# UPDATE 5|24

**FÜR DIE UMWELT. FÜR DIE REGION.**

**Grüezi liebe Leser:innen**

Und wieder haben uns um Spätherbst die Nachrichten schwerer Unwetter aufgewühlt. Diesmal traf es Spanien, Tschechien, Polen und Österreich. Es erreichten uns schockierende Informationen zu Toten und Verletzten sowie apokalyptische Bilder von verzweifelten, sich gegen das Ertrinken wehrenden Menschen, gefluteten Häusern, zerstörten Brücken und Strassen sowie aufgestapelten Autos und Bäumen. In Südspanien fiel so viel Regen an einem Tag wie sonst im ganzen Jahr. Als Verursacher gilt das Wetterphänomen «Kalter Tropfen», der auf warme Luft des für die Jahreszeit viel zu warmen Mittelmeers traf. Ein Journalist kommentierte die Ereignisse sehr einprägsam: «Der Trend geht zum Prinzip Ketchupflasche: erst lange nichts, dann zu viel auf einmal. Wärmere Luft kann mehr Feuchtigkeit speichern, aber auch mehr davon auf einmal wieder abgeben. Die Folge sind längere Trockenphasen und dazwischen stärkere Niederschläge. Auch das trocken-heiss-windige Feuerwetter, das Waldbrände begünstigt, ist heute häufiger als früher. Bei Hitzewellen ist der Zusammenhang von Extremen und Klimawandel ohnehin offensichtlich.» Und der gleiche Kommentator schrieb: «Der globale Kohleverbrauch hat 2023 einen neuen Allzeitrekord erreicht, das darf doch wohl nicht wahr sein. Ist es aber.»
Wir von der erzo hören trotzdem oder gerade deswegen nicht auf, die positiven Signale zu verstärken. Mit unserer täglichen Arbeit tragen wir unter anderem dazu bei, dass die Preise für erneuerbare Energien weiter sinken, während derer Verfügbarkeit steigt. Hier sind wir als Gesellschaft auf Kurs, denke ich. Am letzten Oktobertag verbreitete die Eidgenössische Elektrizitätskommission Elcom Optimismus und kommunizierte, die Stromversorgung für den Winter 2025 sei gesichert.
Ein neues Problem und Phänomen, das uns als erzo sehr beschäftigt, ist hingegen die Cybersecurity. Wie viele Industrieunternehmen sowie alle Organisationen, welche die Infrastruktur von Städten und ländlichen Wohngebieten sicherstellen, sind auch wir nicht gefeit vor feindlichen virtuellen Attacken. Daher engagieren wir uns einerseits für Verbesserungen unserer IT und Datensicherheit und andererseits für Massnahmen, die im Notfall Schlimmes verhindern. Denn wir sind uns unserer Verantwortung der Öffentlichkeit gegenüber bewusst. Schliesslich sind es laut Zukunftsinstitut Wien drei **D**, die über unsere Zukunft entscheiden: **D**igitalisierung, **D**emokratie und **D**ekarbonisierung.
A propos Dekarbonisierung: Beobachten Sie auch den Megatrend, dass extreme Geschehnisse in Natur, Politik und Gesellschaft global und lokal zunehmen? Umso dringender ist es, vorbeugende Massnahmen zu treffen. Nur wenn wir als erzo mithelfen Gefahren in den Griff zu bekommen, bevor sie eingetreten sind, sichern wir die Stabilität Ihres täglichen Lebens. Wir denken an Sie als Bürgerin, Kunde, Stimmvolk, Geschäftspartner oder Politikerin. Ihnen und uns wünschen wir zu Gunsten einer positiven Zukunft erneuerbare Energien, saubere Luft und eine intakte Natur. Damit diese Wünsche sich erfüllen können, realisieren wir als erzo gemeinsam mit unseren Partnern enkeltaugliche Grossprojekte. Im nächsten Jahr werden wir Ihnen mehr dazu berichten.

Bis zu einem Wiederlesen im Neuen Jahr wünschen wir Ihnen eine friedliche und zuversichtliche Adventszeit sowie erholsame Festtage und danken Ihnen für Ihr grosses Interesse an der erzo. Und nun viel Spass bei der Lektüre! Haben Sie Fragen? Ich bin gern für Sie da: friedrich.studer@erzo.ch

Ihr Friedrich Studer, Geschäftsleiter

# «ES GIBT KEINE MAXIMALE SICHERHEIT, NUR MAXIMALE VERZÖGERUNG»

**Energiegewinnung aus Kehrichtverbrennungs- und Abwasserreinigungsanlagen ist eine Erfolgsgeschichte. Doch seitdem Cyber Security weit oben auf der Risikoliste steht, gibt es neue Herausforderungen für die KVA erzo und ARA erzo. Wir sprachen mit Markus Lenzin, bei Alsec Senior Cyber Security Specialist für IT- und OT-Umgebungen wie Netzwerke und Systeme und Spezialist für den Schutz kritischer Infrastrukturen.**



Herr Lenzin, sind Sie schon mal gehackt worden?
Ich kann hier zum Glück sagen, das dies bis anhin noch nicht passiert ist, da ich eher übervorsichtig agiere im Umgang mit meinen digitalen Medien. Es geht auch ein wenig um meinen Berufsstolz.

Wir reden über ein komplexes Thema. Wie lautet Ihre Definition?
Bei Cyber Security oder auf Deutsch IT/OT-Informationssicherheit geht es um den Schutz von Netzwerken und Computersystemen. Der grosse Unterschied zeigt sich hier zwischen kommerzieller IT (Server und Arbeitsplätze) und der OT (Operational Technology). Bei Zweitgenanntem geht es um Maschinensteuerungen wie SPS (Speicherprogrammierbare Steuerungen, Regler, Sensoren etc. zum Schutz von Produktionsanlagen) oder Robotern, aber auch um Diebstahl oder Beschädigung ihrer Hard- und Software. Dies kann sich in Form von Manipulation von ihnen verarbeiteter Daten sowie Unterbrechung oder Missbrauch der Produktionsanlagen äussern.

Cyber Security Unternehmen schiessen wie Pilze aus dem Boden. Wo liegen bei Ihnen und Ihrem Unternehmen Alsec die Kompetenzen und Schwerpunkte?
Wir kennen die Informationssicherheit in der IT als Grundlage des Schutzes im vorgelagerten Perimeter. Unser Fokus gilt aber den OT-Systemen in den Produktionsanlagen. Das Bundesamt für Landwirtschaft definiert als kritische Infrastrukturen Sektoren wie die Stromversorgung, Gasversorgung, Wasserversorgung, medizinische Geräte des Gesundheitswesens etc. Bei Kehrichtverbrennungsanlagen wie bei der erzo geht es aber auch um den Schutz der eingesetzten Technologien, Prozesse und auch um Fähigkeiten des Personals.

Öffentliche Einrichtungen sind beliebte Ziele für sogenannte «Hacktivisten». Sie schützen Energieversorger vor Cyber Crime. Was ist die spezifische Herausforderung von Energieversorgern? Welche Bedrohungen müssen sie frühzeitig erkennen?
Grundsätzlich ist die Stromversorgung die kritischste Infrastruktur, da andere Bereiche im grossen Ausmass von ihr abhängen. In laufenden Kriegshandlungen wird immer wieder auf diese Infrastruktur gezielt, da ein Land ohne oder mit eingeschränkter Stromversorgung beschränkt handlungsfähig ist. Die Bedrohungen werden auch von Seiten des Bundes beobachtet und laufend Informationen an die Betreiber dieser kritischen Infrastrukturen weitergegeben. Die Umsetzung allfälliger Massnahmen brauchen dediziertes Fachwissen hinsichtlich der Prozesse und eingesetzten spezifischen Technologien. Dieses Wissen muss in diesen Betrieben erst aufgebaut werden. Hier schlägt auch der Fachkräftemangel zu. Hinzu kommt, dass mit der Überarbeitung der Stromversorgungsverordnung für die Energieversorgung per 1. 7. 2024 eine gesetzliche Grundlage in Kraft getreten ist, welches den Energieversorgungsunternehmen die Umsetzung entsprechender Massnahmen (IKT-Minimalstandard) vorschreibt.

Geht es eher um die Zerstörung von Daten, Betriebsunterbrechungen, finanziellen Gewinn oder um Spionage?
Bei kritischen Infrastrukturen wie der Energieversorgung geht es eher um Betriebsunterbrechungen, wobei es z.B. bei Forschungsunternehmen eher um Spionage geht. Hier ist es wichtig für den «Angreifer» bei der Abführung von Informationen möglichst lange nicht aufzufallen und die Spuren in den betroffenen Systemen zu verwischen. Beim Vorgehen spielt letztlich das dahinterliegende Motiv des Angreifers eine grosse Rolle.

Markus Lenzin, Senior Cyber Security Specialist für IT- und OT-Umgebungen wie Netzwerke und Systeme und Spezialist für den Schutz kritischer Infrastrukturen bei Alsec.

Verfügen alle Energieversorger über einen Chief Information Security Officer? Oder wer sind Ihre wichtigsten Auftraggeber und Ansprechpersonen?
Dass diese Verantwortung noch nicht zugeteilt wurde, ist in vielen Unternehmen eine offene Pendenz. Es darf auch eine temporäre Verantwortung an einen Projektleiter delegiert werden. So kann der künftige «Ciso» im Verlauf des Projekts erkoren werden. Solange nicht anders definiert, liegt die Verantwortung bei der GL und ihrem vorsitzenden Geschäftsleiter. Dies gilt für die spezifischen Risiken in der IT wie in der Produktion (OT), welche aus den ganzen Bedrohungen resultieren.

Akute Bedrohungen auf systemischer Ebene rufen nach sofortigen Massnahmen. Können Sie uns ein paar Beispiele geben?
Vorab ist es wichtig zu wissen, was man hat – Inventar – bzw. was zu schützen ist. Basierend darauf kann man evaluieren, wie man diese Assets schützt. Eine weitere wichtige Funktion ist die Detektion von auffälligem Verhalten der Systeme und die Reaktion darauf. Wenn schliesslich alles nichts hilft, geht es um die Wiederherstellung der Systeme in der IT und OT mit der notwendigen vorgehaltenen Hardware und Software.

Internationale Studien schätzen die Kosten eines Cyberangriffs auf den öffentlichen Sektor auf 2,6 Mio. USD. Wie teuer ist ein solcher Angriff im Schnitt in Schweizer Dimensionen?
Gemäss Aussage des Bundes geht man bei einem Vorfall von durchschnittlichen Kosten von CHF 1,4 Mio. aus.

Die Angst vor Blackouts ist riesig, seitdem sich die Künstliche Intelligenz (KI) durchsetzt. Der Mensch scheint zunehmend die Kontrolle über Situationen und Infrastrukturen zu verlieren. Wie beurteilen Sie die Lage an der Front?
Allein der Umstand, dass rund um die Produktionsanlagen immer mehr digitalisiert bzw. automatisiert wird und die Angreifer auch für ihre Angriffsszenarien KI einsetzen, erhöht diese Bedrohung.

