Mit DVD

iX KOMPAKT SECURITY

Ein Sonderheft des Magazins für professionelle Informationstechnik, www.ix.de 4/2014

Auf der Heft-DVD

Sponsored Software:
HOB MacGate – Remote-Desktop-Zugriff auf Mac-Computer

Live-Systeme:
Kali Linux, Tails, Grml

Tool-Framework:
Metasploit

Leseprobe:
Klaus Schmeh: Kryptografie; 5. Auflage

Sicher im Netz

IT-Gefährdungen:

Wie Wirtschaftsspionage funktioniert

Cybercrime – gezielter Angriff statt Massenattacke

Computerforensik:

Die Verschleierungstaktiken der Kriminellen

„Forensic Readiness“ im Unternehmen

Mobilgeräte:

Systematische Sicherheitstests für Apps

Sicher programmieren mit Apples Swift

Sicherheitsmanagement:

Grundschutz pragmatisch realisieren

Gretchenfrage: „Wie sicher sind wir?“

Cloud:

Unternehmensdaten sicher hosten

Erstes Audit für Cloud-Provider

Penetration Testing für Android, iOS und Windows Phone

Managed Hosting

zertifiziert nach ISO 27001 und ISO 9001

Sicherheit für Ihre Server und Daten am Standort Deutschland

Individuelles Hosting am Standort Frankfurt/Main mit persönlichem und kompetentem Support.

Professionelle Hostinglösungen vom Server bis zum Cluster-Cloudsystem mit Beratung, Planung und Service 24/7.

Wir bieten über 15 Jahre Erfahrung in Open Source, Systemadministration und Managed Hosting.
Für mehr Performance, Sicherheit und Verfügbarkeit.

hostserver.de/hosting

HOSTSERVER
Berlin ▪ Marburg ▪ Frankfurt am Main

Beratung unter:
0 30 / 47 37 55 50

Hosting made in Germany

Perfekte Welt?

In a perfect world, no one would be able to use anything“, sagt Mordac, der etwas sadistisch anmutende, für IT-Sicherheit zuständige Kollege Dilberts in einem der gleichnamigen Comic-Strips. Benutzbarkeit von Computern ist für ihn ein Fremdwort, alles ist dem hehren Ziel der Sicherheit untergeordnet. So weit wie Mordac muss man zwar nicht gleich gehen, Fakt ist aber, dass Bequemlichkeit und Sicherheit einander in der Regel ausschließen.

Ganz ähnlich sieht es mit der Freiheit aus. Im Zuge der Terrorbekämpfung haben Politik und Gesetzgeber in den letzten 13 Jahren Regulierungen eingeführt, die sukzessive die Überwachungsbefugnisse der Behörden und Strafverfolger ausbauten – und zwar immer weniger einzelfall- oder verdachtsbezogen, sondern anlasslos und massenhaft. Ob der Kontrollwahn und die drohende Totalüberwachung durch in- und ausländische Behörden „nur“ dem Vermeiden von Ereignissen wie Nine Eleven dient oder – wie Sascha Lobo es in einer lesenswerten Kolumne interpretiert – generell dem gewünschten Vorhersagen menschlicher Reaktionen und Handlungsweisen à la Minority Report, sei dahingestellt. Tatsache ist, dass das massive Erfassen und Sammeln von Daten jeder Art die Freiheit massiv bedroht.

Und noch ein Beispiel. Unter Sicherheitsberatern ist es ein alter Witz, dem Kunden „sicher“, „billig“ und „bequem“ auf ein Blatt Papier zu schreiben und zu sagen: „Wählen Sie zwei!“ Wie man es dreht und wendet, alle drei gleichzeitig geht nicht. Während die Redakteurin sich noch über den Stellenwert von IT-Sicherheit Gedanken macht, beschäftigt schon ein neuer Fall von Sicherheitsleck die Nachrichtenticker: So wurden der amerikanischen Baumarktkette Home Depot bei einem Hackerangriff Daten von 56 Millionen Kreditkarten entwendet. Wie es scheint, hat das Management jahrelang Warnhinweise der Mitarbeiter auf mangelnde Sicherheitsmaßnahmen und die Angreifbarkeit der Systeme ignoriert – es hat sich offenbar für „bequem“ und „billig“ entschieden.

Eines haben diese Beispiele alle gemein: Ein Übertreiben in die eine Richtung zieht immer einen gravierenden Verlust einer anderen Sache nach sich. Hüten wir uns also vor Extremen, die Wahrheit liegt häufig in der schon seit der Antike beschworenen „Aurea Mediocritas“, der goldenen Mitte. Auf IT-Sicherheit bezogen heißt das: Ein Zuwenig an Sicherheitsmaßnahmen hat genauso fatale Auswirkungen wie ein Zuviel. Unternehmen sollten keine Sicherheitsstrategien einführen, die die IT komplett unbenutzbar machen. Mitarbeiter könnten dann eine ungeahnte Kreativität zum Aushebeln der Strategien an den Tag legen. Ebenso wenig sollten sie vor den heutigen Bedrohungen resignieren oder diese gar ignorieren, aus falsch verstandener Sparsamkeit. Skandale kommen Unternehmen teuer zu stehen, und das nicht nur finanziell.

Bleibt der Mittelweg: die bestehenden Risiken auszuloten und mit Pragmatismus und Augenmaß ein Sicherheitsbewusstsein und entsprechende Sicherheitsmaßnahmen im Unternehmen zu etablieren. Hilfestellungen und Anregungen gibt es glücklicherweise zahlreiche – einige in diesem Heft.

UTE ROOS

Alle Links: www.ix.de/ix1417003

Sicherheit mit System und Überblick

Zahlreiche Grundlagenwerke erlauben die Erhöhung und Einschätzung des Sicherheitsniveaus der eigenen Firma. Doch ohne Hilfestellungen für die Praxis sind viele im Vorschriftendickicht und Maßnahmenwust verloren. Zahlreiche pragmatische und alltagstaugliche Hinweise finden sich

ab Seite 142

IT-Gefährdungen

Tools & Strategien

Kryptografie

IT-Forensik

Mobile Security

Allgegenwärtige und gefährliche Mobilgeräte

Die erste Welle mobiler Geräte, mit denen die Mitarbeiter aufs Firmennetz zugreifen wollten, haben die Mobile-Device-Management-Systeme weitgehend im Griff. Doch seit es für alles und jeden eine App gibt, gibt es auch eine neue Kategorie mobiler Gefährdungen. Was dagegen hilft,

ab Seite 104

Verschlüsselung und kein Ende

Die älteste aller Sicherheitsmaßnahmen, die schon Cäsar bei der Übermittlung seiner Kriegsstrategien einsetzte, ist die Kryptografie. Ohne sie ist keine sichere Kommunikation möglich. Trotz aller Zertifikats-GAUs und Implementierungs-Katastrophen bleibt festzustellen: Sie ist sicher – nur manchmal sperrig. Eine Bestandsaufnahme

ab Seite 72

Hinweis für Käufer der digitalen Ausgaben

- PDF- und iPad-Version: In der *iX*-App finden Sie einen Button zum Download des DVD-Images.
- PDF-E-Book: Folgen Sie im Browser der unter „Alle Links“ angegebenen URL zum DVD-Image.

Alle Links: www.ix.de/ix1417004

Alle Links: www.ix.de/ix1417SSS Artikel mit Verweisen ins Web enthalten am Ende einen Hinweis darauf, dass diese Webadressen auf dem Server der *iX* abrufbar sind. Dazu gibt man den *iX*-Link in der URL-Zeile des Browsers ein. Dann kann man auch die längsten Links bequem mit einem Klick ansteuern. Alternativ steht oben rechts auf der *iX*-Homepage ein Eingabefeld zur Verfügung.

