

Digitale Risiken in einer KI-gestützten, cloudbasierten Gesellschaft – und die Verantwortung

29. Symposium on Privacy and Security
Dienstag, 24. Juni 2025



1

Über mich:

Studienleiter Digitale Medien & KI am MAZ
Freier Techjournalist für Dnip, NZZ, WoZ & mehr

Ehemals:

Chefredaktor Inside IT
Computerworld, PCtipp, Migros-Magazin etc.



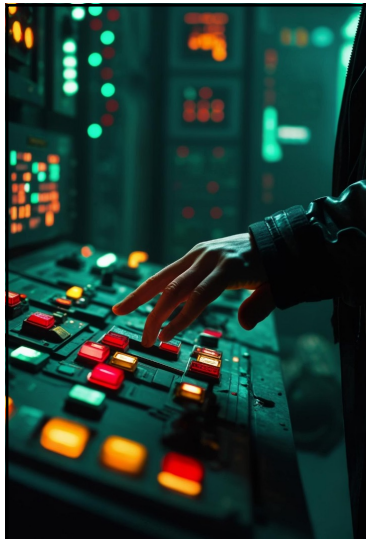
2

Inhalt:

Risikobeurteilung braucht Transparenz – aber KI entzieht sich ihr strukturell.
Wie können wir Risiken beurteilen, wenn wir die Systeme nicht mehr verstehen?

- Risiken beurteilen, ohne die Systeme zu verstehen?
- Die "neuen" Probleme mit KI und Cloud
- Was heisst Verantwortung heute?
- Ideen für neue Ansätze

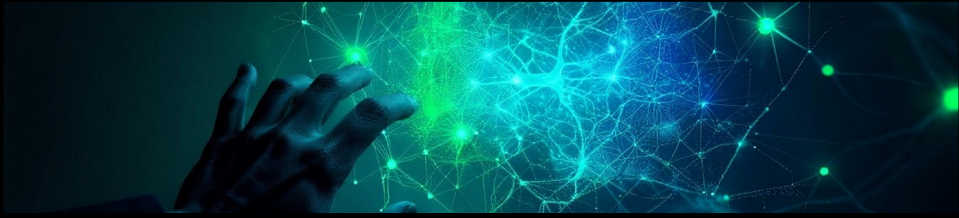
3



Die Illusion der Kontrolle

- ? Risiken im Nebel**
Wie kann man Risiken beurteilen, wenn man die Systeme nicht mehr versteht?
- ⚡ Schneller, nicht weiser**
Technologie hat unsere Prozesse beschleunigt. Unsere Urteilsfähigkeit nicht.
- 📄 Kontrollverlust**
Unsere Kontrollillusion wächst mit der Komplexität der Systeme.

4



Künstliche Intelligenz – Macht ohne Erklärbarkeit

Das Transparenzparadox Risikobeurteilung erfordert Durchblick. KI-Systeme werden zunehmend undurchschaubar.	Komplexität vs. Verständnis Je leistungsfähiger ein KI-System, desto schwieriger wird seine Erklärbarkeit.	Kontrolle abgeben Wir delegieren Entscheidungen an Systeme, deren Funktionsweise wir nicht nachvollziehen können.
---	--	---

5

Blackbox-Problematik

Wahrscheinlichkeit statt Gewissheit KI liefert statistische Wahrscheinlichkeiten. Kein Verständnis. Keine Erklärung. Wir verwechseln Präzision mit Wahrheit.	Vertrauensproblem Vertrauen bedeutet eigentlich: Wir akzeptieren Unsicherheit. Risiken werden übersehen, weil wir die richtigen Fragen nicht stellen können.
---	---

6



Bias & Halluzination: Falsche Sicherheit

-  **Voreingenommene Systeme**
KI reproduziert gesellschaftliche Ungleichheiten in ihren Entscheidungen. Diskriminierung wird unsichtbar automatisiert.
-  **KI-Halluzinationen**
Systeme erfinden überzeugende Falschinformationen. Mit perfekter Selbstsicherheit präsentiert.
-  **Scheinsicherheit**
Fehler werden nicht als solche erkannt. Die Präzision der Antworten täuscht über Ungenauigkeit hinweg.

