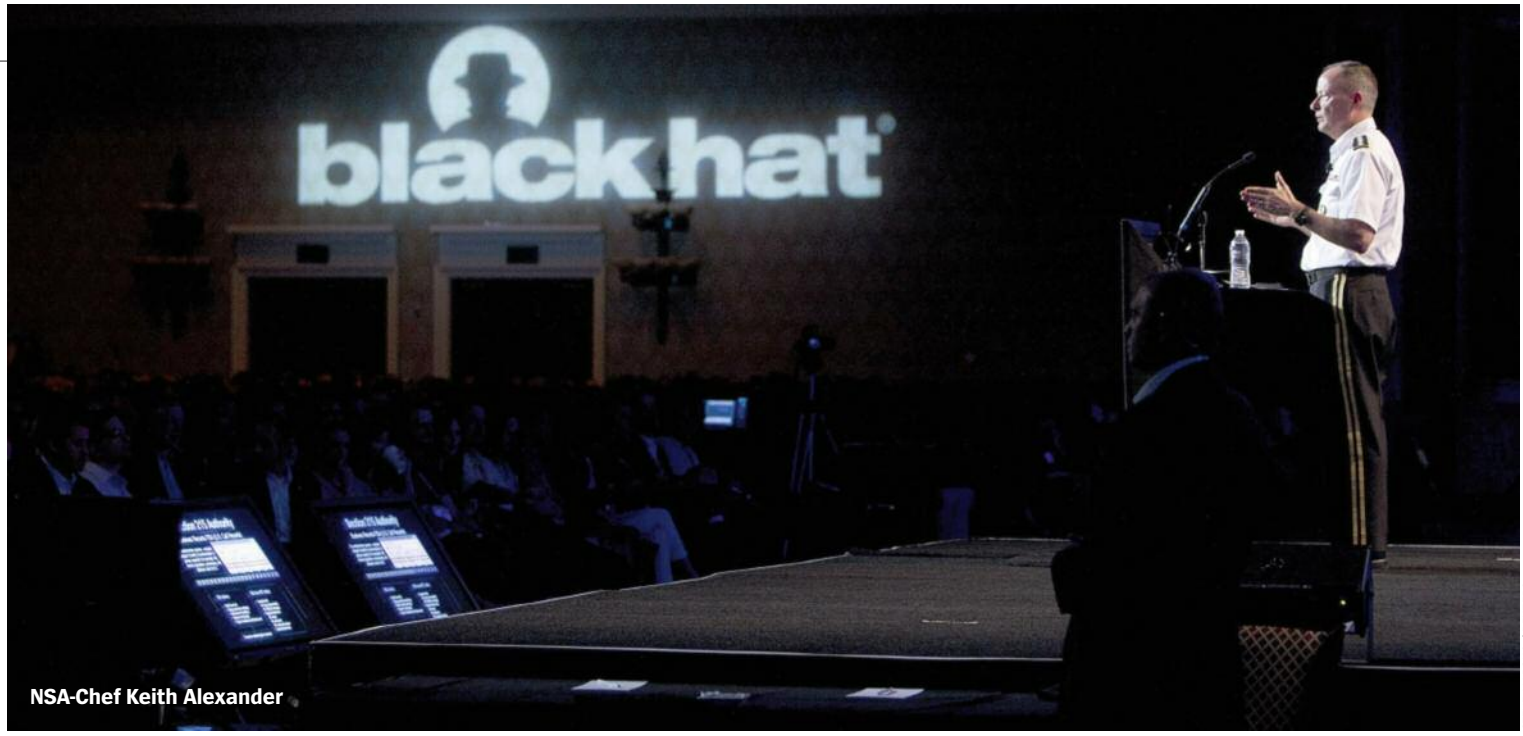


NSA-Chef Keith Alexander

STEVE MARCUS / REUTERS

WIRTSCHAFTSSPIONAGE

Der Feind in meinem Netz

Deutsche Unternehmen sind begehrte Ziele ausländischer Geheimdienste – nicht nur aus China oder Russland. Seit der NSA-Affäre wächst die Sorge vieler Manager, auch die USA könnten ihre Geschäftsgeheimnisse abgreifen.

