Das Internet als Domäne von Militär und Geheimdiensten: die Snowden-Leaks erfordern Konsequenzen für die IT Sicherheitsstrategie von Unternehmen

Sylvia Johnigk, Kai Nothdurft

Die von Edward Snowden zugänglich gemachten Dokumente haben schlaglichtartig transparent gemacht, dass Militärs und Geheimdienste die Informations- und Kommunikationstechnik und insbesondere das Internet und Online Dienste zur massenhaften und flächendeckenden Ausforschung und Überwachung nutzen. Es bleibt aber nicht beim passiven Lauschen sondern es wird auch gezielte Desinformation betrieben. Verschlüsselungsstandards werden geschwächt. IT-Firmen und Internetdienstleister werden mit oder ohne deren Wissen benutzt, und es werden offensive Operationen zur Kompromittierung oder Sabotage von fremden IT-Systemen durchgeführt, die gemeinhin als kriminelle Form von Hacking eingestuft werden müssen.

Der Spähskandal hat Risiken und Bedrohungen offen gelegt, die zum Teil von Fachleuten bereits vorher postuliert wurden. Wurden diese bisher jedoch als paranoide Theorien ignoriert, so müssen sie spätestens jetzt strategisch berücksichtigt werden und rechtliche Konsequenzen nach sich ziehen. Doch viele IT-Sicherheitsverantwortliche, -Berater und -Firmen reagieren nur zögerlich oder gar resigniert auf die Veröffentlichungen oder schweigen betreten, weil ihre eigenen Unternehmen in den Verdacht der Kollaboration geraten sind.

Die Herausforderung ist für die Akteure in der Informationssicherheit gewaltig. Wir glauben, dass Verantwortliche handeln müssen und es durchaus Möglichkeiten gibt, etwas gegen diese Bedrohungen zu tun. Wir beschränken uns hier auf die Sicherheit von Unternehmen, wohl wissend, dass es insbesondere auch einer politischen Veränderung bedarf. Die Zivilgesellschaft muss Druck auf die Exekutive ausüben, aber auch jeder Einzelne ist bei Veränderung in seinem Umgang mit IT im Allgemeinen und mit dem Internet im Besonderen gefragt.

Wir gehen kurz auf die wichtigsten aufgedeckten Fakten ein, aus denen Bedrohungen für die Informationssicherheit von Unternehmen entstehen:

- Ausspähung und Überwachung durch die NSA und die mit ihr kooperierenden Geheimdienste,
- Kollaboration von Unternehmen und
- militärischen Nutzung des Internets.

Anschließend leiten wir den rechtlichen Handlungsbedarf ab, der sich aus diesen Bedrohungen ergibt, und schließlich nennen wir strategische Konsequenzen und schlagen konkrete Sicherheitsmaßnahmen vor. Dieser Artikel kann allerdings keine vollständige und für alle Firmen passende Strategie oder gar eine vollständige Liste aller erforderlichen Sicherheitsmaßnahmen liefern. Es handelt sich um erste Gedanken, welche Strategien und Maßnahmen kurz-, mittel und langfristig in Angriff genommen werden müssen.

Wir reißen einige Themen an, gehen bei anderen exemplarisch etwas tiefer ins Detail. Wir fokussieren uns auch fast ausschließlich auf die Bedrohungen, die aus den Snowden-Dokumenten abgeleitet werden können, und streifen allenfalls allgemeine Risiken von Geheimdienstangriffen. Wir verstehen dies als Denkanstoß und ermuntern zur Kritik, Diskussion und Ergänzung. Wir hoffen damit eine Debatte anzustoßen, an der sich möglichst viele beteiligen, und stellen diese Information unter Creative-Commons-Lizenz (Namensnennung unter gleichen Bedingungen) zur allgemeinen Verfügung.

1. Informationen aus den Snowden-Dokumenten

Massenüberwachung und Ausspähung

Das *PRISM-Programm* beinhaltet eine massenweise Online-Überwachung der digitalen Kommunikation von Personen. Anfang April 2013 standen durch dieses Programm weltweit 117.675 Menschen unter einer Echtzeit-Überwachung der NSA.[1] Dies geschah mit Beteiligung bzw. unter Anzapfung von IT-Firmen sowie Online- und Clouddienstleistern. Explizit wurden in den Snowden-Dokumenten Yahoo, Apple, Google,

[1] Holger Bleich: Globaler Abhörwahn. In: *c't*. Heise Online. 15. Juli 2013. Archiviert vom Original am 14. Juli 2013. Abgerufen am 24. März 2014., Seite 2 (Version vom 17. Juli 2013 im Internet Archive) im Archiv

Youtube, Microsoft, Skype, Facebook, AOL und Paltalk genannt. Unklar ist ob und ggf. in welchem Umfang die genannten Firmen dabei wissentlich mit der NSA kooperieren. Yahoo gab August 2013 zu, sich für die Datenbereitstellung die Kosten rückerstatten zu lassen.[2] Bei Google wurde angeblich ohne deren Wissen die Datenkommunikation zwischen Rechenzentren zur Replizierung und Datensicherung abgehört, die mindestens fahrlässigerweise unverschlüsselt war.

Das *Tempora-Projekt* ist eine Kooperation des britischen Geheimdiensts GCHQ mit der NSA (dort *Upstream* genannt). Dabei wird der gesamte Datenverkehr (*fulltake*) direkt an Hauptglasfaserleitungen eines Internet-Backbone für etwa 3 Tage aufgezeichnet, die darin enthaltenen Metadaten sogar für 30 Tage. Bereits 2012 konnten 46 Kabel mit einer Datentransferrate von je 10GBit/s aufgezeichnet werden.

Durch die Kooperation der so genannten Five-Eyes-Staaten (USA, Großbritannien, Australien, Kanada, und Neuseeland) findet das Belauschung des Internetverkehrs fast weltweit und umfassend statt – in China und Russland nur durch andere Geheimdienste. Die westlichen Geheimdienste kooperieren dabei nicht nur untereinander, sondern sie werden auch von Telekommunikationsdienstleitern aus dem Privatsektor unterstützt, die von vielen Firmen als Infrastrukturanbieter genutzt werden.

Selbst bei Telekommunikationsanbietern, die nicht kooperieren, werden Daten abgegriffen. Im Fall der BelgaCom, der belgischen Telefongesellschaft, fand keine Kooperation statt, sondern das Unternehmen wurde durch einen gezielten Angriff (*targeted attack*) der NSA auf deren Administratoren kompromittiert. Die BelgaCom wurde als Ziel ausgewählt, weil sie Knotenpunkte zu Auslandsleitungen mit Afrika und in dem Nahen Osten betreibt und Datenverkehr von EU-Institutionen abwickelt.

Das Programm *MYSTIC/RETRO* (*retrospective retrieval*) liefert einen Komplettmitschnitt der Telefonie eines gesamten Landes für ca. 30 Tage. Es wird bereits in mehreren Staaten, u.a. in Panama und im Irak, eingesetzt. Die Dishfire Datenbank erfasst massenweise SMS Nachrichten (194 Millionen Datensätze/Tag). Neben der Überwachung der Telefonie werden aus Smartphones zusätzliche Informationen gewonnen. Es werden Bewegungsprofile der Nutzer miteinander korreliert. Die *Fascia*-Datenbank erfasst 5 Milliarden Datensätze zur Geolocation in wenigen Tagen.[3]

---

[2] http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid

[3] Rosenbach, Stark: der NSA Komplex. S.187

Smartphones erfassen über Sensoren und Nutzungsverhalten weitere Daten, die ebenfalls ausgewertet werden. Ein Zugriff ist sowohl auf Android-Geräten als auch auf iPhones möglich.[4] Windows-basierte Smartphones waren zum Zeitpunkt, als Snowden die Informationen in seinen Besitz brachte, noch nicht sehr verbreitet.

