DATENSICHERHEIT UND „E-PRIVACY“

Wie BND, CIA und NSA uns ausspähen …

Der größte Internetknotenpunkt der Welt, DE-CIX, pulsiert in Frankfurt am Main. Und einer der renommiertesten Internetdaten-Experten Deutschlands weiß genau, was dort passiert. Klaus Landefeld gibt Einblick in die komplexe digitale Infrastruktur

VON **MARIO MÜLLER-DOFEL**

Vor etwas mehr als einem Jahr, im April 2016, ist die EU-Verordnung „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ in Kraft getreten. Sie soll das europäische Datenschutzrecht harmonisieren. Im nächsten Jahr, ab dem 25. Mai 2018, wird sie in allen Mitgliedstaaten der Europäischen Union unmittelbares Recht sein – und damit über dem nationalen Recht, etwa dem Bundesdatenschutzgesetz (BDSG), stehen.

Viele Unternehmen halten die Informations- und Konsultationspflichten der EU für zu umfassend und zu teuer. Dagegen sehen Verbraucherschützer schon neue (Daten-)Geschenke für Unternehmen, da ihrer Auffassung nach zu viele Ausnahmeregelungen die Informationspflichten zur Datenerhebung aushöhlen.

Dies ist aber nicht der einzige Datenstreit in Deutschland. Auch die Befugnisse des Bundesnachrichtendiensts (BND) sorgen für Irritationen und Klagen.

Einer, der sich seit 35 Jahren mit Datensicherheit befasst, ist Klaus Landefeld. Der 48-Jährige gründete mit 16 sein erstes Unternehmen. Seit 1997 ist er Vorstand für Infrastruktur und Netze beim eco Verband der Internetwirtschaft e. V., dem die meisten Internetzugang- und Internetinhalte-Anbieter in Deutschland angehören. Seit 2003 ist er Beirat von DE-CIX, seit 2013 auch Aufsichtsrat.

Was DE-CIX ist? Ein Unternehmen, das ausgeschrieben Deutscher Commercial Internet Exchange heißt und nicht gewinnorientiert arbeitet. Es gehört zu 100 Prozent dem eco Verband und betreibt unter anderem den nach Datendurchsatz größten Internetknotenpunkt der Welt – in Frankfurt am Main.

Mehrere deutsche Knotenpunkte

Internetknotenpunkt? Was soll das schon wieder sein? Landefeld (siehe auch Interview ab Seite 57) erklärt erst einmal den Internetknoten: „‚Knoten‘ klingt vielleicht etwas nach Knäuel oder Durcheinander. Das ist es aber nicht. DE-CIX betreibt eine zentrale Schaltstelle, in der momentan rund 750 Internetanbieter verbunden sind, die Daten miteinander austauschen.“ Das Unternehmen organisiere die Verbindungen zwischen den Teilnehmern des Knotenpunkts, damit nicht jeder Teilnehmer zu einem anderen eine eigene Leitung legen muss. Es wären sonst Hunderte von Leitungen pro Unternehmen notwendig. „Das würde nicht funktionieren“, sagt Landefeld.

Und „größter Internetknoten der Welt“ heißt: „In Spitzenzeiten liegen wir bei 5,6 Terabit pro Sekunde. Ein Vergleich: Auf diesen Wert käme man auch, wenn 1,2 Millionen User zugleich ein Video in HD-Qualität anschauten.“ ▶▶