Am Ende sind es nicht die Außenmauern aus meterdickem Stahlbeton, die das Haus Nummer 14 des Software-Konzerns SAP in Sankt Leon-Rot so gesichert erscheinen lassen wie Fort Knox. Auch nicht die Überwachungskameras. Oder das Hightech-Stahltor, das vor ein paar Wochen ohnehin nicht funktionierte, weshalb ein handgeschriebenes Zettelchen dran klebte: „Tor defekt, bitte mit der Hand öffnen“.

Es ist die Sache mit dem Finger: Wer in das Herz des Unternehmens eindringen möchte, in das Rechenzentrum mit all seinen Servern, auf denen nicht nur die Daten von SAP, sondern auch die Tausender Fremdfirmen gespeichert werden, geheimes Firmenwissen über halb Europa, muss an fünf Sicherheitsschranken mit fünf Fingerabdruckscannern vorbei.

Nur autorisierte Finger erhalten Einlass, und auch nur, wenn sie noch vital sind. Mit einem abgeschnittenen Finger kommt niemand rein.

Es ist also nicht so, dass Wirtschaftsgeheimnisse hierzulande schutzlos wären. Im Gegenteil. Die Vorsichtsmaßnahmen deutscher Unternehmen lesen sich teilweise wie ein Kapitel aus einem Grisham-Roman. Oder, wahlweise, aus einem medizinischen Lehrbuch über Paranoia.

Wenn BMW-Manager ins Ausland fliegen, bleiben die Dienst-Handys in München. Die Manager bekommen Einwegeräte, die nach der Reise entsorgt werden.

Beim Chemieriesen Evonik müssen die Manager ihre Mobiltelefone bei Besprechungen in Keksdosen stecken. Die Büchse als Faradayscher Käfig, so die Theorie, soll Mitlauschen verhindern.

VW-Aufsichtsratschef Ferdinand Piëch lässt nicht bloß Besprechungsräume regelmäßig nach Wanzen absuchen. Der Konzern verfügt zudem über eine eigene Fluglinie, Volkswagen Air Services. Die Flugzeuge sind auf den Cayman Islands zugelassen, nicht etwa, um Steuern zu sparen. Sie sollen nicht sofort als Volkswagen-Flieger erkennbar und die Passagierlisten nicht so leicht einsehbar sein.

