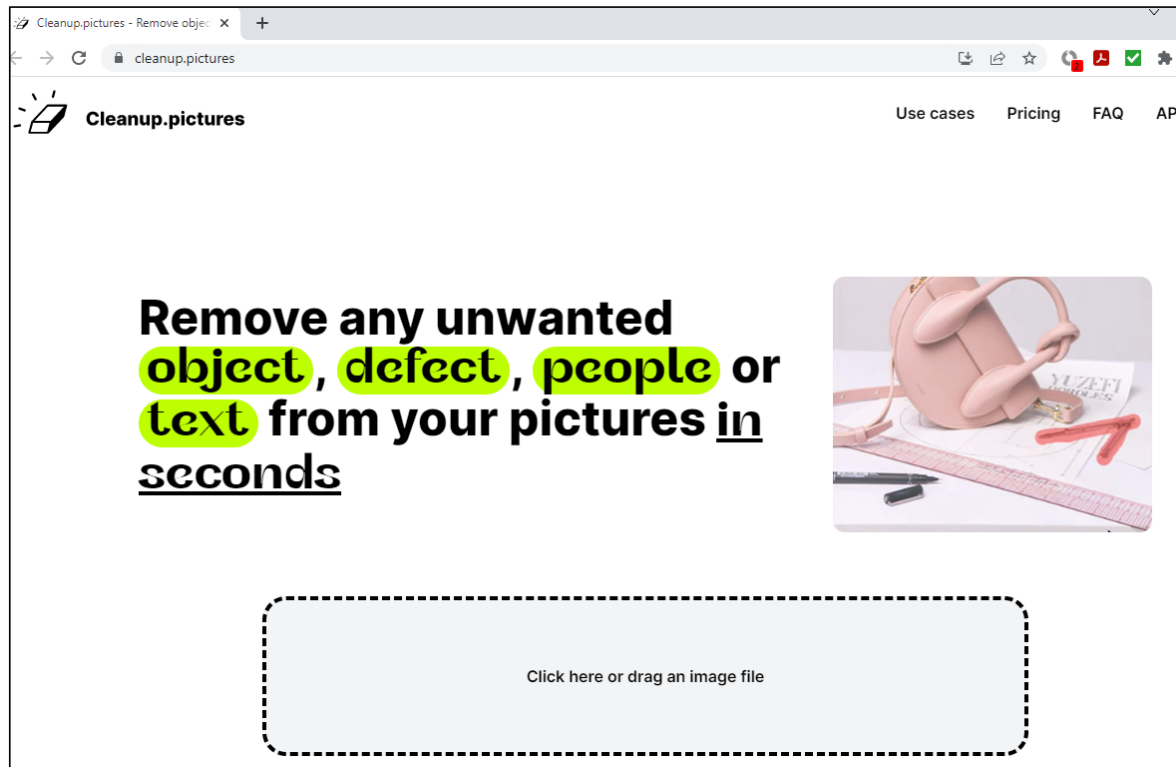


Der «alte» Weg: Man beauftragt einen Adobe Photoshop Spezialisten und hofft, dass es keine Blamage wird



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

Beispiel 2: Bilder bearbeiten (in der Cloud!)




Cleanup.pictures - Remove objec x +

cleanup.pictures

Use cases Pricing FAQ API

Remove any unwanted object, defect, people or text from your pictures in seconds



Click here or drag an image file

The screenshot shows the Cleanup.pictures website interface. At the top, there is a browser tab and address bar. The main content area features a large text block with the service's value proposition, where the words 'object', 'defect', 'people', 'text', and 'seconds' are highlighted in yellow. To the right of this text is a small thumbnail image of a pink bag on a desk with drafting tools. Below the text is a large dashed rectangular box containing the text 'Click here or drag an image file'. The website header includes the logo and navigation links for 'Use cases', 'Pricing', 'FAQ', and 'API'.



