OSB Open Source Business ALLIANCE INFORMATION

GvW Graf von Westphalen

PRISM und die Folgen

Arnd Böken, Rechtsanwalt,
Graf von Westphalen Partnerschaft, Berlin

PRISM und die Folgen

Im Juni veröffentlichten die Zeitungen Guardian und Washington Post Unterlagen, die von dem früheren NSA-Mitarbeiter Edward Snowden stammten und die ein umfangreiches Überwachungsprogramm des US-Geheimdienstes NSA enthüllten. Die Unterlagen zeigen, dass die NSA und andere Geheimdienste, darunter auch der britische GCHQ, das Internet in einem Ausmaß überwachen, das bislang unvorstellbar war. Zahlreiche weitere Veröffentlichungen haben das befürchtete Ausmaß der Überwachung bestätigt.

Die Überwachung des Internets durch die NSA

Die amerikanischen Sicherheitsbehörden haben mehrere Möglichkeiten, auf private Daten zuzugreifen. So kann das FBI zum einen so genannte National Security Letters (NSLs) erlassen und damit Internetunternehmen zur Herausgabe von Informationen verpflichten. Diese NSLs haben große praktische Bedeutung; allein im Jahre 2012 hat das FBI ca. 15.200 NSLs erlassen. Der Kunde des verpflichteten Unternehmens erfährt hiervon nichts, da NSLs geheim sind.

Zum anderen hat das FBI die Möglichkeit, ein spezielles Gericht anzurufen, den so genannten Foreign Intelligence Surveillance Court (FISC). Dieses Gericht kann Unternehmen gemäß Section 215 des Patriot Acts verpflichten, Gegenstände aller Art einschließlich Bücher, Aufzeichnungen, andere Dokumente sowie elektronische Daten an das FBI auszuhändigen. Die Snowden-Dokumente und spätere Veröffentlichungen zeigen, dass Gerichte und Behörden ihre Befugnisse nach dem Patriot Act sehr weit auslegen. Bekannt ist das Beispiel der Telefongesellschaft Verizon: Der FISC hat diese Gesellschaft verpflichtet, für einen Zeitraum von drei Monaten sämtliche Metadaten zu Telefongesprächen herauszugeben („bulk collection“).

Selbst diese flächendeckende Kontrolle reicht der NSA aber nicht aus. Daher hat der US-Gesetzgeber die Überwachung im Jahre 2008 nochmals erleichtert, wenn sie sich gegen Ausländer richtet. Nach Section 702 FISA Amendments Acts 2008 können Ausländer überwacht werden, um Informationen zu erlangen, die im Zusammenhang mit den auswärtigen Angelegenheiten der USA stehen. Das kann Internetunternehmen betreffen, bei denen Daten von ausländischen Kunden gespeichert sind.

Die Empfänger solcher Anordnungen sind nach US-Recht zum Stillschweigen verpflichtet. Daher ist es schwierig, das Ausmaß der Überwachung wirklich abzuschätzen.

Was sind die Folgen für Deutschland?

Die weitgehende Überwachung durch US-Behörden beeinträchtigt die Privatsphäre aller Bürger weltweit, auch in Deutschland. Niemand weiß genau, wie groß der Umfang der Überwachung ist. Deutschland ist aber auf jeden Fall ein attraktives Ziel. Für deutsche Unternehmen besteht noch eine weitergehende Bedrohung, nämlich Industriespionage. Bis vor kurzem wurde heftig darüber diskutiert, ob US-Geheimdienste Industriespionage betreiben. Nunmehr sind Dokumente bekannt geworden, die dies belegen. US-Geheimdienste haben beispielsweise das brasilianische Ölunternehmen Petrobras ausspioniert. Auch deutsche Unternehmen müssen befürchten, dass US-Dienste sie ausspionieren. US-Geheimdienste klären mit hoher Priorität die Einhaltung „fairer Wettbewerbsregeln“ durch europäische Unternehmen auf. Das setzt voraus, vertrauliche Informationen über diese Unternehmen zu erlangen. Die Ergebnisse dienen dem US-Justizministerium als Grundlage für Ermittlungen gegen die betroffenen Unternehmen. Sicher ist allerdings, dass die Geheimdienste anderer Staaten, nämlich China und Russland, in größerem Umfang Industriespionage betreiben. Die größte Gefahr geht aber von Konkurrenzfirmen und von Innentätern im Unternehmen selbst aus. Diese haben das größte Interesse an den Geheimnissen und wissen viel genauer, wonach sie suchen müssen.