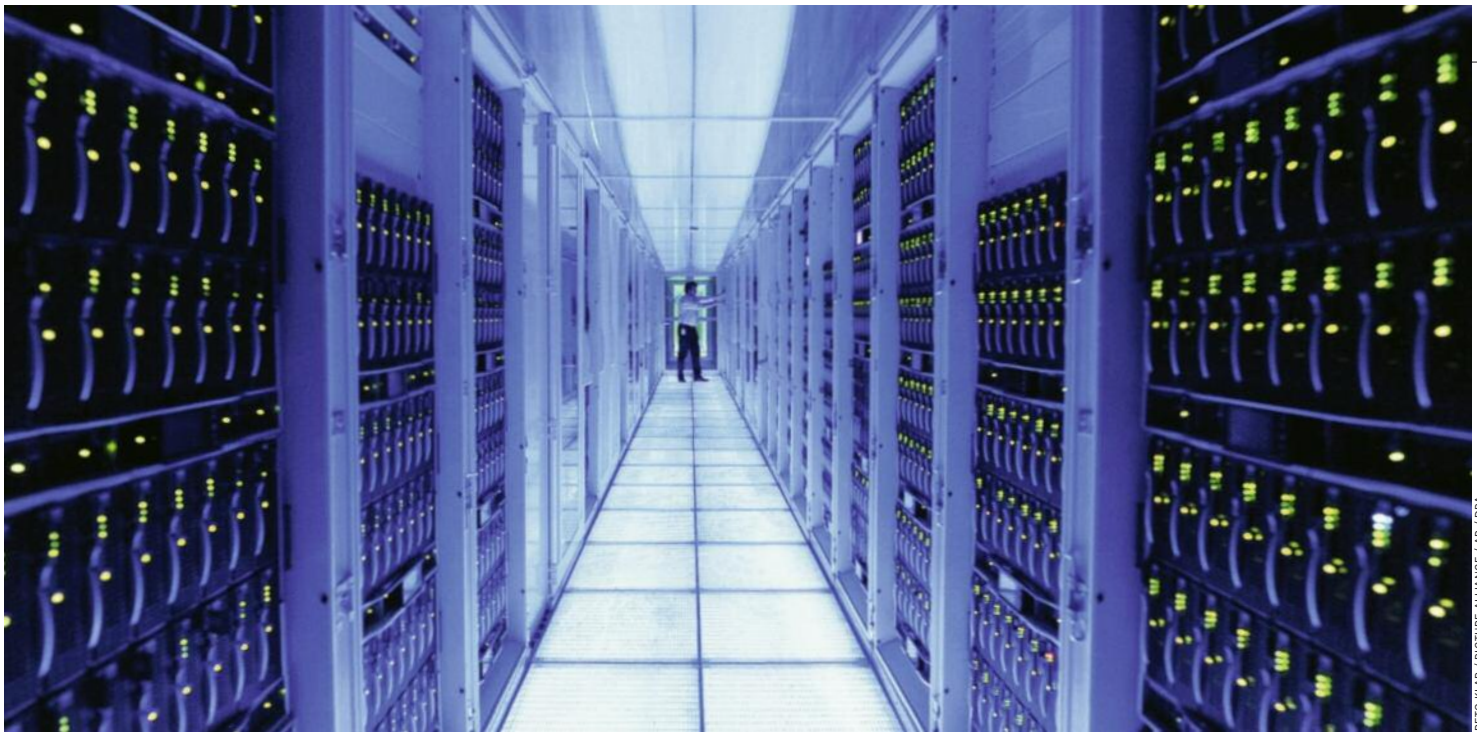

JULIAN STRATENSCHULTE / AP / DPA

Kanzlerin Merkel mit abhörsicherem Handy
Tummelplatz für Industriespione

Beim Luftfahrtkonzern EADS ist die dienstliche Nutzung von iPads und iPhones verboten. Nur BlackBerrys sind erlaubt. Angestellte in besonders sicherheitsempfindlichen Bereichen dürfen außerhalb ihrer abgeschotteten Büros keine E-Mails abrufen.

Nach den Enthüllungen um den massenhaften Datenabgriff aus den USA ist die Nervosität deutscher Manager sogar noch gewachsen. Die EADS-Spitze um Tom Enders hat ihre Abwehrmaßnahmen erneut verschärft. „Viele Dokumente, die früher noch per E-Mail verschickt wurden, reichen wir nun in noch größerer Zahl persönlich an den Empfänger weiter“, sagt ein EADS-Mann. Elektronisch werde nur noch das versendet, was man auch ohne Bedenken am Schwarzen Brett oder „an der Kirchentür“ aushängen könnte.

Enders und seine Leute sind da kein Einzelfall. Viele treibe gerade die Sorge um, was die NSA denn mit all den Daten



RETO KLAR / PICTURE ALLIANCE / AP / DPA

SAP-Serverraum in Walldorf: *„Die Amerikaner sind Profis, die hinterlassen keine Spuren – und wenn, dann falsche“*

anfange, die sie vermutlich auch über deutsche Unternehmen sammelt, sagt Ulrich Brehmer, Vorstandsmitglied der Arbeitsgemeinschaft für Sicherheit der Wirtschaft. Er will damit noch nicht einmal andeuten, dass US-Geheimdienste gezielt Industrie-Know-how aus Deutschland abgreifen und an ihre Heimatfirmen verteilen. Brehmer ist eher kein Verschwörungstheoretiker.