Die NSA ist auch in der Lage, sich Zugriff auf den Datenverkehr von Blackberries mit Blackberry-Internet-Service (BIS) zu verschaffen. Mit gezielten Angriffen gelang der NSA auch der Zugriff auf die angeblich abhörsichere Datenkommunikation mit BES (*Blackberry-Enterprise-Server*, eine auf einer Private-Cloud Lösung basierende Unternehmenslösung). Auf Smartphones installierte Apps wie Angry Birds oder Google Maps aggregieren zum einen weitere Daten, und sie bilden gleichzeitig Einfallstore für die Kompromittierung der Geräte. Die Schadsoftware *Dropoutjeep* verwandelt das iPhone in eine audiovisuelle Wanze, die der Besitzer mit sich herumträgt.

Mit dem Programm *Tracfin* erfolgt eine Überwachung des Zahlungsverkehrs nach dem Prinzip "*follow the money*". Dabei werden alle Daten des elektronischen Zahlungsverkehrs von Kreditkarten (American Express, VISA, Mastercard) ausgewertet und höchstwahrscheinlich mit weiteren verfügbaren Quellen verknüpft, etwa den SWIFT Daten.

Bei XKeyScore handelt es sich um ein mächtiges Werkzeug zur Datenanalyse. Damit ist es möglich, innerhalb kürzester Zeit die riesigen mit Tempora gesammelten Datenberge nach einer bestimmten Zielperson oder anderen Suchkriterien etwa Kommunikation in einer bestimmten Region oder Sprache zu durchforsten, zu filtern und zielgerichtet auszuwerten. Auch der BND nutzt XKeyScore produktiv, der Verfassungsschutz angeblich nur im Testbetrieb.

Firmen als Mitwisser und Beteiligte, Kompromittierung von IT Produkten

Aufgrund der weltweiten verteilten Produktion und Erbringung von Dienstleistungen sind zahlreiche Unternehmen als Mitwisser, Beteiligte oder Betroffene in den Spähskandal verwickelt. Telekommunikationsdienstleister kooperieren direkt mit Geheimdiensten. Explizit genannt

[4] http://www.spiegel.de/spiegel/vorab/nsa-telefon-daten-von-iphone-blackberry-und-android-lesbar-a-920983.html

wurden AT&T, Verizon, Level3, Interroute, Vodafone, Viatel.[5] In vielen Ländern sind Telekommunikationsdienstleister sogar gesetzlich gezwungen, nationalen Behörden Abhörschnittstellen zur Verfügung zu stellen (*lawful interception*), die ihnen technisch keine Kontrolle über Umfang und Art der abgehörten Informationen ermöglichen. Wie weit die Kooperation bei Internet und Cloudanbietern geht, ist unklar. In Einzelfällen wurde die Kollaboration von Unternehmen mit der NSA jedoch aufgedeckt. RSA, Yahoo und viele weitere haben dafür Geld erhalten.

Dienstleister wie CSC, Booz Allen Hamilton oder Stratfor erbingen sogar als Subauftragnehmer Dienstleistungen für die Geheimdienste. In den Snowden-Dokumenten ist von insgesamt über 80 Unternehmen als strategischen Partnern die Rede, die die Spionageziele der NSA unterstützen. In einer Folie werden explizit IBM, HP, CISCO, Microsoft, Intel, Oracle, EDS, Qualcom, AT&T, Verizon und QWest genannt.[6] Ein Spinoff der CIA hält mit 9% Aktienanteil eine strategische Beteiligung an Facebook.

Für US Unternehmen besteht zusätzlich das Problem, dass sie über nationales Recht auch gegen ihren Willen zur Kooperation gezwungen werden können. Twitter gab Verbindungsdaten seiner Kunden erst nach rechtlicher Gegenwehr heraus. Microsoft wurde im April 2014 durch einen Gerichtsbeschluss verurteilt, Daten auch aus europäischen Rechenzentren an Behörden in den USA herauszugeben. Der *Patriot Act* erlaubt es US-Geheimdiensten sogar, mit dem *National Security Letter* (NSL), US Unternehmen zur Kooperation zu zwingen, ohne ihnen eine Möglichkeit zur juristischen Gegenwehr einzuräumen. Durch die rigiden Verschwiegenheitspflichten bei Erhalt eines NSL ist selbst eine Beratung durch anwaltlichen Beistand, erst Recht eine Information der betroffenen Kunden oder der Öffentlichkeit ausgeschlossen, wie der Fall des Emailproviders *Lavabit* gezeigt hat.[7] Der Email Dienst Lavabit, den auch Snowden genutzt hatte, schloss nach Erhalt eines NSL das Unternehmen, da er keine Möglichkeit sah, sein Datenschutzversprechen den Kunden gegenüber einzuhalten.

---

[5] http://www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthuellt-namen-der-spaehenden-telekomfirmen-1.1736791

[6] http://www.infowars.com/direct-nsa-partners-att-verizon-microsoft-cisco-ibm-oracle-intel-qualcomm-qwest-eds/

[7] cryptome.org/2013/12/lavabit-027.pdf

In den Veröffentlichungen werden zudem zahlreiche IT-Produkte genannt, die als kompromittiert gelten müssen, da die NSA unerkannte Schwachstellen kennt, dafür Hintertüren besitzt oder diese sogar gezielt einbaut wurden. In einem Bestellkatalog namens *ANT* (*Advanced/Access Network Technology*)[8] werden Werkzeuge und Techniken zum Kompromittieren von IT-Produkten mit Stückpreisen aufgeführt. Die Liste umfasst u.a. Produkte für die Netzwerkausrüster Cisco Systems, Dell, Hewlett-Packard, Huawei, Juniper Networks sowie die Festplattenhersteller Samsung Electronics, Seagate Technology (einschließlich der übernommenen Maxtor Corporation) und Western Digital.

Für gezielte Angriffe wird zudem Hardware auf dem Versandweg abgefangen und mit Hintertüren oder zusätzlichen Spionagekomponenten wie Keyloggern versehen, bevor sie wieder verpackt und zum Empfänger weiter geleitet wird. [9]

Die NSA verwendet einen Großteil ihrer Ressourcen auf Verschlüsselungstechnik. In die NIST-Standardisierung wurden gezielt schwache Kryptoverfahren aufgenommen. In einem RSA-Produkt wurde gegen Bezahlung ein unsicherer Zufallszahlengenerator verwendet. Unklar ist welche weiteren Verschlüsselungsprodukte und Hersteller kompromittiert sind. Das Bullrun-Programm der NSA dient dem Brechen von Verschlüsselung (Kryptoanalyse). Schwache Kryptoverfahren wie RC4 und Hashes wie MD5 halten Angriffen der NSA nicht Stand.

Militärische Nutzung des Internets

Die Aktivitäten der NSA (aber auch anderer Geheimdienste) beschränken sich nicht auf Spionage durch Ausforschung. Das Internet wird zunehmend militärisch für offensive Aktivitäten genutzt. Im Projekt *Quantum Insert* werden Zero-Day-Exploits für Anwendungen entwickelt oder von Dritten eingekauft. Dabei handelt es sich um Programme zur Ausnutzung von Schwachstellen, für die kein Patch verfügbar ist. Das US Repräsentantenhaus hat einen Beschluss gefasst, der dies zukünftig verbieten soll.[10]

---

[8] https://en.wikipedia.org/wiki/NSA_ANT_catalog

[9] Auch deutsche Firmen sind bekannt dafür, dass sie mit verschiedenen Geheimdiensten kooperieren, etwa Siemens, Utimaco oder Rohde & Schwarz.

[10] http://www.spiegel.de/netzwelt/web/us-gesetz-gegen-nsa-online-spionage-a-976356.html

Mit dem *FoxAcid*-Verfahren werden gezielt Angriffe (targeted attacks) auf Zielpersonen durchgeführt: Dabei kann es sich um Personen handeln, die selbst von Interesse sind (VIPs, Wissensträger, Feinde) oder IT-Beschäftigte, die administrative Zugriffsrechte auf relevante IT-Infrastrukturen oder -Systeme mit wertvollen Informationen besitzen.