Auf der Heft-DVD

Die dem Heft beigelegte DVD bietet eine Auswahl an bootfähigen Linux-Distributionen. Thematischer Schwerpunkt ist die Sicherheit von IT-Systemen, darüber hinaus findet sich dieses Mal auch ein Live-Betriebssystem darunter, das den Anwender vor der Neugierde Dritter schützen soll. Das auch „Snowden-DVD" genannte **Tails** [a] beinhaltet zahlreiche Tools, die dem Nutzer helfen, verschlüsselt und möglichst unerkannt zu kommunizieren. So kann er mit der DVD einen beliebigen PC mit Internetanschluss in einen etwas sichereren Arbeitsplatz verwandeln.

Des Weiteren befindet sich auf der DVD **Kali** [b], vormals Backtrack. Die Zusammenstellung ist speziell für die Untersuchung von IT-Systemen, Webanwendungen und Netzwerken auf Sicherheitsprobleme geeignet. Fast alle Open-Source-Tools, die man dafür benötigt, sind enthalten. Für das Retten eines Systems ist die auf der DVD enthaltene Distribution **Grml** [d] nützlich. Sie bringt Werkzeuge mit, die den Administrator beim Finden und Beheben von Fehlern auf Unix-Systemen unterstützen.

Auf der DVD befindet sich außerdem die für *iX*-Leser vorab verfügbare neue Version 1.5 des **HOB MacGate** (Sponsored Software). Die Software ermöglicht den Remote-Desktop-Zugriff auf Mac-Computer über ein Netzwerk – im LAN oder über das Internet. Dieser Zugriff ist von jeder beliebigen Client-Plattform möglich: Windows-PC, Linux-PC, Thin-Client oder von einem anderen Mac aus. In der beigefügten Datei findet sich ein bis zum 31.12.2014 gültiger Lizenzschlüssel nebst Kontakt zum Hersteller HOB, falls eine Verlängerung erwünscht ist.

Einblicke in die hohe Schule des Entwerfens von Krypto-Algorithmen gewährt Verschlüsselungsexperte Klaus Schmeh in der aktuellen Ausgabe seines Grundlagenwerkes „Kryptografie" (erschienen im dpunkt-Verlag, Heidelberg, 5. erweiterte Auflage, 2013). Eine **Leseprobe** aus dem Kapitel „Chriffren-Design" findet sich auf der DVD.

Tails

Die Privatsphäre der Bürger, aber auch der Regierungschefs, steht seit letztem Jahr verstärkt im Fokus der Berichterstattung. Die Veröffentlichungen von Edward Snowden haben gezeigt, dass Kommunikation sowohl im Internet als auch in privaten Netzen ohne Verschlüsselung nicht ausreichend geschützt ist und mehr Menschen mitlesen als nur die beabsichtigten Empfänger. Snowden nutzte für seine vertrauliche Kommunikation mit der Presse diese Distribution: Sie enthält alle Werkzeuge, die notwendig sind, Nutzerspuren maximal zu verwischen und die Inhalte der Kommunikation zu verschleiern.

Basis ist ein Debian-Linux, das von DVD oder USB auf einem beliebigen PC startet. Ohne Installation oder anderweitiges Verändern der Festplatte startet eine Arbeitsumgebung, die die Anonymisierungsfunktion des Tor-Projekts (The Onion Router) und die Verschlüsselung PGP (Pretty Good Privacy) bereitstellt. Theoretisch könnte man die Distribution auch für die tägliche Arbeit nutzen. Allerdings raten die selbst anonym agierenden Herausgeber davon ab, da jede Aktion das Risiko in sich trägt, zugeordnet zu werden, und daher die Nutzung von Tails ebenfalls „datensparsam", sprich selten, erfolgen sollte.

Beim Start wird ein Minimum an notwendigen Daten abgefragt. Ein typischer Desktop erwartet den Benutzer und Tor ist bereits gestartet. Wer möchte, kann alternativ I2P (Invisible Internet Project) verwenden, einen anderen Onion Router. Tools zum Bearbeiten von Daten und zum Verschlüsseln sind installiert. Wer möchte, kann – sofern er Tails von einem USB-Stick gestartet oder installiert hat – auch einen Speicherbereich einrichten, der über mehrere Sitzungen hinaus bestehen bleibt.

Kali

Die bekannteste Linux-Distribution für Sicherheitsforscher ist ohne Zweifel Kali. Sie ist der Nachfolger von Backtrack und verfolgt die gleichen Ziele, das Überprüfen des Sicherheitsstatus eines Systems durch Einbruchstests. Die Entwickler haben alle für die Untersuchung von IT-Systemen frei verfügbaren Werkzeuge auf einer DVD zusammengefasst. Die neueren Versionen ergänzt eine umfangreiche Sammlung von Forensik-Werkzeugen.

Kali lässt sich direkt von der DVD starten oder lokal auf der Festplatte installieren. Nach dem Installieren kann der Benutzer es mit *apt-get* auf den neuesten Stand bringen. Nach dem Bootvorgang stellt es einen Arbeitsplatz für Sicherheits- und Einbruchstests gegen Webserver, Netzwerkinfrastruktur, Betriebssysteme sowie sonstige Angriffsziele zur Verfügung. Vom ersten Erforschen eines Netzwerks mit Portscannern wie *nmap* bis zum Ausführen von Exploits mit dem Angriffs-Framework Metasploit (zusätzlich separat auf der Heft-DVD) lassen sich alle Arbeitsschritte innerhalb der bereitgestellten Umgebung durchführen. Nur das Schreiben eines Berichts ist etwas eingeschränkt, da ein WYSIWYG-Editor fehlt. Im Lieferumfang ist nur Keep-Note und Vim enthalten, sogar Emacs fehlt.

Insgesamt ist Kali für Anfänger wie Profis eine gelungene Arbeitsplattform, die Sicherheitsberater auch gerne als Basis für ihr Audit-Notebook nutzen. *Christoph Puppe* (ur)

Onlinequellen

[a] „Snowden-DVD" Tails	https://tails.boum.org
[b] Einbruchstestwerkzeug Kali	www.kali.org
[c] Angriffs-Framework Metasploit	www.metasploit.com
[d] Systemwerkzeuge Grml	https://grml.org

IT-Gefährdungen: Über unseren Köpfen

Dass unser gesamtes Arbeitsleben und mehr von der IT abhängig ist und jede IT-Bedrohung auch die Wirtschaft und die Existenz aller gefährdet, ist wahrlich keine neue Erkenntnis. Neu ist allerdings dank Edward Snowden das Wissen, dass unsere Daten und Geheimnisse nicht nur von Feinden wie der russischen Internetmafia oder chinesischen Wirtschaftsspionen bedroht sind, sondern auch von befreundeten Mächten.

Datenschutz: Update dringend erforderlich!

Die lauernde Gefahr

Peter Schaar

Alles kontrollierende Geheimdienste, datensammelwütige Unternehmen, aber auch die soziale Vernetzung hat in den letzten Jahren dazu geführt, dass der einstmals so fortschrittliche deutsche Datenschutz nicht mehr ausreicht, die Datenhoheit des Einzelnen angemessen zu schützen. Eine Bestandsaufnahme.

Im Jahr 1973, wenige Jahre nach Inkrafttreten des hessischen Datenschutzgesetzes – des weltweit ersten überhaupt –, stellte einer der deutschen Datenschutzpioniere, der Kirchenrechtler und Informatiker Wilhelm Steinmüller fest: „Die Datenschutzproblematik kann heute, was ihre wissenschaftliche und praktische Konzeptbildung betrifft, prinzipiell als gelöst angesehen werden; sie ist zudem unter vertretbaren Kosten praktisch realisierbar“ [1].