Ihm macht Sorge, dass die US-Geheimdienste mit privatwirtschaftlichen Beratern zusammenarbeiten. „Wer weiß denn, ob die nicht die eine oder andere Info an interessierte Seiten weiterverkaufen“, so Brehmer. Die Gefahr des Datenmissbrauchs sei „hoch“, sagt der Fachmann.

Auch SAP-Firmengründer Hasso Plattner sind die Spähaktionen der angelsächsischen Geheimdienste nicht ganz geheuer. „Es ist schon eigenartig, dass besonders viel im Süden Deutschlands ausgeschnüffelt wird“, sagt er, „genau dort, wo all die großen und kleinen Technikfirmen sitzen.“

Die Verunsicherung ist allgegenwärtig in Deutschland. „Wir registrieren, dass die Unternehmen in den letzten Wochen sensibel geworden sind. Sie hatten beim Thema Spionage fast nur den Osten im Blick und sind unsicher, ob sie nicht auch nach Westen schauen müssen“, sagt der Leiter des Cyber-Allianz-Zentrums beim Bayerischen Landesamt für Verfassungsschutz, Michael George.

Vor allem Mittelständler melden sich mit ganz simplen Fragen bei den Fachleuten vom Verfassungsschutz: Was ist eigentlich mit den Produkten von US-Software-Firmen wie Microsoft, die in deutschen Unternehmen Standard sind? Dürfen sich Manager weiter über Skype unterhalten? Muss jeder Mittelständler nicht mehr nur mit Hacker-Attacken aus China, sondern auch aus den USA rechnen?

Sicher ist bislang nur: Das Vertrauen gegenüber allem, was aus den USA kommt, hat arg gelitten in der deutschen Wirtschaft.

Zwar ist bisher kein Fall bekanntgeworden, in dem die US-Dienste versucht haben, Know-how zu stehlen. Aber vielleicht liegt das auch nur daran, dass man nicht richtig hingeschaut hat. Wer bei einer Hacker-Attacke am Ende an der Tastatur sitzt, bleibt meist ja ohnehin im Dunkeln, und vielleicht stellen sich die amerikanischen Geheimdienste ja bloß geschickter an beim Verwischen der Spuren?

Neugier der Konkurrenz muss sich jeder schützen, aber Gefahr von Staats wegen droht vor allem aus China und Russland, wo das Ausspähen fremder Volkswirtschaften durch eigene Geheimdienste Programm ist.

Deutschland, so viel war immer klar, ist ein Tummelplatz für Industriespione. Dutzende Fälle wurden da in den vergangenen Jahren publik. Unterschiedlich sind nur die Interessen der Späher. Die Iraner wollen wissen, wo sie sich Einzelteile für ihr Atomprogramm in Deutschland heimlich zusammenkaufen können. Die Russen sind auf alles begierig, was mit Militär zu tun hat. Und die Produktkopierer aus China lassen gar nichts aus. Von Militär-

Auch in Zeiten von Trojanern ist die empfindlichste Stelle – der Mensch.

technologie bis zum Highend-Plattenspieler haben sie alles im Visier.

Sie müssen nicht einmal direkt deutsche Unternehmen abgreifen. Es kommt vor, dass die US-Dienste bei ihrer umfangreichen Suche im Netz Datenpakete aus deutschen Firmen aufstöbern, „die da nicht hingehören“, sagt ein hoher Beamter vom Verfassungsschutz. Oft reichen sie diese Informationen über Datenlecks an deutsche Behörden weiter, die dann das betroffene Unternehmen informieren.