7



Schatten-KI

KI wird sowieso eingesetzt
Ob das die Organisation will, oder nicht

8

Was passiert?

(I)

9

Allgemeiner Kontext

 20250502_71160_Brief.pdf
PDF

Um was für ein Dokument handelt es sich hier?

Wie ist der Name der Schuldnerin?

Die Schuldnerin im Dokument ist:

Y:

S:

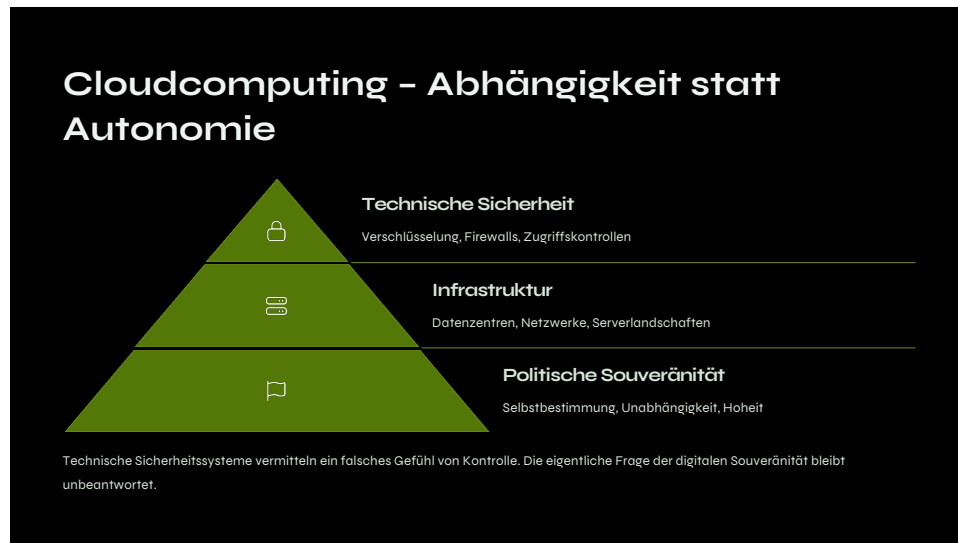
Bi:

Diese Angaben stammen direkt aus dem hochgeladenen PDF „20250502_71160_Brief.pdf“. Wenn du weitere Informationen zur Person oder zur Betreuung benötigst, gib mir bitte Bescheid – z. B. für das Verfassen eines Schreibens, das Einlegen eines Rechtsvorschlages oder das Prüfen auf öffentliche Betreibungsregister.

- Gläubigerin: Zalando SE, Berlin
- Vertreterin: Intrum AG, Schwerzenbach
- Schuldnerin: [Name wurde entfernt], wohnhaft in Zürich

Der soziale Rückzug, Isolation und Schamgefühle werden wiederholt erwähnt.