Diese optimistische Aussage mag seinerzeit richtig gewesen sein und sie steht für die beachtliche Leistung und das Selbstbewusstsein der Datenschützer der ersten Stunde. Aus heutiger Sicht erscheint die Zukunft des Datenschutzes unsicherer denn je. Immerhin: Die vor mehr als vierzig Jahren entwickelten Konzepte prägen das derzeitige deutsche und europäische Datenschutzrecht immer noch, aber die Regeln erfüllen heute ihren Zweck nur noch unvollkommen. Dies verdeutlichen Vorfälle der letzten Jahre, von denen hier beispielhaft einige erwähnt werden sollen:

In verschiedenen deutschen Unternehmen wurden Beschäftigte einer Art „Rasterfahndung“ unterworfen, obwohl gegen sie keinerlei Verdacht eines Fehlverhaltens vorlag. Ihre Daten wurden mit unterschiedlichsten Dateien abgeglichen. Bei „Trefferfällen“ wurden die Betroffenen bis in ihr Privatleben hinein heimlich ausgeforscht. Zudem wurden – unzulässigerweise – heimlich Videokameras an Arbeitsplätzen installiert. Trotz der massenhaften Rasterung gelang in den wenigsten Fällen der Nachweis strafbaren oder anderweitig rechtswidrigen Handelns.

Bei der Datenerfassung für seinen Dienst „Street View“ hatte Google nicht nur Aufnahmen von Hausfassaden angefertigt, sondern auch heimlich und systematisch Daten aus privaten WLAN-Netzen erfasst. Dabei handelte es sich sowohl um Kenndaten der jeweiligen Geräte als auch um Inhalte. Datenschutzbehörden gelang der Nachweis, dass dabei auch Passwörter und Identifikationsdaten für Internetdienste durch Google erfasst wurden.

Facebook hat – im Rahmen einer durch das US-Verteidigungsministerium mitfinanzierten Studie – ein verdecktes Ex-

periment durchgeführt, um die Beeinflussbarkeit von Emotionen durch Social Media zu untersuchen. Dazu manipulierte das Unternehmen bei 700 000 Nutzern den Inhalt der Newsfeeds. Nur zufällig erfuhr die Öffentlichkeit davon.

Viele Smartphone-Apps sammeln neben den für die Erbringung des Dienstes jeweils erforderlichen Daten auch vielfältige sonstige Informationen über die Nutzer und die von ihnen verwendeten Geräte. Diese Daten werden gespeichert und zur Bildung von Nutzerprofilen verwendet.

Immer wieder erfährt die Öffentlichkeit von Fällen, in denen millionenfach Passwörter, Bank- und Kreditkartendaten und sonstige sensible Informationen ausgespäht und missbraucht werden. Dabei nutzen die Täter nicht nur technische Schwachstellen bei den Anbietern. Sie bedienen sich auch weltweiter „Botnets“, die aus manipulierten ferngesteuerten Rechnern bestehen. Vielfach gelingt es nicht, die Täter zur Verantwortung zu ziehen, weil sie aus Staaten und Regionen operieren, in denen sie vor Identifizierung und Strafverfolgung geschützt sind.

Durch Edward Snowden und andere Whistleblower hat die Weltöffentlichkeit einen Eindruck davon bekommen, dass auch Geheimdienste demokratischer Staaten, allen voran die amerikanische NSA und der britische Geheimdienst GCHQ, nach einer flächendeckenden Überwachung der elektronischen Kommunikation streben und dabei ziemlich erfolgreich sind (Abb. 1).

Und auch der deutsche Bundesnachrichtendienst (BND) ist bei der elektronischen Überwachung kein Waisenknabe. Die zur Sicherung der Vertraulichkeit verwendeten Verschlüsselungsmechanismen wurden gezielt geschwächt, unbekannte Sicherheitslücken ausgenutzt. Geschäftsmodelle von Internetunternehmen, bei denen massenhaft Nutzerdaten gesammelt und zu Profilen zusammengefasst werden, spielen den Geheimdiensten dabei in die Hände.

Diese Beispiele belegen, dass in der durch globale Kommunikation, Internet und Ubiquitous Computing geprägten Welt die Datenschutzregeln zunehmend ihre Schutzwirkung verlieren und dringend einer Modernisierung bedürfen.

Der in den Gesetzen gewählte Begriff „Datenschutz“ führt in die Irre. Das Wort legt nahe, das Schutzobjekt seien die Daten, nicht aber die Gewährleistung von Persönlichkeitsrechten. Immer wieder wieder kommt es deshalb zu Missverständnissen: Datenschutz wird mit Datensicherheit verwechselt. Aber nicht alle Daten sind Gegenstand des Datenschutzrechts, sondern nur diejenigen, die einen Personenbezug aufweisen.

Um was es eigentlich geht

Andererseits streiten verschiedene Interessengruppierungen und Experten darüber, inwieweit auch technische Daten, die im Umfeld elektronischer Dienste anfallen, sogenannte Metadaten, schutzwürdig sind. Nicht erst seit den auf Snowden zurückgehenden Veröffentlichungen wissen wir aber, dass die Metadaten und nicht die Kommunikationsinhalte die eigentliche Goldader der nach Totalüberwachung strebenden Dienste bilden. Sie geben nicht nur Aufschluss darüber, wer wann mit wem kommuniziert hat, sondern auch über Aufenthaltsorte und weitere Parameter, die Rückschlüsse über die Nutzer, ihr Verhalten, ihre Interessen und Beziehungen ermöglichen, wenn sie zu Profilen zusammengefasst werden. Statt die Metadaten – wie nach US-Rechtsverständnis – schutzlos zu stellen, sind diese Angaben wegen ihrer großen Aussagekraft schutzwürdig. Sie dürfen auch nicht ohne jeden Anlass auf Vorrat gespeichert werden, wie der Europäische Gerichtshof kürzlich in seinem Urteil festgestellt hat, mit dem er die EU-Richtlinie zur Vorratsdatenspeicherung

Quelle: NSA

Durch die Snowden-Enthüllungen hat die NSA zwar an Bekanntheit, aber nicht unbedingt an Popularität gewonnen (Abb. 1).

annulliert hat [2] (dieser und weitere Links sind zu finden über „Alle Links“ am Ende des Artikels).

Am besten beschreibt die vom Bundesverfassungsgericht bereits 1983 geprägte Formel vom „Grundrecht auf informationelle Selbstbestimmung“ [3], um was es tatsächlich geht: Um das Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen und nicht auf ein Objekt der Fremdbestimmung – jener, die über die Daten verfügen – reduziert zu werden. Dieses Recht wurde nach einem Urteil des Verfassungsgerichts von 2008 [4] ergänzt um ein Grundrecht zur „Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme“, das sogenannte „Computergrundrecht“. Danach ist es staatlichen Stellen versagt, im Rahmen ihrer regulären Aufgabenwahrnehmung IT-Systeme mittels Trojaner zu infiltrieren und zu überwachen. Derartige Maßnahmen sind nur in absoluten Ausnahmen auf Basis eines Gesetzes erlaubt, soweit im Einzelfall überragend wichtige Rechtsgüter wie die Existenz eines Menschen oder des Staats gefährdet sind.

Überwachung – unser Schicksal?

Je tiefer IT in unseren Alltag eindringt, desto größer wird ihr Überwachungspotenzial. Die Segnungen der Informationstechnik bezahlen wir – so die inzwischen kaum noch hinterfragte Botschaft – mit dem Verlust von Privatsphäre und Datensouveränität. Andererseits kann es sich heute kein Unternehmen, keine staatliche Stelle leisten, die Digitalisierung zu ignorieren. Dennoch sollte man mit der Beschwörung eines unausweichlichen Schicksals vorsichtig sein. So ist auch die zunehmende Registrierung und Überwachung kein Naturgesetz. Wie viele andere technische Entwicklungen – Buchdruck, Dampfmaschine, Auto, Flugzeug, Atomkraft, Gentechnik – hat die Digitalisierung Licht- und Schattenseiten. Stets sind es Menschen und ihre Organisationen (Staaten, Unternehmen, Universitäten), die über ihre Weiterentwicklung und ihren Einsatz entscheiden und die mit ihren Konsequenzen umgehen müssen.