WEITERE THEMEN

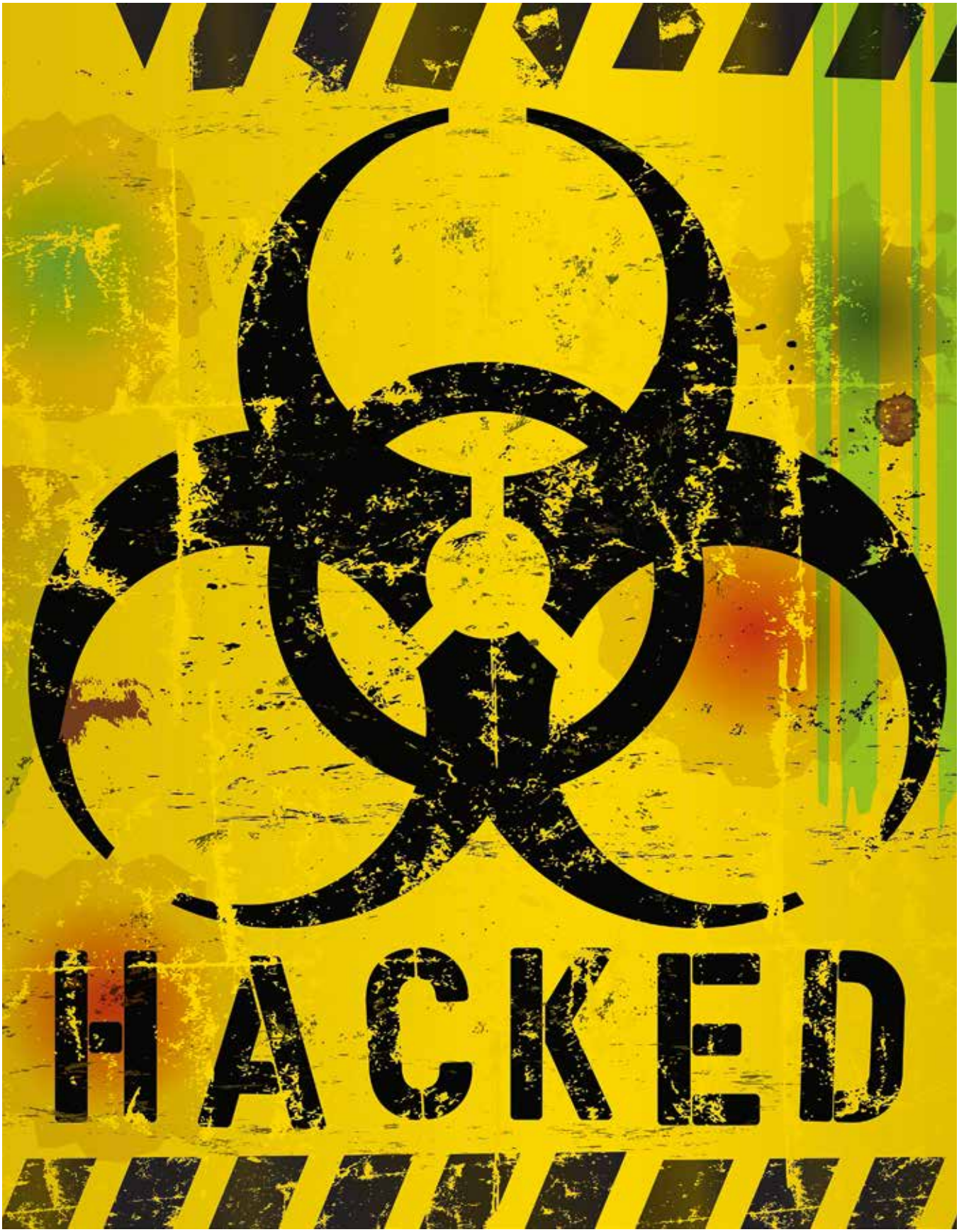

FOTO: WAMSLER/123RF

Der weltweite Cyber-Angriff „WannaCry“ Mitte Mai nutzte eine Sicherheitslücke im Betriebssystem Windows

Die Nutzer der DE-CIX-Knotenpunkte in Frankfurt, Hamburg, Düsseldorf und anderen Städten heißen Microsoft, Apple, Deutsche Telekom – um nur ein paar Beispiele zu nennen. Aber auch Firmen, die Internetzugänge an Endkunden verkaufen wie 1&1, sind dabei. „Nur wenn Anbieter große Datenvolumina untereinander austauschen, lohnt es sich, zwischen ihnen separate Leitungen zu schalten", sagt Landefeld. „Aber für die meisten Verbindungen ist ein Knotenpunkt wie unserer perfekt."