Sie schreiben auf Ihrer Website: «Beratung hat in erster Linie mit Vertrauen zu tun.» Wie haben Sie das Vertrauen der erzo KVA und erzo ARA verdient?
Das kann ich nur vermuten, aber wir haben immer wieder in Fachgesprächen mit den Spezialisten unsere Kompetenzen aufzeigen können, weil wir in der OT ihre Sprache sprechen.

Wie sichern Sie den Betrieb der erzo? Wie lautet Ihr Auftrag der erzo in für Laien verständlichen Worten? Wo beginnt Ihre Arbeit, und wo endet sie?
Wir basieren auch hier auf dem IKT-Minimalstandard für die Abfallentsorgung. Wir starten mit der «Ist»-Aufnahme, definieren dann das «Soll» und erarbeiten anschliessend mit der erzo und ihren Dienstleistern einen Projektantrag zur Füllung dieser «Gaps». Diesen Prozess begleiten wir zudem in Form einer Qualitätssicherung.

Wie finden Sie heraus, wo Hacker angreifen könnten? Und wie prüfen Sie, ob Ihre Massnahmen erfolgreich sind?
Hier spielt die Detektion von Ereignissen eine zentrale Rolle. Zusätzlich machen wir auch Audits existierender IT- und OT-Umgebungen für bestehende, aber viel wichtiger auch für neue Anlagen, um allfällige Schwächen aufzuzeigen.

Setzt Alsec «weisse» Hacker ein, um Schwächen der IT-Infrastruktur aufzuspüren?
Ich nehme an unter «weisse» verstehen Sie «ethische» Hacker. Wir arbeiten in diesem Bereich mit Partnern zusammen, welche die Methode mitbringen, die wir dann an die Begebenheiten der OT anpassen.

Wie verkraften Sie den Frust, dass Sie als IT Security Experte sowie die von Ihnen betreute Kundschaft den IT-Bösewichten immer hinterherrennen, statt ein paar Schritte voraus zu sein?
Für uns entsteht hier kein Frust, das ist «Part of the Game», also Teil des Spiels. Wir bzw. unsere Kunden reagieren immer auf neue Bedrohungen, auf welche wir dann zusammen mit der Kundschaft neue Massnahmen entwickeln. Es gibt keinen maximalen Schutz, sondern nur maximale Verzögerung eines Angriffs, in dem möglichst viele «Hindernisse» überwunden werden müssen.

Inwiefern sind Ihre Handlungen mit Massnahmen auf internationaler Ebene verknüpft und abgestimmt?
Wie schon vorab erwähnt, gibt es hier eine internationale Zusammenarbeit beim Bund, das NCSC (National Cybersecurity Center), welches das aktuelle Lagebild an die kritischen Infrastrukturen der Schweiz weitergeben.

Ist es in dieser Hinsicht ein Problem, dass die Schweiz nicht der EU angehört?
Dies kommt in diesem Bereich weniger zum Tragen, da man sich hier an international anerkannte Standards anlehnt, welche dann in den verschiedenen Regionen und sektorspezifisch an die Begebenheiten angepasst werden.

Wie schulen und trainieren Sie sich und Ihre IT/OT Security Kollegen? Wie lernen Sie zu denken wie ein Cyberkrimineller?
Es gibt verschiedene Gefässe, um sich auf dem aktuellen Stand zu halten. Man bekommt ebenfalls von diesem NCSC wertvolle Informationen, aber auch produktspezifische Informationen von der Seite der Hersteller und Lieferanten, den Sektoren und Branchen sowie von verschiedenen Organisationen, welche sich um diese Themen kümmern.

Laut Ihrer Website blickt Ihr Unternehmen auf 150 Projekte bei 70 Kunden zurück, das ist eine grosse Menge. Welche schlimmen Hacking-Ereignisse haben Kunden von Ihnen schon erlebt?
Einige Kunden von uns wurden, bevor wir ein Mandat hatten bei ihnen(!), verschlüsselt. Und Lieferanten wurden erfolgreich angegriffen, weil sie einen Remote Access für Wartungsarbeiten auf Systemen von Kunden hatten.

Zurück zu den Abfallkraftwerken und Abwasseranlagen. Die lokalen Turbinen, Generatoren, Pumpen und Feuer sind gewaltig. Doch die interne und dezentrale IT-Infrastruktur ist ebenso filigran wie im Homeoffice privater Individuen. Denn letztlich ist alles, das an Computernetzwerke angeschlossen ist, gefährdet. Ist diese Betrachtung richtig?
Das ist so: Alles ist vernetzt, und mit der Vernetzung steigt die Gefahr, wenn die sogenannten Zonenübergänge zwischen den Systemen nicht entsprechend geschützt bzw. überwacht werden.

Haben Sie den Roman «Blackout» von Marc Elsberg gelesen? Er beschreibt die verheerende Manipulation von öffentlicher Infrastruktur so drastisch, dass ich mir erstmals vorstellen konnte, aufgrund eines grossflächigen Hackerangriffs in Europa und den USA plötzlich ohne Wasser, Strom, Benzin, Geld und Nahrung zu sein … eine grausige Lektüre!
Ich kenne das Buch. Es war ein Weihnachtsgeschenk bzw. eine Pflichtlektüre bei einem meiner früheren Arbeitgeber. Es ist sehr gut recherchiert, und alles, was darin beschrieben wird, kann auch so passieren oder ist schon ähnlich passiert.

Laut einer Umfrage des Bundesamts für wirtschaftliche Landesversorgung und des Branchenverbands der Schweizer Elektrizitätswirtschaft (VSE) aus dem Jahr 2020 ist das Bewusstsein für Cyber Crime bei Kraftwerkbetreibern auf Stufe 1 von maximal 4. Wie oft stossen Sie bei Ihrer Kundschaft in Bezug auf solche Katastrophen nach wie vor auf eine gewisse Naivität?

**Über Markus Lenzin**
Markus Lenzin begann seine Karriere als Schaltanlagenmonteur und sammelte erste Erfahrungen mit speicherprogrammierbaren Steuerungen. Bei der damaligen Elektrizitätsgesellschaft Laufenburg (EGL) arbeitete er an Netzwerken und Leitsystemen der Energieversorgung und brachte die Ablösung der Relais-Technik durch Fernsteuerungen von Schweizer Kraftwerken und Schaltanlagen voran. Schnell übernahm er Führungsrollen in der Projektleitung, im Applikationsbetrieb und in der Substation Automation Technology im Höchstspannungsnetz bei den Nachfolgefirmen Etrans bzw. Swissgrid. Hier trieb er die Neuorganisation des schweizweiten Betriebs der Unterwerke und die Digitalisierung mit Bedarf an Cyber Security voran. Seine umfassende technische wie prozessuale Erfahrung im Aufbau und Betrieb von kritischen Infrastrukturen fliesst nun bei Alsec und den Kunden ein.

Ich betrachte das nicht als Katastrophe. Es ist eine neue Disziplin, welcher in der Vergangenheit aus verschiedenen Gründen wie mangelndes Budget, fehlende Fähigkeiten, Personaldecke, andere Prioritäten etc. zu wenig Beachtung geschenkt wurde. Deshalb hat man diesem Umstand jetzt mit einer Anpassung der Stromversorgungsverordnung gesetzlich entgegengewirkt.

Konzerne und KMU sind es gewohnt, mehrjährig gültige Strategien zu entwickeln und diesen dann unter Beizug einer Portion Agilität operativ zu folgen. Die Sicherheitslage im Bereich Cyber Security ist indessen morgen schon anders als heute, geschweige denn übermorgen. Wie handhaben Sie und Ihre Kundschaft die Volatilität dieser Herausforderung?
Es gilt mit der Umsetzung des IKT-Minimalstandards eine gute Ausgangslage hinsichtlich Prozesse, Technologien und Fähigkeiten in einer Organisation zu schaffen, welche dann über die Jahre kontinuierlich und risikobasiert verbessert werden, damit auf neue Bedrohungen reagiert werden kann.

Seit 2018 empfiehlt der Bund Betreibern von kritischen Infrastrukturen, den IKT-Minimalstandard* (siehe Infobox am Ende des Interviews) umzusetzen. Sind die Betreiber öffentlicher Infrastrukturen inzwischen gezwungen, ihre Anlagen vor Cyber Attacken zu schützen?
Wie gesagt, für die Energieversorgung ist der IKT-Minimalstandard unterdessen verbindlich. Weitere wie z.B. zur Gasversorgung werden voraussichtlich im Jahr 2025 folgen. Grundsätzlich müssen alle Unternehmen, im speziellen die Betreiber kritischer Infrastrukturen, ihre Risiken kennen. Informationssicherheit ist eine davon. Sie kann in der IT wie in der OT direkt auf die Produktivität einwirken.

Ist es obligatorisch, Cyber Angriffe den Behörden zu melden? Wenn ja, wem?
Es gibt heute schon eine Meldepflicht für vorbestimmte Ereignisse, welche dem NCSC gemeldet werden müssen. Auch dies wird künftig auf eine gesetzliche Grundlage gestellt, damit Unternehmen voneinander profitieren können.

Wie überall liegt die grösste Schwachstelle bei den Menschen. Eine konstruktive Fehlerkultur hat sich in vielen Betrieben noch nicht durchgesetzt.

Was raten Sie den Mitarbeitenden der erzo KVA und erzo ARA? Wie könnten sie einen Hackerangriff bemerken?
Hier spielt die grundsätzliche «Awareness» bei den Mitarbeitenden eine grosse Rolle. Diese sollte funktionsbezogen noch ergänzt werden. Mitarbeitende der IT-Abteilung sind mit anderen Bedrohungen konfrontiert als Mitarbeitende in der Produktion (OT), zum Beispiel am Ofen oder am Leitsystem (Schaltwarte).

Wo steht die erzo in puncto Cyber Sicherheit im Vergleich zu ihren Mitbewerbern?
Die erzo hat hier sicher einen Vorsprung, da sie die «Ist»-Analyse abgeschlossen und das «Soll» weitgehend definiert hat. Das heisst, die erzo kennt ihre Risiken weitgehend und muss nun ein Projekt auf den Weg bringen, welches diese Lücke füllt.

Ist es Ihnen bereits gelungen, einen Angriff auf die erzo KVA oder erzo ARA zu verhindern?
Wir haben in einem Gespräch festgestellt, dass vermutlich eine mögliche Fehlüberweisung bei der erzo wie bei einem Lieferanten instinktiv verhindert werden konnte. Dies wirkt sich auch bei der täglichen Arbeit aus.

Wieviel Zeit bleibt Ihnen als IT-Experte zwischen dem Feststellen einer Anomalie und Ihrer Handlung?
Da dieser Prozess komplett beim Kunden abläuft, liegt die Reaktion in seinen Händen. Entscheidend ist, ob er schon eine Pikettorganisation hat oder nicht und ob er entsprechende Detektoren solcher Anomalien (z.B. Intrusion Detection Systeme) bereits in Betrieb hat.

