Sichere IT ist möglich

Es ist möglich, hochsichere österreichische und europäische IT-Systeme zu bauen, wenn man alle Teile des Systems selber plant, baut, programmiert und prüft.

Der „NSA-Skandal“, aufgedeckt durch den Geheimnisbruch von Edward Snowden, zwingt uns alle zum Umdenken. Doch wohin? Was ist technisch möglich? Müssen wir uns alles gefallen lassen? Sind wir nun auf ewig gläsern? Niemand hat sich vertieft mit der Frage befasst, wie Schlüsselinformationen aus Politik, Wirtschaft und Privatsphäre genutzt wurden. Wer sind die Verlierer und was ist der Preis dafür, dass Europa die Informationshoheit so leichtfertig aus der Hand gegeben hat? Das eigentlich kritische Thema ist Wirtschaftsspionage – schädlicher Know-how-Transfer im großen und im kleinen Stil, Diebstahl von Wertschöpfung, Exportgut und Zukunft.

Dem Top-Level der Techniker war die Möglichkeit des systematischen Informationsdiebstahls lange bekannt. Eine E-Mail ist wie eine Postkarte, die jeder gute Techniker mitlesen kann, wenn sie nicht verschlüsselt ist. Ein anderes Thema ist die Verfolgung unserer Interessen. *Google* speichert jede Suchabfrage. Derzeit sind das fünf Milliarden Abfragen täglich. Das ist so bequem, dass wir über Konsequenzen wenig nachdenken.

Die *NSA* ging und geht einen Schritt weiter: Sie hat sich Nachschlüssel zu den weit verbreiteten Verschlüsselungsverfahren organisiert und kann amerikanische Unternehmen über den „Patriot Act“ zur Herausgabe zwingen. Allein aufgrund der Gesetzeslage könnte man einem Hersteller von Datenbanken in den USA keine Daten mehr überlassen, die man unter eigener Kontrolle halten möchte.

Um eine sichere IT-Technik zu bauen, sollte man sie auf das Benötigte reduzieren und vereinfachen.

Das „E-Mail-ist-Postkarte“-Problem gilt für fast alle „sicheren Kommunikationsverfahren“. Es wird nur der technische Aufwand – und damit die Kosten – für die Ausspionierenden höher, wenn man elektronische Kommunikation „ein bisschen sicherer“ macht. Das Ausmaß und der unbedingte Wille, auch die kleinsten Informationsfetzchen von Teenager-Chats zu speichern, überraschte am Ende auch uns Spezialisten, aber nicht die Tatsache an sich.

Spezialisten schützen sich schon seit Jahren vor solchen Angriffen, weil sie damit gerechnet haben. Da wir heute wissen, dass „Nachschlüssel“ zu den am weit verbreitetsten Verschlüsselungsfirmen im Umlauf sind, müssten wir die Schlüsselfirma wechseln. Das ist in der Elektronik nicht anders als in der Physik.

Es überrascht, wie langsam Europa vorangeht. Wir haben nach wie vor Tausende Systeme am Laufen, wie *Oracle, IBM, Google, Facebook, HP,* für die einige wahrscheinlich Nachschlüssel haben. Das müsste nicht sein. Das heißt nicht, dass man sich prinzipiell davon verabschieden muss, integre, private, elektronische Kommunikation zu wollen und zu erwarten.

Es ist möglich, sichere Kommunikationssysteme zu bauen, wenn der Auftraggeber klar sagt, vom wem und vor welchen Angriffen diese Kommunikation geschützt werden sollen. Man kann E-Mails so verschlüsseln, dass die NSA nicht an sie heran kommt. Man kann Österreich nicht von heute auf morgen zur IT-Hochsicherheitszone erklären. Das ist praktisch und logistisch unrealistisch. So ein gesamter „Umbau“ dauert Jahre. In definierten Bereichen geht das aber und sehr schnell.

Die Lösung eines IT-Sicherheitsproblems liegt im notwendigen technischen Vermögen und dem wirtschaftlichen Willen sowie in einer angemessenen Form der Offenheit und Transparenz darüber, wogegen man am Ende abgesichert sein will. Es ist modern geworden, schlicht alles und jedes als unsicher zu bezeichnen. Das stimmt nicht.

Die meisten alten Systeme sind angreifbar und löchrig, weil sie in Zeiten entstanden sind, in denen Sicherheit und Privatheit der Informationen wenig Rolle spielten.

Mittlerweile sind wir aufgewacht. Informationstechnik kann mit angemessenem Aufwand sicher gemacht werden, sofern Sicherheitsbedarf, Angriffsaggressionen und Kostenaufwand in ein harmonisches Gleichgewicht gebracht werden. Wenn wir wollen, dass unser Auto der Zukunft nicht gehackt werden kann, dann werden wir das auch schaffen. Wenn wir wollen, dass ein elektronischer Liebesbrief unter vier Augen bleibt, dann wird das gelingen.

