

ab 13. Oktober



Einbrüche

ab 20. Oktober



Verkehr

ab 27. Oktober



Arbeitsplatz

ab 3. November



Kinder

ab 10. November



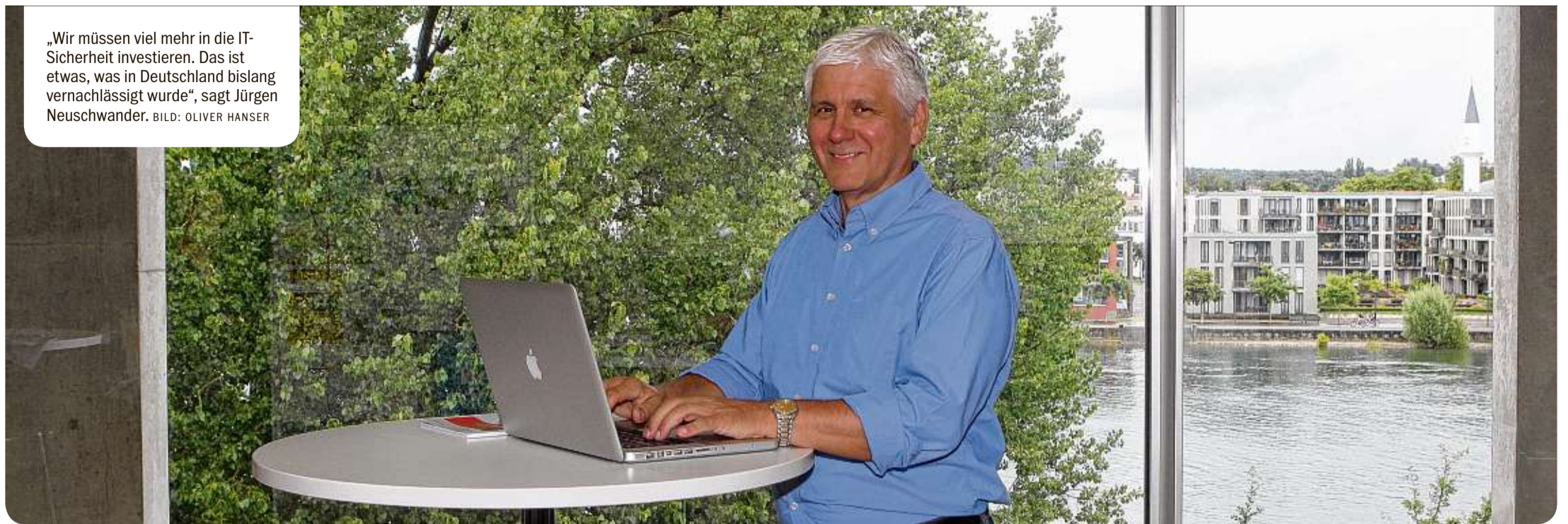
Internet

ab 17. November



Unwetter

„Wir müssen viel mehr in die IT-Sicherheit investieren. Das ist etwas, was in Deutschland bislang vernachlässigt wurde“, sagt Jürgen Neuschwander. BILD: OLIVER HANSER



# „Das Ende der Privatheit ist in Sicht“

**Sicherheit:** Jürgen Neuschwander, Dekan der Fakultät Informatik an der Hochschule Konstanz, spricht über Datensicherheit, Voyeurismus sowie die Vor- und Nachteile des großen Daten-Sammelns

**Herr Neuschwander, in Vorträgen zum Thema Digitalisierung sprechen Sie unter anderem von der „digitalen Apokalypse“. Was heißt das?**

Darunter verstehe ich die Kombination von einem physischen terroristischen Angriff, verknüpft mit einem informationstechnischen Angriff auf kritische Infrastrukturen. Kritische Infrastrukturen sind Institutionen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltige Störungen der öffentlichen Sicherheit oder Versorgung eintreten würden. Beispielsweise die Energieversorgung, Wasserversorgung, Verkehr und Transportwesen, Gesundheitswesen. Alle diese Infrastrukturen sind in den vergangenen Jahren massiv mit IT ausgestattet worden und sind mit anderen Systemen kommunikativ oder steuerungstechnisch vernetzt. Dadurch wird die Möglichkeit eines Cyberangriffs auf solche Systeme geschaffen. Stellen Sie sich einen terroristischen Bombenangriff auf einen Flughafen vor, der begleitet wird von einem teilweisen Ausfall der Energieversorgung, einem Ausfall der Kommunikationsverbindungen und der Verkehrssteuerer. Es kommt keine Hilfe an, da alle Straßen verstopft sind, die erforderliche Kommunikation und Kooperation von Rettungskräften funktioniert nicht und dergleichen mehr. Wir müssen in Zukunft davon ausgehen, dass solche

Cyberangriffe auf kritische Infrastrukturen zunehmend als Option terroristischer oder schwerkriminalischer Angriffe auftreten werden und heute schon geplant werden.