Zur Sicherheit mit Stacheldraht

Dass Frankfurt und nicht etwa das Silicon Valley der größte Internetknotenpunkt der Welt ist, liegt daran, dass insbesondere in den USA die Infrastrukturbereitstellung – in erster Linie aus geografischen Gründen – regional statt zentral organisiert ist. Aber je größer ein Knotenpunkt ist, desto mehr teilnehmende Firmen erreichen andere Teilnehmer mit ihrer Leitung. Und das ist attraktiv, weil unkompliziert und kostengünstig für Unternehmen. Zudem agiert DE-CIX neutral.

Der Frankfurter Knotenpunkt verteilt sich auf über 20 Rechenzentren an verschiedenen Standorten – etwa in der Hanauer Landstraße, in der Gutleutstraße und in der Daimlerstraße. Dort hat DE-CIX große sogenannte Umschalter, im Englischen „switches" genannt, aufgestellt, die verschiedene Netzwerke miteinander verbinden.

Die Anzahl der Menschen, die dort regelmäßig arbeiten, ist laut Landefeld „überschaubar", und sie werden zumeist vom Betreiber der Rechenzentrumsfläche bezahlt. Sie kümmern sich um die Belüftung, Energieversorgung und Objektbewachung. Mitunter seien auch Netzwerktechniker von Teilnehmerfirmen oder vom Netzwerkbereitsteller DE-CIX vor Ort, die nach Switches und Verkabelungen schauen.

Für Geheimdienste und auf Datenklau spezialisierte Kriminelle könnten solche Knotenpunkte interessante Angriffsziele sein – auch deshalb sind die Flächen hochsicher und von Stacheldrahtzäunen umgeben. Klaus Landefeld kennt sich mit den Feinheiten des Datenschutzes und mit Spionagemethoden aus. Darüber gibt er im folgenden Interview Auskunft. ■

Klaus Landefeld, Vorstand Infrastruktur und Netze beim Internetverband eco e. V.

INTERVIEW

„Die BND-Befugnisse gehen zu weit“

Der Internetpionier Klaus Landefeld über Hochsicherheit, Geheimdienstbegehren, Datenklaumethoden, die widersprüchlichen Interessen der Politik und die Inkompetenz der Gesellschaft, staatliche und industrielle Datensammelwut richtig zu bewerten

Mario Müller-Dofel: ***Herr Landefeld, wahrscheinlich durchqueren auch jede Menge Daten der Leserinnen und Leser von Tichys Einblick Ihre Internetknotenpunkte. Wie hoch ist das Sicherheitslevel dort?***

Klaus Landefeld: Unterschiedlich – von sicher bis hochsicher, je nach Geschäftsmodell der Betreiber. Die Rechenzentren werden von anderen Firmen zur Verfügung gestellt, DE-CIX kümmert sich nur um die korrekte gegenseitige Verschaltung der Teilnehmerfirmen.

Und was macht DE-CIX, um unsere Daten zu schützen?

Da ist zunächst der öffentliche Teil: Wir unterliegen dem Telekommunikationsgesetz, genau wie jeder andere Telekommunikationsanbieter. Als solcher müssen wir ein von der Bundesnetzagentur geprüftes Sicherheitskonzept vorhalten; unseres ist 800 DIN-A4-Seiten dick. Darin geht es um mögliche Bedrohungen und darum, wie wir uns und unsere Kunden dagegen wappnen. Zudem unterliegen wir der Sonderaufsicht des Bundesinnenministeriums, weil unsere Knotenpunkte zur sogenannten kritischen Infrastruktur gehören.

Gibt es auch nichtöffentliche Teile?