Schützenswerte Daten im Unternehmen

Unternehmen verfügen über zahlreiche schutzbedürftige Daten, beispielsweise Aufzeichnungen über Technologien oder Forschungsergebnisse. Die Konkurrenz späht solche Geheimnisse aus, aber nicht ausschließlich. Genauso interessant ist es, die Unternehmensstrategie zu kennen, Produktionskosten zu erfahren oder Kundenlisten zu erhalten.

In vielen deutschen Unternehmen ist das Bewusstsein für den Wert der Firmengeheimnisse in den letzten Jahren stark gewachsen. Es gibt aber immer noch Unternehmen, die den Wert der Daten unterschätzen. Betriebswirtschaftlich gesehen entspricht der Wert der Daten den (abgezinsten) zukünftigen Gewinnen, die man mit ihnen erzielen kann. Das gilt für Forschungsergebnisse und geheime Technologien genauso wie für Kundendatenbanken. Betrachtet man diese Werte, so wird einem schnell bewusst, dass in vielen Unternehmen die Daten wertvoller sind als die vorhandene Hard- oder Software.

Muss ein Unternehmen seine Daten schützen?

Wenn deutsche Unternehmen personenbezogene Daten verarbeiten, beispielsweise Namen von Mitarbeitern oder von Kunden, sind sie an das Datenschutzrecht gebunden. Das Datenschutzrecht regelt nicht nur die Voraussetzungen dafür, wann Unternehmen solche Daten erheben und nutzen dürfen, sondern schreibt auch Sicherheitsmaßnahmen zum Schutz dieser Daten vor. Dazu gehört die Pflicht, durch Maßnahmen entsprechend dem Stand der Technik, den Zugang von Nichtberechtigten zu IT-Systemen sowie den Zugriff auf Daten zu verhindern.

Viele Daten im Unternehmen sind nicht personenbezogen, zum Beispiel Forschungsdaten oder Finanzdaten. Auch diese Daten muss das Unternehmen schützen. Das Aktiengesetz schreibt vor, dass der Vorstand eine angemessene Risikovorsorge betreiben muss, einschließlich der Vorsorge gegen IT-Risiken. Die Rechtsfolgen sind eindeutig: Der Vorstand muss sicherstellen, dass die wichtigen Schutzziele der IT-Sicherheit erreicht werden, nämlich Vertraulichkeit, Integrität und Verfügbarkeit der Daten. Diese Pflicht trifft nicht nur den Vorstand von deutschen Aktiengesellschaften, sie gilt genauso für GmbHs oder Unternehmen anderer Rechtsformen.

Welche Folgen haben Verstöße gegen die Datensicherheit?

Wenn deutsche Unternehmen personenbezogene Daten verarbeiten und die Sicherheitsanforderungen nicht einhalten, so drohen Bußgelder bis zu 50.000,00 EUR, unter Umständen sogar bis zu 300.000,00 EUR. In anderen Fällen drohen Schadensersatzansprüche. Sichert ein Unternehmen seine IT nicht fachgerecht und fällt dadurch ein Dokument über eine bestimmte Technologie in die Hände der Konkurrenz, können erhebliche Schäden entstehen. Es gibt immer wieder Unternehmen, die plötzlich auf einer Messe den Nachbau ihres neuesten Produktes entdecken. Häufig kann die Konkurrenz dieses Produkt viel günstiger anbieten, da sie die Entwicklungskosten gespart hat. Die entgangenen Einnahmen sind ein Schaden des Unternehmens; ersatzpflichtig ist die Geschäftsführung, es sei denn, sie hat die notwendigen Maßnahmen zur IT-Sicherheit veranlasst.

Schäden können genauso drohen, wenn die Unternehmensstrategie ganz oder in Teilen bekannt wird, Daten über die Markteinführung eines neuen Produktes an die Konkurrenz geraten oder wenn einem Wettbewerber ein geheimes Angebot in einem Bieterverfahren in die Hände fällt.