**Welche Lösung sehen Sie für dieses Problem?**

Wir müssen viel mehr in die IT-Sicherheit investieren. Das ist etwas, was in Deutschland bislang vernachlässigt wurde. Wir haben vor 20 Jahren angefangen, in der öffentlichen Verwaltung und auch in der Bundeswehr aufgrund des Kostendrucks seriengefertigte Produkte aus dem Regal zu bestellen, also PCs von Microsoft oder Dell zum Beispiel. Die Frage hätte lauten müssen: Wie können wir diese Ware sicherer machen? Zum Beispiel in Form eigener entwickelter, sicherer Hard- und Software. Stattdessen gibt es überall Standard-Betriebssysteme mit den bekannten Schwachstellen, mit denen im Darknet sogar gehandelt wird. Wenn wir da jetzt noch gute Lösungen und Produkte entwickeln würden, könnten wir eine Marktlücke besetzen. Denn dieses Sicherheitsproblem hat nicht nur Deutschland.

**Wo steht das Thema Datenschutz in Deutschland – und wo wird es Ihrer Meinung nach in fünf Jahren sein?**

Das ist eine spannende Frage. Momentan haben wir in Deutschland – im Gegensatz zu den USA beispielsweise – sehr restriktive Datenschutzgesetze. Das ist stellenweise gut, verhindert aber auch Innovationen. Ein einfaches Beispiel: Industrie 4.0 ist in aller Munde. Ein Thema in diesem Komplex ist die automatisierte Fabrik. Werkstücke laufen über die Produktionsstraße und teilen den Fertigungsmaschinen mit, was mit ihnen gemacht werden soll. Eine Frage ist: Wer haftet eigentlich dafür, wenn diese Maschine dann Ausschuss produziert? Das ist im Moment rechtlich noch ziemlich unklar. Das andere Thema ist das Internet der Dinge, in dem selbst der Regenschirm oder die Kaffeemaschine „smart“ und digital wird. Smartphones, vernetzte Navigationsgeräte, selbstfahrende Autos, Fitnessarmbänder und smarte Uhren, überall hinterlassen wir Datenspuren, die letztlich zum Verlust der Privatsphäre führen können. Ich habe noch erlebt, wie die Menschen zu Beginn der 80er Jahre demonstriert haben, als die Volkszähler vor der Tür standen und wissen wollten, wie viele Quadratmeter die Wohnung habe. Dann gab es 1983 das Urteil des BGH auf informationelle Selbstbestimmung. Jeder hat das Recht, über seine eigenen Daten zu entscheiden. Heute, in der jungen Ge-

neration, hat das überhaupt keine Bedeutung mehr. Heute stellt man seine Daten freiwillig ins Netz. Sehen Sie sich YouTube an. Den größten Zulauf haben die Blogger, die ihr tägliches Leben ins Netz stellen. Denen folgen Millionen von Usern. Das ist so eine Trivialität, denen zuzuschauen, aber irgendwie sind die Follower begeistert davon. Ich habe den Eindruck, dass man in der heutigen Welt nur noch etwas zählt, wenn man eine mediale Gestalt ist. Aber ist das denn beklagenswert? In einer Zeit des Voyeurismus à la Dschungelcamp, einer Zeit des transparenten Lebens, in einer Zeit, in der man die kleinsten Belanglosigkeiten in Netzwerken posten muss, um öffentlich wahrgenommen zu werden, in dieser Transparenzgesellschaft hat das Offenlegen persönlicher Daten ihren Schrecken verloren. Das Ende der Privatheit ist in Sicht. Informationelle Selbstbestimmung ist wohl ein Auslaufmodell.