Dies war den „Vätern“ des Datenschutzes (Mütter gab es leider kaum) durchaus schon bewusst. Gerade weil sie frühzeitig erkannt haben, dass die zunehmende Erfassung und Verwendung von Daten erhebliche Folgen für die Gesellschaft und auch den Einzelnen haben würde, wendeten sie sich gegen ein ungeregeltes „Laissez-faire“ in der Informationstechnik und setzten sich zumindest in Europa recht erfolgreich für rechtliche Dämme gegen die Datenflut ein. In den USA fehlt dagegen bis heute ein umfassender rechtlicher Rahmen für den Umgang mit persönlichen Informationen.

Die in den letzten Jahrzehnten des 20. Jahrhunderts errichteten Dämme sind inzwischen brüchig geworden und halten den

seit der Jahrtausendwende immer höher auflaufenden Datenfluten kaum noch stand. Viele Dienste im Internet sind vordergründig kostenlos. Tatsächlich werden sie aber über personalisierte Werbebotschaften finanziert, die durch die Auswertung möglichst vieler individueller Informationen möglich werden. Daten über persönliche Interessen, Lebensumstände und Gewohnheiten werden auf diese Weise zum entscheidenden Wettbewerbsfaktor. Diejenigen Unternehmen sind im Vorteil, die über möglichst viele personenbezogene Daten verfügen und diese mit immer effektiveren IT-Instrumenten auswerten können. Die datenschutzrechtlichen Grundsätze der Begrenzung der Datenverarbeitung auf das erforderliche Maß und der Zweckbindung sind damit kaum vereinbar.

Immer mehr Daten in immer weniger Händen

Zwischen der Digitalisierung des Alltags, der engmaschigen Vernetzung unterschiedlichster Systeme und datenbasierten Geschäftsmodellen einerseits und zunehmender Registrierung, Profilbildung und Überwachung andererseits besteht ein unübersehbarer Zusammenhang. Die Gefahren für das informationelle Selbstbestimmungsrecht werden durch die Konzentration und Monopolbildung im IT-Bereich verschärft, denn immer weniger „Big Player" beherrschen die Szene und sie verfügen über eine Datenmacht, die geschichtlich ohne Beispiel ist.

Verschärfend wirkt sich dabei aus, dass die Rechtsordnungen ganz überwiegend national ausgerichtet sind, während die Datenverarbeitung sich immer weiter globalisiert. Gesetze entfalten ihre Schutzwirkung grundsätzlich im jeweiligen territorialen Geltungsbereich. Das Internet ist dagegen so konstruiert, dass Landes- oder auch Kontinentalgrenzen technisch keine Rolle spielen. Wenn etwa ein deutscher Internetnutzer die Webseite eines deutschen Anbieters abruft, können die übertragenen Daten durchaus über amerikanische Netzknoten geleitet (geroutet) werden. Global agierende Internetunternehmen speichern Daten auf Servern, die auf verschiedenen Kontinenten verteilt sind.

Insbesondere nach den terroristischen Anschlägen von 2001 wurden die Grenzen der Datenerfassung und -verarbeitung durch die Sicherheitsbehörden verschoben und zum Teil völlig aufgehoben. Resultate waren die überbordende Überwachung elektronischer Aktivitäten, neue Datenbanken, in denen nicht nur Terrorverdächtige sondern auch massenhaft andere „auffällige" Personen gespeichert werden, und ein weitgehend ungehinderter Datenaustausch von Behörden mit völlig unterschiedlichen Aufgaben und Befugnissen.

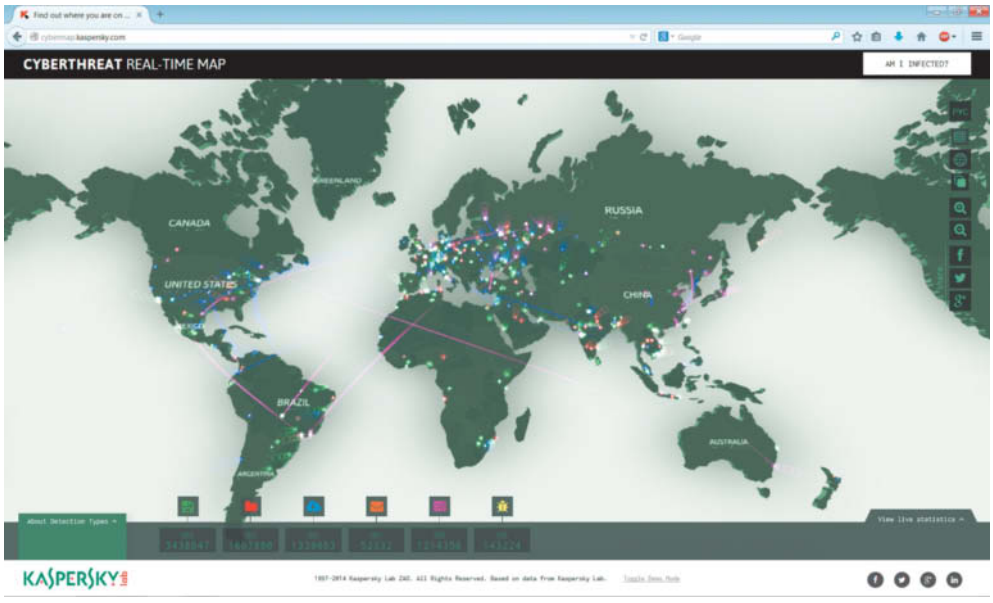
Welches sind nun die Stellschrauben, mit denen sich der Datenschutz im 21. Jahrhundert gewährleisten lässt?

Millionen- oder milliardenfacher Daten„diebstahl", Computerspionage und -sabotage machen immer wieder deutlich, dass vertrauliche Informationen unbeschadet gesetzlicher Regelungen zur Datensicherheit vielfach unzureichend geschützt werden. Das Bundesdatenschutzgesetz (BDSG) von 1977 enthielt Vorgaben zur Datensicherheit, die nahezu unverändert heute noch gültig sind. § 9 des aktuellen BDSG gibt vor: „Öffentliche und nichtöffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes (…) zu gewährleisten".

Diese Anforderungen konkretisiert die Anlage zum Bundesdatenschutzgesetz. Nach diesen etwas scherzhaft als „zehn Gebote" bezeichneten Vorgaben müssen Unternehmen und Behörden etwa Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren (Zutrittskontrolle) und verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle). Sie haben zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle) und so weiter.

Systeme sind nicht mehr isoliert

Das Gesetz stellt dabei weitgehend auf eine Datenverarbeitungslandschaft ab, die längst der Vergangenheit angehört. Anders als in den 1970er- und 1980er-Jahren werden Daten heute nicht mehr ausschließlich in großen, abgeschotteten Rechenzentren verarbeitet, sondern auch dezentral oder in Client-Server-Strukturen. Vernetzte Computer stehen heute an jedem Arbeitsplatz,



Quelle: cybermap.kaspersky.com

Eine der größten Bedrohungen für den Datenschutz ist die Auswertung riesiger Datenmengen. Es existieren jedoch auch sinnvolle Big-Data-Anwendungen, etwa die Analyse von Sicherheitsdaten zum Erkennen von Cyberbedrohungen (Abb. 2).

Your knowledge.
Your people.
Your future.

HOB
Secure Business Connectivity

Security Powered by HOB

Uncle Sam Wants YOUR Data!