Die Abteilung Tailored Access Operations (TAO) widmet sich der Angriffsvorbereitung durch Spionage und ermittelt gezielt Schwachstellen in Systemen, nutzt diese aus und infiltriert die Systeme damit. Die NSA besitzt inzwischen ein eigenes Botnetz (Gruppe automatisiert fern gesteuerter Computerprogramme) als virtuelle Angriffsressource. 2011 wurden von fast 69.000 befallenen Computern nur 8448 voll ausgebeutet,[11] also nur ein Bruchteil des Potentials wirklich genutzt, weil nicht genug Ressourcen für die Kontrolle zur Verfügung standen.

Ziele, Prioritäten, Vorgehensweise und Motivation der NSA

Unter den von Edward Snowden ‚geleakten' Papieren befand sich auch das von Präsident Obama autorisierte NIPF (*National Intelligence Priority Framework*), das den politischen Rahmen und deren Prioritäten für die NSA Aktivitäten beschreibt. Zusammen mit den ebenfalls enttarnten Etatplänen lässt sich erkennen, dass es der US Regierung nicht (nur) um die Bekämpfung von Terrorismus geht. Nur 35% des Etats dient der Terrorbekämpfung, der überwiegende Teil dient jedoch der Spionage für wirtschaftspolitische und militärische Zwecke.[12] So sind z.B. internationale Finanzinstitutionen mit Priorität 2 von 10 als Ziele mit der zweithöchsten geheimdienstliche Priorität ausgewiesen.[13] Neben ausländischen Politikern aus Regierung und Opposition werden auch NGOs und internationale Organisationen der UNO (WTO, WHO) und der EU abgehört und deren IT Systeme kompromittiert, um verschlüsselte Kommunikation mitlesen zu können.

Neben den offiziellen Spionagezielen der Regierung werden von Geheimdienstmitarbeitern auch private Interessen verfolgt und die technischen Möglichkeiten sogar bezüglich deren eigener offiziellen Regelun-

---

[11] http://www.heise.de/newsticker/meldung/US-Geheimdiensthacker-infizierten-Zehntausende-Computer-1946251.html

[12] Rosenbach, Stark: der NSA Komplex. S.147ff

[13] Ebenda S. 151

gen missbraucht. Im NSA internen Jargon gibt es für das Ausforschen von Expartnern, Flirts und potentiellen Sexpartnern sogar einen offiziellen Begriff, „*Loveint*“.[14] Aus den Dokumenten geht auch hervor, dass die internen Kontrollen gegen Verstöße von internen Vorschriften und US-Gesetzen lax gehandhabt werden. Die Außenkontrolle ist ebenfalls unzureichend. Ein Richter des FISC (Fisa Gericht), des offiziellen externen Kontrollorgans, hat mehrfache verfassungsrechtlich verbotene Abhöraktivitäten gegen US Bürger moniert.[15]

Infowarfare, Propaganda, Desinformation, Fälschung von Informationen

Die Veröffentlichungen zeigen, dass alles, was technisch möglich ist, auch genutzt wird und dass der Anspruch besteht, alles und jeden zu überwachen und zu belauschen. Geheimdientsliche Arbeit besitzt jedoch noch eine weitere Dimension: Geheimdienste betreiben gezielt Desinformation und Propaganda. Informationen zu Bedrohungen oder Schwachstellen aus Geheimdienstquellen können einseitig gefärbt, gefälscht oder irreführend, verharmlosend oder übertrieben sein.

Aufgrund ihrer Intransparenz sind Geheimdienste kaum kontrollierbar und weiten ihre Aktivitäten immer weiter aus. Die ohnehin sehr weit gefassten legalen Befugnisse werden übertreten (z.B. illegales Abhören auf US Territorium) und demokratische Kontrollorgane desinformiert oder belogen[16]. Es wurde sogar bekannt, dass die NSA Finanztransaktionen manipuliert hat, denn die Obama-Kommission, die als Reaktion auf die Veröffentlichungen in Leben gerufen wurde, empfahl, diese Praxis einzustellen.

2. Was bedeutet dies für Unternehmen, für ihre Bedrohungslage?

Potentiell kann jedes Unternehmen angegriffen werden, wobei strategisch wichtige Unternehmen (z.B. Betreiber kritischer Infrastrukturen) oder Unternehmen, die in einem Marktsegment führend sind, besonders gefährdet sind. Aber auch kleinere, scheinbar unbedeutende Un-

---

[14] Ebenda S. 176

[15] Ebenda S. 177ff

[16] Glen Greenwald: No place to hide. S. 77

ternehmen können zum Ziel und Opfer werden, etwa weil sie Zulieferer oder Subauftragnehmer eines Primärziels sind. In der Folge drohen ihnen Reputationsverlust, Schadenersatzforderungen und die Beendigung von bestehenden Verträgen. Gerade Mittelständler mit innovativen Produkten sind Ziel von Wirtschaftsspionage. Ebenso sind Hersteller von Sicherheitsprodukten oder Kommunikationstechnologie betroffen, deren Kompromittierung eine Hintertür zu Regierungseinrichtungen, Rüstungsbetrieben und Großunternehmen öffnet.

Die flächendeckende Ausspähung und Überwachung erleichtert es den Geheimdiensten, Personen mit speziellem Wissen und Rechten aus einem Unternehmen zu identifizieren und dann gezielt nach verwertbaren Informationen über diese Personen zu suchen. Mit diesen Informationen können *‚social-engineering'*-Angriffe der fortgeschrittenen Art durchgeführt werden, die diese Form des Trickbetrugs mit glaubwürdigen Legenden unterstützen. Die über Menschen gesammelten Informationen können aber auch direkter dazu genutzt werden, einzelne Personen oder ganze Organisationen mit potentellem Reputationsschaden bei Veröffentlichung zu erpressen und gefügig zu machen, um so an schwer zugängliche Unternehmens- oder Regierungsgeheimnisse zu kommen oder Entscheider zur Kooperation zu zwingen. Letzteres ist besonders gefährlich, wenn es sich dabei um IT-Dienstleister, etwa Hosting-Provider oder Anbieter von Cloud-Services handelt, die von vielen Kunden Daten verarbeiten.

Die umfassende Überwachung und Auswertung verlangt daher, dass jede Information geschützt werden muss, selbst wenn diese für sich genommen nur einen minimalen Schutzbedarf besitzt, da die scheinbar harmlosen Details später mit anderen Informationen verknüpft und missbraucht werden können. So lassen sich aus Verbindungs- und Metadaten, Geodaten oder persönlichen Kontaktdaten und Kalendern Rückschlüsse ziehen auf Intensität und Art von bestehenden Geschäftsbeziehungen oder auf vertrauliche Treffen zur Anbahnung von Geschäften.

Das komplette Abhören des Internetverkehrs bedeutet, dass es praktisch keine sicheren Kommunikationskanäle mehr gibt. Festnetz-, Voice-over-IP und Mobiltelefon, Email, Chat, Fax, SMS werden belauscht und ausgewertet. Zudem sind viele vermeintlich sichere Verschlüsselungstechniken kompromittiert worden. Zwar gibt es einige Algorithmen, die selbst die Geheimdienste nicht oder nur mit erheblichem Aufwand knacken können. Stattdessen werden Endgeräte oder Software kompromittiert oder schwächere Verfahren oder Hintertüren in kommerzielle, nicht offengelegte Verschlüsselungsprodukte eingebaut.