<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

1	Einleitung	4
1.1	Die Cyberbedrohungslage.....	4
1.1.1	Bedrohung durch Cyberangriffe	4
1.1.2	Menschliches Fehlverhalten und technische Ausfälle.....	6
1.1.3	Einflussfaktoren auf die Bedrohungslage	6
1.2	Stand des Schutzes der Schweiz vor Cyberbedrohungen	8
1.2.1	Die ersten beiden nationalen Cyberstrategien.....	8
1.2.2	Strategischer Kontext der Cyberstrategie	8
1.3	Organisation zum Schutz vor Cyberbedrohungen in der Schweiz.....	9
1.3.1	Organisation und Zuständigkeiten im Bund.....	9
1.3.2	Organisation und Zuständigkeiten bei den Kantonen	10
1.3.3	Gemeinsame Steuerung der NCS durch Bund, Kantone, Wirtschaft und Hochschulen	10
2	Ausrichtung der NCS	11
2.1	Vision und strategische Ziele.....	11
2.1.1	Vision.....	11
2.1.2	Strategische Ziele	11
2.2	Grundsätze	11
2.3	Zielgruppen	12

3	Massnahmen der NCS	13
3.1	Massnahmen für das Ziel «Selbstbefähigung»	13
	M1 Bildung, Forschung und Innovation in der Cybersicherheit.....	13
	M2 Sensibilisierung.....	15
	M3 Bedrohungslage.....	16
	M4 Analyse von Trends, Risiken und Abhängigkeiten.....	17
3.2	Massnahmen für das Ziel «Sichere und verfügbare digitale Dienstleistungen und Infrastruktur»	19
	M5 Schwachstellen erkennen und verhindern.....	19
	M6 Resilienz, Standardisierung und Regulierung.....	20
	M7 Ausbau der Zusammenarbeit zwischen den Behörden.....	22
3.3	Massnahmen für das Ziel «Wirksame Erkennung, Verhinderung, Bewältigung und Abwehr von Cyberangriffen»	23
	M8 Vorfallmanagement.....	23
	M9 Attribution.....	25
	M10 Krisenmanagement.....	26
	M11 Cyberdefence.....	27
3.4	Massnahmen für das Ziel «Effektive Bekämpfung und Strafverfolgung der Cyberkriminalität»	28
	M12 Ausbau der Zusammenarbeit der Strafverfolgungsbehörden.....	29
	M13 Fallübersicht.....	30
	M14 Ausbildung der Strafverfolgungsbehörden.....	31

3.5	Massnahmen für das Ziel «Führende Rolle in der internationalen Zusammenarbeit»	32
	M15 Stärkung des digitalen internationalen Genfs	32
	M16 Internationale Regeln im Cyberraum	33
	M17 Bilaterale Zusammenarbeit zu strategischen Partnern und internationalen Kompetenzzentren	34
4	Umsetzung der Strategie	35
5	Abkürzungsverzeichnis	36
6	Glossar	37

-
- 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 Digitalausserpolitik usw.
 - 3 Bundeszuständigkeiten: Cybersicherheit, Cyberdefence, Cyberstrafverfolgung

Bericht diverser Cybersicherheitsgehörden zu «Security by Design and Default»



TLP:CLEAR



National Cyber Security Centre
a part of GCHQ



Australian Government
Australian Signals Directorate

ACSC

Australian Cyber Security Centre



Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité



National Cyber Security Centre
Ministry of Justice and Security

certnz

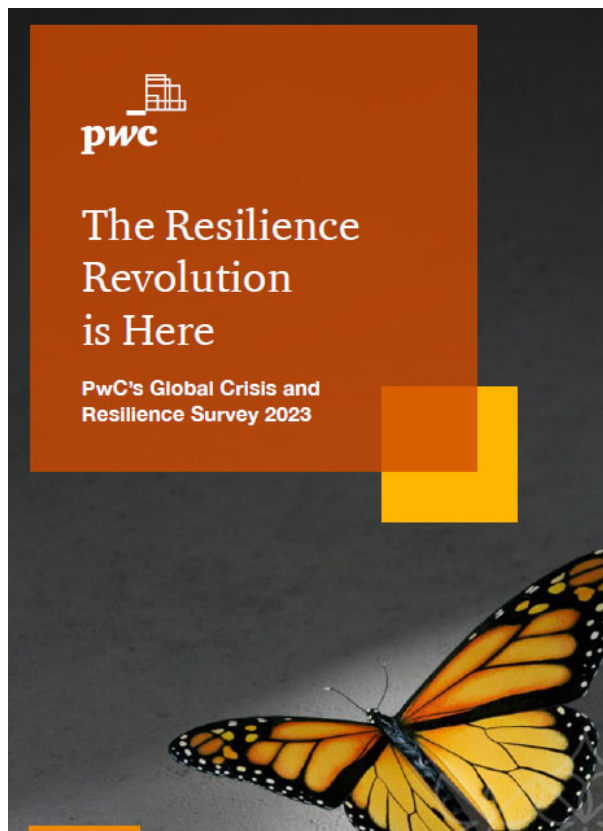


National Cyber Security Centre
PART OF THE GCSB

Table of Contents

<i>Table of Contents</i>	2
Overview: Vulnerable by Design	3
<i>Secure-by-Design</i>	4
<i>Secure-by-Default</i>	5
Recommendations for Software Manufacturers	6
<i>Software Product Security Principles</i>	6
<i>Secure-by-Design Tactics</i>	8
<i>Secure-by-Default Tactics</i>	10
Hardening vs loosening guides	12
Recommendations for Customers.....	12
Disclaimer	13
Resources	13

PwC Global Crisis and 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.