„Die Amerikaner sind Profis, die hinterlassen keine Spuren – und wenn, dann falsche“, sagt Christoph Fischer von der Beratungsfirma BFK in Karlsruhe. „Es ist immer einfach, so zu tun, als käme der Angriff aus China. Die machen zwar gerade auch ganz viel – aber den Chinesen wird momentan natürlich auch alles in die Schuhe geschoben.“

Bislang galt als Faustregel für den Umgang mit Wirtschaftsspionage: Vor der

Das Problem bei der Abwehr von Spionage ist: Man muss ziemlich viele Türen auf einmal bewachen. Etwa 3000 Angriffe muss allein SAP jeden Monat abwehren. Deutschlandweit geht die Zahl der Attacken angeblich in die Hunderttausende – pro Tag. „Für Angriffe auf Mittelständler muss man nicht einmal ein Top-Know-how haben“, sagt ein hoher Beamter beim Verfassungsschutz.

Und keiner weiß, woher sie genau kommen. Sind es Wirtschaftsspione? Geheimdienste? Oder einfach nur Hobby-Hacker? Sicher ist nur: Es sind komplette Söldnerheere im Netz unterwegs, die sich an den Meistbietenden verkaufen. Und sie sind gut. „Wir haben Fälle, da tummelten sich Angreifer mehr als hundert Tage in den Computern der Unterneh-

men, bevor sie entdeckt wurden. In dem Fall müssen Sie davon ausgehen, dass da nichts mehr geheim geblieben ist“, sagt BFK-Mann Fischer.

Eigentlich müsste Thorsten Schröder der Schrecken aller Unternehmen sein. Er bezeichnet sich selbst als „Hacker“ und trägt auch gern die Markenzeichen der Szene: T-Shirts von Hacker-Konferenzen, praktische Cargohosen, und am liebsten alles in Schwarz.

Erst neulich hat Schröder wieder ein Unternehmen der Medizinbranche angegriffen. In kurzer Zeit konnte er sich von seinem eigenen Rechner aus erfolgreich als Außendienstler des Unternehmens ausgeben, hatte damit alle Zugriffsrechte eines Mitarbeiters – und so die Firewall überwunden, die das Unternehmen vor Zugriffen von außen schützen soll.

„Ist man erst mal drinnen, ist es nur noch eine Frage der Zeit und des Aufwands, bis man an sensible Kundendaten oder die interne Finanzplanung kommt“, sagt Schröder. In diesem Fall kam es für das Unternehmen noch schlimmer. Er konnte sogar eigene Software auf deren Servern installieren und sich so zum Administrator und „Superuser“ machen – für einen Hacker von außen der größte Triumph, für das Unternehmen ein Alptraum.

Doch in diesem Fall bezahlte es Schröder sogar dafür, denn der Hacker hat, wie viele seiner Kollegen, sein Hobby zum Beruf gemacht. Der 36-Jährige ist selbst Unternehmer und berät mit seiner im schweizerischen Winterthur ansässigen Firma Modzero und vier festangestellten Kollegen Unternehmen in Sachen IT-Sicherheit und Abwehr von Cyberspionage.

Die Erfolgsquote bei diesen in der Regel fünf bis zehn Tage dauernden Operationen liege bei nahezu 100 Prozent, sagt Schröder: „Wir finden eigentlich immer etwas.“ Das gelte auch für größere Firmen mit eigenen Konzernsicherheitsabteilungen, die zuweilen selbst sogenannte Red Teams unterhalten, also Trupps, die regelmäßig die eigenen Systeme angreifen und testen. Häufig würden besonders die höheren Etagen der Hierarchie die größten Sicherheitsrisiken bergen. „Top-Manager sind oft lohnende Ziele, denn sie haben einen Sonderstatus und oft auch besonders viele Zugriffsrechte.“

Womit wieder das Grundproblem jeder Spionageabwehr auftaucht, das der vielen Türen, die es zu bewachen gilt. Auch wenn es gelänge, die Firmennetze sicher zu machen, käme der Feind eben über ganz andere Wege – zum Beispiel übers Bett, wie erst vor ein paar Wochen der Mitarbeiter einer deutschen Medizintechnikfirma zu spüren bekam.