Ja. Unabhängig von den genannten Datenschutzmaßnahmen haben wir alle möglichen Zertifizierungen, wie zum Beispiel ISO oder IT-Grundschutz, um unseren Kunden den höchsten Sicherheitslevel zu bieten.

Kunden welcher Art?

Insbesondere jene, deren Geschäftsmodell es ist, hochsichere Kommunikation abzuwickeln. Es gibt sogar Zonen in manchen Rechenzentren, die nur wenige ausgewählte DE-CIX-Mitarbeiter betreten dürfen. Da muss 100-prozentig gesichert sein, dass niemand sonst zum Beispiel Kabel umstecken kann. Natürlich erstrecken sich die Sicherheitsbestimmungen auch auf andere technische Geräte, die wir nutzen.

Spätestens seit 2013, als herauskam, dass der US-Geheimdienst NSA hierzulande digitale Spionage im großen Stil betreibt, ist Datenschutz in aller Munde. Der damalige Innenminister Hans-Peter Friedrich hat gesagt, der Frankfurter Internetknoten würde nicht von US-Geheimdiensten ausgespäht – und DE-CIX suggerierte Zustimmung. Mussten Sie gute Miene zum bösen Spiel machen?

„Ein winziger gefühlter Nutzen, und zack – schon werden auch die persönlichsten Daten zur Nutzung freigegeben.“

Absolut nicht. Wir halten es nach wie vor für unrealistisch, dass sich ein fremder Geheimdienst an unseren Internetknoten zu schaffen machen könnte.

Weshalb sind Sie da so sicher?

Um das zu verstehen, muss man zwei Leitungsarten unterscheiden: erstens die Leitungen, die von den Teilnehmern auf unseren Knoten zuführen, und zweitens die Leitungen, mit denen wir innerhalb unserer Knoten die Rechenzentren und Switches vernetzen.

Sie haben Einfluss auf Letztere?

So ist es, also auf den inneren Bereich der Vernetzung. Was mit den dort vorhandenen Leitungen passiert, wissen wir genau. Und klar ist auch: Eine einzige oder einige wenige Leitungen anzuzapfen bringt nichts.

Wie meinen Sie das?

Den kaum vorstellbaren, theoretischen Fall angenommen, dass in unserem Internetknoten Kriminelle oder ein Geheimdienst Daten abzweigen würden: Die Ausbeute wäre marginal! Denn wer nur eine Leitung anzapft, bekommt auch nur einen minimalen Ausschnitt der Kommunikation zwischen zwei Teilnehmern mit. Es ist nicht einmal sicher, ob auch nur eine einzige komplette Verbindung erfasst würde.

Wie viele Leitungen sind momentan im Frankfurter Knoten verschaltet?

Intern rund 1100. Und nach außen führen rund 2000. Über diese vielen Leitungen verteilt sich die Kommunikation. Das heißt, jemand müsste sehr viele Verbindungen anzapfen, um eine sinnvolle Datenmenge abzuzweigen.

Abzweigen, anzapfen, abhören – welche Methode käme sonst infrage?

Spionage ließe sich etwa an Glasfasermuffen praktizieren, die alle paar Kilometer in den Übertragungsstrecken existieren. Man brauchte geeignetes Werkzeug zum Öffnen der Muffe, Klamotten wie das Wartungspersonal, einen Biegekoppler, um Licht aus der Glasfaser umzuleiten – und schon kann es losgehen. Wenn Glasfasern leicht gebogen werden, tritt ein Teil des Lichts aus, das die Daten transportiert. Dieses kann dann zu einem Speichersystem weitergeleitet und später im stillen Kämmerlein analysiert werden.

Nachts Kabel zu verbuddeln brauchen Lauscher also nicht mehr?