Ihre Arbeit kostet. Müssen die Gemeinden und letztlich die Endverbraucher:innen davon ausgehen, dass die Zunahme an Hackerangriffen auch den Strom verteuern wird?
Ja, das ist so! Die Strom-Regulierungsbehörde ElCom hat hier bereits reagiert und verfügt, dass diese Investitionen (rund 6% bis 14% der IT-Ausgaben oder rund 0,3 bis 0,5% des Jahresumsatzes) anrechenbar sind. Da sie die Verfügbarkeit des Stroms beeinflussen, dürfen sie auf den Strompreis umgewälzt werden.

Zurzeit sind viele Stellen in Ihrer Branche nicht besetzt. Also sieht so aus, als sei Ihr Beruf

zukunftssicher. Empfehlen Sie Jugendlichen, Ihren Beruf zu ergreifen? Oder könnten sich die Bedürfnisse massiv verändern?
Ich kann Jugendlichen nur empfehlen, sich in diese Richtung zu entwickeln. Das Potenzial im Bereich der kritischen Infrastruktur ist enorm, und mit den gesetzlichen Vorgaben steigt die Marktanforderung für diese «Spezies».



Die Alsec arbeitet im Bereich Informationssicherheit mit der Hochschule Luzern HSLU zusammen. Welche Vorteile bringt das den Partnern und der Kundschaft?
Wir bilden in diesen Lehrgängen künftige Cybersecurity Spezialisten in Richtung OT weiter aus. Ebenso haben wir zusammen mit der HSLU-Informatik ein OT-Labor in der Form eines kleinen Energieversorgers aufgebaut, in welchen die Studenten das Erlernte praxisorientiert anwenden und so ihren künftigen Arbeitgebern zur Verfügung stellen können.

Springen wir zehn Jahre nach vorne ins Jahr 2035. Wo stehen wir dann mit dem Thema Cyber Security? Und wie könnte sich Ihr Beruf verändern?
Nebst dem Umstand, dass ich dann schon zwei Jahre pensioniert sein werde, wird sich bis dahin einiges an neuen Technologien, Methoden und Taktiken entwickelt haben. Nicht zuletzt, weil – wie bereits erwähnt – auch hier KI Einzug hält.

**Alsec auf einen Blick**
Von Markus Lenzin und Reto Amsler am 1. März 2019 gegründet, fokussiert sich die Alsec Cyber Security Consulting AG auf das Erbringen von Cyber Security Dienstleistungen im Operational Technology Umfeld (OT) nach höchsten Standards. Die schnell wachsende Belegschaft der ALSEC vereint langjährige Erfahrung im OT-/IT Security Umfeld in der Energieversorgung mit State-of-the Art- Wissen zum Thema in Branchen mit kritischer Infrastruktur.

Wie klein ist die Chance, dass Cyber Crimes aus dem Alltag verschwinden?
Die Chance ist sehr, sehr klein! Im Gegenteil, wir müssen lernen damit umzugehen. Das Stichwort heisst Awareness, Awareness, Awareness …

Eine Fee schenkt Ihnen je einen freien Wunsch für Ihr berufliches und privates Leben. Was wünschen Sie?
Dass es mir gelingt meine Energiespeicher für die steigenden Herausforderungen und Potenziale im beruflichen Leben weiterhin in der Balance zu halten mit dem privaten Energiehaushalt. Denn dort lade ich meine Batterien in musischen wie in sportlichen Aktivitäten.

Markus Lenzin, wir danken Ihnen für das Gespräch.

## IKT-MINIMALSTANDARD

Bei kritischen Infrastrukturen wie jenen der Energieversorgung trägt der Bund gemäss Verfassung eine Verantwortung gegenüber der Bevölkerung. Er muss Mittel zur Verfügung stellen, um die Infrastruktur zu schützen. Bei der Informations- und Kommunikationstechnologie (IKT) tut er das mit dem Minimal Standard. Dieses Framework aus fünf Modulen und 106 Kontrollpunkten befähigt die Energieversorger, ihre IR-Resilienz zu steigern. Die Hauptmodule sind:

- **Identifizieren:** Welche Assets haben wir und von welchen Gefahren sind diese bedroht?
- **Schützen:** Mit welchen präventiven Massnahmen können wir unsere Assets vor diesen Gefahren schützen?
- **Erkennen:** Wie stellen wir sicher, dass wir Anomalien oder Attacken frühzeitig erkennen?
- **Reagieren:** Welche reaktiven Massnahmen ergreifen wir, wenn wir von Attacken betroffen sind?
- **Wiederherstellen:** Wie können wir die Systeme wiederherstellen, wenn eine Attacke erfolgreich war und zum Beispiel Daten verschlüsselt hat?

# GESICHERTE STROMVERSORGUNG FÜR DIESEN WINTER



**Die Behörden sind zuversichtlich, dass die Schweiz diesen Winter genügend Strom haben wird. Auch dank neuer «virtueller Reservekraftwerke».**

«Wir sind zuversichtlich für den Winter», heisst es bei der Eidgenössischen Elektrizitätskommission Elcom, welche die Stromversorgung in der Schweiz überwacht. Im dritten Winter nach dem russischen Überfall auf die Ukraine dürfte sich die Energieversorgung in Europa weiter normalisieren, fasst Jürg Rauchenstein, Mitglied der Elcom-Geschäftsleitung, die Situation zusammen. «Zurzeit gibt es viel mehr Importe von Flüssigerdgas, sodass die europäischen Gasspeicher gut gefüllt sind. Die Schweizer Kernkraftwerke sind alle in Betrieb, und auch die französischen AKW liefern wieder viel zuverlässiger Strom als in den vergangenen Wintern», betont Rauchenstein.

Zudem sind die Speicherseen in den Schweizer Alpen zurzeit mit 84 % gut gefüllt, wie die aktuellen Daten auf dem Dashboard des Bundesamts für Energie zeigen. Die Winterstromreserve in den alpinen Speicherkraftwerken und die Gasreservekraftwerke in Birr AG, Cornaux NE und Monthey VS sind bereit.

**Notstromanlagen als Reservekraftwerk**

Neu setzt der Bund zudem stärker auf das Potenzial von Notstromgeneratoren, um einen Strommangel zu verhindern. Rund 6000 Notstromgeneratoren stehen in der Schweiz in den Kellern von Industrieunternehmen, Gewerbebetrieben und Rechenzentren: kleine Reservekraftwerke für den Eigenbedarf. Mehr als 100 Anlagen erbringen insgesamt 260 MW Leistung. Das ist so viel wie das grösste der Gasreservekraftwerke in Birr AG.

Daraus mache man nun ein einziges, gesamtschweizerisches «virtuelles» Reservekraftwerk, erklärt Thomas Reithofer vom Stromunternehmen CKW: «Diese Notstromanlagen werden über ein Leitsystem bei der CKW gekoppelt, und im Bedarfsfall können wir über ein Signal alle diese Notstromanlagen einschalten, sodass sie Strom ins Netz einspeisen.»

CKW betreibt neben BKW, Primeo Energie und anderen Stromunternehmen das Pooling der

Die Stromversorgung in der Schweiz dürfte auch in den kommenden Monaten sichergestellt sein.

Notstromanlagen. Es sorgt dafür, dass genügend Besitzer ihre Anlagen zur Verfügung stellen und auch technisch dafür gerüstet sind. Ein schweizweiter Testlauf habe ergeben, dass das System funktioniere und die benötigten Strommengen auch tatsächlich abgerufen werden konnten, so Rauchenstein von der Elcom.

**Preisgünstiges Pooling**

Wie teuer ist das Pooling? Der Bund muss für die bereitgestellte Leistung bloss CHF 2,6 Mio. bezahlen. Das Reservekraftwerk Birr hingegen, das noch bis zum Winter 2025/26 zur Verfügung steht, kostete CHF 450 Mio.

Für Thomas Reithofer von CKW ist klar: «Das Pooling ist volkswirtschaftlich der weitaus günstigste Weg, um Stromreserven für den Notfall bereitzuhalten. Denn die Anlagen bestehen bereits, es entstehen nur geringe Zusatzkosten für die Steuerung.» Der Bund und die CKW laden deshalb weitere Besitzer von Notstromanlagen motivieren, bei der Reserve mitzumachen.

# ZÜRICH VERSENKT DAS $CO_2$ AUS DER GRÖSSTEN KLÄRANLAGE DER SCHWEIZ KÜNFTIG IN DER NORDSEE

**Die Stadtzürcher Stimmbevölkerung stellt sich deutlich hinter ein teures Pilotprojekt zur $CO_2$-Abscheidung. Auch für neuen Schulraum und Strom aus erneuerbaren Energien gibt es Mehrheiten.**



**Der Klärschlamm in der Anlage Werdhölzli wird heute verbrannt. Neu soll das dabei verursachte $CO_2$ abgeschieden werden.**

Heute werden in der grössten Kläranlage der Schweiz, dem Werdhölzli, etwa 100 000 Tonnen Klärschlamm im Jahr verbrannt. Dabei entstehen Rauchgas und $CO_2$. Dieses $CO_2$ will die Stadt künftig nicht mehr in die Luft blasen, sondern abscheiden und verflüssigen. Rund 25 000 Tonnen $CO_2$ sollen in einer neuen Anlage herausgefiltert werden.

Über dieses Werk haben die Zürcher abgestimmt. 35,5 Millionen Franken kostet die Abscheidungsanlage, hinzu kommen jährlich wiederkehrende Ausgaben von 14 Millionen Franken. Die Zürcher Stimmbürger stellen sich klar hinter das Projekt. 76 % sagten Ja, alle Stadtkreise stimmten deutlich zu. Entsprechend zufrieden zeigte sich die zuständige Stadträtin Simone Brander (SP). Die Anlage habe «Pioniercharakter», sie sei die erste ihrer Art in der Schweiz. «Das ist ein bedeutender Schritt in Richtung Netto null», sagte Brander.

Mit Ausnahme der SVP unterstützten alle Parteien das Vorhaben. Schliesslich will die Stadt bis 2040 klimaneutral werden; ohne Anstrengung gehe es nicht, fanden die Befürworter. Es brauche auch sogenannte Negativemissionen, die der Klimabilanz zugeschrieben werden könnten. Genau solche entstehen mit der Abscheidungsanlage im Werdhölzli.

### Hohe Kosten

Kritische Stimmen gab es zu den hohen Kosten. Für Stirnrunzeln sorgte auch, was mit dem abgeschiedenen $CO_2$ geschehen soll. Das verflüssigte Gas kommt zur einen Hälfte in Schweizer Recyclingbeton, die andere wird wortwörtlich im Meer versenkt. Das $CO_2$ soll in der dänischen Nordsee etwa 2000 Meter unter dem Meeresgrund unter einer Schicht aus Deckgestein verpresst werden.

### Viel Verkehr

Dazu sind tägliche Transportfahrten mit Lastwagen, Zug und Schiff nötig. Die Stadt rechnet damit, dass fünf bis sieben Lastwagen pro Tag das Werdhölzli verlassen werden. Trotzdem ist die Bilanz laut den Behörden positiv. 2026 ist der Baustart für die neue Anlage, 2028 soll sie in Betrieb gehen.