Der konnte sein Glück zunächst kaum fassen, als er einen heftigen Flirt mit einer Chinesin begann. Sie war jung, sie war hübsch, und sie war offenbar interessiert. Erst als er mit kompromittierenden Fotos erpresst wurde, die ihn und die schöne Chinesin zeigten, wusste der Manager, was wirklich geschehen war. Er war in die Venusfalle getappt, ein Uralttrick der Geheimdienste. Das Opfer sollte Informationen liefern über ein Erfolgsprodukt seiner Firma.

In diesem Fall schlug die Attacke fehl. Der China-Reisende offenbarte sich seinem Chef – und seiner Ehefrau. Doch das Beispiel zeigt, dass auch in Zeiten von „Prism“ und Trojanern am Ende eine alte Schwachstelle immer noch die empfindlichste ist, wenn es darum geht, dem Opfer Geheimnisse zu entlocken – der Mensch. Oder, in diesem Fall genauer, der Mann.

Es sind simple, aber effektive Tricks, die von den Angreifern angewendet werden. Da kommt etwa ein Mann an den Messestand, gibt sich als Manager eines Konkurrenzunternehmens aus und lässt wie aus Versehen seinen Schlüsselbund liegen, an dem – verlockend – ein USB-Stick hängt.

Das Opfer wähnt sich im Vorteil, steckt den Stick in seinen Computer, um zu schauen, was die Konkurrenz so treibt – und lädt sich auf diese Weise ein Spähprogramm auf den eigenen Rechner.

Am liebsten kombinieren die Angreifer neue Technik und altbewährte Methoden. Um sich das Vertrauen einer Zielperson zu erschleichen, werden heute die sozialen Netzwerke auf Informationen durchsucht. In wenigen Tagen sind dort Daten zu beschaffen, für die früher wochenlange Operationen nötig waren.

Vorlieben, Kontakte, Freunde, ja sogar Hinweise auf mögliche Passwörter für Mail-Account oder Firmennetzwerk lassen sich oft aus den Profilen bei Facebook oder Xing ermitteln. Mit diesem Wissen kann dann weiteroperiert werden.

Social Engineering nennt sich dieses Ausspionieren über das persönliche Umfeld. Es ist neben dem Hacking eines der wichtigsten Werkzeuge für Geheimdienste. Doch nach einer Studie der Beratungsfirma Corporate Trust ist nur jeder vierte Mitarbeiter deutscher Unternehmen auf diese Gefahr vorbereitet.

Überhaupt scheint in vielen Firmen die Losung zu gelten, dass die IT-Abteilung das Sicherheitsproblem schon irgendwie allein lösen müsse. In den meisten Firmen gibt es nicht einmal Klarheit darüber, welche Daten denn besonders schützenswert sind. Die „Kronjuwelen“, wie sie im Jargon der Branche heißen. Nur jedes fünfte Unternehmen hat eine solche Analyse für sich erstellt.

Ein Problem der deutschen Verfassungsschützer ist, dass sie eigentlich nicht mal wissen, was vor sich geht. Die Unternehmen sind verschlossen und melden lediglich jeden fünften Fall von Spionage an die Geheimdienstler.

Verfassungsschutzmann George wirbt deshalb bei Mittelständlern unermüdlich um Vertrauen. „Das Fatale an der jetzigen Situation ist, dass jedes Unternehmen eine Insel ist und keiner weiß, was auf der Nachbarinsel geschieht.“ So können sich Angreifer mit ein und derselben Masche zu mehreren Unternehmen Zugang verschaffen – und es merkt nicht mal jemand, dass es eine Masche ist. Erst seit kurzem reicht etwa der bayerische Verfassungsschutz Erkenntnisse über Angriffe von einem Unternehmen an andere weiter, anonymisiert.