Nein, das gibt’s bestenfalls noch in alten Agentenfilmen und wäre nicht sinnvoll. Denn Abhörinstrumente brauchen Platz. Und für jede Leitung, die Sie abhören wollen, müssen Sie auch eine „Abschöpfleitung“ haben, die die Daten weiterleitet. ▶▶

Datenschutz privat: „Verschlüsselungen einsetzen, unnötige Apps und Programme löschen, nicht jeden Trend mitmachen“

Das heißt, wer 1000 Leitungen anzapfen will, braucht …

… 1000 Leitungen, um die Daten zu entführen. Und es braucht Platz, um die Biegekoppler zu installieren. Dies unbeobachtet hinkriegen zu wollen ist heute Humbug. Und wenn in DE-CIX-Knotenpunkten jemand Licht abschöpfen wollte, würden wir es sofort merken, weil wir genau wissen, welche Lichtmengen in unsere Kabel reingehen – und folglich am Ende wieder rauskommen müssen.

Welche Methode eignet sich für Datendiebe und Geheimdienste besser?

In der Praxis infiziert man die Kommunikationsmittel des Spionageziels, zum Beispiel dessen Computer am Arbeitsplatz oder sein Smartphone, direkt mit sogenannter Spy-Software, .

Und wie gelangen die Daten von dort aus zum Spion?

Unauffällig über die Netzanbindung. Denn würde der Späher eine eigene Datenverbindung nach außen installieren, auf der quasi NSA oder CIA draufstünde, könnten selbst Laien dies über ihre Firewall bemerken.

Wie funktioniert die Netzanbindung?

Stellen wir uns einen Güterzug vor, der Daten in seinen Waggons geladen hat. Es sind aber selten alle Waggons voll. Also füllen Spione die „Waggons“ mit den Daten, die sie interessieren, auf. Oder sie hängen einen „Waggon“ dran, der den anderen ähnelt. Wer beobachtet schon, wie viele Daten er transferieren müsste, wenn er zum Beispiel einen Film streamt – und wie viele Daten es tatsächlich sind?

Aber die Daten des Spionageziels gehen doch erst mal zum Server des Zielunternehmens, im Fall eines Filmstreams beispielsweise YouTube, Netflix oder Amazon?

Richtig. Und jetzt wird es richtig spannend. Nun müssen die Spione nämlich nur noch gezielt die Leitungen der Empfängerunternehmen abhören, um an die Daten zu kommen – oder diese Daten auf dem Weg dorthin absaugen.

Und das ist Realität?

Das ist die Praxis. Nehmen wir mal das Karrierenetzwerk LinkedIn: Dieses wurde mal abgehört, obwohl die Datendiebe gar nicht an ihm interessiert waren, sondern an Daten eines anderen Unternehmens, das LinkedIn als Dienst verwendet hat. Beim IT-Konzern Cisco wurden auch schon Hintertüren der NSA gefunden, die Cisco – gesetzlich verordnet – bei seinen Switches einbauen musste. Und die hat der Geheimdienst dann ausgenutzt.

DE-CIX hat im September 2016 beim Bundesverwaltungsgericht Leipzig gegen die Bundesrepublik Deutschland Klage eingereicht, um die Rechtslage bezüglich der Befugnisse des BND prüfen zu lassen. Sind Sie inzwischen schlauer als vor einem Dreivierteljahr?

Die Bundesregierung hat sich mit ihrer Reaktion sehr lang Zeit gelassen. Inzwischen hat sie der Klage widersprochen. Dagegen müssen nun wieder wir vorgehen. Allzu schnell sollen wir offenbar nicht schlauer werden.

Welche Spähbefugnisse hat der BND in Ihren Internetknoten?

Es gibt gesetzlich gedeckte Anordnungen, die Telekommunikationsunternehmen wie DE-CIX zwingen, zu kooperieren, wenn der BND Internet- oder Telefonleitungen ausspioniert. Wir klagen dagegen, weil wir die BND-Befugnisse als zu weitreichend ansehen.