Umfassende Remote-Access Lösungen für alle Einsatzzwecke, alle Betriebssysteme, alle Geräte, auch Mobile Devices

- Kostenersparnis durch clientless; keine Installation am Client
- Absolut sicher, nachgewiesen durch Zertifizierung durch das BSI nach **Common Criteria EAL 4+**

HOB RD VPN
Die umfassende SSL VPN Komplettlösung

HOBLink VPN
Modulare IPsec Connectivity

Vereinbaren Sie ein unverbindliches Beratungsgespräch!
Tel.: 09103-715-3715 E-Mail: marketing@hob.de

www.hob.de

sie befinden sich selbst in der Hosen- oder Jackentasche, und sie sind zunehmend in Fahrzeuge und Gebrauchsgegenstände eingebaut. In Teilbereichen der Medizin kontrollieren und steuern Chips schon heute menschliche Vitalfunktionen. Konzepte, die auf einer physikalischen Abschottung der Informationsverarbeitung basieren („Zutrittskontrolle“) tragen dieser Situation nicht mehr angemessen Rechnung.

Sicherlich: Das Datenschutzrecht ist nicht auf die Verwendung einer bestimmten Technik fixiert. Auch die allgemeinen Anforderungen des Datenschutzrechts zur Gewährleistung der Datensicherheit lassen sich mit etwas gutem Willen auf die moderne IT-Landschaft übertragen. So ist es grundsätzlich möglich, Geschäftsprozesse auch im Internet sicher abzuwickeln. Und mobile Hard- und Software können gegen externe Angreifer durchaus geschützt werden.

Nicht ohne Verschlüsselung – gute Verschlüsselung

Von zentraler Bedeutung sind dabei heute kryptografische Verfahren. Nur mit ihnen lassen sich die Vertraulichkeit und Integrität der Daten gewährleisten. Unternehmen und öffentliche Stellen, die elektronische Geschäftsprozesse anbieten, haben hier eine Bringschuld. Sie müssen dafür sorgen, dass die von den Nutzerinnen und Nutzern stammenden Daten durchgängig, also bei der Erhebung, Speicherung und späteren Verwendung, geschützt sind. Webformulare und andere Kommunikationsschnittstellen über das Internet müssen durchgängig verschlüsselt werden, und zwar nicht irgendwie, sondern in sicheren Verfahren, die dem Stand der Technik entsprechen. Welche Gefahren hier lauern, haben die Berichte über „Heartbleed“ verdeutlicht, eine Sicherheitslücke in der verschlüsselten Webkommunikation.

Unternehmen, die E-Mail- und sonstige Telekommunikationsdienste anbieten, müssen den aktuellen und absehbaren Gefahren für die Vertraulichkeit und Integrität der Informationen Rechnung tragen. Eine reine Verschlüsselung auf der Datenleitung (Verbindungsverschlüsselung) reicht nicht aus. Denn dabei speichert der Anbieter im Regelfall die Daten unverschlüsselt auf seinen Servern, wo sie prinzipiell ausgelesen oder manipuliert werden können.

Umso wichtiger ist eine Ende-zu-Ende-Verschlüsselung, bei denen die Daten zwischen den jeweiligen Beteiligten durchgängig verschlüsselt werden. Allerdings schützt diese im Regelfall nicht die Metadaten, die für die Zustellung der Datenpakete erforderlich sind. Eine sichere Verbindungsverschlüsselung kann das Auslesen der Metadaten (insbesondere wer mit wem kommuniziert) durch Dritte verhindern. Nur wenn sowohl Inhalte als auch Metadaten geschützt werden, kann man von einem zeitgemäßen Schutz der elektronischen Kommunikation reden. Die Ende-zu-Ende-Verschlüsselung muss also mit einer Verbindungsverschlüsselung kombiniert werden.

Zwischenergebnis: Ohne IT-Sicherheit lässt sich der Datenschutz nicht gewährleisten. Die entsprechenden technischen Mittel sind durchaus vorhanden, werden aber nur unzureichend eingesetzt. Die Verantwortlichen in Politik, Behörden und Unternehmen müssen das Thema ernster nehmen. Wichtig sind auch klare rechtliche Vorgaben.

Privacy by Design und by Default

Auch über die IT-Sicherheit hinaus stellt sich die grundlegende Frage nach der Integration des Datenschutzes in die Technik. Das Grundrecht auf informationelle Selbstbestimmung kann nicht allein durch rechtliche Regelungen garantiert werden. In weitaus stärkerem Maße als bisher bedarf es technischer Gestaltungsanforderungen und verfahrensmäßiger Sicherungen. Im Mittelpunkt steht dabei, die technischen Systeme datenschutzfreundlich zu gestalten („Privacy by Design“).

Dies bedeutet einerseits, dass Hersteller solcher Systeme datenschutzrechtliche Anforderungen bereits in einer frühen Phase des Entwicklungsprozesses berücksichtigen. Nachträglich „aufgepfropfter“ Datenschutz ist vielfach wesentlich weniger effektiv und zudem teurer als Lösungen, bei denen er bereits im Systemdesign verankert wird. Zudem müssen die Mechanismen der Datenerhebung und -Verarbeitung transparent sein. Der Nutzer oder Betroffene muss mit einfachen Mitteln und ohne großen Aufwand erkennen können, welche Daten von wem für welchen Zweck erhoben werden.

Inhaltlich geht es darum, IT-Systeme so zu gestalten, dass sie mit möglichst wenigen personenbezogenen Daten auskommen („Datensparsamkeit“). Zudem müssen elektronische Dienste grundsätzlich so angeboten werden, dass sie keine persönliche Identifizierung verlangen (anonyme und pseudonyme Nutzungsmöglichkeiten). Entsprechende Anforderungen enthält das deutsche Datenschutzrecht schon seit Jahren. Immerhin enthält das derzeit in Brüssel diskutierte Datenschutz-Reformpaket vergleichbare Anforderungen.

Wichtig ist ist auch „Privacy by Default“, also die Gewährleistung datenschutzfreundlicher Grundeinstellungen von Systemen und Diensten. Es reicht eben nicht aus, dem Nutzer etwa eines sozialen Netzwerks im Internet alle möglichen Einstelloptionen in „Privatsphäreneinstellungen“ zu geben. Mindestens genauso wichtig ist es, die Voreinstellungen datenschutzgerecht zu setzen, denn viele Nutzer können bei komplexen Diensten und Systemen gar nicht einschätzen, welche Konsequenzen Änderungen der Einstellungen haben. Deshalb belassen sie es in den allermeisten Fällen bei dem, was der Anbieter voreingestellt hat.

Die systematische Abschätzung der entsprechenden Risiken (Privacy Impact Assessment) kann dazu beitragen, mit bestimmten Systemen oder Verfahren verbundene Gefahren für den Datenschutz frühzeitig zu erkennen und technologische Vorkehrungen zu treffen, die diesen entgegenwirken.

Zwischenergebnis: Die Techniknutzer müssen alle notwendigen Informationen, Optionen und Kontrollmöglichkeiten erhalten, um ihre Privatsphäre zu schützen. Rechtlich verbindliche Vorgaben für die Konzeption der Geräte, Verfahren und Infrastrukturen sowie für deren Einsatz müssen geschaffen und durchgesetzt werden.

Datenschutzrechtliches Rollenmodell

Von besonderer Bedeutung ist die Verteilung der Verantwortung in arbeitsteiligen Prozessen, an denen vielfältige Akteure, Software- und Hardware-Entwickler, Systemintegratoren und Informationsvermittler beteiligt sind. Das deutsche und europäische Datenschutzrecht kennt prinzipiell nur drei Rollen: Den Betroffenen, die verantwortliche Stelle und den Auftragnehmer.