10



11

54 Ausschreibungen

1 Selektives Verfahren

3 Offene Verfahren

51 Freihändige Zuschläge

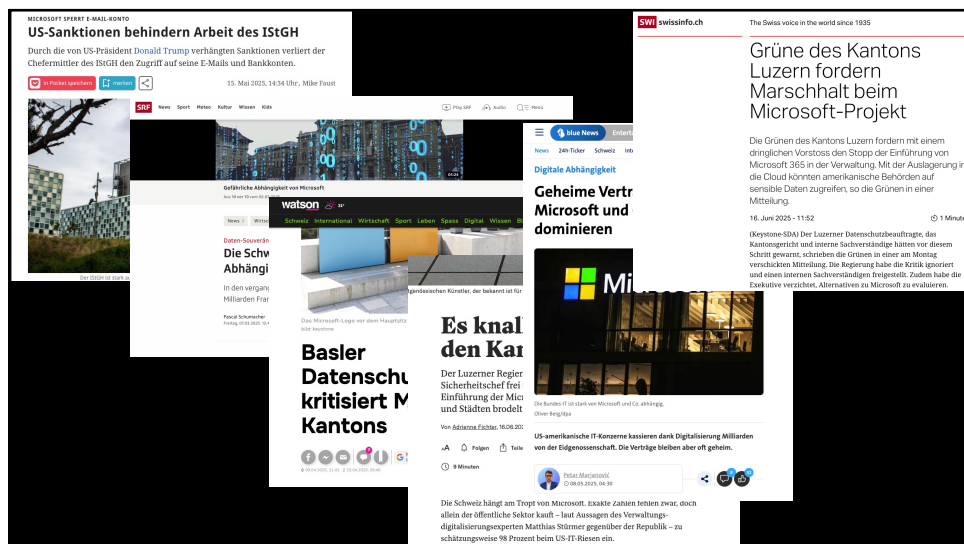
Total 749 Millionen Franken

12

Was passiert?

(II)

13



MICROSOFT SPERRT E-MAIL-KONTEN
US-Sanktionen behindern Arbeit des IstGH
 Durch die von US-Präsident Donald Trump verhängten Sanktionen verliert der Chefermittler des IstGH den Zugriff auf seine E-Mails und Bankkonten.
 15. Mai 2025, 14:34 Uhr, Mike Faust

SRF
 News Sport Kultur Wissen Kids
 15. Mai 2025, 14:34 Uhr, Mike Faust

Watson
 Schweiz International Wirtschaft Sport Leben Spezial Digital Wissen B
Digitale Abhängigkeit von Microsoft
 Die Schweiz ist stark von Microsoft und Co. abhängig.
 Die Bundes IT ist stark von Microsoft und Co. abhängig.
 Eine Analyse

Blue News
 News 24h-Ticker Schweiz Info
Digitale Abhängigkeit
Geheime Verträge Microsoft und dominieren
 Die Bundes IT ist stark von Microsoft und Co. abhängig.
 Eine Analyse

swissinfo.ch
 The Swiss voice in the world since 1935
Grüne des Kantons Luzern fordern Marschhalt beim Microsoft-Projekt
 Die Grünen des Kantons Luzern fordern mit einem dringlichen Vorstoss den Stopp der Einführung von Microsoft 365 in der Verwaltung. Mit der Auslagerung in die Cloud könnten amerikanische Behörden auf sensible Daten zugreifen, so die Grünen in einer Mitteilung.
 16. Juni 2025 - 11:52 1 Minute
 (Keynote-SDA) Der Luzerner Datenschutzbeauftragte, das Kantonsgericht und interne Sachverständige hätten vor diesem Schritt gewarnt, schrieben die Grünen in einer am Montag verschickten Mitteilung. Die Regierung habe die Kritik ignoriert und einen internen Sachverständigen freigesetzt. Zudem habe die Exekutive versichert, Alternativen zu Microsoft zu evaluieren.

Basler Datensicherheitskritik
 Der Luzerner Regier Sicherheitschef frei Einführung der Mica und Städten brodet
 Von Adriaan Fichtler, 16.06.2025
 9 Minuten

Es knallt den Kai
 Der Luzerner Regier Sicherheitschef frei Einführung der Mica und Städten brodet
 Von Adriaan Fichtler, 16.06.2025
 9 Minuten

US-amerikanische IT-Konzerne kassieren dank Digitalisierung Milliarden von der Eigenwirtschaft. Die Verträge bleiben aber oft geheim.
 Die Schweiz hängt am Tropf von Microsoft. Exakte Zahlen teilen zwar, doch allein der öffentliche Sektor kauft – laut Aussagen des Verwaltungsdigitalisierungsexperten Matthias Stimmer gegenüber der Republik – zu schätzungsweise 98 Prozent beim US-IT-Riesen ein.