### KVA als nächstes Projekt

Gut möglich, dass es nicht bei dieser einen Anlage bleibt. Die Stadt hat bereits erklärt, dass sie künftig auch bei der Kehrichtverbrennungsanlage Hagenholz $CO_2$ abscheiden wolle. Da geht es dann um eine wesentlich grössere Menge, nämlich 360 000 Tonnen im Jahr. Auch die Kosten dürften noch einmal deutlich höher sein.

# Entdeckt! Google plant Minireaktoren. Eine Renaissance der Kernenergie?

**Die Ankündigung von Tech-Giganten, Rechenzentren mit neuartigen kleinen Reaktoren betreiben zu wollen, lässt aufhorchen. Liegt dies an der Künstlichen Intelligenz?**

Ein Blick in den aktuellen Nachhaltigkeitsbericht verblüfft: Die Treibhausgasemissionen und der Stromverbrauch des Konzerns haben sich seit 2019 fast verdoppelt. Dies trotz ehrgeiziger Klimaziele: Bis 2030 möchte der US-Technologiekonzern unter dem Strich keinen Emissionen mehr verursachen. Schuld am Anstieg soll der erhöhte Energiebedarf der Datenzentren und damit der Künstlichen Intelligenz (KI) sein. «Während wir KI zunehmend in unsere Produkte integrieren, könnte es schwierig werden, die Emissionen zu reduzieren», heisst es im Bericht.

Um den durch KI verursachten Mehrbedarf an Energie zu decken, so heisst es in einem anderen Bericht, plane der Internetkonzern Rechenzentren künftig auch mit Kernenergie zu betreiben. Ihr Vorteil gegenüber anderen regenerativen Energien: Kernenergie liefert rund um die Uhr bei jedem Wetter Strom. Diese Eigenschaft entspricht dem Strombedarf der Rechenzentren.

**Kleine atomare Reaktoren**

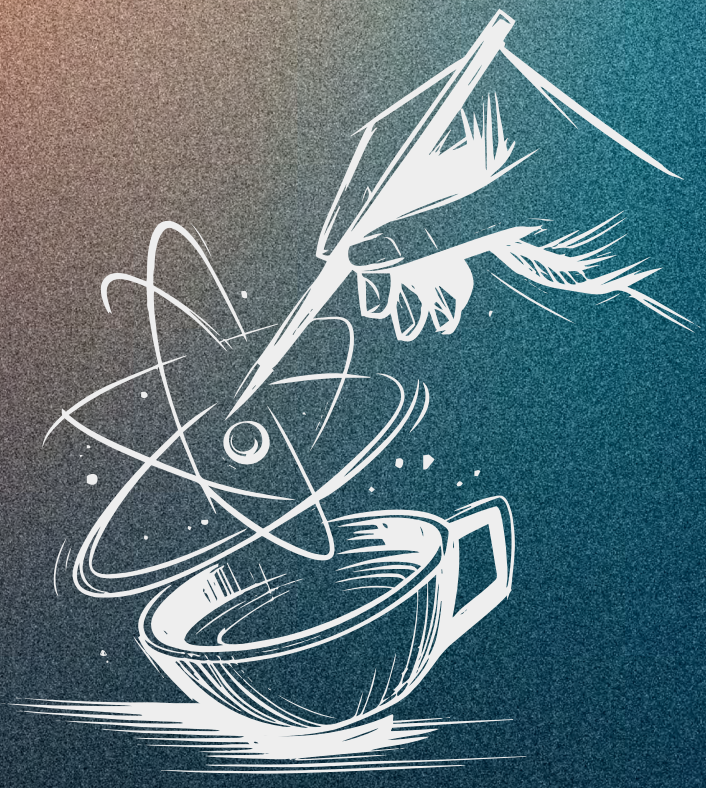
Daher möchte Google ab 2030 neuartige kleine modulare Reaktoren (Small Modular Reactors) der Firma Kairos Power kaufen. Sie werden nicht mit Wasser, sondern mit geschmolzenem Salz gekühlt – genau wie jene, die am Schweizer Paul-Scherrer-Institut getestet werden sollen.

**Google ist nicht allein**

Ähnliche Nachrichten wie die von Google erreichen die Schweiz von Microsoft und Amazon. Die Schlagzeilen der Medien dazu lauten in etwa immer gleich: «Big Tech erweckt die Kernkraft wieder zum Leben» oder «KI sehnt sich nach Atomkraft». Tatsache ist, dass Abfragen bei Chat-GPT 2,9 Wattstunden Strom benötigt, statt 0,3 Wattstunden für eine Google-Recherche. KI-Trainings- und KI-Anwendungen steigern also den Strombedarf enorm. Bis 2026 rechnet die Internationale Energieagentur mit einer Verdoppelung des weltweiten Stromverbrauchs durch Rechenzentren. Goldman Sachs Research schätzt den Anstieg des globalen Strombedarfs bis 2030 auf 100 Terawattstunden (TWh) pro Jahr, das wären im Jahr 2030 1100 TWh.

**Standortfrage Rechenzentren**

Die USA verantwortet einen grossen Teil des globalen Stromverbrauchs. Fragt sich, wo neue Rechenzentren künftig gebaut werden. Mutmasslich dort, wo der Strom billig ist. Denn Kosten, olitische Rahmenbedingungen, gesellschaftliche Relevanz und technische Errungenschaften werden die weitere Entwicklung prägen. Ebenso offen ist die Frage, was uns ausser KI in den kommenden Jahren beschäftigen wird. Vor vier Jahren hatte noch kaum jemand KI auf dem Radar, schon gar nicht als Stromfresser …



# CYBER-BEDROHUNGSMARKT UND RECHT



**Unternehmen stehen vor einer immer komplexeren Cyber-Bedrohungslandschaft. Neben den bereits bekannten Angriffsformen wird deutlich, welche Abhängigkeiten vor allem von externen Dienstleistern bestehen. Risikobewertungen spielen im Cyber-Markt eine ebenso grosse Rolle wie der Mensch.**

**Rechtliche Veränderungen: evDSG**
Die rasant fortschreitende Technologie erfordert kontinuierliche Anpassungen der Gesetzgebung. Seit dem 1. September 2023 ist das revidierte Datenschutzgesetz (revDSG) in Kraft. Es lehnt die Schweizer Datenschutzbestimmungen enger an die europäische Datenschutz-Grundverordnung (DSGVO) am. Diese Reform verbessert den Schutz personenbezogener Daten.

Wesentliche Neuerungen sind die erweiterten Auskunfts-, Melde- und Informationspflichten. Unternehmen müssen Betroffene umfassend über die Erhebung und Verarbeitung ihrer Daten informieren und Datenschutzverletzungen dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) melden.

Bisher sind über 200 Meldungen beim EDÖB eingegangen – aus verschiedenen Branchen. Das revDSG bringt grössere Verantwortung, Anpassungsbedarf bei den Unternehmen sowie höhere Compliance-Kosten und mögliche Änderungen der Geschäftspraktiken.

Am 14. August 2024 wurde ein neuer Datenschutzrahmen bestimmt, der einen sicheren Austausch von Personendaten zwischen der Schweiz und zertifizierten US-Unternehmen ermöglichen soll – ohne zusätzliche Garantien. Das «Swiss – U.S. Data Privacy Framework» soll sicherstellen, dass die Datenschutzmassnahmen eingehalten werden. Die offizielle Liste führt alle zertifizierten Unternehmen auf https://www.dataprivacyframework.gov/list

**Gesetzmässigkeit Ransomware Zahlungen**
Während der Schweizer Bundesrat und weitere Regierungen nach effektiven Wegen suchen, um das Problem mit Ransomware (Verschlüsselungstrojaner oder Erpressungssoftware genannt; sie ermöglichen das Eindringen auf fremde Computer) zu bewältigen, bieten die gesetzlichen Rahmenbedingungen bereits relevante Regelungen. Auch ohne spezifisches Verbot bestehen für Lösegeld zahlende Organisationen erhebliche rechtliche Risiken. Eine Zahlung könnte gegen Art. 260ter Abs. 1 lit. b StGB verstossen, wenn sie an eine kriminelle Gruppierung erfolgt.

Daher ist es essenziell, einen Entscheid zur Lösegeldzahlung sorgfältig und fundiert zu treffen. In der Schweiz zeigt die Praxis bisher eine opferfreundliche Handhabung der gesetzlichen Bestimmungen. Unternehmen, die sich mit Lösegeldzahlungen zu helfen versuchten, wurden bislang nicht mit zusätzlichen behördlichen Strafen konfrontiert. Besser ist natürlich das Verhindern von Erpressungsfällen.

**Künstliche Intelligenz**
Die Bedrohungen, die aus KI-generierten Angriffsformen entstehen, sind nach wie vor sehr aktuell. Dass es weiteren Schutz durch Regulatorien bedarf, beweist das Inkrafttreten des EU AI Act am 1. August 2024. Dieser wurde zur Wahrung der ethischen Werte und Grundrechte als Verordnung von der EU entwickelt und soll ein sicheres Umfeld schaffen – sowohl für die User als auch für die Wirtschaft.

**Risiko: Faktor Mensch**
Publikation von Beratungsfirmen bezeichnen in Bezug auf Cyber-Kriminalität nach wie vor den Menschen als den gefährlichsten Faktor. Cyber-Kriminelle greifen häufig gezielt Mitarbeitende an, um über sie die Sicherheitsvorkehrungen von Unternehmen zu umgehen und in IT-Systeme einzudringen. Dies kann erhebliche Schäden verursachen. Das Verhalten der Mitarbeitenden hat direkten Einfluss auf die Cyber-Sicherheit und auch auf die Minderung der Folgen eines Angriffs. Schutz und Schadensbegrenzung sind zentrale Elemente der Cyber-Resilienz.


Die aktuelle Forschung besagt, dass die Einstellung der Mitarbeitenden gegenüber Cyber-Risiken entscheidend ist. Verstehen Mitarbeitende, dass sie täglich mit vertraulichen Informationen arbeiten, stärkt dies ihre Sensibilisierung und erhöht die Sicherheit. Es ist wichtig, den Einfluss jedes Einzelnen auf die Cyber-Resilienz zu verdeutlichen. Konkrete Beispiele, branchenspezifische Bezüge sowie regelmässige Weiterbildungen fördern nachhaltiges Bewusstsein.

**Risiko: Berufshaftpflicht für Technologieunternehmen**

Technologieunternehmen hängen stark von komplexen IT-Systemen ab, gleichzeitig nehmen technische Risiken stetig zu. Diese können je nach Unternehmensart und den angebotenen Dienstleistungen schwerwiegende Folgen haben. Pflichtverletzungen, Versäumnisse, Systemausfälle und Softwarefehler führen zu erheblichen Problemen und Haftungsansprüchen. Eine Berufshaftpflichtversicherung (PI) ist daher eine sinnvolle Massnahme, um sich gegen berufliche Risiken abzusichern.