Im Mittelpunkt der datenschutzrechtlichen Überlegungen steht der Betroffene, den es zu schützen gilt. Im Zuge interaktiver Anwendungen („Web 2.0“), vor allem bei den sozialen Netzwerken und Bewertungsplattformen, wird der Betroffene aber selbst zum Datenverarbeiter, etwa wenn er Informationen über Dritte ins Netz stellt. Er ist insofern zugleich Akteur und Objekt der Informationsverarbeitung. Der Autofahrer, der die mit der Dashcam aufgenommenen Fotos und Videos ins Netz stellt, ist für dieses Handeln datenschutz- und zivilrechtlich verantwortlich. Wer seine beim Baumarkt erworbene Drohne vor dem Schlafzimmerfenster seiner Nachbarn positioniert und in das Haus hinein fotografiert, macht sich eventuell sogar strafbar.

Mindestens genauso schwierig ist die Abgrenzung zwischen der Rolle der verantwortlichen Stelle („Controller“) von der Rolle des Auftragnehmers („Processor“) bei der Auftragsdatenverarbeitung. Bei ihr ist der technische Dienstleister an die Vorgaben der verantwortlichen Stelle gebunden, die den Auftrag erteilt. Die Verantwortung des Auftragnehmers beschränkt sich im Wesentlichen darauf, die Aufträge ordnungsgemäß abzuwickeln und dabei für angemessene technische Schutzmaßnahmen zu sorgen. Dagegen muss die verantwortliche Stelle letztlich den Kopf für den Gesamtprozess der Datenverarbeitung hinhalten. Sie muss dafür sorgen, dass die Anforderungen an die IT-Sicherheit genauso erfüllt werden wie die inhaltlichen Vorgaben des Datenschutzrechts. Sie ist Adressat der Rechte der Betroffenen, etwa auf Auskunft über die eigenen Daten.

In der interaktiven Welt der Informationsverarbeitung überlappen sich die verschiedenen Rollen zunehmend. So ist etwa der Betreiber einer Suchmaschine nicht bloß ein technischer Helfer, der das Auffinden von Informationen im Internet ermöglicht, sondern er gestaltet die Suchalgorithmen und entscheidet über die Darstellung der Treffer. Damit ist er nicht nur Auftragnehmer der Nutzer, sondern selbst verantwortliche Stelle, wie der europäische Gerichtshof kürzlich in seiner Entscheidung zu Google Spanien deutlich gemacht hat. Viele Dienste werden zudem von einer Vielzahl verantwortlicher Stellen erbracht, die jeweils personenbezogene Daten für eigene Zwecke erheben, speichern und auswerten.

Zwischenergebnis: Alle an arbeitsteiligen Prozessen Beteiligten müssen sich ihrer jeweiligen rechtlichen Rolle und den daraus resultierenden Pflichten bewusst sein. Ohne klare vertragliche Regelungen und Abgrenzungen bestehen für die Unternehmen und die Nutzer erhebliche rechtliche und materielle Risiken.

Weil aus technischen oder wirtschaftlichen Gründen immer mehr Daten erzeugt werden, wächst auch die Phantasie, was man mit ihnen anstellen kann – mit dramatischen Konsequenzen für den Einzelnen und für die Gesellschaft. Während bei der klassischen Datenverarbeitung früherer Zeiten schon wegen der knappen Speicher- und Verarbeitungskapazitäten stets danach gefragt wurde, welche Daten für die Erfüllung einer Aufgabe erforderlich sind, wird heute unter dem Stichwort „Big Data" umgekehrt argumentiert. Die Kernfrage derartiger Ansätze lautet: Welche Erkenntnisse lassen sich aus den riesigen Datenbeständen gewinnen? Wie lässt sich das Datenvolumen möglichst effektiv durchforsten? Ergeben sich aus statistischen Zusammenhängen Hinweise auf Wirkungszusammenhänge? Welche Prognosen lassen sich aus der massenhaften Erhebung und Speicherung von Daten über alltägliche Vorgänge ableiten? Ist es möglich, das Verhalten einzelner Menschen vorherzusagen?

Derartige Modelle funktionieren nur, wenn einerseits eine Vielzahl von Daten digital verfügbar ist und andererseits die technischen Möglichkeiten bereitstehen, sie auszuwerten (Abb. 2). Abnehmende Speicherkosten, steigende Prozessorleistung und neue Datenverarbeitungs- und Prognosemodelle sind der Schlüssel zur Bewältigung riesiger Datenberge. Viele Beispiele für die Möglichkeiten mittels Big Data individuelles Verhalten zu interpretieren und vorherzusagen, kommen aus der Geschäftswelt: Schon seit langem werden Big-Data-Methoden (auch wenn dieser Begriff seinerzeit nicht bekannt war) in der Kreditwirtschaft eingesetzt. Die weit verbreiteten Scoring-Verfahren führen dazu, dass bestimmte Kunden aufgrund rein statistischer Risiken für weniger kreditwürdig gehalten werden als andere. Sie müssen mehr Zinsen für ein Darlehen zahlen oder bekommen einen Kredit überhaupt nicht. Ähnliche Methoden halten in der Versicherungswirtschaft Einzug. Durch die Auswertung unterschiedlichster Quellen werden individualisierte „Risikoprofile" erzeugt und damit Leistungen und -tarife personalisierbar (etwa bei „pay as you drive"-Modellen in der Kfz-Versicherung). Auch im Handel werden die Warenströme und das Kundenverhalten immer umfassender verfolgt. Die Unternehmen ziehen daraus individualisierte Schlussfolgerungen, bis hin zu Schwangerschaften oder Gesundheitsproblemen.

Diskriminierung durch Big Data

Zunächst „harmlose" Informationen können so zur Quelle teilweise höchst sensibler Einschätzungen über persönliche Eigenschaften werden. Aus riesigen Datensammlungen werden Prognosen gewonnen, die wiederum in Entscheidungsprozesse einfließen, die für die Betroffenen existenzielle Bedeutung haben können. Im Ergebnis kann Big Data zur Diskriminierung führen, wenn der Einzelne nicht anhand seines tatsächlichen Handelns beurteilt wird, sondern lediglich auf Basis statischer Wahrscheinlichkeitswerte, denen er nicht entrinnen kann.

Es ist nicht verwunderlich, dass auch Sicherheitsbehörden vergleichbare Modelle anwenden. Ihnen geht es dabei um das möglichst frühe Erkennen auffälligen Verhaltens, um so potenzielle Terroristen oder Kriminelle zu erkennen. Das Stichwort heißt „Predictive Policing": Die Polizei soll nicht erst dann ausrücken, wenn eine Straftat passiert ist. Sie soll schon vor Ort sein, ehe sich etwas ereignet. Dies setzt allerdings eine umfassende Beobachtung und Registrierung des alltäglichen Verhaltens voraus. Die Datenmodelle funktionieren umso besser, so die Hoffnung, je umfassender der Alltag überwacht wird und umso umfangreicher die Datenmengen sind, die einbezogen werden können. Nicht mehr das verdächtige Verhalten steht dabei im Mittelpunkt, sondern die umfassende Beobachtung des Alltags. Nur so lassen sich Anomalien erkennen. Die Maxime „Im Zweifel für die Sicherheit" mündet auf diese Weise in einen Generalverdacht.

Zwischenergebnis: Das Datenschutzrecht ist auch gefragt, wenn die aus großen Datenmengen gewonnenen statistischen Werte zur Bewertung individuellen Verhaltens herangezogen werden. Wirksame Vorkehrungen zur Verhinderung einer „informationellen Diskriminierung" müssen rechtlich verankert werden. Eine umfassende staatliche Überwachung darf es genauso wenig geben wie den allein auf statistischen Auswertungen basierenden Generalverdacht.

Globalisierung – das größte Problem?

Die vielleicht größte Herausforderung für den Datenschutz ist die Globalisierung der Informationsverarbeitung. Praktisch alle gesetzlichen Regulierungsansätze beschränken sich bisher auf den nationalen oder, in der EU, auf einen regional abgegrenzten Bereich. Internationale Abkommen zum Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung sind rar.