Mängel beim IT-Sicherheitskonzept können nicht nur zu Schadensersatzansprüchen führen, sondern sogar dazu, dass das Unternehmen seinen Versicherungsschutz verliert. Dann bleibt die Geschäftsführung auf dem Schaden sitzen.

Viele Unternehmen erhalten von ihren Geschäftspartnern vertrauliche Unterlagen. Das gilt für Berater genauso wie für Softwareentwickler oder für Auftragsfertiger und Zulieferer. In den Verträgen wird regelmäßig eine

Vertraulichkeitsvereinbarung getroffen. Kommen solche Unterlagen dann abhanden, zieht dies Schadensersatzforderungen nach sich und belastet außerdem das Verhältnis zum Auftraggeber schwer.

Eine weitere Folge eines Datenlecks ist der Reputationsschaden in der Öffentlichkeit. Es gibt kaum ein Ereignis, das ein Unternehmen so sicher in die Schlagzeilen bringt, wie ein Datenleck. Das gilt für alle Branchen.

Was müssen deutsche Unternehmen tun?

Jedes Unternehmen benötigt eine IT-Sicherheitsstrategie. Die Sicherheitsstrategie besteht aus technischen und organisatorischen Maßnahmen. Zu den technischen Maßnahmen gehören Programme zum Schutz gegen Viren und andere Schadsoftware sowie die Nutzung von Firewalls und von IDS (Intrusion Detection Systems). Genauso wichtig sind aber die organisatorischen Maßnahmen zum Schutz der IT.

Zentrales Dokument ist die IT-Sicherheitsrichtlinie. Hierin gibt die Geschäftsleitung sämtlichen Unternehmensbereichen klare Vorgaben für den sicheren Umgang mit der IT. Das betrifft z. B. die Internet- und E-Mail-Nutzung durch die Arbeitnehmer, denn beides sind Einfallstore für Angreifer. Um ein Abhören zu verhindern, ist eine Verschlüsselung der gesamten unternehmensinternen Kommunikation wichtig. Für die Kommunikation zwischen mehreren Standorten eines Unternehmens sind VPN-Tunnel Standard.

Komplizierter ist es, den E-Mail-Verkehr mit Kunden zu verschlüsseln, denn viele Kunden verfügen nicht über notwendige Zertifikate. Jedes Unternehmen sollte hier aber Strategien entwickeln. Bei der Kommunikation mit anderen Unternehmen ist es technisch überhaupt kein Problem, für Verschlüsselung zu sorgen. Am besten regelt man dies vertraglich. Dann besteht Klarheit, und beide Unternehmen können sich darauf verlassen. Die Kosten für die Beschaffung von Signaturkarten und Lesegeräten sind so gering, dass sie für Unternehmen kaum ins Gewicht fallen. Um Mitarbeitern die Arbeit zu erleichtern, sind Gateway-Lösungen sinnvoll.

Häufig wird eingewandt, Verschlüsselungen nützten nichts, da Geheimdienste sie überwinden könnten. Das ist eine gefährliche Haltung und sie ist auch falsch. Edward Snowden, der die Praktiken bei der NSA gut kennt, hat hierzu erklärt, selbst die NSA könne moderne Verschlüsselungsmethoden nicht überwinden. Hinzu kommt der Aufwand: Selbst die inzwischen als unsicher geltende DES-Verschlüsselung stellt einen Geheimdienst vor Probleme. Das „Knacken" dieser Verschlüsselung nimmt viel Zeit und Rechenleistung in Anspruch.

Die Sicherheitsstrategie muss auch gegen Innentäter aus dem Unternehmen selbst schützen, was schwierig ist, da diese Mitarbeiter meist das Vertrauen des Unternehmens genießen und das IT-System gut kennen. Wichtige Bausteine eines Anti Fraud Managements sind Gefährdungsanalysen, Fraud Risk Mapping und Fraud Prevention/Detection.

Smartphones – die mobile Gefahr

Ein anderes Einfallstor in Unternehmen sind Smartphones. Smartphones und andere Mobile Devices sind wichtige Kommunikationsmittel, auf die kein Unternehmen mehr verzichten kann. Genauso wichtig ist es, die notwendigen Sicherheitsmaßnahmen zu ergreifen. Mit einem Mobile Device Management muss das Unternehmen dafür sorgen, dass die Geräte gegen unberechtigten Zugriff gesichert sind, gerade bei Verlust des Geräts. Das Unternehmen muss festlegen, welche Apps der Nutzer installieren darf (White Listing oder Black Listing), ohne die Sicherheit zu gefährden.