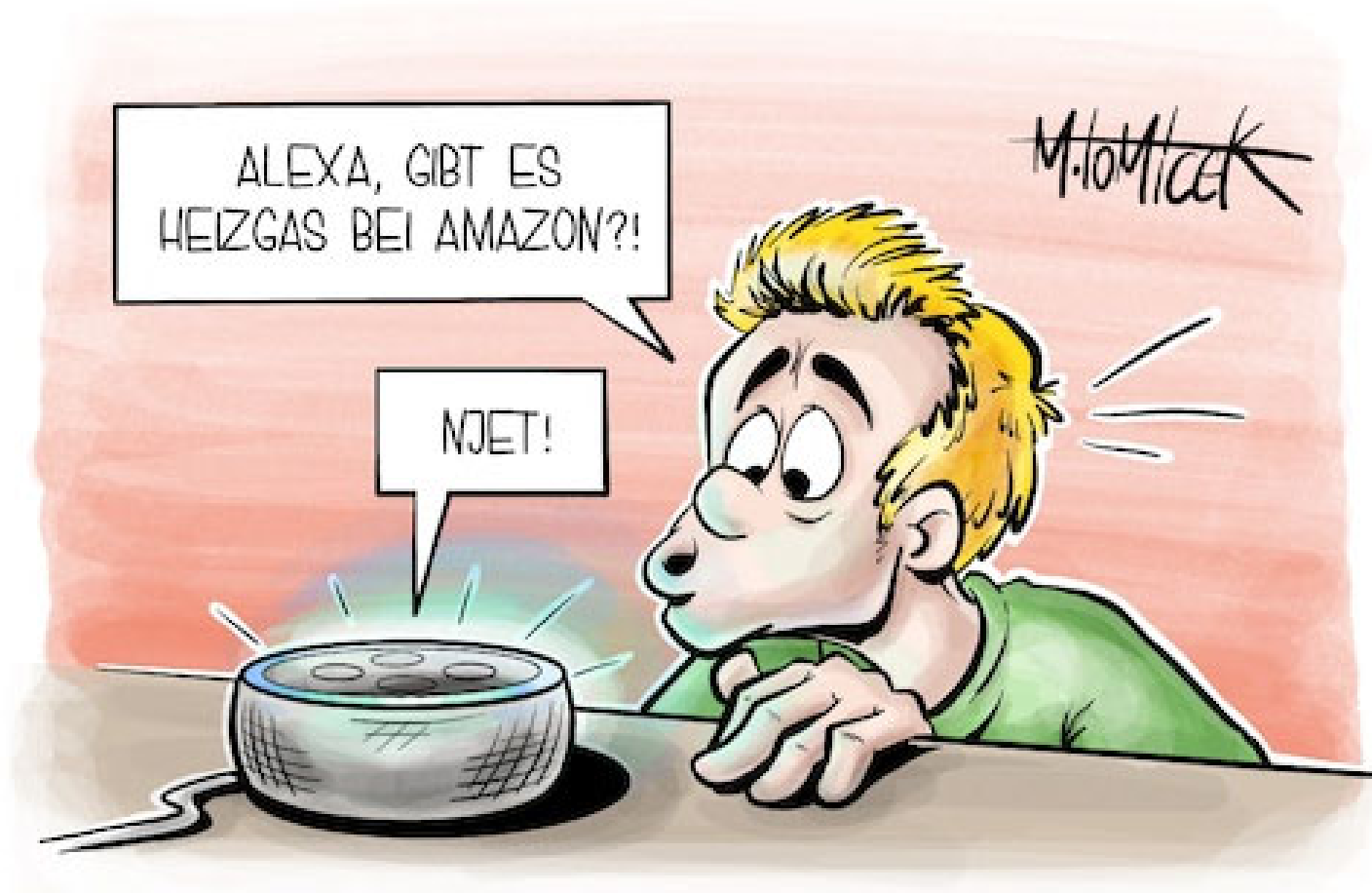
Leadership

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