14

Globale Infrastrukturen vs. lokale Gesetze



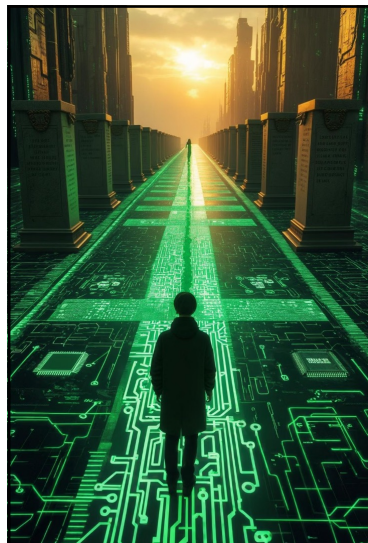
15

Strategische Abhängigkeit: Vendor Lock-ins



Die kurzfristigen Vorteile führen zu langfristigen Risiken. Die wahren Kosten werden erst sichtbar, wenn ein Ausstieg nötig wird.

16



Zwischen Technik & Ethik – Was heisst Verantwortung heute?

- 
Die richtigen Fragen stellen
 Nicht nur "Können wir?", sondern "Sollten wir?"
- 
Abwägungen transparent machen
 Welche Werte stehen auf dem Spiel? Wer profitiert, wer trägt Risiken?
- 
Verantwortung definieren
 Klare Zuständigkeiten schaffen. Rechenschaftspflicht festlegen.
- 
Langzeitperspektive einnehmen
 Auch zukünftige Generationen berücksichtigen. Nachhaltigkeit der Entscheidungen prüfen.

17

Risiko als gesellschaftlicher Aushandlungsprozess

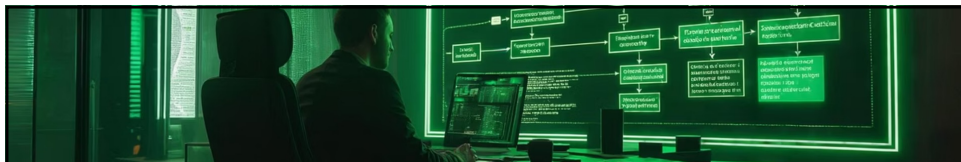
		
Technokratischer Ansatz	Demokratischer Diskurs	Brückenbau
Risiken werden berechnet. Expertenmeinungen dominieren. Gesellschaftlicher Kontext fehlt.	Betroffene werden einbezogen. Verschiedene Perspektiven fliessen ein. Werte werden berücksichtigt.	Technische Expertise und gesellschaftliche Werte müssen verbunden werden. Dialog statt Diktat.

18

Wir sind nicht nur Nutzer:innen – wir sind Ermöglicher:innen



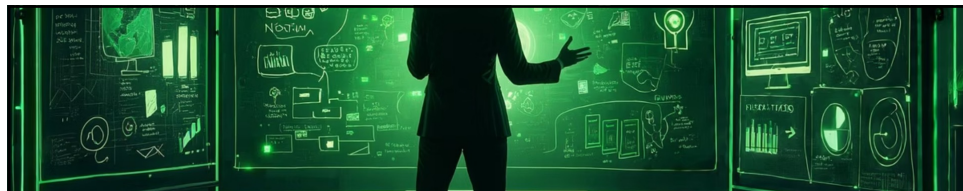
19



Was heisst das für die Praxis?

Traditioneller Ansatz	Verantwortungsvoller Ansatz
Risiken isoliert betrachten	Systemisches Risikoverständnis entwickeln
Compliance-Checklisten abarbeiten	Ethische Reflexion institutionalisieren
Technologie als gegeben hinnehmen	Technologieeinsatz aktiv gestalten
Reaktive Schadensbegrenzung	Proaktive Risikokultur etablieren
Verantwortung delegieren	Verantwortung gemeinsam tragen

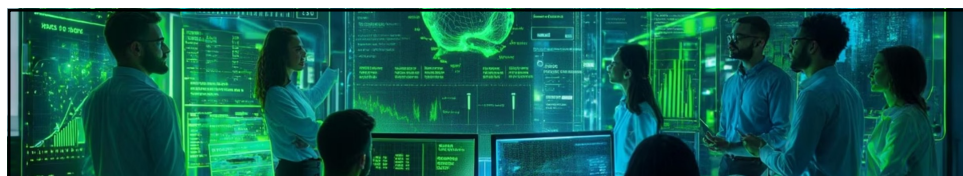
20



Führung statt Toolfixierung

Toolfixierung	Digitale Führung	Kulturwandel
- Fokus auf einzelne Technologien - Diskussion über Features - Komplexität durch Toolvielfalt	- Fokus auf strategische Ziele - Diskussion über Werte und Zweck - Klarheit durch Priorisierung	- Kompetenzaufbau fördern - Experimentierräume schaffen - Fehlertoleranz kultivieren