**Technologie = Risiko**

Das Risiko für Cyber-Vorfälle steigt bei Technologieunternehmen, da sie vermehrt externen Angriffen ausgesetzt sind. Während die «PI Tech-Versicherung» Risiken abdeckt, die durch Fehler oder Versäumnisse bei der Erbringung von Dienstleistungen oder durch technische Produkte entstehen, schützt die «Cyber-Versicherung» vor externen Bedrohungen wie Hackerangriffen, Datenlecks oder Betriebsunterbrechungen. Die Kombination beider Versicherungen bietet Technologieunternehmen umfassenden Schutz. Tatsache ist, dass es darum geht, hohe finanzielle Schäden zu vermeiden. Damit sind nicht nur Lösegelder gemeint. Der Schaden beginnt bei den Ausgaben für das Krisenmanagement und umfasst auch die Ausgaben für die Wiederherstellung der Systeme sowie die Auswirkungen eines Betriebsunterbruchs.

**Der cyberbedingte Betriebsunterbruch**

Die Berechnung von Umsatzausfällen nach Cyber-Vorfällen ist laut Kessler, ein Schweizer Unternehmen für Risiko-, Versicherung- und Vorsorgeberatung, herausfordernd, da sie von saisonalen und konjunkturellen Schwankungen beeinflusst werden. Dazu müssen die Umsätze mit den Budgetzahlen und dem Vorjahr verglichen werden. Lösungsansätze wie eine Business Impact Analysis sind zeit- und kostenintensiv. Auch die Dokumentation von Mehrkosten ist problematisch. Kessler empfiehlt, Überstunden und zusätzliche Massnahmen zu dokumentieren, um die Nachweisbarkeit und Krisenbewältigung zu verbessern. Neben den Arbeitsstunden sollten die in dieser Zeit ausgeführten Tätigkeiten erfasst werden, um später nachvollziehen zu können, was geleistet wurde.

# WENN DER MENSCH DER SCHWACHPUNKT IST



**Aus einem Anlass des Smart City Verein Bern zum Thema «Wie sich die smarte Stadt gegen Cyberangriffe wappnet» ging einhellig der Mensch als grösstes Sicherheitsrisiko hervor, dies nicht nur in puncto Cyber.**

Ob Sandro Volery im Kapuzenpulli, ein «weisser» Hacker und IT-Tester der Firma cyllective, Katja Dorlemann Expertin für Sicherheitsbewusstsein bei Switch und Präsidentin der Swiss Internet Security Alliance SISA, Laetitia Ramelet, Projektleiterin der TA-Swiss Stiftung für Technologiefolgen-Abschätzung, Tom Winter als CEO von BernExpo oder Michael Denzler, AI & Data Consultant bei Zühlke: Alle Redner sprachen bei der Erwähnung von 30 000 Cyber Crime Vorfällen im laufenden Jahr in der Schweiz (doppelt so viele wie im Vorjahr!) eher wenig von Technologie und stellten stattdessen den Menschen als Risikofaktor ins Zentrum ihrer Vorträge.

**Achtung Passwort**
Jeder erwachsene Mensch nutze im Schnitt rund 200 Konti und ebenso viele Passwörter, wurde am Event verkündet. Da wir Menschen noch andere Interessen hätten als Arbeit und Cyber Security – genannt wurden beispielhaft der Hund, Musik, Sport und Kochen – seien wir entsprechend nachlässig im Umgang mit IT-Sicherheit. Illegale Hacker würden von unserer legeren, ja leichtsinnigen Haltung profitieren. Es sei nicht zielführend sich einzureden, man sei ja als Person für die Internetwelt völlig uninteressant. Sobald man in einem Unternehmen oder Verband eine Funktion habe, sei man als potenzieller Zugang zu dieser Organisation für Hacker sehr spannend. Der Gebrauch eines Passwortmanagers wurde dringend empfohlen.

**Vorsicht mit Mails und Passwörtern**
Treffe eine Mail beim Empfänger ein, so solle dieser nicht sofort reagieren, sondern zuerst in Ruhe den Kontext reflektieren und sich drei Fragen stellen: Wer? Was? Wie? Am auffälligsten seien per Telefon, Mail oder Social Media geäusserte Befehle mit Wörtern wie: «jetzt», «sofort», «dringend», «in Gefahr», «in Not», «Unfall», «Schock», «Zahlung» etc.

Bestehe auch nur der geringste Zweifel an der Echtheit einer Mail respektive des Absenders, so dürfe die Zusendung keinesfalls geöffnet werden. Microsoft hingegen öffne und teste jede Mail und jedes PDF, um sicherzugehen, dass der Empfänger möglichst nicht in die Irre geführt werde, um also Spam und Betrug zu vermeiden.

Eine für Unternehmen wichtige Massnahme zur Vermeidung kann sein, dass sich die Geschäftsleitung im Rahmen einer Risikoanalyse proaktiv überlegt, wer das Unternehmen aus einem bestimmten Interesse an einem Mehrwert heraus (Geld, Daten, Fakten, Waren) virtuell attackieren könnte. Dies kann bei der Identifikation effektiver Angreifer helfen. Um selbst verursachte Schadenfolgen zu vermeiden, sollte eine Organisation zudem über einen strategisch, taktisch und operativ belastbaren Notfall- und Krisenplan verfügen.

**Deepfakes mit Ton und Bild**
Fälschungen und Deepfakes seien zunehmend schwierig zu entlarven, lernten die Gäste des Smart City Verein Bern. Betrügereien würden immer gezielter, günstiger und besser versteckt platziert. Die Fälschungen von Bild, Video und Ton seien für Laien kaum mehr zu entlarven. Man habe zwecks Erkennens von Fälschungen Tests gemacht mit trainierten und untrainierten Personen. Die fachlich geschulten Personen hätten dabei kaum besser abgeschnitten als Laien. Die Herausforderung liege im Bedürfnis, Maschinen, Menschen und ihren Botschaften vertrauen zu

können. «Doch wir wissen nicht, was wir nicht wissen.» Fazit: «Wir sind die Eigentümer unserer Daten. Dafür müssen wir Verantwortung übernehmen.»

### Angst vor Überwachung

Eine Schweizer Langzeitstudie mit dem Namen Digital-Radar Schweiz der Bank WIR vom Januar 2024 behandelt die Sorgen und Gefahren sowie die Vorteile und Kompetenzen im Zusammenhang mit digitalen Technologien. Dieser Studie zufolge schätzt die Schweizer Bevölkerung die Gefahren, welche von digitalen Technologien ausgehen, zunehmend hoch ein: Ein Drittel der Befragten bewertet die Gefahr von Künstlicher Intelligenz hoch. Die Angst vor Überwachung ist seit Jahren präsent. Nun kommen Skepsis und eine gewisse Müdigkeit dem Digital-Hype gegenüber hinzu.

### Schwindende Tech-Begeisterung

Als Apple vor 17 Jahren das erste iPhone präsentierte, war die Euphorie noch gross. Nie zuvor hatte ein so kleines Gerät so viele Funktionen vereint. Mit steigendem Tempo gelangten neue digitale Technologien auf den Markt: Blockchain, Internet of Things, Cloud, Roboter, Augmented Reality und Virtual Reality und jüngst auch die Künstliche Intelligenz. KI wird als Zeichen dafür interpretiert, dass wir uns in Richtung 5. Industrielle Revolution bewegen. Sie wird von der Interoperabilität geprägt. Alles ist mit allem und alle sind mit allen digital vernetzt.

### Höhere Sichtbarkeit von Gefahren durch KI

Im Zentrum dieser Entwicklung stehen die IT, das Internet und Daten. Mit Rechnerleistung und Algorithmen ermöglichen sie ständig neue Anwendungen. KI führt laut Studie der Bank WIR «zu einer erhöhten Abhängigkeit, zu neuen Bedrohungsszenarien wie beispielsweise der Internetpropaganda, welche die Gesellschaft und unsere Demokratie beeinflussen, und damit zu Ängsten». Gemäss der schweizweiten Umfrage steigt die Wahrnehmung der Gefahren und Nachteile der KI, während die Einschätzung der Vorteile digitaler Technologien stabil bleibt.

## IT-CHECKLISTE FÜR VORGESETZTE

**Verantwortungsvolle Chef:innen können mit diesen Tipps das Cyber-Risiko ihres Unternehmens reduzieren.**

- Stärken Sie Ihre Cloud-Sicherheit
- Reduzieren Sie das Diebstahlrisiko verschlüsselter Daten
- Setzen Sie auf Krypto-Agilität
- Sichern Sie 5G-Netzwerke
- Beheben Sie Schwachstellen alter Infrastrukturen
- Beobachten Sie die Bedrohungslage und passen Sie sich an
- Stärken Sie das Cybersicherheits-Wissen Ihrer Mitarbeitenden
- Analysieren und bewerten Sie Risiken
- Ernennen Sie eine Leitung für Digitalisierung
- Richten Sie eine Zero-Trust-Architektur ein
- Lernen Sie aus Vorfällen und ergreifen Sie Massnahmen
- Führen Sie regelmässige Schwachstellenbewertungen durch
- Organisieren Sie regelmässige Feedback- und Lagegespräche
- Führen Sie personalisierte Trainingsprogramme ein
- Nutzen Sie effektive Threat Detection-Tools
- Automatisieren Sie die Analyse von E-Mails
- Automatisieren Sie Routineaufgaben
- Förderung Sie Training und Weiterbildung
- Investieren Sie in die Bindung von Mitarbeitenden
- Machen Sie Work-Life-Balance zur Priorität

# «WENN DU ETWAS GLAUBEN WILLST, SOLLTEST DU ZWEIFELN»

**Künstliche Intelligenz (KI) generiert immer realistischere Medieninhalte (Deepfakes). Wie wir als Gesellschaft damit umgehen können, hat BFH-Forscher Reinhard Riedl im Interview mit der Wirtschaftsförderung des Kanton Bern erklärt.**



Prof. Dr. Reinhard Riedl, BFH-Forscher

### Können wir lernen Deepfakes zu erkennen?

Nein. Wir täuschen uns, wenn wir glauben, dass wir Deepfakes erkennen können. Studien zeigen, dass es rein zufällig ist, ob wir ein Deepfake als solches erkennen oder nicht. Wir müssen lernen mit dieser Unsicherheit umzugehen.

### Müssen wir uns künftig bei jedem Bild, Video und Text fragen: Ist das Realität oder Fiktion?

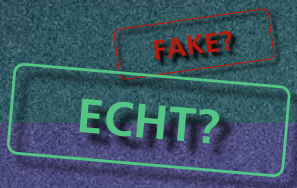
Wir müssen uns eine Art Generalverdacht antrainieren. Man muss immer die Möglichkeit miteinbeziehen, dass ein Artefakt ein Deepfake sein könnte. Wie brisant dies ist, hängt aber vom Kontext ab. In der Schweiz etwa reisen Bundesräte meist ganz allein im öffentlichen Verkehr, in anderen Situationen brauchen sie dagegen Leibwächter. Soll heissen: Wie genau wir aufpassen müssen, hängt vom Kontext ab.

