[securemsp]

Analyse

Sicherer Datenaustausch trotz Internetüberwachung

Gefahren und Lösungen für deutsche Unternehmen

Secure-MSP GmbH

[securemsp]

Inhalt

1 Zielsetzung

Prism, Tempora und kein Ende: Kaum ein Tag vergeht derzeit, ohne dass neue Meldungen über Abhörprogramme der NSA und anderer Geheimdienste die Öffentlichkeit erreichen. Doch während in den Medien meist die politische Dimension des Überwachungsskandals diskutiert wird, betrachtet dieses Dokument die jüngsten Entwicklungen aus der Perspektive deutscher Unternehmen – denn diese müssen sich nun mit einer Gefährdungslage auseinandersetzen, wie sie vor ein paar Monaten noch kaum vorstellbar war. Besonders die Kommunikation über das Internet sowie die Speicherung von Daten in der Cloud sind betroffen. Die vorliegende Analyse soll einen Überblick über die Bedrohungen liefern und mögliche Lösungen für den sicheren Datenaustausch aufzeigen.

2 Geltungsbereich

Dieses Dokument bezieht sich hauptsächlich auf die Überwachungsprogramme, die durch die Enthüllungen von Edward Snowden öffentlich bekannt wurden. Berücksichtigt wurden die Medienberichte, die bis zum Redaktionsschluss Ende Juli verfügbar waren. Der Fokus liegt auf der Überwachung des elektronischen Datenaustauschs, da dies eine reale Gefahr für die breite Masse deutscher Unternehmen darstellt.

3 Die Überwachungspraktiken im Überblick

3.1 Welche ausländischen Geheimdienste überwachen den Datenaustausch in Deutschland?

Grundsätzlich ist davon auszugehen, dass Deutschland das Ziel von Abhöraktionen verschiedenster Länder und ihrer Geheimdienste ist. Die jüngsten Enthüllungen haben jedoch gezeigt, dass insbesondere die folgenden ausländischen Geheimdienste mit bisher weitgehend unbekannten Methoden und in kaum vermutetem Ausmaß Kommunikationsdaten, u. a. aus Deutschland, sammeln:

National Security Agency (NSA)

Die NSA verfügt über mehr Macht und mehr Budget als alle anderen 15 US-Spionagedienste. Sie wurde Anfang der 1950er Jahre als Abhör- und Entschlüsselungsstelle für die Streitkräfte gegründet [1]. Vor allem mit ihrem Spähprogramm Prism ist die NSA in den Fokus des aktuellen Überwachungsskandals gerückt.

Government Communications Headquarters (GCHQ)

Das GCHQ ist ein britischer Nachrichtendienst, der seit den 1940er Jahren für Nachrichtengewinnung mit technischen Methoden zuständig ist [2]. Vor allem sein Programm Tempora, mit dem weltweite Datenströme abgehört werden, ist Thema der aktuellen Berichterstattung. Es besteht eine enge Zusammenarbeit mit der NSA [3].

3.2 Welche Methoden kommen bei der Überwachung des Datenaustauschs im Internet zum Einsatz?

Zugriff auf Daten von Cloud-Diensten

Über Prism, das derzeit wohl bekannteste Abhörprogramm, überwacht die NSA nicht-US-amerikanische Nutzer der Cloud-Anbieter Microsoft, Skype, Google, Facebook, Yahoo, AOL, Apple und Paltalk [4]. Dadurch erhält der Geheimdienst Zugriff auf Inhalte wie E-Mails, deren Anhänge sowie sonstige beim Cloud-Dienst gespeicherte Dokumente. Auch Echtzeitüberwachung ist möglich: So wird eine Nachricht an Prism generiert, wenn sich ein überwachter Benutzer z. B. in einem der Dienste anmeldet, einen Chat startet, oder eine E-Mail-Nachricht sendet [5]. Unklar ist derzeit, wie genau der Zugriff verläuft: Einige der betroffenen Anbieter haben öffentlich dementiert, der NSA direkten Zugriff auf ihre Server zu gewähren. Dies schließt jedoch nicht aus, dass andere Methoden genutzt werden, die zum selben Ergebnis führen [6].

Auf den ersten Blick scheinen davon hauptsächlich Privatanwender betroffen zu sein, immerhin hat die mangelnde Vertraulichkeit von Facebook- oder YouTube-Daten für viele Unternehmen keine große Relevanz. Jedoch werden bei-

spielsweise die Cloud-Dienste von Microsoft häufig von Firmen genutzt. So ist die Vertraulichkeit als gefährdet zu betrachten, wenn geschäftliche E-Mails via Outlook.com versendet werden oder sensible Dokumente bei Skydrive lagern. Microsoft setzt bei seinen Cloud-Diensten zwar Verschlüsselungsmechanismen ein, doch auch diese bringen den Benutzern keine Sicherheit: Die NSA hat die Möglichkeit, diese Verschlüsselung zu umgehen und direkt auf Klartextinhalte zuzugreifen [7]. Und auch US-Cloud-Anbieter, die nicht offiziell mit Prism in Verbindung gebracht werden, sind an Gesetze wie den Patriot Act gebunden, der Behörden Zugriff auf Daten ohne gerichtlichen Beschluss erlaubt. Diese Verpflichtung gilt auch für Tochterfirmen in Europa [8].