Viele Firmennetze nutzen angemietete Leitungen für die interne Datenkommunikation wie interne Email oder Client-Server-Anwendungen. Doch das so genannte interne und vermeintlich vertrauenswürdige Netz ist spätestens bei global agierenden Unternehmen kein Intranet mehr, sondern in der Regel wird für Fernverbindungen Bandbreite von Leitungskapazität in Form von MPLS-Verbindungen bei Telekommunikationsunternehmen angemietet, von denen viele mit Geheimdiensten kooperieren. Zum einen wird der MPLS-Datenverkehr in der Regel ohnehin nicht verschlüsselt, zum anderen besitzen die Betreiber jederzeit die Möglichkeit, die MPLS-Verbindungen umzuleiten oder zu manipulieren und eine Verschlüsselung zu deaktivieren. Werden, wie bei Tempora, flächendeckend wichtige Glasfaser Leitungen angezapft, so wird damit nicht "nur" der gesamte Internetdatenverkehr sondern auch der scheinbar firmeninterne MPLS-Datenverkehr abgehört.

Viele Unternehmen nutzen VPN-Verbindungen (*Virtual Private Networks*), um Netzwerkverkehr über öffentliche Leitungen zu verschlüsseln. Kommerzielle VPN-Produkte besitzen das Risiko von Hintertüren oder der Manipulation auf dem Lieferweg. VPN-Verbindungen können zudem mit verschiedenen Protokollen betrieben werden. Während das L2TP/IPSec-Protokoll zwar als relativ sicher aber umständlich zu konfigurieren gilt, baut das häufig verwendete PPTP-Protokoll auf dem MS-Chapv2-Autentisierungsprotokoll auf, das bereits als gebrochen gilt.[17]

Die militärische Nutzung des Internets, der Cyberwarfare und die Botnetze der NSA, stellen selbst ohne konkreten Kriegshandlungen eine ernste Bedrohung für die Verfügbarkeit der IT von Unternehmen dar. Die eingebauten oder geheim gehaltenen Schwachstellen haben oft das Potential, dass Infrastrukturen einfach ausgeschaltet oder unbrauchbar gemacht werden. Zudem besteht das Risiko, dass diese auch von nichtstaatlichen Kriminellen ausgenutzt werden. Durch das Geheimhalten von Schwachstellen bleiben die betroffenen Unternehmen auch gegen diese ungeschützt. Die militärischen Geheimnisse verbleiben nicht ausschließlich und unbegrenzt bei staatlichen Stellen. Sicherheitslücken können auch von anderen entdeckt und ausgenutzt werden. Private Dienstleister unterstützen die NSA selbst bei hoheitlichen Aufgaben. So brach der Code des als Cyberwaffe gezielt in Natanz genutzten STUXNET-Wurms durch einen Programmierfehler in die ‚Wildnis' aus. Auch könnten Mitarbeiter in den Geheimdiensten versucht sein, ihr

[17] http://vpnverge.com/can-nsa-crack-vpn/, Moxy Marlinspike (Defcon20, 2012), https://www.cloudcracker.com/blog/2012/07/29/cracking-ms-chap-v2/

Wissen um Schwachstellen durch die organisierte Kriminalität vergolden zu lassen.

Rechtlich gesehen sind Datenschutzverträge nach dem Safe-Harbour-Abkommen noch gültig, sie bieten allerdings offensichtlich keinen realen Schutz mehr, weshalb das EU Parlament auch konsequenterweise bereits die Aussetzung gefordert hat.[18] Auch Non-Disclosure-Agreements (zivilvertragliche Verschwiegenheitsverpflichtungen) mit US-Unternehmen müssen angesichts der Enthüllungen in Frage gestellt werden. Insbesondere muss ausgeschlossen werden, dass es darin Ausnahmeregelungen für die Weitergabe an Geheimdienste gibt, die unter den Begriff Regierungsstellen oder Behörden subsummiert werden.

Nach einem Urteil eines US Gerichts gegen Microsoft im April 2014 sind US Unternehmen selbst dann zur Herausgabe von Daten verpflichtet, wenn die Daten auf Servern außerhalb der USA gespeichert werden, wenn ein Ersuchen einer US-Ermittlungsbehörde vorliegt und auch wenn dies ggf. lokalen Gesetzen, etwa dem EU-Datenschutz, widerspricht.[19]

Kann man dem Staat trauen?

Von der Bundesregierung oder anderen deutschen Exekutivorganen können Unternehmen kaum Hilfe oder Schutz erwarten. Spätestens seit den Anschlägen vom 11. September 2001 betreiben alle Bundesregierungen eine im Grundsatz überwachungs- und geheimdienstfreundliche und datenschutzfeindliche Politik. Staatliche Großprojekte mit Sicherheitsinfrastrukturen wie E-Government mit biometrischen Ausweisen, die Nutzung von Staatstrojanern, die Vorratsdatenspeicherung, Antiterrordatei und viele weitere Ausdehnungen von Geheimdienstbefugnissen lassen eine Grundeinstellung erkennen, die im Zweifelsfall eher der staatlichen Überwachung den Vorrang gibt, als der Sicherheit und dem Datenschutz der Bürger – und der Unternehmen. Diese "Sicherheits"-Politik, zu der auch der Aufbau einer offensiven Cyberwar-Einheit bei der Bundeswehr gehört, gefährdet eher die (IT-)Sicherheit, als sie zu schützen. Die plakativsten Beispiele sind die Nutzung von Staatstroja-

[18] http://www.heise.de/newsticker/meldung/NSA-Affaere-EU-Parlament-fordert-Kuendigung-des-Safe-Harbour-Abkommens-2087185.html

[19] http://www.nysd.uscourts.gov/cases/show.php?db=special&id=398, http://www.heise.de/ix/meldung/US-Internetunternehmen-muessen-im-Ausland-gespeicherte-Daten-herausgeben-2178454.html

nern und Cyberwaffen, mit denen Sicherheitslücken ausgenutzt werden, anstatt sie zu schließen. Auf EU-Ebene blockiert die Bundesregierung die neue Datenschutzgrundverordnung. Welches Vertrauen kann man staatlich anerkannten Signatur- und Zertifizierungsstellen oder der DE-Mail entgegenbringen, wenn diese Geheimdiensten Hintertüren offen lassen oder diese gar öffnen können.[20]

Anstatt über die Risiken zu informieren und politisch Druck auszuüben, boykottiert die Bundesregierung auch in der Späh-Affäre die Aufklärung mit Druck auf Abgeordnete und der Weigerung, Edward Snowden Asyl zu gewähren und ihn in Deutschland aussagen zu lassen. Erst als bekannt wurde, dass die Kanzlerin selbst abgehört wurde, begann ein halbherziger Versuch, mit der US-Regierung ein No-Spy-Abkommen abzuschließen, der von Anfang an zum Scheitern verurteilt war. Auch der Generalbundesanwalt leitete bisher nur zu dieser Causa Merkel, nicht jedoch zu den übrigen Sachverhalten des Skandals ein Ermittlungsverfahren ein.

Neben dem G10-Gesetz, das dem BND offiziell die Weitergabe von Daten an andere Geheimdienste erlaubt, belegen die Snowden-Dokumente auch weitere Kooperationen deutscher Geheimdienste mit der NSA und ihre Verstrickungen in den Skandal.[21] Neben der Nutzung von XKeyscore betreibt der BND gemeinsam mit der NSA auch die Abhöranlage der NSA in Bad Aibling. Der Bau des NSA-Dagger-Komplexes bei Darmstadt wurde mit deutschen Steuergeldern mitfinanziert. Diese Anlage dient u.a. der Abhörung des Internetverkehrs am nahegelegenen Backbone. Über den DE-CIX-Knoten in Frankfurt wird der Großteil der Emails von deutschen Sendern und Empfängern geleitet.