### Was können wir also tun?

Die harte Botschaft lautet: Wir haben kein Patentrezept und wir wissen, dass das viele Menschen enttäuscht. Als Forscher:innen können wir Beispiele zeigen und Erfahrungen teilen, aber keine Rezepte liefern. Die Rezepte muss jeder für sich selbst machen.

### Warum sind Patentrezepte bei Deepfakes nicht möglich?

Das ist einfach: Gute Deepfakes funktionieren vor allem dort, wo sie unsere Schwächen adressieren. Jede Person hat ein anderes Gefährdungsmuster. Wir müssen als Individuen herausfinden, wann wir besonders gefährdet sind. Diese Situationen und Kontexte müssen wir uns merken. Wenn wir hereingelegt worden sind, müssen wir bereit sein, uns den Fehler einzugestehen.




## WAS IST EIN DEEPFAKE, WAS SIND SYNTHETISCHE MEDIEN?

**Deepfakes sind synthetische Medien, die mit KI hergestellt werden. Es sind Multimedia-Kreationen, die auf existierenden Inhalten basieren.**

Originaldaten von Menschen (z.B. Videomaterial) dienen dabei als Basis. Dank KI entstehen aus menschgemachten Originaldaten, neue Multimedia-Artefakte. Deren Inhalt ist fiktiv, aber sie wirken authentisch, weil sie das Aussehen, die Bewegungen und die Sprachmelodie von dargestellten Personen sehr gut nachahmen können.

Synthetische Medien bezeichnet das gleiche wie Deepfakes. Anders ist aber die Konnotation der beiden Begriffe: Deepfakes werden primär negativ wahrgenommen, synthetische Medien sind neutraler.

**Wahrnehmung als Herausforderung**
Es sind sehr menschliche Dinge, bei denen wir besonders aufpassen müssen. So glaubt man eine Nachricht gerne, wenn sie die eigene Weltsicht bestätigt oder einem als Wissenschafter den fehlenden Puzzlestein zur Erarbeitung einer neuen Theorie liefert.

Wer etwas glauben will, sollte immer nach- und hinterfragen, statt Information unreflektiert zu übernehmen. Gerade im Umgang mit Deepfakes brauchen wir also kritisches Denken. ChatGPT ist ein schönes Bespiel dafür, weil es gern halluziniert. Wer kritisch denken kann, erkennt leichter, ob das Tool zuverlässig arbeitet oder Anwender*innen gerade ins Schilf schickt.

**Positive Deepfakes**
Es gibt auch positive Deepfakes, zum Beispiel personalisierte Unterrichtsmaterialien an Bildungsinstitutionen sowie Anwendungen in der Filmindustrie, in der Kunst, im Theater und in der Musik. Deepfakes könnten beliebige Stücke im Stil bestimmter Pianisten spielen. Dies könnte für die Ausbildung angehender Pianist*innen sehr spannend sein.

**Schädliche Deepfake**
Deepfakes richten Schaden an, wenn sie eingesetzt werden, um zu täuschen. Aber auch wenn ein Deepfake etwas zeigt, von dem wir wissen, dass es nicht real ist, kann es Schaden anrichten, einfach dadurch, dass es Dinge zusammenbringt, die nicht zusammengehören. Zum Beispiel ein echter Pornofilm mit dem Gesicht eines Hollywood-Stars, eines Politikers oder einer ex-Partnerin.

**Schwierig zu unterscheiden**
Wichtig wäre, ein Deefake zu deklarieren. Das Publikum muss die Möglichkeit haben zu erkennen, dass es manipuliert wird.

# GUT ZU KENNEN: DEEPFAKES




**Deepfakes – oder synthetische Medien – nennt man Fotos, Videos oder Tonaufnahmen, die mit KI hergestellt werden und einen Sachverhalt zeigen, der sich in dieser Form nie ereignet hat.**

Bei Deepfakes kann es sich um manipulierte Dateien handeln oder um solche, die vollständig künstlich sind, erzeugt von Software, die sich auf Trainingsdaten aus riesigen Datenbeständen im Internet stützt. Aktuelle etablierte Deepfake-Programme decken eine breite Spannweite ab, von einfach zu nutzender Software für den Austausch von Gesichtern bis zu anspruchsvollen Anwendungen für das «virtuelle Puppenspiel» mit künstlichen Personen. Zudem gibt es bereits Programme, die rudimentäre Videos aufgrund von Textbefehlen – sogenannten «Prompts» erzeugen können.

**Tiefgreifende Täuschungen**
Deepfakes können missbraucht werden, um Personen bei intimen Handlungen, die sie nie gemacht haben, zu zeigen, oder um ihnen Worte in den Mund zu legen, die sie nie gesagt haben. Solche Videos oder Audioaufnahmen können dazu dienen, Menschen zu erpressen oder zu kompromittieren, etwa in politischen Auseinandersetzungen oder in privaten Beziehungen. Ein Beispiel sind erfundene Rachepornos. Eine geklonte Stimme kann auch dazu dienen, aus Angehörigen Geld herauszupressen, indem sie mit einer gefälschten Notsituation einer nahestehenden Person konfrontiert werden. Allein schon deswegen sollten möglichst wenig private Bilder und Videos ins Netz hochgeladen werden. Auch von Ereignissen wie Naturkatastrophen oder Explosionen existieren bereits täuschend echt aussehende Deepfakes. Die Software dazu basiert auf künstlichen neuronalen Netzwerken.

**Hauptsache Eigenverantwortung**
Welche Tipps hat TA-Swiss, Stiftung für Technologiefolgen-Abschätzung, in ihrer Studie «Augen und Ohren auf dem Prüfstand – Deepfakes und manipulierte Realitäten» auf Lager? Die Antwort klingt einfach, die Umsetzung ist anspruchsvoll: «Selbstverantwortung übernehmen. In sämtlichen Branchen sollte die Aus- und Weiterbildung zu Medien- und Informationskompetenz ganz oben auf der Prioritätenliste stehen. Bürgerinnen und Bürger wiederum sollten eigenverantwortlich die Bildungs- und Aufklärungsangebote verschiedener Stellen nutzen. Selbstverantwortung ist auch bei der Bewertung, Weiterverbreitung und Herstellung von Deepfakes ein Gebot der Stunde. Zudem sollte jeder und jedem bewusst sein, dass das Hochladen von Bildern und Sprachaufnahmen die Produktion von Deepfakes begünstigen kann. Der Grundsatz, wonach das Internet nicht vergisst, gilt besonders mit Blick auf Deepfakes.»

## AUSWIRKUNG VON ChatGPT

**Seit der offiziellen Einführung von ChatGPT im November 2022 schreiten KI-getriebene Innovationen in rasantem Tempo voran, und unsere Interaktion mit Technologie hat sich von Grund auf geändert.**

Im Bereich der IT-Sicherheit agiert KI als zentrale Antriebskraft. Sie stärkt unsere Abwehrmechanismen und ermöglicht Cyberkriminellen gleichzeitig, immer ausgereiftere Angriffstaktiken zu entwickeln. Cyber-Crime wird als Geschäftsmodell immer professioneller und profitabler. Kriminelle brauchen immer weniger Skills und Organisationsfähigkeiten, um einen effektvollen und lukrativen Angriff zu realisieren.

Das Tempo der Entwicklungen nimmt rasant zu. Die Vielzahl an Herausforderungen ist komplex; die Situation ist verworren. Die Professionalisierung der Cyber-Kriminalität und wachsende Präsenz von Cyber-Angriffen verbreiten Angst. Es wird immer klarer, dass keine neue Technologie immun ist gegen Cyber-Kriminalität. Und stoppen lässt sich KI auch nicht mehr: Sie breitet sich wie ein Lauffeuer aus und soll schon von mehreren 1000 Millionen Usern genutzt werden.

**Gefährlicher Fachkräftemangel**
Cyber ist ein geopolitisches Machtinstrument und gleichzeitig ein neuer Angriffsvektor geworden. Der Anstieg von Cyber-Attacken in globalen politischen Krisen und die gezielte Verbreitung von Falschinformationen machen die Weltlage unsicher und gefährlich. Es droht eine globale Spaltung durch digitale Irreführung. Und während sich die Situation weiter zuspitzt, kämpfen Cyber-Sicherheitsteams mit Fachkräftemangel und Burnout.

Es bleibt die Hoffnung auf eine starke Sicherheitskultur in Unternehmen, Organisationen und bei Behörden sowie auf den gesunden Menschenverstand der Bevölkerung, insbesondere der Schweizer Bevölkerung. Denn insbesondere der öffentliche Sektor und kritische Infrastrukturen sind bei Hackern beliebt und haben ein Problem, wenn ihre Daten und Infrastrukturen nicht genügend geschützt werden. Es geht schliesslich einen langfristigen Schutz der öffentlichen Sicherheit.

# URBANE SCHUTZMASSNAHMEN GEGEN ÜBERSCHWEMMUNGEN



**Das aufgeheizte Klima verstärkt massive Niederschläge. Dicht gebaute Städte können diese Wassermassen nicht schlucken. Metropolen wie Tokio, London und Chicago schützen sich mit gigantischen Anlagen vor Überschwemmungen. Auch Schweizer Städte wie Zürich ergreifen bauliche Gegenmassnahmen.**