IT-Systeme macht man sicher, indem man alle Teile eines Systems selber baut, programmiert und prüft und den Betrieb der Systeme in der eigenen Hand hält. Niemand – auch die *NSA* nicht – kann eine ihr fremde Code-Zeile aus einem Programm herausreißen und sie so manipulieren und wiedereinsetzen, dass sie jedes Mal, wenn sie aktiv ist, unbemerkt Nachrichten ins Headquarter sendet.

Man kann diese Bedingung sogar abschwächen. Man muss nicht alles selbst gemacht haben, man sollte nur alles prüfen können und geprüft haben. Wer das selbst nicht prüfen kann, muss jemandem vertrauen – das heißt, genau aussuchen, wem man warum was anvertraut.

Foto: Kiekol/Fotolia

Sichere IT-Systeme sind möglich, indem man Software- und Hardwareteile selber plant, prüft und zusammenbaut.

Selbst vielen guten Technikern ist nicht bewusst, dass die eigene Software oft nur zu 20 Prozent aus eigener Herstellung und zu 80 Prozent aus Import von im Detail unbekannten Fremdsystemen entsteht. Um eine sichere Technik zu bauen, sollte man sie auf das Benötigte reduzieren und vereinfachen. Das heißt, alle Software- und Hardwareteile selber fertigen, oder genau kontrollieren und selbst zusammenbauen.

Sichere staatliche IT-Infrastruktur. Wer das Gesetz zum elektronischen Gesundheitsakt *ELGA* liest, stellt fest, dass Gesundheitsdaten in Österreich schwach geschützt werden. Bei der Vorratsdatenspeicherung ist es in Zusammenarbeit mit dem Bundesministerium für Inneres gelungen, ein sehr sicheres System für den Austausch der Daten zwischen Polizei und Providern zu installieren, und die Sicherheitsanforderung gesetzlich zu verankern. Man kann sichere staatliche IT-Infrastruktur bauen. Die Prinzipien dafür sind auf allen Ebenen zu etablieren: technisch, organisatorisch, institutionell und rechtlich. Technisch braucht es ein System auf Weltklasse-Niveau. Das können wir in Österreich. Dafür braucht es keinen Hersteller aus China, Indien oder den USA.

Organisatorisch ist die Sache schwieriger: Die Zuständigkeiten sind teils unklar. Ohne effektive Führung gibt es keine sicheren Systeme. Das Innenministerium wäre ein „natürlicher" Promotor der digitalen Sicherheit. Vor vier Jahren waren diese Themen Spezialisten-Themen für Eingeweihte. Inzwischen hat das Thema die Öffentlichkeit und die Politik erreicht. Heute interessiert sich die Tagespresse für das Thema Datensicherheit.

Man kann IT-Projekte – auch eine staatliche hochsichere Kommunikation in definierten Bereichen und für private Nutzung – zügiger bauen als oft üblich. Gesetze kann man aus dem Blickwinkel der technischen Möglichkeiten gezielt abstimmen, sodass Organisationen und Abläufe schrittweise angepasst werden können: Große Ziele und hohes Niveau, machbare und vernünftige Umsetzung.

Ministerien, Ämter, Polizei müssen ja zur Erfüllung ihrer Aufgaben entweder täglich improvisieren, am Rande der Legalität agieren oder sie geben auf und tun nichts. Das ist widersinnig. Die Verwaltung sollte in definiertem Rahmen ihren Job unter profunder Kontrolle machen können. Es gibt ein koordinatives Manko zwischen Technik, Legistik und Alltag der Exekutive. Technik kann man heute so bauen, dass sie zum Beispiel ein elektronisches Vieraugenprinzip realisiert. Die Sache ist einfach: der Gesetzgeber und die Regierung beschließen: Wir wollen ein Vieraugenprinzip und ein echtes Briefgeheimnis in bestimmten elektronischen Medien. Dann baut man es und stellt es zur Verfügung.

Thomas Grechenig

Univ.-Prof. DI Dr. Thomas Grechenig ist Professor für Softwaretechnik an der TU Wien. Er berät mehrere Regierungen in Fragen der IT-Strategie und hat staatliche IT-Infrastruktursysteme geplant und mitgebaut, wie die Bankomartkarte am Handy oder die Sicherheitsarchitektur der Deutschen Gesundheitstelematik. Als IT-Architekt für staatliche IT-Infrastruktursysteme ist er weltweit anerkannt.

FOTO: JIDOMATHAI/FOTOLIA