Die Kooperation zwischen den Geheimdiensten hat eine lange Tradition. Bereits 2012 wies der Historiker Foschepoth nach, dass in Deutschland in der Nachkriegszeit während des kalten Krieges Postsendungen und Telefonate im größeren Umfang abgehört und ausgewertet wurden[22]. Grundlage waren neben offiziellen Alliierten Verträgen auch

---

[20] Zertizierungsstellen könnten gefälschte Zertifikate ausstellen und damit Man-in-the-middle-Angriffe auf verschlüsselte Kommunikation ermöglichen. DE-Mail bietet aufgrund der nicht bereit gestellten End-to-end-Verschlüsselung für staatliche Stellen potentielle Abhörmöglichkeiten bei den Dienstleistern.

[21] http://www.spiegel.de/netzwelt/web/snowdens-deutschland-akte-alle-dokumente-als-pdf-a-975885.html

[22] Foschepoth: Überwachtes Deutschland

Geheimverträge zwischen den westlichen Alliierten (USA, Großbritannien und Frankreich) und der Bundesregierung. Diese Geheimverträge sind teilweise immer noch gültig und räumen den Geheimdiensten umfangreiche Rechte zur Überwachung ein. Foschepoth spricht von nahezu symbiotischen Zuständen zwischen den bundesdeutschen und alliierten Geheimdiensten mit dem Segen und Wissen der Bundesregierungen. So war oder ist jede Bundesregierung nach dem zweiten Weltkrieg Mitwisser umfangreicher Vereinbarungen zur Überwachung.[23]

Intransparenz, Nebelkerzen und Verschleierung

Aufgrund der Desinformation im Rahmen des Infowarfare müssen sich Unternehmen auch die Frage stellen, welchen Informationen, Beratern und Untersuchungsergebnissen sie noch vertrauen können und wollen. Unternehmen, die Closed-Source-Sicherheitsprodukte verkaufen, lassen sich nicht unabhängig auditieren. Auch Informationen zu Sicherheitstechnologien, Testergebnisse, Studien von Beratern, Artikel und Untersuchungen müssen hinterfragt werden, da sie Teil des Infowarfare sein können, etwa Informationen von Herstellern von Sicherheitsprodukten, die über Lobbyverbände wie den Teletrust publiziert werden, oder von Beratungsunternehmen, die ebenfalls für Geheimdienste und für das Militär arbeiten. Auch Sicherheitsberater und Dienstleister von US-Geheimdiensten veröffentlichen Studien, deren Seriosität nur selten nachprüfbar ist.[24] Whistleblower werden diskreditiert.[25] Man muss dabei auch bedenken, dass selbst Massenmedien immer weniger selbst recherchieren und immer seltener unabhängig informieren. Stattdessen veröffentlichen viele Medien aus Kostengründen oder im Interesse ihrer Werbekunden oft ungeprüft Informationen, die ihnen zugespielt werden.

Gesamtbewertung der Bedrohung

---

[23] http://www.sueddeutsche.de/politik/historiker-foschepoth-ueber-us-ueberwachung-die-nsa-darf-in-deutschland-alles-machen-1.1717216

[24] Ein Beispiel ist der so genannte "Mandiant Report", http://intelreport.mandiant.com/, der behauptet, bestimmte Angriffe eindeutig dem chinesischen Geheimdienst zuordnen zu können

[25] In den Snowden-Dokumenten sind z.B. Planungen des GCHQ erwähnt, gefälschte Nachrichten im Namen von unliebsamen Personen zu versenden.

Anhand der Dimension des Ausspähskandals mit dem Absolutheitsanspruch der Geheimdienste, alles mithören und auswerten zu können, und mit der Skrupellosigkeit ihres Vorgehens in der Übertretung von gesetzlichen Befugnissen, im Bruch von Völker- und Verfassungsrecht und im Ausspionieren auch verbündeter Nationen müssen die bestehenden Risiken in den Unternehmen grundlegend neu bewertet werden. Bei entsprechend hohem Wert der Information wird es sehr schwer, sich zu schützen und bisher als paranoid verunglimpfte Bedrohungsszenarien müssen als reale Gefahren mit betrachtet werden. Alles was mit entsprechend viel Geld und Macht als Angriff möglich ist, wird auch getan.

Rechtliche Konsequenzen

Das oben erwähnte Urteil gegen Microsoft, das US-Regierungsstellen dazu berechtigt, die Herausgabe von Daten von europäischen Töchtern US-amerikanischer Unternehmen zu verlangen, zwingt betroffene US Unternehmen gegen europäischen Datenschutzrecht zu verstoßen. ‚Lawful Interception' nach dem US Patriot Act ist nach deutschem Recht nicht mehr „lawful", da das Verfahren nicht den Anforderungen des deutschen Grundrechts für Eingriffe in die informationelle Selbstbestimmung entspricht.

Das Safe-Harbour-Abkommen soll europäische Datenschutzstandards bei einer Datenverarbeitung in den USA gewährleisten. Das Europaparlament hat seit letztem Herbst in einer Arbeitsgruppe prüfen lassen, ob das massenhafte Ausspähen von personenbezogenen Daten durch die USA Konsequenzen haben muss. Der Abschlussbericht forderte, dass das Safe-Harbor-Abkommen zur Übermittlung gewerblicher Daten ebenso wie das Swift-Abkommen, welches die Übermittlung von Bankdaten europäischer Bürger an US Behörden regelt, ausgesetzt werden soll. Das Parlament stimmte im März 2014 mit der überwältigenden Mehrheit von 544 Ja-Stimmen, 78 Nein-Stimme und 60 Enthaltungen einer entsprechenden Vorlage der Arbeitsgruppe zu.[26] Obwohl Safe-Harbour, solange es noch in Kraft ist, rein formal die Datenverarbeitung Europäischer Bürger in den USA legalisiert, zeigt der Skandal, dass das Abkommen keinerlei Schutzfunktion entfalten kann, weder für vertrauliche Unternehmensdaten noch für Kundendaten. Eine Verschlüsselung

[26] http://www.zeit.de/digital/datenschutz/2014-03/usa-eu-datenschutz-datenaustausch-swift-safe-harbour

unter Kontrolle des Betreibers, wie sie einige Cloudanbieter anbieten, bietet keinen effektiven Schutz vor einem Zugriff durch US-Regierungsstellen, da US-Unternehmen als Diensteanbieter zur Herausgabe und Kooperation gezwungen werden. Unternehmen, die weiter Kundendaten bei US-Providern verarbeiten lassen, riskieren das Vertrauen, ihre Kunden zu verlieren.

Nach §11 BDSG muss bei einer Auftragsdatenverarbeitung der zu beauftragende Dienstleister sorgfältig ausgewählt und vorab bezüglich seiner Zuverlässigkeit geprüft werden. Aufgrund der Erkenntnisse aus dem Spähskandal müssen bestehende Outsourcing-Verträge und die Nutzung von Clouddiensten überprüft werden, und einige müssen auch beendet werden. Die in den Snowden-Dokumenten als Kooperationspartner der Geheimdienste genannten Unternehmen kommen dafür nicht mehr in Frage. Eine weitere Nutzung ihrer Dienste ist datenschutzrechtlich extrem bedenklich und nicht mehr glaubwürdig vertretbar. Erst recht verbietet sich eine Beauftragung, wenn es sich um besonders sensible Daten wie Gesundheitsdaten oder politische Überzeugungen handelt.

Schon aus Eigeninteresse sollte kein Unternehmen seine Geschäftsgeheimnisse unzuverlässigen Dienstleistern anvertrauen. Unternehmen, die vertrauliche Daten bei fragwürdigen Dienstleistern verarbeiten lassen, die mit Geheimdiensten kooperieren, gehen aber auch erhebliche Haftungsrisiken ein. Kunden oder Geschäftspartner können Schadensersatz fordern, wenn vertrauliche Informationen ausspioniert werden. Bestehen zivilrechtliche Geheimhaltungspflichten, kann grobe Fahrlässigkeit unterstellt werden. Ein Haftungsrisiko kann auch entstehen, wenn die IT-Infrastrukturen unzureichend gesichert sind und etwa als Bot für Angriffe gegen Dritte missbraucht werden. Handelt es sich um Aktiengesellschaften, können deren Aktionäre bei Wirtschaftsspionage gegen Geschäftsgeheimnisse wegen Vermögensverlusten klagen.