Viele Unternehmen gestatten den privaten Gebrauch des Smartphones oder dulden ihn jedenfalls stillschweigend. In einem solchen Fall muss das Unternehmen für eine strikte Trennung des geschäftlichen- von dem privaten Bereich auf dem Smartphone sorgen, beispielsweise durch Containerlösungen. Auch Virtual Desktop-Architekturen sind geeignet. Hier kann der Mitarbeiter per Smartphone auf die Unternehmens-IT zugreifen, aber keine Dateien auf dem Smartphone speichern. Gerät das Smartphone in die falschen Hände, sperrt die IT-Abteilung den Zugriff auf die Unternehmens-IT, sodass nichts mehr passieren kann.

Cloud Computing

Die PRISM-Berichte haben das Vertrauen in Cloud Computing empfindlich beeinträchtigt. Ein Grund hierfür liegt darin, dass die veröffentlichten PRISM-Unterlagen den Eindruck erwecken, als hätten NSA-Mitarbeiter direkten Zugriff auf die Server einiger US-Internetunternehmen. Ob diese Behauptung richtig ist, ist bisher nicht bewiesen. Die betroffenen Unternehmen wehren sich heftig gegen die Vorwürfe. Ein solcher direkter Zugriff wäre auch nach US-Recht illegal.

PRISM und die weiteren Überwachungsprogramme der NSA und anderer Geheimdienste sind kein Grund, auf Cloud Computing zu verzichten. Cloud Computing bringt Kostenvorteile und erleichtert die flexible IT-Nutzung. Bei genauer Betrachtung erhöht Cloud Computing die IT-Sicherheit. Cloud-Anbieter können mehr Geld in Sicherheitsmaßnahmen investieren, als dies mittelständische Unternehmen üblicherweise können. Außerdem führt die verbindliche vertragliche Vereinbarung von Sicherheitsmaßnahmen zu größerer Transparenz und Sicherheit. Für vorsichtige Kunden empfiehlt sich eine Hybrid Cloud Strategie, bei der unkritische „Workloads" in die Public Cloud verlagert werden und sicherheitsrelevante in der privaten Cloud bleiben. Die flexible IT-Nutzung wird erleichtert, wenn man schon bei Abschluss des Cloud-Vertrages an das Ende denkt. Wenn der Cloud-Anbieter auf Basis von offenen Standards arbeitet, erleichtert dies dem Kunden später den Wechsel zu einem anderen Anbieter und vermeidet einen Vendor lock-in.

Technische Schutzmaßnahmen helfen nicht, wenn Cloud-Nutzer befürchten müssen, dass ihr Cloud-Anbieter Daten unkontrolliert an Geheimdienste weitergibt.

Die deutschen Datenschutzbehörden haben in einer Entschließung von Juli 2013 vor der umfassenden Überwachung durch die NSA und andere ausländische Geheimdienste gewarnt. Nach den gegenwärtigen Erkenntnissen gehen die Datenschutzbehörden davon aus, dass diese Geheimdienste umfassend und ohne Einhaltung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit und Zweckbindung auf Daten zugreifen, die deutsche Unternehmen in die USA übermitteln.

In der Tat ist es so, dass auch nach US-Recht ein direkter unkontrollierter Zugang von Geheimdiensten zu Rechenzentren von Cloud-Anbietern illegal wäre. Allerdings haben US-Geheimdienste weitgehende legale Zugriffsbefugnisse. Die Möglichkeiten nach Section 702 FISA-Amendments Act bestehen dann, wenn die Zielperson Ausländer ist und sich außerhalb der USA aufhält. Die US-Behörden können dann den FISA Court (FISC) einschalten und Cloud-Anbieter zur Herausgabe gespeicherter Informationen zwingen, die einen Bezug zu den auswärtigen Angelegenheiten der USA haben. Das ist eine sehr weitgehende Überwachungsbefugnis.