Immerhin hat die 1995 verabschiedete europäische Datenschutzrichtlinie einiges bewirkt, etwa im Hinblick auf die Verankerung von Mindeststandards in den EU-Mitgliedstaaten. Inzwischen hat sich gezeigt, dass nach wie vor erhebliche Unterschiede beim Datenschutz in den verschiedenen Mitgliedstaaten bestehen. So flüchten sich manche international handelnde Unternehmen in solche EU-Staaten, in denen sie ein niedrigeres Datenschutzniveau oder eine weniger konsequente Datenschutzaufsicht erwarten.

Auch wirkt sich die Richtlinie auf den internationalen Datentransfer aus. Die Übermittlung personenbezogener Daten aus der EU in ein Drittland darf grundsätzlich nur erfolgen, wenn bei dem Empfänger ein „angemessenes Datenschutzniveau" garantiert ist. Die Europäische Kommission hat für einige Drittstaaten ein „angemessenes Datenschutzniveau" festgestellt. Die Anerkennung setzt voraus, dass die wesentlichen Prinzipien des europäischen Datenschutzrechts einschließlich einer unabhängigen Datenschutzaufsicht gewährleistet werden. Auch das im Jahr 2000 in Kraft getretene Safe-Harbor-Abkommen [5] mit den USA folgt diesem Ansatz. Heute ist klar: Die Wirksamkeit des Systems der „Angemessenheit" des Datenschutzniveaus beim Datenexport in Drittländer ist begrenzt. So bleiben die Safe Harbor-Prinzipien hinter den Anforderungen der EU-Datenschutzrichtlinie zurück. Zudem klammert es staatliche Zugriffe auf exportierte Datenbestände weitgehend aus. Welche Konsequenzen diese Schutzlücke hat, wurde spätestens durch die Snowden-Veröffentlichungen deutlich. Schließlich haben verschiedene Studien ergeben, dass etliche Unternehmen, die sich dem Safe Harbor-System angeschlossen haben, gegen dessen Vorgaben verstoßen.

Das von der Europäischen Kommission im Januar 2012 vorgelegte Reformpaket zum Datenschutz [6] bietet die Chance, die längst überfällige Modernisierung des Datenschutzrechts in Angriff zu nehmen und diese mit einer stärkeren europäischen Harmonisierung zu verbinden. Es ist zu hoffen, dass die Harmonisierung zu einem möglichst hohen Datenschutzstandard führt und nicht bloß einen kleinsten gemeinsamen Nenner definiert. Gemessen daran gibt es an vielen Stellen des Reformpakets manches zu verbessern, insbesondere hinsichtlich des technisch-organisatorischen Datenschutzes sowie der internen Datenschutzbeauftragten.

Letztlich lässt sich das datenschutzrechtliche Territorialdilemma nur dann überwinden, wenn endlich wirksame, durchsetzbare

Instrumente geschaffen werden, die die Menschenrechte, insbesondere das Menschenrecht auf Gewährleistung der Privatsphäre, mit Leben füllen. Die Alternative wäre eine territoriale Aufteilung des Internets entsprechend nationaler oder regionaler Rechtsordnungen. Eine solche Aufteilung des Internets anhand nationaler Grenzen („Deutschlandnetz“) oder regionaler Zuordnungen („Schengen-Routing“) mag die eine oder andere Überwachungsmaßnahme erschweren. Allerdings überwiegen auf längere Sicht doch die Nachteile. Der Preis der Abschottung bestünde in verstärkten Einwirkungsmöglichkeit der nationalen Autoritäten – bis hin zur politischen Zensur. Die europäische Politik sollte sich deshalb sehr gründlich überlegen, ob sie diesen Kurs einschlägt.

Zwischenergebnis: Die einzige realistische und vertretbare Perspektive zur Durchsetzung des informationellen Selbstbestimmungsrechts in Zeiten der Globalisierung besteht in der Entwicklung internationaler Mindestanforderungen und Standards. Die EU-Datenschutzreform kann dazu ein wichtiger Zwischenschritt sein.

Fazit

Wir brauchen einen erweiterten Blick auf den Datenschutz. Das Problem fängt nicht erst mit der Erhebung und Speicherung personenbezogener Daten an. Und es hört auch nicht auf, wenn bei einem Verfahren, einem Geschäftsmodell, einer Anwendung „alles läuft“. Datenschutz ist vielmehr eine Management-Aufgabe, die bei der Konzeption einer Anwendung beginnt und im täglichen operativen Handeln fortlaufend erfüllt werden muss. Die dafür erforderlichen rechtlichen, technischen und kulturellen Voraussetzungen müssen stärker in den Mittelpunkt der Debatte rücken. Dazu muss der rechtliche Rahmen für die Informationsverarbeitung modernisiert und und im Sinne der Gewährleistung von Bürger- und Menschenrechten weiterentwickelt werden. Nur dann hat das informationelle Selbstbestimmungsrecht auch in der Informationsgesellschaft des 21. Jahrhunderts eine Chance. (ur)

Peter Schaar
ist Vorsitzender der Europäischen Akademie für Informationsfreiheit und Datenschutz, Berlin, und Bundesbeauftragter für den Datenschutz und die Informationsfreiheit a.D.

Literatur

[1] Wilhelm Steinmüller; DuD 1973, S. 830
[2] EuGH beerdigt die Vorratsdatenspeicherung; www.heise.de/-2166159.html
[3] Bundesverfassungsgericht, sog. Volkszählungsurteil v. 19. Dezember 1983; https://dejure.org/dienste/vernetzung/rechtsprechung?Text=BVerfGE%2065,%201
[4] Bundesverfassungsgericht, Urteil zur Zulässigkeit der Online-Durchsuchung vom 27. Februar 2008; https://dejure.org/dienste/vernetzung/rechtsprechung?Text=1%20BvR%20370/07
[5] Entscheidung der Europäischen Kommission, des Europäischen Parlaments und des Rates über den „sicheren Hafen“ vom 26. Juli 2000; eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF
[6] Entwurf einer Datenschutz-Grundverordnung der Europäischen Kommission; ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_de.pdf

Alle Links: www.ix.de/ix1417008

Digitale Angriffe auf alles und jeden

Räuberische Absichten

Christoph Puppe

Die kriminelle Energie und Kreativität der Cyberverbrecher macht vor nichts und niemandem halt. Kleine Unternehmen und Privatpersonen sind ebenso bedroht wie Großkonzerne oder Behörden. Die globale Vernetzung und IT-Durchdringung aller Lebensbereiche leistet der Bedrohung noch Vorschub. Ob sich die Gefahr durch gesetzgeberische Vorhaben wie das geplante IT-Sicherheitsgesetz wesentlich reduzieren lässt, bleibt fraglich.

Beachtliche 88 722 Fälle von Computerkriminalität für 2013 verzeichnet die aktuelle „Polizeiliche Kriminalstatistik“ (PKS; dieser und weitere Links sind zu finden über „Alle Links“ am Ende des Artikels), die Innenminister Thomas de Maizière Anfang Juni 2014 vorstellte. Dies ist insgesamt ein Zuwachs von 1 % und circa 1,5 % aller registrierten Straftaten. Die Aufklärungsquote sank um 1,2 % auf 25,3 %. Beachtenswert ist der Zuwachs von 14,5 % bei den Straftatbeständen Datenveränderung und Computersabotage bei gleichzeitiger Halbierung der Aufklärungsquote auf 9 %. Einen starken Anstieg verzeichnete das Bundeskriminalamt auch bei der digitalen Erpressung: Allein 2013 gab es 6745 Fälle, in denen Betroffenen sogenannte Ransomware untergeschoben wurde. Diese Schadprogramme verhindern den Zugang zum eigenen Rechner oder verschlüsseln gar die darauf gespeicherten Daten. Cybercrime ist von der Zahl der Fälle her unbedeutend, doch die Zahl der Betroffenen und die Höhe der Schäden sind teilweise so erheblich, dass diese Form der Kriminalität ein Wirtschaftsfaktor ist.