Besonders zu beachten ist die Haftung bei vermeidbaren Fehlern und Pannen bei dem Risikomanagement, bei dem Notfallmanagement und insbesondere bei dem Outsourcing an externe Dienstleister. Nach §14 StGB kann im Rahmen der Stellvertreterhaftung der vertretungsberechtigte Vorstand haften, wenn er ein anderes Unternehmen mit der Durchführung des Betriebs beauftragt hat und dieses durch Vorsatz oder Fahrlässigkeit, Begehung oder Unterlassung ein Schaden verursacht, ein Strafdelikt verwirklicht und/oder wenn ein zivilrechtlicher Haftungsanspruch begründet wurde.

Zusätzlich besteht gemäß dem Gesetz zur Kontrolle und der Transparenz (KonTraG) im Unternehmensbereich einer Kapitalgesellschaft eine weitgehende Haftungsbegründung der Unternehmensleitung bei mangelnder oder fehlerhafter Risikovorsorge. Gemäß § 93 Abs. 1 Satz 1 KonTraG müssen bei Aktiengesellschaften die Vorstandsmitglieder eine besondere Sorgfalt bei der Ausführung ihrer Geschäftstätigkeiten an den Tag legen. Im § 91 Abs. 2 AktG heißt es zusätzlich: "Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden." Wird diese Rechtspflicht missachtet, die zur Einrichtung und zum Betrieb eines Risiko und Notfallmanagementsystems verpflichtet, so begründet sich ein verschärfter Haftungsanspruch gegen das leitende Management gemäß §93 Abs 2 Satz 1 KonTraG. Für die Betreiber von IT-Services wie Internetdiensteanbieter oder Betreiber von kritischen Infrastrukturen kann bei einem Missbrauch für Spionage oder Cyberwarfare auch eine Störerhaftung zum Tragen kommen, wenn diese ihre Systeme nicht sorgfältig genug gegen Geheimdienstangriffe sichern.

Unabhängig von der rechtlichen Haftung ist es aber im Eigeninteresse eines Unternehmens, seine Positiva wie Geschäftsgeheimnisse und Kundendaten oder den Betrieb wichtiger Infrastrukturen nur Partnern anzuvertrauen, die dieses Vertrauen nicht durch Kollaboration mit Geheimdiensten verspielen.[27] Die Reputation eines Unternehmens und das Vertrauen von Kunden und Geschäftspartnern können durch eine falsche Wahl schnell zerstört werden.

3. Konsequenzen für die gesamte IT Strategie

Angesichts der Dimension der Ausspähung und der technischen und organisatorischen Angriffsmöglichkeiten der Geheimdienste laufen wir Gefaht, in Resignation zu verfallen und den Versuch, die Unternehmen dagegen zu schützen, aufzugeben oder gar nicht erst damit zu beginnen. In der Tat ist es weder einfach noch schnell noch kostengünstig möglich, sich umfassend zu schützen. Es gibt die ‚Silver Bullet' nicht. Trotzdem sind Gegenmaßnahmen möglich – und im Interesse des Unter-

[27] Die Eigentums- und Abhängigkeitsverhältnisse sind oft von außen nur schwer nachvollziehbar, erst Recht bei Subdienstleistern. Sie können sich zudem während der Vertragslaufzeit ändern.

nehmens dringend notwendig! –, die die Angriffe erschweren oder das Schadenspotential eines erfolgreichen Angriffs begrenzen.

In den deutschen Medien und von Regierungsseite wurde häufiger als Ansatz eine nationale Sicherheitsstrategie, etwa ein deutsches oder europäisches Internet genannt. Dieser Ansatz geht an den Interessen global agierende Unternehmen und der deutschen exportorientierten Wirtschaft völlig vorbei.Angesichts der Verstrickung der deutschen, britischen und weiterer europäischer Geheimdienste in den Skandal ist dies ohnehin kein ernst zu nehmender Lösungsansatz.[28] Denn die nationalen Geheimdienste verschaffen sich durch gesetzliche Abhörbefugnisse und vorgeschriebene Abhörschnittstellen selbsverständlich Zugriff auf Leitungen unserer deutschen Telekommunikationsanbieter (lawfull interception). Im Fall des mit der NSA kooperierenden BND geschieht dies auch ohne richterliche Prüfung. Auch bieten die weltweiten Zulieferketten und verteilten Produktionsprozesse gerade im Bereich IT-Hardware keine technische Basis für den Aufbau einer vertrauenswürdigen nationalen Infrastruktur. Unternehmen müssen und können sich wie in der Bedrohungsanalyse angedeutet nicht auf staatlichen Schutz verlassen, sondern müssen selbst die Initative ergreifen.

Die Herausforderungen sind erheblich. Es reichen keine kleineren Kurskorrekturen, sondern jahrelang verfolgte Strategien müssen grundlegend korrigiert werden. Dies ist weder kurzfristig und kostengünstig möglich noch ohne auf lieb gewonnene Gewohnheiten zu verzichten. Über Jahrzehnte akkumulierte Investitionen und damit geschaffenene Abhängigkeiten von kompromittierten Produkten oder Produkten von nicht vertrauenswürdigen Herstellern müssen aufgegeben, etablierte Geschäftsprozesse und Kooperationen überdacht und ersetzt werden. Mit besonderem Misstrauen muss Blackboxes und komplexen Closed-Source-Produkten begegnet werden wie Appliances, Hardwareverschlüsselungsprodukten oder ganz allgemein Closed-Source-Software, speziell Security-Produkten von mit der NSA kooperierenden US-Unternehmen.

Mitarbeiter einbeziehen

[28] http://www.heise.de/newsticker/meldung/NSA-Skandal-Deutschland-zapft-angeblich-fuer-NSA-Glasfaserkabel-an-2235190.htmlpFIfF30SJKN_v2.doc und http://www.spiegel.de/netzwelt/web/snowdens-deutschland-akte-alle-dokumente-als-pdf-a-975885.html

Mitarbeiter müssen den Umgang mit alternativen Betriebssystemen und Softwareprodukten erlernen. Viele Unternehmen setzen standardmäßig unverschlüsselte Email in Geschäftsprozessen ein. Ebenso werden Fax und Telefonie selbst für äußerst sensible vertrauliche Kommmunikation genutzt.

In den letzten Jahren hat zudem eine Entgrenzung zwischen privater und dienstlicher Nutzung der IT stattgefunden, wodurch Consumer-Produkte wie private Smartphones und Tablets im betrieblichen Kontext etabliert wurden. Dies wurde zum Teil sogar im Rahmen von BYOD (bring your own device) gefördert oder zumindest geduldet. Eine Vermischung von privater und dienstlicher Nutzung findet auch auf Applikationsebene bei der Nutzung von PIM-Daten wie Kontaktdaten, Kalendern oder Emailkonten statt. Eine besonderes Problem ist die geduldete oder gar offiziell erlaubte dienstliche Nutzung von sozialen Netzwerken und Cloudservices wie Google Mail, Calender, Dropbox, Office 360 oder Google Docs. Facebook erlaubt einer natürlichen Person nur die Nutzung einer Identität, was zwangsläufig eine Vermischung der dienstlichen und privaten Nutzung zur Folge hat, wenn der Mitarbeiter auch dienstlich dort tätig ist, etwa um eine Fanseite zu betreuen. Die Entgrenzung setzt sich fort durch Home-Office-Arbeitsplätze, die über das Internet mit dem Firmenetz verbunden sind, und mobile Arbeitsplätze, die auf Internet-Connectivity und Smartphones angewiesen sind, um auch unterwegs per Telefon, Email und Chat erreichbar zu sein. Durch das massiv gewachsene Outsourcing werden zudem immer mehr externe Partner auch im Ausland wiederum mit eigener Infrastruktur an die IT-Systeme der Unternehmen angebunden.