In Europa und den USA besteht eine grundlegend andere verfassungsrechtliche Lage. Im deutschen und im europäischen Recht ist der Datenschutz ein Grundrecht, das in Artikel 8 der Grundrechtecharta verankert ist. Jeder Zugriff von Behörden auf personenbezogene Daten ist ein Grundrechtseingriff und bedarf einer entsprechenden Rechtfertigung. In den USA gibt es dagegen kein Grundrecht auf Datenschutz. Das oberste amerikanische Gericht, der US Supreme Court, gewährt zwar einen gewissen Schutz durch ein Grundrecht, das gegen Durchsuchungen und Beschlagnahme schützt (Fourth Amendment). Dieser Grundrechtsschutz erfasst aber nicht das Cloud Computing. Nach der sogenannten „Third Party Doctrine" schützt das Grundrecht keine Daten, die der Betroffene bei einem Dritten gespeichert hat, also beim Cloud-Anbieter. Außerdem schützt das Grundrecht keine Personen, die keine US-Amerikaner sind und die sich außerhalb der USA aufhalten. Diese Personen genießen keinen verfassungsrechtlichen Schutz gegen Datenzugriffe. Dies ist der Grund dafür, dass der US-Gesetzgeber den Behörden überhaupt solch einen weitgehenden Eingriff wie in Section 702 FISA-Amendments Act gestatten kann.

Den Grundrechtsschutz durch Art. 8 der Europäischen Grundrechtecharta hat ein Cloud-Kunde, wenn er die Cloud eines Anbieters mit Sitz im Europäischen Wirtschaftsraum (EWR) nutzt und vertraglich sicherstellt, dass die Daten in Rechenzentren bleiben, die innerhalb des EWR liegen, das sind die EU-Staaten sowie Island, Liechtenstein und Norwegen.

Schwachstellen und Hintertüren

Im September musste die NSA auf Anfrage einräumen, dass sie gezielt Informationen über Software-Sicherheitslücken kauft, beispielsweise bei dem Anbieter VUPEN Security. Allerdings soll die NSA nicht nur vorhandene Schwachstellen ausnutzen. Geheime Dokumente, die Snowden dem Guardian zugespielt hat, legen nahe, dass die NSA gezielt Verschlüsselungen im Internet angreift, das geheime Projekt trägt den Codenamen BULLRUN. Noch schwerwiegender ist der Vorwurf, dass die NSA mithilfe von IT-Herstellern gezielt Schwachstellen in Software und IT-Systeme einbauen lässt (Projekt SIGINT), um sie auszuwerten. Das Ausmaß des Projekts zeigt sich darin, dass die NSA hierfür im Jahr mehr als 250 Mio. US-Dollar gezahlt haben soll, weit mehr als für das gesamte PRISM-Programm. Welche Hersteller hier betroffen sind, ist nicht bekannt.

Sofern die Vorwürfe zutreffen, ist das Projekt SIGINT ein gefährlicher Angriff auf die Sicherheit im Internet. Wenn gezielt Lücken in Software und IT-Systeme eingebaut werden, kann nicht nur die NSA diese Lücken ausnutzen, sondern andere Geheimdienste oder Spione aus der Industrie können dies ebenfalls. Im Jahr 2010 zeigte das Schadprogramm Stuxnet, wie effektiv Industrieanlagen angegriffen werden können. Dieser Angriff galt dem iranischen Atomprogramm und hat die Sicherheit weltweit erhöht. Würde aber beispielsweise ein ausländischer Konkurrent Softwarelücken ausnutzen, um die Produktionsanlagen eines deutschen Unternehmens lahmzulegen, wäre dies gefährlich.

Open Source Software und IT-Sicherheit

Das Gefährliche an Backdoors oder anderen undokumentierten Softwarefunktionen ist, dass sie nur sehr schwer zu finden sind, bevor sie ausgenutzt werden. Bruce Schneier, einer der führenden Experten für Verschlüsselungssoftware, hat angesichts der jüngsten Enthüllungen zu SIGINT empfohlen, Open Source Verschlüsselungsprogramme einzusetzen, da es schwieriger sei, dort Backdoors einzubauen.

Hier zeigt sich ein Vorteil von Open Source Software. Da der Quellcode offen ist, kann jeder ihn lesen und analysieren. Vor allem können IT-Security-Experten weltweit den Quellcode analysieren und auf Sicherheitslücken hinweisen.