**Das hört sich alles ziemlich pessimistisch an.**

Das soll keine Dystopie sein. Es gibt immer eine andere Seite. Social Media sind eine der größten kulturellen und gesellschaftlichen Entwicklungen unserer Neuzeit. Ich würde es sogar disruptive Innovation nennen. Soziale Netzwerke haben uns neue Formen der Interaktion und Kommunikation untereinander eröffnet. Facebook, Twitter oder jetzt Snapchat bedingen neue Umgangsformen der Kommunikation. Systemkritische Blogger haben Geschichte geschrieben, politische Umbrüche und Willensbildungen wurden über diese Netzwerke organisiert und koordiniert. Die Etablierung von Communities für spezielle Themenbereiche, sei es Gesundheit, Politik, Umwelt oder einfach Teilhabe am Leben von anderen Menschen, hat einen neuen gesellschaftlichen Informationsaustausch initiiert. Crowdfunding-Plattformen verhelfen zur Verwirklichung von Träumen innovativer Gründer. Die Sharing Economy kann die gesamtwirtschaftliche Ressourcenproduktivität erhöhen und auch die Umweltbilanz verbessern. Aber auch hier kommt wieder die Janusköpfigkeit zum Vorschein. Die „Big 4“ des Silicon Valley (Amazon, Apple, Facebook und Google) haben mittlerweile einen ungeheuren Einfluss auf unser Leben, was den meisten gar nicht bewusst ist. Wir erleiden dabei einen zunehmenden Kontrollverlust unserer Daten, paradoxerweise basierend auf der freiwilligen Zuarbeit der Betroffenen. Durch neue Plattformen und Technologien werden Infrastrukturen geschaffen, die fast alle Bereiche der Ökonomie und Lebenswelt durchdrin-

gen. Manche sprechen auch vom „Plattformkapitalismus“.

**Wenn wir all das mal in einer Gesamtschau betrachten: Macht die Digitalisierung die Welt nun letztlich besser oder schlechter?**

Sie macht sie anders. Es ist letztlich wie immer, es gibt viele gute Seiten, tolle Innovationen, die unsere Industrie oder unsere Zivilgesellschaft weiter voranbringen, und es gibt Nachteile und Gefahren, die diese Neuerungen mit sich bringen. Mit den heute verfügbaren Plattformen besteht das erste Mal auch für kleine Unternehmen und Dienstleister die Möglichkeit, weltweit die eigenen Produkte zu vermarkten und direkt mit Kunden in Kontakt zu treten. So werden Barrieren abgebaut, die früher von etablierten Händlern und Produzenten beherrscht wurden. Mit Big Data lassen sich neue Erkenntnisse gewinnen, die sonst nicht gefunden werden könnten. Denn der Preis der Präzision theoretischer Modelle ist oft die Unfähigkeit, Fragen des realen Lebens zu behandeln. So kann man heute mit Big Data Grippewellen voraussagen, seltene Krankheiten sicherer diagnostizieren oder autonomes Fahren ermöglichen. Aber Big Data kleidet sich in die Gewänder des Lustgewinns und verspricht ein besseres Leben und eine gesteigerte Bequemlichkeit. Das Versprechen des optimierten Lebens ist aber eine Falle. Wir alle bezahlen dies mit unseren persönlichen Daten, deren Aggregation, deren Verknüpfung mit anderen Daten über uns. Die Vorstellung, dass nur das öffentlich wird, was der Einzelne explizit von sich preisgibt, stellt sich in der vernetzten Welt zunehmend als Illusion heraus. Selbst Menschen, die die Website von Facebook nie besucht haben, finden sich bereits in deren Datenbanken, inklusive ihrer möglichen Bekanntschaften mit anderen Facebooknutzern. Always Online bedingt durch die vielen Sensoren, die uns in allen möglichen Geräten umgeben, dass wir transparent werden, dass unser „digitaler Schatten“ sichtbar wird. Und diese mögliche Überwachung macht etwas mit der Gesellschaft. Das Verhalten der Menschen passt sich situativ an. Aber dort, wo unser Grundrecht auf informationelle Selbstbestimmung zur Disposition steht und der Mensch einer Totalüberwachung unterworfen wird, die ihn zu konformem Verhalten zwingt, hört die Freiheit auf und eine Form der Diktatur beginnt. Diese mögliche Transparenz und Überwachung ist letztlich antidemokratisch.

FRAGEN: SANDRA PFANNER

## Die Serie

Überwachungskameras, Warnwesten und Viren-Scanner – vieles macht das Leben sicherer. Aber was hilft wirklich? Und was tun, wenn doch ein Unglück passiert? Wissenswertes und Nützliches rund ums Thema Sicherheit finden Sie sechs Wochen lang donnerstags und samstags in dieser SÜDKURIER-Serie.



Wie sich Unternehmen gegen Cyberkriminalität schützen und was zu tun ist, wenn Kriminelle Zugang zum Rechner haben, lesen Sie im exklusiven Online-Dossier: [www.suedkurier.de/sicherheit](http://www.suedkurier.de/sicherheit)