Auswahl von Outsourcing Partnern und Anbietern von IT Produkten

Wie oben erwähnt diskreditieren sich bestimmte Unternehmen bereits durch ihre Kollaboration mit den Geheimdiensten. Entsprechend müssen Ausschreibungsrichtlinien dies als Ausschlusskriterium berücksichtigen. Ferner müssen Klauseln in Verträge aufgenommen werden, die eine Datenweitergabe oder andere Formen von Kollaboration untersagen und mit empfindlichen Vertragsstrafen belegen. Diese Regeln müssen auch für die Subkontraktoren der Dienstleister gelten. Bestehende Altverträge müssen geprüft und nachgebessert oder gekündigt werden, wenn sich die Vertragspartner nicht zu einer entsprechenden Erklärung verpflichten wollen. Als Positivkriterium für die Auswahl von Partnern

kann eine Selbstverpflichtung im Unternehmenskodex (code of conduct)[29] herangezogen werden, die eine Zusammenarbeit mit Geheimdiensten negiert.

Bei IT-Produkten und Dienstleistungen ist eine besondere Sorgfalt in der Auswahl der Anbieter geboten. Dies gilt insbesondere für sicherheitssensitive Produkte wie Verschlüsselungslösungen, Firewalls, Malware- und Intrusiondetektions-Systeme, SIEM-Produkte oder ‚Security-as-a–service'-Lösungen, aber auch für deren Infrastrukturbasis wie Betriebssysteme, Middletear, Kommunikationsmittel und Netzwerkkomponenten. Es kann nicht ausgeschlossen werden, dass diese ausgerechnet bei Angriffen von Geheimdiensten aus dem Land, in dem der Hersteller seinen Firmensitz hat, absichtlich versagen, Schwachstellen oder Fehler enthalten, die entsprechende Angriffe verschleiern und so den Diensten als Hintertüren dienen.[30] Die schlechte Qualität vieler Produkte und die damit verbundene hohe Anzahl von Schwachstellen gewährt den Herstellern "plausible deniability", d.h. die Möglichkeit, die Absicht bei einer entdeckten Hintertür abzustreiten und von einem Fehler oder Versehen zu sprechen. Die absichtliche Kollaboration wird nur durch Veröffentlichungen von geheimen Interna wie im Fall der Snowden-Leaks transparent.

Transparenz durch Open Source

Als Gegenmittel bietet sich an, keine Closed-Source-Produkte mehr zu kaufen, sondern ausschließlich Open-Source-Produkte einzusetzen und deren Einsatz auch bei den Mitarbeitern im Privatbereich durch Information und Schulung zu fördern. Im Software-Bereich sind diese inzwischen relativ weit verbreitet, und sie können häufig auch qualitativ mit Closed-Source-Produkten konkurrieren, oder sie übertreffen diese sogar. Bei den ebenfalls kompromittierten Hardware-Produkten, insbesondere bei Microprozessoren oder gar hochintegrierten Endgeräten wie Smartphones sind dagegen bisher nur wenige Alternativen verfügbar. Eine Möglichkeit ist, die Hardware soweit irgend möglich selbst aus vertrauenswürdigen Quellen zu beziehen und zusammenzusetzen. Eine weitere Möglichkeit besteht darin, wieder stärker auf eigene Produktion zu setzen und wichtige Software intern selbst zu entwickeln.

---

[29] http://de.wikipedia.org/wiki/Deutscher_Corporate_Governance_Kodex

[30] Die überwiegende Anzahl von IT-Produkten stammt zur Zeit aus den USA und Asien. Die Aussage gilt aber generell

Mittelfristig sollten Unternehmen die für sie strategisch wichtige Soft- und Hardware-Projekte im Open-Source-Bereich fördern oder Dienstleister, die derartige Lösungen anbieten, und so zur allgemeinen Verfügbarkeit von sicheren Open-Source-Alternativen beitragen. Dies gilt auch für die Unterstützung von Pentest, Audits, Code-Reviews und anderen Sicherheits-Evaluierungen, etwa automatisierten Schwachstellentests, dieser Produkte. Die Ergebnisse dieser Tests sollten öffentlich verfügbar gemacht werden. Für Schwachstellen in der eigenen Infrastruktur oder in eigenen Produkten sollten Unternehmen ‚Bugfinder' belohnen, kooperativ mit ihnen zusammenarbeiten oder sogar proaktiv Wettbewerbe zum Auffinden von Schwachstellen ausloben.

Der Heartbleed-Bug in Open-SSL blieb als schwerwiegende Sicherheitslücke zwar auch in dieser Open-Source-Bibliothek monatelang unentdeckt. Trotzdem kann dieser Sicherheitsgau in einem Open-Source-Produkt eher als Beleg dafür angesehen werden, dass der Open-Source Ansatz sicherheitstechnisch grundsätzlich funktioniert. Die Lücke wurde nämlich überhaupt erst durch eine Code-Review von Dritten (in diesem Fall Google) entdeckt, und sie konnte dann auch relativ schnell geschlossen werden. Durch gezielte Finanzierung von Sicherheitsprüfungen und bessere finanzielle Ausstattung sicherheitskritischer Projekte kann für alle ein besseres Sicherheitsniveau erreicht werden. So könnten gezielt elementare ‚Trusted Modules' gefördert werden, auf die höher integrierte Gesamtlösungen aufsetzen können, etwa Kryptomodule für die Sicherstellung von Vertraulichkeit und Authentizität.

Es muss mittelfristig eine komplette nachvollziehbar vertrauenswürdige Basis für IT-Produkte geschaffen werden, die von der Hardware über Firmware, Betriebssystem, Compiler sowie die quelloffene Software, die damit compiliert wird, die manipulationsfreie Integrität und Transparenz des Gesamtprodukts sicherstellt. Unternehmen können auch ihren politischen Einfluss nutzen, dass Open-Source-Projekte auch von staatlicher Seite besser gefördert werden.

Bei staatlichen Validierungen und Zertifizierungen von Produkten ist dagegen ein gesundes Misstrauen angebracht.[31] Verlässlicher sind nach-

[31] Problematisch sind hier staatliche Prüfungen und Empfehlungen, die in Teilen der Geheimhaltung unterliegen, weil sie für die Sicherheitsorgane selbst sicherheitsrelevant sind. Common-Criteria-EAL-Zertifikate sind zu unflexibel, da zertifizierte Produkte nicht mehr zeitnah gepatcht werden können, ohne dabei ihre Zertifizierung zu verlieren. Außerdem sind die Zertifizierungsstellen staatlich und nicht un-

vollziehbare transparente Auditierungen und Untersuchungen im Rahmen einer freien Sicherheitsforschung etwa durch Wissenschaftler oder unabhängige Hacker. Wichtig ist hierbei immer die vollständige Transparenz, was von wem wie und mit welchen Ergebnis geprüft wurde.

Verschlüsselung als Heilsbringer?

Aus den Snowden-Dokumenten geht auch hervor, dass sich selbst die NSA schwer tut, starke Verschlüsselung zu brechen. Das bedeutet, dass starke Verschlüsselung wo immer möglich eingesetzt werden sollte, auch bei scheinbar geringem Schutzbedarf, bei möglichst allen Kommunikationsvorgängen ebenso wie bei der Speicherung. Bei allen Webanwendungen sollte standardmäßig TLS-Verschlüsselung mit Perfect-Forward-Secrecy und starken Chiffren aktiviert sein. Email-Verschlüsselung und verschlüsselter Daten-Up- und Download sollten allen Kunden und Partnern angeboten werden. Alle Mitarbeiter sollten auf ihrem Arbeitsrechnern eine Anwendung zur Datenverschlüsselung und Email-Clients mit End-to-end-Verschlüsselung (GnuPG oder S/mime) installiert haben und das Unternehmen eine vertrauenswürdige am besten interne PKI besitzen und die öffentlichen Schlüssel der Mitarbeiter publizieren.