Vor einigen Wochen gingen Wikileaks-News durch die Medien, wonach aus US-Konsulaten wie in Frankfurt Datenspionage betrieben würde. Rechtliche Konsequenzen sind nicht bekannt.

Hierzu fehlt mir Tatsachenkenntnis, sodass ich mich dazu nicht äußern kann. Die Rechtslage in Deutschland ist jedenfalls eindeutig. Allerdings haben die meisten Botschafts- und Konsulatsmitarbeiter anderer Länder Diplomatenstatus. Und Diplomaten werden nach Straftaten normalerweise bestenfalls des Landes verwiesen.

Wie sehen Sie das seit Januar 2017 gültige neue BND-Gesetz?

Wir sehen das neue BND-Gesetz kritisch und bezweifeln, dass es verfassungskonform ist. Es ist aber nicht Bestandteil unserer Klage gegen die Bundesregierung, weil es ja erst seit diesem Jahr gilt und die Anordnungen von einem Gremium gemacht werden, das sich gerade erst konstituiert.

Wer sitzt in diesem Gremium?

FOTO: PEOPLEIMAGES/ISTOCKPHOTO

Zwei Richter des Bundesgerichtshofs und ein Vertreter der Generalbundesanwaltschaft.

Gut so?

Nein, das ist eher seltsam.

Warum?

Man muss sich nur vorstellen, dass neben den beiden bisher zuständigen Gremien – dem parlamentarischen Kontrollgremium und der G10-Kommission – jetzt noch eine weitere Kommission für die Überwachung der BND-Anordnungen zuständig wird, die eine neue Form der Überwachung genehmigen soll. Diese neue Form stellt alles bisher Dagewesene in den Schatten und hebelt alle anderen Formen der Genehmigungen aus. Entgegen der G10-Kommission und dem Kontrollgremium, welche vom Parlament eingesetzt werden und demokratisch legitimiert sind, wird dieses Gremium aber allein von der Regierung bestellt. Die Richter des BGH hatten bisher mit derartigen Genehmigungen nichts zu tun, durch den Vertreter der Generalbundesanwaltschaft wird zudem die Gewaltenteilung verwischt.

Wer überwacht die Überwachung?

Mit dem neuen Gesetz ist die Anordnungsbefugnis vom Innenministerium auf das Kanzleramt übergegangen.

Da wandert also die nächste Kompetenz von de Maizière zu Altmaier …

Personalien möchte ich nicht bewerten.

Dann noch einmal zum neuen BND-Gesetz. Wie bewerten Sie dieses?

Kritisch. Nur zwei Gründe dafür: Damit der BND Ausländer besser überwachen kann, darf er jetzt unter anderem auf inländische Leitungswege zugreifen und diese analysieren. Zwar ist es ihm untersagt, inländische Daten auszuspähen, es ist aber nicht nachprüfbar, ob der BND diese Daten tatsächlich herausfiltert und wegwirft – denn diese Filterung unterliegt keiner Kontrolle irgendeiner Stelle. Nach Meinung vieler Experten ist die Grundrechtsverletzung zudem bereits eingetreten, wenn der BND diese Daten bekommt. Und: Der BND darf im Ausland keine Europäer ausspionieren. Diese Verbote zu umgehen ist aus unserer Sicht durch mangelhafte Geheimdienstkontrollvorgaben leichter geworden.

Sie haben 35 Jahre Datenschutzerfahrung. Trauen Sie dem Internet noch – zumal Sie ein Spähziel sein könnten?

Ich gehe davon aus, ein Überwachungsziel zu sein, und bin diese Unsicherheit gewohnt. Ein kleiner Vorteil gegenüber vielen anderen Menschen ist, dass ich mich etwas besser vor Überwachung schützen kann.

Nutzen Sie ein Smartphone?

Selbstverständlich. Ich lebe ja auf dieser Welt.

Welche Marke?

Apple.

Ist Apple sicherer als andere?