21

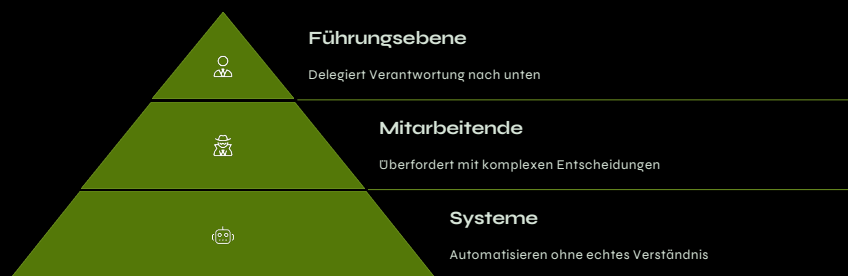


Kommunikation als Teil der Sicherheitskultur

 Transparenz über Risiken Offene Kommunikation über bekannte Schwachstellen und mögliche Gefahren.	 Klare Sicherheitsrichtlinien Verständliche und begründete Regeln statt Vorschriftenkataloge.
 Kompetenzaufbau Kontinuierliche Schulung und Sensibilisierung aller Mitarbeitenden.	 Gemeinsame Verantwortung Sicherheit als Aufgabe aller, nicht nur der IT-Abteilung.

22

Das Dilemma der delegierten Verantwortung



23

Separate Risikoabwägung für jede Dienststelle
funktioniert nicht. Die Umsetzung in der Praxis ist nicht
machbar, weil Verantwortlichkeiten delegiert werden.

(auch bei der Swiss Government Cloud nicht)

24



Ausblick

Ausgangslage

Technologien entwickeln sich exponentiell. Unser Verständnis ihrer Risiken nicht.

Wohin geht die Reise?

Zunehmende Abhängigkeit von KI-Systemen und der Cloud.
Abnehmende Transparenz und Kontrolle.

Was können wir tun?

Neue Governance-Strukturen entwickeln. Interdisziplinäre Zusammenarbeit fördern. AI- und Data-Literacy etablieren.

25

Was also tun?

🔍

KI-Transparenz schaffen
Inventar aller Systeme erstellen, Verantwortungen festlegen

☁️

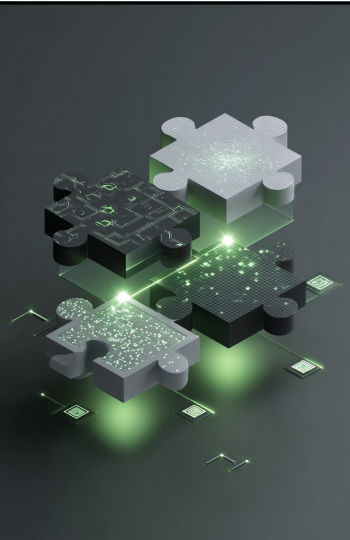
Cloud-Abhängigkeiten bewerten
Exit-Szenarien durchspielen, Kosten für Vendor-Wechsel kalkulieren

👤

Nationale, interdisziplinäre Gremien
z.B. Tech Ethics Board, regelmäßige Digital Sovereignty Checks

💡

Procurement neu denken
"Exit-Fähigkeit" als Kriterium bei Vendor-Wahl, bewusste Diversifizierung bei Services, Transparenz bei Verträgen



26

Technologie ist gestaltbar,
Verantwortung auch.
Wer übernimmt sie? Und wann?

27

Was passiert?

(III)

28

¯_ (ツ) _ /

(Das liegt an uns)

29

Merci <3

Reto Vogt
+41 79 699 82 17
hallo@retovogt.ch

30