Zwischen Behörden und Firmen, zwischen Politik und Wirtschaft regierte in Sachen Spionage jahrelang Misstrauen. Die Wirtschaft fühlt sich von Innenministerium und Verfassungsschutz bei dem Thema alleingelassen. Die Sicherheitsbehörden kritisieren, die Industrie unterrichte sie zu wenig über Hacker-Angriffe oder Fälle möglicher Werksspionage. Ein Teufelskreis. Der FDP-Innenpolitiker Hartfrid Wolff sieht Deutschland im Bereich der Abwehr von Wirtschaftsspionage bisher schlecht aufgestellt. Gerade kleine und mittelständische Unternehmen seien überfordert. „Universitäten und wei-

STEFAN BONESS / IPON

BND-Zufahrt in Berlin: *Es geht darum, sich gegenseitig zu warnen*

tere Forschungseinrichtungen brauchen ebenfalls einen deutlich besseren Schutz."

Doch nun, im Zuge der NSA-Enthüllungen, scheinen sich die Fronten aufzuweichen. Ende August wollen Vertreter beider Seiten ein Papier zum Wirtschaftsschutz unterzeichnen. Geplant ist etwa eine Internetplattform, auf der sich Unternehmen und staatliche Behörden über mögliche Angriffe austauschen sollen. „Es geht darum, sich gegenseitig zu warnen und so Sicherheitslöcher zu stopfen", sagt der IT-Chef eines Dax-Konzerns.

Auf wenig Gegenliebe stößt dagegen das von Bundesinnenminister Hans-Peter Friedrich geplante IT-Meldegesetz. Unternehmen, die einen Angriff auf ihre Computersysteme feststellen, sollen das unverzüglich melden. Doch die Wirtschaft hält den bisherigen Gesetzentwurf für unausgereift. Was denn der Herr Minister mit all den tollen Daten anzufangen gedenke, fragt der Sicherheitschef eines Rüstungskonzerns. Den Vorstoß nennt er „eine Lachnummer", die zeige, wie hilflos die Politik in Wahrheit sei.

Politisch heikel ist auch das sogenannte Safe-Harbour-Abkommen, das die USA und die EU bereits im Jahr 2000 abschlossen und das den Datenschutz für US-Firmen regelt, die in Europa aktiv sind.

Danach können sich US-Firmen quasi freiwillig zur Einhaltung bestimmter Datenschutzbestimmungen verpflichten, wenn sie Daten europäischer Bürger speichern und verarbeiten wollen. Safe Harbour gilt dann quasi als Gütesiegel. Die Zertifizierung und Überwachung des Regelwerks sollte von US-Behörden übernommen werden.

Mehr als 3000 Unternehmen und Konzerne ließen sich in den USA bisher auf die Spielregeln ein. Darunter Giganten wie Google, Facebook oder Microsoft. Sie alle konnten fortan mit Billigung der EU Milliarden Datensätze von europäischen Bürgern speichern, verarbeiten und austauschen.

Im Jahr 2004 enthüllte eine von der EU-Kommission in Auftrag gegebene Studie aber die fehlende Überwachung der Datenschutzrichtlinien – besonders auf US-Seite. Damals gelobten die Amerikaner Besserung bei dem noch ungewohnten Regelwerk.

Nur vier Jahre später erschien eine zweite von der EU in Auftrag gegebene Studie. Angefertigt wurde sie von einer belgischen Universität in Zusammenarbeit mit norwegischen und amerikanischen Kollegen. Doch das 192 Seiten dicke Werk wurde – anders als die Studie des Jahres 2004 – nur einem kleinen Expertenkreis bekannt.

Das Werk, sagt die EU heute auf Nachfrage, sei in ihre Gesamtbewertung von Safe Harbour eingeflossen. Manager großer deutscher Konzerne vermuten andere Beweggründe für die Schweigsamkeit. Denn die Ergebnisse der Studie waren so verheerend, dass die Vereinbarung schon damals hätte aufgekündigt werden müssen.

So stellen die Wissenschaftler unumwunden fest, dass die Einhaltung der Datenschutzbestimmungen auf US-Seite im Jahr „2008 nicht besser" war „als im Jahr 2004, eher sogar schlechter". So werde, heißt es in dem Bericht, die Zertifizierung und Einhaltung der Datenschutzbestimmungen durch die zuständigen US-Behörden „völlig unzureichend" überprüft. Sanktionen der US-Behörden gab es in solchen Fällen kaum.