Leider ist Verschlüsselung nur dann sicher, wenn auch das System (Hardware und Software) integer ist, auf dem entschlüsselt wird, und das Schlüsselmaterial gespeichert und genutzt wird. Spätestens bei der Bearbeitung einer Information (im einfachsten Fall beim Lesen einer Nachricht) muss die Information entschlüsselt werden und kann potentiell mitgelesen werden, auch wenn die Verschlüsselung selbst nicht überwunden werden konnte. Damit stellt sich allerdings die Frage, auf welchen Endgeräten ein hinreichendes Sicherheitsniveau existiert. Die marktüblichen Smartphones inklusive der im Business Umfeld noch weit verbreiteten Blackberries gehören nach den Informationen aus den Snowden-Dokumenten jedenfalls nicht dazu. Auch ein typischer Win-

abhängig. Das BSI berät auch die deutschen Geheimdienste und wird von dessen Dienstherrn finanziert. Interessen von Herstellerfirmen konkurrieren mit dem Interesse an Offenlegung von Schwachstellen. Die negative Einflussnahme der NSA auf Sicherheitsstandards oder staatliche Behinderung der Verbreitung von starker Kryptographie veranschaulichen diesen Interessenkonflikt ebenso wie die Definition von DE-Mail als vermeintlich sicheres Verschlüsselungsverfahren per Gesetz.

dows-PC mit der üblichen Ausstattung an Closed-Source-Anwendungen ist für einen versierten Angreifer ein leicht zu kompromittierendes Ziel. Trotzdem ist es besser, grundsätzlich zu verschlüsseln als gänzlich im Klartext zu kommunizieren, da zumindest der Aufwand für eine Massenauswertung steigt und besonders sensible Informationen in einer großen Menge verschlüsselter Kommunikation leichter einer Kenntnisnahme durch die Geheimdienste entgehen. Man darf sich nur nicht zu sehr in falscher Sicherheit wiegen, dass die Information wegen der Verschlüsselung tatsächlich vertraulich bleibt.

Netzwerk und wichtige Systeme dezentralisieren und segmentieren, Redundanzen schaffen

Dass es staatlichen Angreifern gelingt, in einzelne Systeme eines Unternehmens einzudringen muss leider als wahrscheinliches Szenario angenommen werden. Ein flächendeckendes Abhören, aber auch Sabotageangriffe werden jedoch deutlich erschwert, wenn die Unternehmensnetzwerke stark segmentiert und die sonstigen wichtigen Anwendungs- und Infrastruktur-Systeme redundant ausgelegt und nicht zentral auf einer Serverfarm, sondern auf dedizierten Systemen in eigenen Netzsegmenten und an dezentralen Standorten betrieben werden. Wird ein System kompromittiert, wird es damit schwieriger, von dort "Innenangriffe" zu starten und weitere Systeme anzugreifen. Allerdings steigt das Risiko von Fehlkonfigurationen ebenso wie der Aufwand für die Absicherung der Einzelsysteme durch die erhöhte Komplexität. Ein Kompromiss ist, nur besonders sensible Systeme weitgehend zu isolieren.

Geheimdienstangriffe erfordern im Extremfall konspirative Gegenmaßnahmen

Wenn ein Unternehmen davon ausgehen muss, ein primäres Ziel für Spionage zu sein, müssen auch die Bestellprozesse für IT-Produkte überdacht werden, um die Manipulation insbesondere von Hardware auf dem Lieferweg zu unterbinden. Die Bestellung sollte dann nur indirekt über einen Mittelsmann und die Bezahlung erst mit Lieferung anstelle per Kreditkarte erfolgen, damit nicht von außen erkennbar ist, dass die Bestellung von dem Unternehmen ausgeht..

Bei besonders vertraulichen Treffen (‚konspirative' Treffen) muss auch die Reiseplanung anders als allgemein üblich durchgeführt werden.

Weder sollten Bahn- oder Flugverbindungen online als Dienstreise gebucht noch mit Firmenkreditkarte bezahlt werden. In Frage kommt eine Tarnung als private Urlaubsreise. Die Einladungen zu einer Konferenz müssen unbedingt verschlüsselt an die Teilnehmenden übertragen werden, idealerweise sogar über TOR oder vergleichbare Anonymisierungsdienste, um auch die Metadaten zu verschleiern. Thema, Ort und Agenda des Treffens dürfen nicht ohne Verklausulierung (z.B. Urlaubsreise) in den dienstlichen Kalendern auftauchen. Zum Treffen müssen eigens aufgesetzte Notebooks und bisher ungenutzte Mobiltelefone mit Prepaidkarten eingesetzt werden.

Priorisierung und langfristige Perspektiven

Angesichts der Vielzahl der Bedrohungen und Herausforderungen stellt sich die Frage, mit welchen Maßnahmen begonnen, wie priorisiert werden soll. Diese Frage lässt sich nicht pauschal beantworten. Einige der hier vorgeschlagenen Maßnahmen sind relativ schnell umsetzbar, etwa die Änderung von Ausschreibungsrichtlinien und die Prüfung und Überarbeitung von bestehenden Zulieferverträgen. Einige Closed-Source Produkte können gut durch Open-Source-Alternativen ersetzt werden, und die Sicherheitspolicy kann für die interne Kommunikation standardmäßig den Einsatz von Verschlüsselung von Email fordern, wenn alle Mitarbeiter einen entsprechend ausgestatteten Email-Client auf ihrem Arbeitsplatz vorfinden. Auch Kunden und Partnern kann damit zumindest angeboten werden, verschlüsselt mit dem Unternehmen zu kommunizieren. Eine ausschließliche Nutzung von Open-Source-Produkten ist nur mittelfristig umsetzbar, mit der Förderung entsprechender Projekte kann aber sofort begonnen werden. Hier müssen Unternehmen auch nicht alleine tätig werden, sondern sie können zusätzlich entsprechende Initiativen über ihre Verbände anstoßen. Die Bedrohung gilt schließlich allen. Zusätzlich sollte der Einfluss der Wirtschaft auf die Politik genutzt werden, die überwachungsaffine Grundeinstellung zu überdenken. In jedem Fall wird Beharrlichkeit und mittelfristige Aktivitäten für eine radikale Strategieänderung nötig sein, um der Herausforderung staatlicher Angriffe durch Geheimdienste und Militär wirksam entgegen zu treten.

Die Bedrohungen durch Cyberwarfare werden auch den deutschen Staat zum Handeln zwingen. Besonders KRITIS-Unternehmen, die kritische Infrastrukturen betreiben, sind “too big to fail” für die Gesellschaft. Ein

neues IT-Sicherheitsgesetz ist bereits in Vorbereitung. Wenn die Unternehmen nicht handeln, werden sie von staatlicher Stelle dazu gezwungen, nicht unbedingt mit den sinnvollsten und sichersten Lösungen, wie das Beispiel DE-Mail zeigt.

Rechtzeitiges Planen macht Investitionen günstiger. Investitionen etwa Umstellung auf Open-Source kann auch Schritt für Schritt erfolgen, wenn ohnehin investiert wird oder Altsysteme aus der Wartung laufen. Die Unternehmen müssen aber angesichts der Bedrohungen umgehend damit beginnen.

Erscheint in:

Gesellschaftliche Verantwortung in der digital vernetzten Welt.
Peter Bittner, Stefan Hügel, Hans-Jörg Kreowski,
Dietrich Meyer-Ebrecht, Britta Schinzel (Hrsg).
Reihe Kritische Informatik
Lit-Verlag (www.lit-verlag.de), 2014