Es ist völlig egal, welche Marke oder welches Betriebssystem wir nutzen. Alle herkömmlichen Smartphones sind ausspähbar. Leute wie ich analysieren allerdings mit sportlichem Ehrgeiz ihren Datenverkehr. Wir wissen aber auch: Wer beispielsweise ein Überwachungsziel der NSA ist, hat kaum Chancen, dies mitzubekommen.

„Es ist schlimm, dass nicht mal die Schulen geeignete Konzepte haben, um Medien- und Kommunikationskompetenz zu vermitteln."

Vor wem schützen Sie sich dann?

Vor Cyberkriminellen zum Beispiel, die von unbedarften Internetnutzern Daten und Geld ergaunern wollen. Bei mir können die mit ihren Phishing-Attacken nicht landen.

Was raten Sie Otto Normalverbraucher, damit er seine Daten besser schützen kann?

Verschlüsselungen einsetzen, möglichst wenige private Daten im Internet preisgeben, unnötige Apps und Programme konsequent löschen und nicht jeden Trend mitmachen.

An welche Trends denken Sie?

Wir beliefern die Anbieter von zum Beispiel Smart-Home-Anwendungen mit unendlich vielen Daten. Die verdienen damit Geld. Und wir müssen damit rechnen, dass unsere Daten auch zu unserem Nachteil verwendet werden.

Wir reden gern von Freiheit – und davon, wie das Internet diese befördert. Ist das wirklich so, wenn die Privatsphäre offenbar vor die Hunde geht?

Eigentlich könnten wir mit dem Internet unsere Freiheit erhöhen – wenn die Gesellschaft medienkompetent wäre.

Ist sie aber nicht?

Die meisten Menschen konsumieren moderne Kommunikationsmittel nur noch, ohne darüber nachzudenken, welche Folgen dies haben könnte. Wenn es so weitergeht, werden wir bald die negativen Seiten von mehr Konsum, mehr Beeinflussung und mehr Überwachung zu spüren bekommen. Das liefe dann eher auf Gefangenschaft als auf Freiheit hinaus. Es ist schlimm, dass nicht mal die Schulen geeignete Konzepte haben, um Medien- und Kommunikationskompetenz zu vermitteln.

Will der Staat überhaupt, dass wir kompetenter werden?

Den Staat gibt es nicht. Allein schon die verschiedenen Ministerien: Eines fördert die Datenverschlüsselung – und ein anderes versucht, Verschlüsselungen zu knacken. Das ist schizophren. Oder die Politik redet von mehr Datenschutz, wünscht aber auch mehr digitale Geschäftsmodelle, was wiederum nur mit weniger Schutz funktioniert.

Schließlich soll Deutschland auch irgendwann einmal ein Unternehmen wie Google oder Facebook gebären.

Mit Blick auf diese Unternehmen wird ja oft kolportiert, dass in Deutschland der Gründergeist zu schwach und die Bürokratie zu stark ausgeprägt seien. Ich halte diese Argumente für Quatsch. Die US-Internetkonzerne sind heute führend, weil es ihnen erlaubt war, Geschäftsmodelle auf Basis des hemmungslosen Sammelns und Auswertens von Daten umzusetzen, die hier und in den meisten anderen europäischen Ländern bislang unmöglich sind.

Bislang?

Ich fürchte, die Nutzer in Deutschland sind nicht kritisch genug, um die Datensammelwut zu verhindern. Ein winziger, gefühlter Nutzen, und zack – persönlichste Daten werden zur Nutzung freigegeben. Dazu kommt, dass wir uns in der EU arrangieren müssen. Das heißt, dass wir Ländern, die weit weniger Datenschutz praktizieren wollen als wir, nachgeben werden. Und wenn sich in ein paar Jahren die Digitalisierung in Form von Assistenzsystemen in Autos, Büros und Haushalten durchsetzt, lässt sich das Rad kaum noch zurückdrehen. ■