Nun scheint es aber auch der zuständigen EU-Kommissarin Viviane Reding zu reichen. Das Abkommen, sagt sie, sei offenbar eher ein „Schlupfloch als eine Absicherung für unsere Bürger". Sogar eine einseitige Kündigung der Vereinbarung schließt Reding nun nicht mehr aus.

Das amerikanische Anti-Terror-Gesetz „Patriot Act" erlaubt den US-Behörden in ihrem Heimatland immerhin, Zugang zu allen Daten zu erhalten, privat wie geschäftlich.

Mehr noch: Software-Entwickler können gezwungen werden, Hintertüren in die Programme einzubauen, durch die die Geheimdienste später spähen können. Erzählen dürfen sie das nicht einmal ihren Chefs, sie müssen eine Schweigeerklärung unterschreiben.

Angst, dass sich in der zugekauften US-Software Schnittstellen der US-Geheimdienste befinden könnten, hat der deutsche Software-Riese SAP dennoch nicht. Vor dem Kauf, wenn SAP noch nicht auf den Quellcode zugreifen darf, suchen externe Spezialfirmen solche „Loopholes". Danach kontrolliere eine vergangenes Jahr eingerichtete Abteilung bei SAP den Quellcode. „Man muss schon sehr gewieft sein, um solche Scans zu umgehen", sagt Sicherheitschef Gordon Mühl.

Gefährliche Lecks können jedoch an den Schnittstellen entstehen, sobald verschiedene Programme aufeinander abgestimmt werden müssen. Oder aber, wenn die Schutzsoftware nicht ständig aktualisiert wird. „Tausende SAP-Systeme mit Internetzugang sind nicht auf dem neuesten Stand", sagt Alexander Polyakov vom Sicherheitsspezialisten ERPScan. „Das sind Einfallstore für Datendiebe."

Aber es gibt auch Profiteure des neuen Sicherheitsbooms, etwa die Düsseldorfer Firma Secusmart, die sich auf abhörsichere Handys spezialisiert hat und zu ihren Kunden auch die deutsche Kanzlerin zählt.

Secusmart soll die Bundesregierung in einigen Wochen mit handelsüblichen BlackBerrys ausstatten, die mit einer speziellen Karte arbeiten, kaum größer als ein Fingernagel. Sobald der Anrufer ins Mikrofon des Handys spricht, werden die Wörter verschlüsselt. Gleichzeitig lässt sich das Gerät wie ein Smartphone nutzen.

Ein neues IT-Meldegesetz nennen Profis „eine Lachnummer".

Seit Bekanntwerden der Abhörmethoden der NSA registriert Secusmart ein gestiegenes Interesse von Unternehmen an abhörsicheren Handys. „Vorher haben uns die Firmen oft nicht geglaubt, dass es nicht nur sehr einfach ist, Telefonate abzufangen, sondern dass das auch geschieht", frohlockt Jörg Goronzy, Vertriebschef bei Secusmart. „Die Spionageaffäre hat vielen die Augen geöffnet."

Das Beste: Um sich effektiv zu schützen, müsse ein Konzern nicht nur Vorstände und Manager mit Krypto-Handys ausstatten – sondern auch deren Sekretärinnen und Referenten. Denn die Verschlüsselung funktioniert nur dann, wenn Anrufer und Empfänger ein abhörsicheres Gerät besitzen. Für ein Dax-Unternehmen sei es deshalb sinnvoll, für 500 bis 1000 Mitarbeiter solche Telefone anzuschaffen, behauptet Secusmart. Preis: 2500 Euro. Pro Stück.

Markus Brauck, Dinah Deckstein, Frank Dohmen, Ann-Kathrin Nezik, Marcel Rosenbach, Michaela Schiessl, Jörg Schmitt