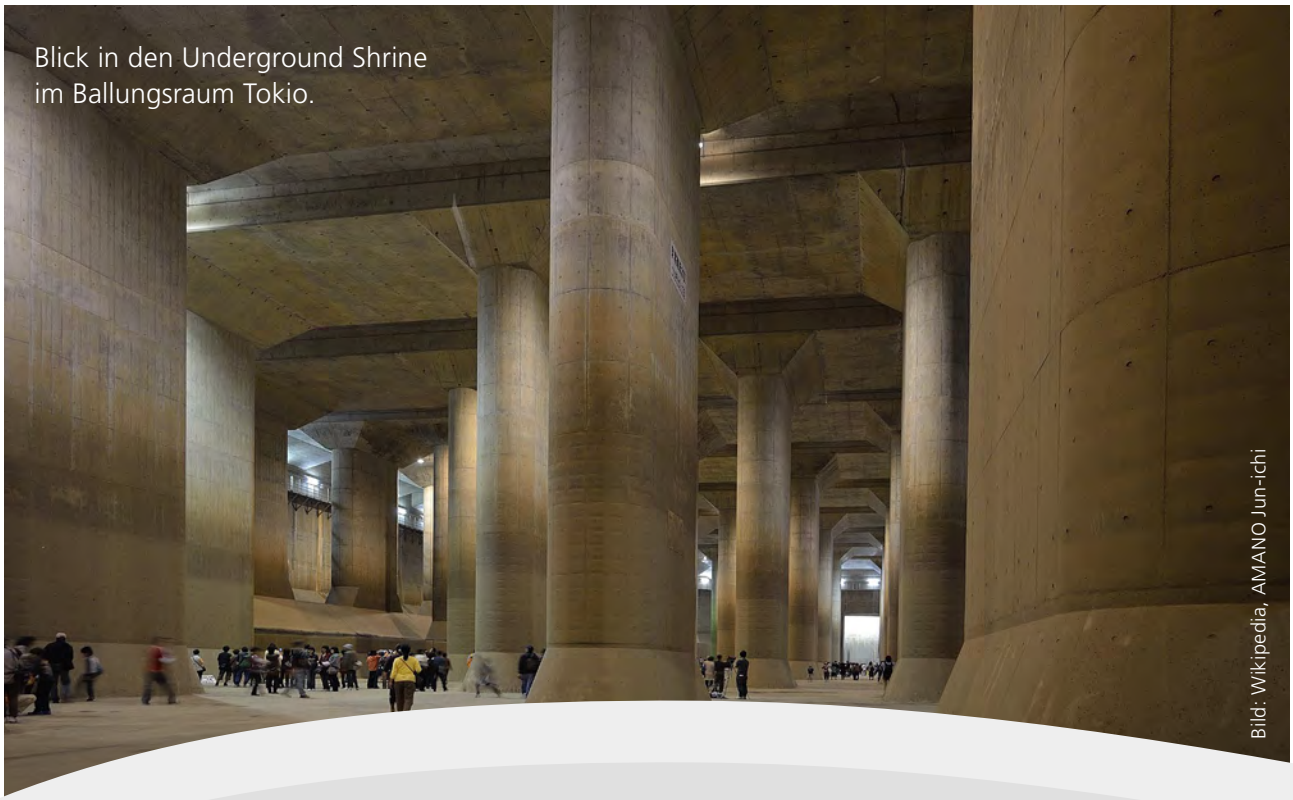
Der Underground Shrine bei Tokio wird von einem NZZ-Journalisten so beschrieben: «Wow! Dieser Schrein verdient seinen Namen. In die Halle – 177 Meter lang, 78 Meter breit und 18 Meter hoch – würde locker das Wasser von 66 olympischen Schwimmbecken hineinpassen. Man ist plötzlich sehr winzig. Besonders eindrücklich wirken die 59 Säulen, jede einzelne 500 Tonnen schwer. Sie tragen nicht nur die Decke, wie die Tourleiterin auf Japanisch erklärt, sondern bewahren die leere Halle auch davor, vom Wasserdruck im Boden angehoben zu werden. Deshalb sind es so viele. Um die Decke zu tragen, hätten auch weniger gereicht.»

Die 20 Grad kühle Halle ist Teil des Metropolitan Outer Area Underground Discharge Channel, auch «G-Cans» genannt. Das 6,3 Kilometer lange Tunnelsystem an Tokios Stadtrand wird bei starken Regenfällen geflutet, um die oberirdische Überschwemmung von Gemeinden und Feldern zu verhindern. Über fünf zylinderförmige Schächte fällt das Wasser der ansteigenden Flüsse in die Tiefe, wird durch einen Tunnel zum Wassertank, dem Schrein, geführt und hier von den vier grössten Turbinen Japans in den Edogawa-Fluss gepumpt. Er bringt das Wasser in die Meeresbucht von Tokio. Allein im Juni dieses Jahres kam das System viermal zum Einsatz, öfter als im gesamten vergangenen Jahr.

Dieses Tunnelsystem ist nicht neu, doch es ist noch immer eines der grössten weltweit. Gebaut wurde es von 1993 bis 2006 für umgerechnet etwa 1,3 Milliarden Franken. Damit war Tokio sehr früh dran. Die Region ist wie eine Schüssel geformt, so dass Starkregenfälle und der stark verbaute Boden schon damals zu Überschwemmungen geführt haben. Seither soll das System rund 150 Mal genutzt worden sein und Überschwemmungen von geschätzt über 860 Millionen Franken verhindert haben. Für Japan werden mit dem Temperaturanstieg mehr Taifune mit sintflutartigen Regenfällen prognostiziert.

**Ein sehr teures Projekt**

Japan investiert bis 2040 umgerechnet über 214 Millionen Franken, um den Hochwasserschutz



Blick in den Underground Shrine im Ballungsraum Tokio.

Bild: Wikipedia, AMANO Jun-ichi

der Hauptstadtregion Tokio auszubauen. Es ist Teil des milliardenschweren Tokyo Resilience Project, das die Stadt nicht nur sicherer vor Hochwasser und Stürmen machen soll, sondern auch vor Erdbeben und Vulkanausbrüchen, vor Stromausfällen und Pandemien – eine Stadt, «die nicht zusammenbricht, nicht brennt und in der Menschen überleben», schreiben die Projektverantwortlichen auf der Website.

Tokio ist mit diesen Problemen nicht allein. Auch andere Städte sind daran, unter- und oberirdisch mehr Kapazität zu schaffen, um Wasser abfliessen zu lassen.

London zum Beispiel. Die Neun-Millionen-Stadt entwässert über eine 150 Jahre alte Kanalisation. Diese ist für eine Bevölkerung gebaut worden, die halb so gross war wie heute. Infolgedessen fliessen jedes Jahr viele Millionen Kubikmeter ungeklärtes Abwasser in die Themse.

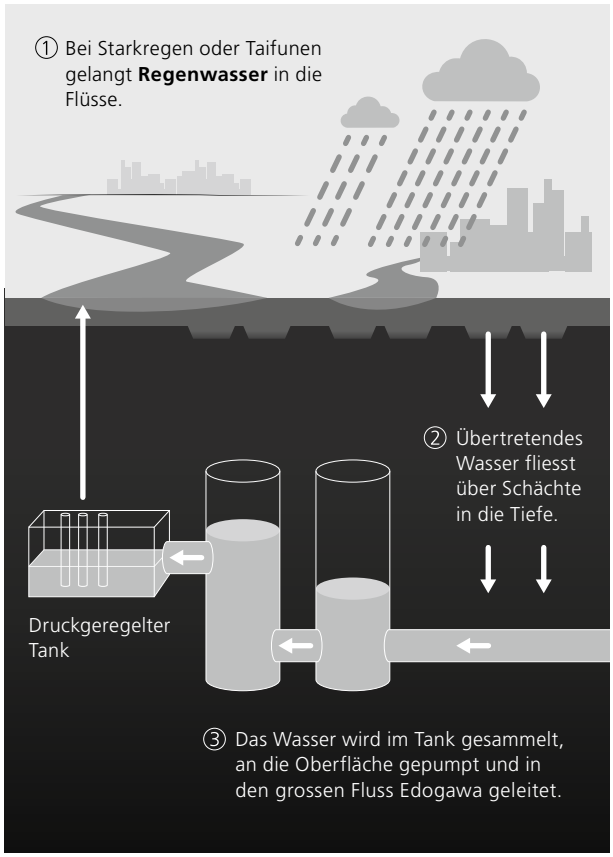
Nun baut die Stadt einen 25 Kilometer langen Kanal, den «Super Sewer», zu Deutsch Supersauger, wie die Tideway auch genannt wird. Er verläuft unter der Themse und soll zum einen das Abwasser der Londoner statt in die Themse in eine Kläranlage ausserhalb der Stadt leiten. Zum anderen soll er die Wassermassen der zunehmenden Stark- und Extremregenfälle auffangen, damit diese die marode Kanalisation nicht noch häufiger zum Überlaufen bringen.

Wie Tokio baut auch Chicago das Abwassersystem seit vielen Jahren aus. Nun entsteht die grösste Abwassergrube der Welt, das oberirdische McCook-Reservoir. Fertiggestellt im Jahr 2029, wird es fast 38 Millionen Kubikmeter Wasser fassen und 150-mal grösser sein als der Underground Shrine in Tokio. Ist der Starkregen vorbei, wird das gesammelte Wasser gereinigt und in Flüsse geleitet.

Doch man weiss schon heute: Das Reservoir wird nicht reichen. Bei der Planung hatte man die Auswirkungen des Klimawandels, wie wir sie heute kennen, nicht einberechnet.

**Auch in der Schweiz nimmt Starkregen zu**

Und was macht die Schweiz? Klar, Zürich ist nicht Tokio, Bern nicht London, Lugano nicht Chicago. Doch auch ohne Taifune wie in Japan hat die Niederschlagsmenge von einzelnen Starkniederschlägen in der Schweiz seit 1901 um 12 Prozent zugenommen. Und mit der fortschreitenden




Grafik: angelehnt an Infografik von Edogawa River Office.

Erderwärmung ist damit zu rechnen, dass Stark- und Extremniederschläge in allen Jahreszeiten noch intensiver werden, selbst wenn die durchschnittliche Niederschlagsmenge zurückgeht. Der Boden, die Kanalisation, die Oberflächengewässer müssen in kurzer Zeit viel Wasser aufnehmen und ableiten können.

Schweizer Städte setzen primär auf Entsiegelung statt auf Abfluss. «Zentral für den Umgang mit grossen Wassermengen ist eine moderne Siedlungsentwässerung», schreibt Maria Colon, Mediensprecherin Entsorgung und Recycling Zürich, auf Anfrage. Regenwasser soll nicht so schnell wie möglich in die Kanalisation fliessen, wie es früher der Fall war, sondern im Boden zurückgehalten werden. Versiegelte Flächen würden gar vermehrt vom Kanalnetz abgetrennt

Damit das Regenwasser von Bäumen und Pflanzen aufgenommen werden kann sowie beim Verdunsten die Hitze mildert, muss es auf Dächern, Plätzen und im Boden temporär zurückgehalten werden. Das soll gleichzeitig Trockenperioden überbrücken und die Kanalisation und die Abwasserreinigungsanlagen entlasten. Denn fliesst zu viel Regenwasser in die Abwasserreinigungsanlagen, kann mit ihm auch ungereinigtes Abwasser in die Bäche und Flüsse gelangen.

# ENERGIE AUS DEM GRUNDWASSER



**Klimafreundliche Wärme: Jeder fünfte Haushalt heizt mit einer Wärmepumpe. 1990 heizten noch fast 60% der Haushalte mit Öl, jetzt sind es noch 37%. Das zeigt die neuste Gebäudestatistik der Schweiz.**

Heizen wird immer umweltschonender: Schon drei Viertel der neuen Gebäude haben eine Wärmepumpe. Seit dem Jahr 2000 hat sich der Anteil an Wärmepumpen in Schweizer Gebäuden verfünffacht. Dies zeigt die neue Gebäude- und Wohnungsstatistik des Bundesamtes für Statistik (BFS). Laut BFS wurden im vergangenen Jahr 37 Prozent der Gebäude mit Heizöl geheizt, 21 Prozent mit einer Wärmepumpe und 17 Prozent mit Gas. Hinzu kommen 12%, die mit Holz geheizt wurden, und 8%, die auf Elektrizität setzten.

Der Anteil der Wärmepumpen hat sich somit seit dem Jahr 2000 verfünffacht. Dabei zeigt sich ein deutlicher Unterschied zwischen älteren und neueren Gebäuden. Bereits drei Viertel der Gebäude, die in den letzten zehn Jahren gebaut wurden, haben eine Wärmepumpe. Jedes vierte Einfamilienhaus besitzt eine.