SIGINT beruht auf Geheimhaltung. Ob es der NSA wirklich gelungen ist, geheime Absprachen mit einem Softwarehersteller über den Einbau von Backdoors in seine Software zu treffen, wird man möglicherweise nie erfahren, wenn die Beteiligten die Geheimhaltung wahren. Bei Open Source Projekten wäre die Geheimhaltung wesentlich schwieriger. Berücksichtigt man, dass bei großen Open Source Projekten Entwickler aus zahlreichen Unternehmen und anderen Einrichtungen mitarbeiten, scheint es ausgeschlossen, dass ein Geheimdienst hier heimlich Vereinbarungen über Hintertüren treffen kann. Schon die bloße Zahl der Ansprechpartner steht dem entgegen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sagt zu Open Source und anderer freier Software, dass zwei technische Aspekte besonders wichtig seien: Warnmeldungen über Fehler, die bei Sicherheitsüberprüfungen gefunden würden, könnten veröffentlicht werden, da kein Non Disclosure Agreement bestehe. Die Prüfung von Software auf Sicherheitslücken solle immer möglich sein, dies könne ein K.-o.-Kriterium für den Softwareeinsatz sein.

Insgesamt kommt das BSI zu dem Fazit, Unabhängigkeit, Software-Vielfalt und Verwendung offener Standards würden eine Basis für IT-Sicherheit bieten. Da Sicherheit ein Prozess sei, müssten die Verantwortlichen ihr System genau kennen, regelmäßig warten und Sicherheitslücken schnell beheben. Der Einsatz von Open Source und anderer freier Software sei allein noch keine Gewähr für ein sicheres System, biete in diesem Prozess jedoch bedeutende strategische Vorteile.

Fazit

Die NSA Überwachungsaffäre zeigt, wie groß das Risiko für Unternehmen ist, ausgespäht zu werden. Unternehmen können die Gefahr der Industriespionage nicht einfach hinnehmen, sondern die Unternehmensleitung ist rechtlich verpflichtet, für Schutzmaßnahmen zu sorgen. Die Haltung, niemand habe Interesse an den Unternehmensgeheimnissen, ist falsch. Industriespionage ist ein großes Problem, böswillige Konkurrenten und Geheimdienste sammeln alle Informationen, die sie bekommen können. Genauso unrichtig ist die Haltung, man könne sowieso nichts tun, was Geheimdienste erfahren wollten, würden sie erfahren. Snowden hat aber berichtet, dass selbst die NSA moderne Verschlüsselungsverfahren nicht überwinden könne. Auch sonst gibt es viele effektive Schutzmöglichkeiten, vor allem wenn man berücksichtigt, dass der gefährlichste Gegner nicht die NSA ist, das Risiko der Industriespionage durch Konkurrenten im In- und Ausland und durch Innentäter aus dem eigenen Unternehmen ist höher.

Quellen:

Greenwald, Glenn: "On Prism, partisanship and propaganda"
Guardian, 14.06.2013

Ball, James / Borger, Julian / Greenwald, Glenn: "Revealed: how US and UK spy agencies defeat internet privacy and security"
Guardian Weekly, 06.09.2013

Schneier, Bruce: "NSA surveillance: A guide to staying secure"
theguardian.com, 06.09.2013

Watts, Jonathan: "NSA accused of spying on Brazilian oil company Petrobras"
theguardian.com, 09.09.2013

Böken, Arnd: „Wer lauscht denn da? Industriespionage: Unternehmen müssen ihre Daten schützen"
iX 9/2013, Seite 82

Heise: „NSA-Überwachungsskandal: Von NSA, GCHQ, BND, PRISM, Tempora, XKeyScore und dem Supergrundrecht – was bisher geschah"
heise online, 19.09.2013

Horchert, Judith: „Verschlüsselungsexperte Phil Zimmermann: „Die Leute müssen sich empören" "
Spiegel Online, 27.09.2013

OSB Open Source Business ALLIANCE INFORMATION

Graf von Westphalen

OSB Alliance - Open Source Business Alliance e.V.

Breitscheidstraße 4
D-70174 Stuttgart

Tel: +49 (0) 711 / 90 715-390
Fax: +49 (0) 711 / 90 715-350
E-Mail: info@osb-alliance.com