Aber was genau bedeutet „Cyber“ in „Cyberraum“ oder englisch „Cyberspace“? William Gibson hat den Begriff in seinem 1984 erschienenen Science-Fiction-Roman Neuromancer geprägt und dort findet sich auch die Definition: Alles, was einen Computer hat und vernetzt ist. Also könnte man denken, dass Cybersecurity sich nur um vernetzte IT-Systeme dreht. Das würde aber voraussetzen, dass es nichtvernetzte Computer gibt. Wir schreiben 2014 und es gibt praktisch keine IT-Systeme mehr ohne Netz. Vom PC des Internetnutzers über die Steuerung der Kraftwerke bis hin zu unseren Autos, alles ist vernetzt. Teilweise in abgeteilten Netzen, die keine Verbindung zum Internet haben, aber auch hier gibt es einen Trend zur Anbindung.

Wer von Cyberspace redet, hat verstanden, dass es nicht mehr um „wirkliches Leben versus Internet“ geht. Cyberspace ist wie eine Dimension in der Physik. Sie ist überall und durchwebt die gesamte Realität. Was man heute als Ubiquitious Computing oder Internet der Dinge bezeichnet, ist nur der Anfang. Vom Herzschrittmacher bis zum Großrechner: Internet ist überall. Man geht nicht mehr ins Internet, man ist schon da. Von Google Maps bis zum Fahrkartenautomaten, wo man ist, ist Internet, und wo man hingeht auch. Wenn der Cyberspace überall ist, trifft das auch auf „Cybercrime“ zu, und damit ist „Cybersecu-

rity“ überall notwendig. Vom Cockpit bis zur Armbanduhr. Cybersecurity ist damit mehr als IT-Sicherheit, weil der reine IT-Betrieb Vergangenheit ist. IT steht für Computer, die man als Computer erkennt und behandelt. Doch Cyberspace ist mehr, es ist Teil des Alltags. Somit bedroht Cybercrime mehr als Bankkonten, es bedroht jeden Aspekt des Lebens und der Gesellschaft. Cybercrime ist auch das Auslöschen einer Person durch Veränderung der Daten in den Unterlagen eines Krankenhauses oder wenn ein selbstfahrendes Auto absichtlich in eine Menschenmenge gesteuert wird. Oder, nicht ganz so gravierend, der Einbruch in die Wohnung, nachdem der Dieb durch Auswertung der Tweets einer Person deren Abwesenheit ausnutzte.

Wer eine Perspektive der möglichen Entwicklungen sucht, wird in „Rainbows End“ fündig. Das Buch ist von einem Autor, der drei Jahre vor Gibson in der Kurzgeschichte „True Names“ vernetzte Computer, Angriffe auf sie, Cyberwar et cetera vorhergesagt hat: Vernor Vinge. Wohl zusammen mit den Werken von Daniel Suarez das wichtigste Buch für jeden, der eine Vorstellung davon bekommen will, wie in 10 bis 20 Jahren vernetzte, eingebettete Computer unser aller Leben bestimmen könnten. Das Buch ist von 2006 und bis jetzt trifft schon ein nicht unerheblicher Teil seiner Vorhersagen zu.

Vermögensschäden schwer zu beziffern

Zurück zu den aktuell greifbareren Dingen. Schätzungen zu den weltweit oder auch nur in Deutschland durch Cybercrime bewegten Summen gehen weit auseinander. Verlässliche Zahlen sind kaum zu erhalten. Die Sicherheitsunternehmen Verizon, RSA und andere nennen alleine für Phishing Zahlen von 5,9 Milliarden US-$. Eine Untersuchung aus Brandenburg vergleicht die Studien von Verizon und RSA miteinander und wie erwartet sind die Unterschiede so erheblich, dass diese Zahlen kaum mehr sein können als Schätzungen.

Die einzig verlässlichen Zahlen sind die der statistischen Ämter des Bundes und der Länder. Wobei diese leider nicht die Schadenshöhe, sondern nur die Anzahl der Vorfälle angeben. Zumindest sind Einzelfälle bekannt, die einen Einblick in die von Cyberkriminellen bewegten immensen Summen geben können. So konnte Brian Krebs in einem Webforum Hinweise auf illegale Gewinne der Betreiber eines Botnetzes von rund einer viertel Million US-$ durch 384 Transaktionen mit brasilianischen Boletos nachweisen. Boletos sind Schecks, die zum Bezahlen von Rechnungen und allerlei Transaktionen in Brasilien sehr populär sind. RSA fand im gleichen Zeitraum eine Malware, die wohl knapp eine halbe Million illegale Transaktionen durchgeführt hat. Wenn bei diesen die durchschnittliche Transaktionshöhe auch 650 US-$ betrug, wären dies immerhin über 300 Millionen US-$ insgesamt. Da die Höhe einer Boleto-Transaktion begrenzt ist, konnten die Kriminellen maximal bis zu 3,75 Milliarden US-$ erbeuten. Wie viel Geld tatsächlich so den Besitzer gewechselt hat, wird wohl niemand je erfahren. Die Geschädigten waren in diesem Fall überwiegend nicht die großen Firmen, sondern Privatpersonen, kleine und mittlere Unternehmen (KMU) sowie Handwerksbetriebe.

Auch in Deutschland ist der Fokus der Cyberkriminalität beständig auf Privatpersonen und kleine Unternehmen gerichtet. Die Opfer können sich in der Regel weniger gut verteidigen als Unternehmen, in denen es eine IT-Abteilung oder sogar eigene Sicherheitsbeauftragte gibt, und die Wahrscheinlichkeit, dass ein Angriff gelingt, ist ungleich höher. Dass viele Anwender den Schutz der Rechner durch das Installieren von Updates vernachlässigen, hilft den Angreifern genauso wie der kontinuierliche Nachschub an neuen Schwachstellen.

Wo bei den KMU das direkte Abschöpfen von Geld im Vordergrund steht, sind es bei großen Firmen eher die Image- und Vertrauensschäden sowie Angriffe auf die Verfügbarkeit von Daten oder Diensten, die zu erheblichen Verlusten führen. Anders als noch vor einigen Jahren führen heutzutage Unternehmen deutlich mehr Erhebungen solchermaßen verursachter Schadenssummen durch. Der Bericht „e-Crime“ der KPMG („Alle Links“) gibt für 2013 an, dass immerhin 88 % der befragten Unternehmen die Schadenshöhen ermitteln. Es ist zumindest zu hoffen, dass dadurch die Schätzungen realistischer werden.

Die Meldepflicht soll kommen

Zu mehr und verlässlicheren Daten über Ausmaß und Folgeschäden von Cyber-Angriffen könnte eine Meldepflicht beitragen, wie sie die Bundesregierung für ihr im Entwurf vorliegendes IT-Sicherheitsgesetz plant. Nicht überraschend kritisiert die Industrie die Meldepflicht. Der Branchenverband BITKOM geht von 1,1 Milliarden Euro Kosten für die Wirtschaft aus, sollte der Bundestag den aktuellen Entwurf so beschließen. Eine sehr hohe Zahl, wenn man bedenkt, dass nur Betreiber kritischer Infrastrukturen und Telekommunikationsanbieter davon betroffen sind. Die Folgekosten einer Meldepflicht fallen sicherlich an, allerdings sind sie wohl kaum so hoch wie die Autoren im Auftrag der deutschen Wirtschaft schätzen. Auch muss man sie in Relation zu den volkswirtschaftlichen Folgen von Cybercrime