Bei der Energiequelle zeigt sich auch ein langfristiger Trend: Waren 1990 noch 58% der Gebäude mit Heizöl beheizt, waren es 2023 noch 37. An zweiter Stelle folgt Gas: Beim Gas waren es 1990 noch 8%, der Anteil stieg bis 2021 auf gut 17%, ging dann 2023 aber wieder leicht zurück. Auch die Zahl der Elektroheizungen ging zurück, jener von Fernwärme stieg von 1% 1990 auf knapp 4% 2023.

Das BFS unterscheidet zwischen dem Beheizen von Gebäuden und von Haushalten und schreibt: «Auf Ebene der Haushalte sieht die Situation etwas anders aus.» Knapp zwei Drittel der Haushalte heizten demnach im vergangenen Jahr mit fossilen Energieträgern (38% Heizöl und 25% Gas). Zudem nutzen 18% der Haushalte eine Wärmepumpe.

**Einfamilienhäuser mit wenigen Bewohnern**
Wie aus der Statistik weiter hervorgeht, gab es im Jahr 2023 in der Schweiz 1,79 Millionen Gebäude, die zum Wohnen benutzt werden. Mehr als eine Million davon waren Einfamilienhäuser. Von ihnen wurden gut die Hälfte nur von einer oder von zwei Personen bewohnt. Neben den Einfamilienhäusern wurden 4,79 Millionen Wohnungen gezählt.

In den Wohnungen lag die durchschnittliche Wohnfläche bei gut 102 m². Etwas über die Hälfte der Wohnungen hat drei oder vier Zimmer. Die durchschnittliche Wohnfläche einer bewohnten Wohnung betrug somit 46,2 m² – dieser Wert ist damit seit 2022 gleichgeblieben.

## DIE STROMPREISE FÜR 2025 SINKEN

Plus ein Viertel im Jahr 2023, plus ein Fünftel im 2024: Die Strompreise waren in den letzten zwei Jahren stark gestiegen. Doch jetzt können die Konsument:innen aufatmen: Für 2025 sinken die schweizerischen Strompreise in der Grundversorgung für Haushalte im Mittel (Median) um rund 10%.

Dies teilte die Eidg. Elektrizitätskommission (Elcom) mit. Ein typischer Haushalt bezahlt somit nächstes Jahr rund 29 Rappen pro Kilowattstunde (Rp./kWh). Das sind gut 3 Rp. weniger als 2023. Auf 12 Monate hochgerechnet, spart dieser Haushalt auf eine Stromrechnung von CHF 1305 rund CHF 141, er zahlt also nur noch CHF 1164. Auch sinken die Netzkosten um 4%.

Die Gründe liegen in der Stabilisierung des Strom-Grosshandelmarkts. Dort sind die Grosshandelpreise von 150 Euro/MWh auf 90 Euro/MWh gesunken. Auch sind die Kosten für die Winterreserve tiefer, ebenso die Kapitalverzinsung für das Netz.

# Entdeckt! Gespeicherter August dank Solarthermieanlage

**Warme Sommer haben ihr Gutes: Von der Sonne erhitztes Wasser bleibt in speziellen Becken oder unter der Erde bis im Winter warm. Diese Technologie hilft, im Winter Strom zu sparen und Emissionen zu vermeiden.**



Langfristig nutzbare Wärmespeicher dienen auf clevere Weise dem Klimaschutz. Und sie entlasten die Stromnetze, indem sie im heissen Sommer Strom beziehen, statt mit einer Masse an erneuerbarem Strom die Leitungen zu fluten. In Dänemark sind solche Anlagen schon etabliert. Nun wird die Technik auch in Deutschland und in der Schweiz immer öfter eingesetzt.

### Und so funktionierts

Die Speicher werden mit Energie aus einer Solarthermieanlage oder mit Solarstrom betriebene Wärmepumpen versorgt. Auf beide Weisen wird im Sommer auf Vorrat Strom für den Winter erzeugt. Photovoltaik-Anlagen liefern im Sommer ein Vielfaches mehr Energie als im Sommer. Mit Batterien lässt sich der Strom nur für wenige Tage speichern. Im Gegensatz dazu dienen Wärmespeicher als Langzeit-Stromspeicher.

### Nah- statt Fernwärmenetz

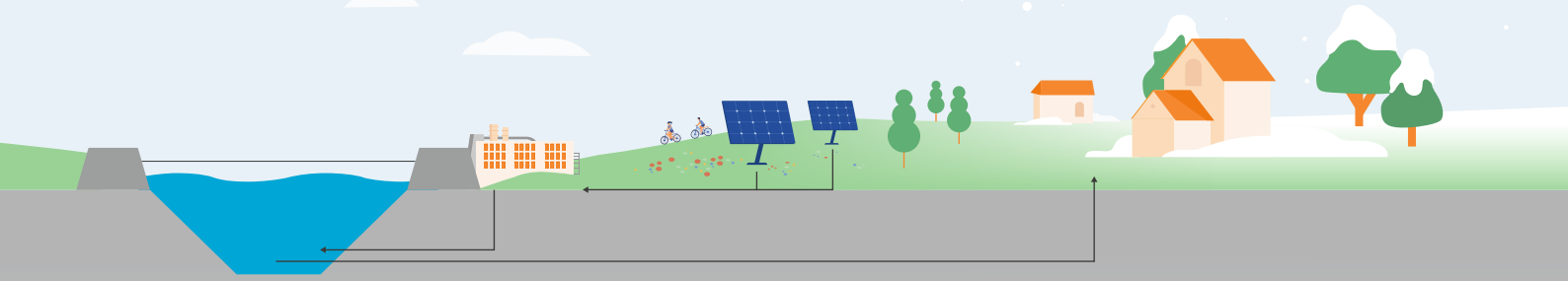
Im Winter wird der Speicher entladen: Wärmepumpen nutzen die Wärme, um Heizenergie zu erzeugen. Wie kann denn ein Becken saisonal Wärme speichern? Die umgebenden Erdmassen und eine isolierende Abdeckung sorgen dafür, dass das Wasser bis weit in den Winter hinein heiss genug bleibt, um Wohnungen und Häuser zu wärmen. Die Gebäude sind mit kurzen Leitungen über ein Nahwärmenetz (Gegensatz zum Fernwärmenetz) mit dem Speicher verbunden und werden somit klimaneutral erwärmt.

Für die Schweiz hat das Konzept mit den Wärmepumpen den Vorteil, dass sie den laufenden Umstieg von Gas- und Ölheizungen auf Wärmepumpen besser bewältigen kann. Für die Reduktion des Strombedarfs ist auch wichtig, dass die Wärmespeicher ebenso Abwärme aus KVA und Industriebetrieben aufnehmen können. Speziell im Sommer wird diese Abwärme oft zu einem grossen Teil ungenutzt in die Umwelt abgegeben.

### Bern als Vorreiterin

Eine Anlage mit Wärmespeicher entsteht derzeit am Stadtrand von Bern. Der Versorger Energie Wasser Bern richtet in bis zu 500 Meter tief gelegenen Sandschichten einen Speicher ein, der Abwärme aus der nahe gelegenen KVA aufnehmen soll.

An Universitäten, Instituten und in Startups wird derzeit an weiteren Anlagen geforscht, welche Wärme speichern könnten. Die Ideen reichen von Wassergefüllten Speicherballons, die in Seen verankert würden, bis zu Luftschutzkellern, die als Wasser-Wärmespeicher genutzt werden könnten. Die Zukunft der klimaneutralen Energie wird laufend weitergeschrieben.



Die Solarthermieanlage erhitzt das Wasser. Das erwärmte Wasser wird dann im Betriebsgebäude mit Wärmetauschern richtung Becken gepumpt. Hier bleibt es bis im Winter warm und wird dann genutzt um nahe gelegene Häuser zu heizen.

# GELESEN Finstere Zeiten

**Der international bekannte Geschichtswissenschaftler und Bestsellerautor Yuval Noah Hariri schreibt in seinem neuen Werk «Nexus» über die Auswirkung der Künstlichen Intelligenz auf die Menschheit. Ein finsteres Buch.**

Weder der Daumen noch die Sprache oder die Abstraktionsfähigkeit, um in die Zukunft zu denken, sei der entscheidende Faktor, der die Menschen zur Menschheit gemacht habe, sondern ihre Fähigkeit, Informationsnetzwerke zu bilden. Dies stellt der israelische Historiker und Weltbestsellerautor Yuval Noah Hariri gleich zu Beginn seines Buchs «Nexus» fest. Damit zitiert er sich selbst, denn diese These vertritt er in mehreren seinen Werken.

In der Steinzeit beginnend und im Konjunktiv mögliche Zukünfte projizierend, ist das Buch auch eine Warnung vor einer Zukunft, in der die Künstliche Intelligenz (KI) mehr Macht erlangen könnte, als es den Menschen lieb ist und guttut. Die von ihm beschriebene Zukunft stellt bisherige Apokalypse-Szenarien in den Schatten

Oft geäusserte Hypothesen wie die, dass KI eine Evolution sei wie damals der Buchdruck, schiesst er ab. Denn damals wie heute sei der Mensch der zentrale Knoten eines Informationsnetzwerks gewesen. Doch dies ändere sich zurzeit. KI schaffe sich Netzwerke ohne Menschen und übernehme damit die Deutungshoheit. Hariri positioniert KI weniger als technisches, wissenschaftliches oder ökonomisches Phänomen, sondern interpretiert KI als gesellschaftliche Triebkraft und neuen Akteur in der Geschichte unseres Planeten.

Die englische Abkürzung für KI – AI für Artificial Intelligence – deutet der Autor um in «Alien Intelligence», zu Deutsch «Andersartige Intelligenz». Sie sei ohne Bewusstsein und Gefühle und könne trotzdem handeln. Das sei eine unfassbare Macht.

Dieser Alarm und viele apokalyptische Szenen, denen zufolge die menschliche Herrschaft auf der Erde enden könnte, führen in «Nexus» zum Thema Transhumanismus: Ist der Mensch überhaupt fähig, sich gegen die Machtansprüche der KI zur Wehr zu setzen? Und ist KI für die Menschheit ein Segen oder fataler Fehler? Die Zukunft wird es zeigen. ■


**IMPRESSUM**

**Konzept, Text und Redaktion:** Alice Baumann, yourconsultant.ch
**Recherche und Faktencheck:** NZZ, NZZ am Sonntag, Studie Cyber Message 2024 Kessler, Studie Cybercrime Trends 2024 sosafe, Studie Deepfakes und manipulierte Realitäten, TA-Swiss, SRF News, TX Group
**Fotos:** Ruben Ung, Stefan Kubli
**Layout:** Burki Scherer AG

**Herausgeber:**
**erzo KVA + erzo ARA,** Wiggertalstr. 40, 4665 Oftringen

**Newsletter Download unter:**