Abhören von Internetleitungen

Die Geheimdienste machen sich bei der Datensammlung auch eine Grundproblematik des Internets zunutze: dessen zentrale Ausrichtung. Internationale Kommunikation verläuft meist über einige wenige Verbindungswege. Wer diese abhört, hat Zugriff auf einen großen Teil der internationalen Internetkommunikation. Daher ist das Anzapfen zentraler Leitungen eine sehr ergiebige und häufig eingesetzte Methode, von der praktisch jeder betroffen ist, der per Internet kommuniziert [9].

Internetverbindungen werden auf verschiedene Arten überwacht. So wurde beispielsweise bekannt, dass das britische GCHQ 200 Glasfaserkabel im Atlantik anzapft, darunter wohl auch das aus Deutschland kommende TAT-14-Kabel [10]. Auch die NSA sammelt internationale Telefon- und Internetverbindungsdaten. Dabei sollen unter anderem U-Boote zum Einsatz kommen, die Glasfaserkabel zwischen Kontinenten abhören [11]. Darüber hinaus wird vermutet, dass die NSA, teilweise mit Unterstützung des BND und anderer deutscher Behörden, auf Internetknoten wie z. B. den DE-CIX in Frankfurt zugreift [12].

Besonders interessant sind für den amerikanischen Geheimdienst Daten aus dem Nahen Osten, aus Pakistan und Afghanistan. Doch auch Deutschland liegt im Fokus des Geheimdiensts: Hier werden allein 500 Millionen Datensätze monatlich gesammelt – so viele wie in keinem anderen europäischen Land [10].

4 Die Konsequenzen für deutsche Unternehmen

4.1 Welche Gefahren gehen von den Abhöraktionen aus?

Viele Unternehmen sind angesichts der umfassenden Überwachung beunruhigt – denn dass die Aktionen, wie häufig behauptet wird, ausschließlich der Terrorbekämpfung dienen, scheint kaum mehr vorstellbar. Die enorm große Menge der gesammelten Daten sowie die Tatsache, dass auch befreundete Nationen überwacht werden, lassen zumindest die Vermutung zu, dass die Geheimdienste noch weitere Ziele verfolgen. Ein denkbares solches Ziel ist die Wirtschaftsspionage. Während von offizieller Seite angegeben wird, die Datensammlung diene dem Schutz des eigenen Landes vor Wirtschaftsspionen durch andere Länder wie z. B. China, sind die Methoden objektiv betrachtet zumindest auch dazu geeignet, selbst Wirtschaftsspionage zu betreiben [13].

Damit stehen die aktuellen Programme in der Tradition des NSA-Abhörprogramms Echelon, dessen Existenz seit etwa 12 Jahren als gesichert gilt: Aus einem EU-Bericht aus dem Jahr 2001 geht hervor, dass mit Echelon „sämtliche europäische Kommunikation via E-Mail, Telefon und Fax routinemäßig abgehört wird“. Derselbe Bericht stellt fest, dass sich Echelon zur Wirtschaftsspionage eignet, wenn „sensible Daten über Leitungen oder via Funk (Satellit) nach außen gelangen“. Ergänzend listen die Autoren eine Reihe bekannt gewordener Fälle auf. [14].

Den aktuell diskutierten Abhörprogrammen lässt sich bisher zwar noch keine Nutzung zur Wirtschaftsspionage nachweisen – für viele deutsche Wirtschaftsvertreter wären solche Angriffsszenarien jedoch keine große Überraschung. „Wirtschaftsspionage gehört zu den Aufgabenbeschreibungen der amerikanischen und britischen Geheimdienste“, so Dieter Kempf, Präsident des Branchenverbandes Bitkom. „Dass wir nun vom Einsatz nachrichtendienstlicher Mittel in diesem Zusammenhang hören, braucht niemanden zu wundern.“ [15]. Auch die Tatsache, dass gerade in Deutschland große Datenmengen gesammelt werden [11], passt ins Bild, denn hier sind laut Mario Ohoven, Präsident des Bundesverbands der mittelständischen Unternehmer, mehr als 1300 Weltmarktführer ansässig, die sowohl für Konkurrenten als auch für ausländische Geheimdienste ein lohnendes Ziel darstellen [16].

Darüber hinaus zeigen auch die Zahlen, dass Wirtschaftsspionage ein ernstzunehmendes Problem für deutsche Unter-

nehmen ist: Das Bundesamt für Verfassungsschutz (BfV) beziffert den Schaden bei 30 bis 60 Milliarden pro Jahr [17]. Im aktuell verfügbaren Verfassungsschutzbericht geht das BfV hauptsächlich von Ländern wie China und Russland als „Verursacher“ aus und nennt Angriffe mittels Schadsoftware als klassisches Beispiel für Spionage über das Internet [18]. Angesichts der neuen Informationen scheint die Lage jedoch weit komplexer zu sein als bislang angenommen: Auch westliche Geheimdienste und deren Methoden zur Datensammlung über das Internet müssen nun als potentielle Gefahrenquellen betrachtet werden.

4.2 Wer ist gefährdet?

Besonders gefährdet sind die sogenannten „Hidden Champions“, also mittelständische Weltmarktführer, die hochspezialisierte Produkte anbieten, viel Geld in Forschung und Entwicklung investieren und daher über besonderes Know-how verfügen. Klassische Beispiele aus der deutschen Wirtschaft sind Firmen im Bereich Luft- und Raumfahrt, Satellitentechnik, Rüstung oder Automotive [19]. Aber auch Patentanwälte sind im Besitz sensibler Entwicklungsdaten und können daher ein interessantes Ziel darstellen.

Grundsätzlich sind jedoch alle Unternehmen betroffen, die über das Internet kommunizieren bzw. Cloud-Dienste US-amerikanische Anbieter nutzen. Die „Schleppnetz“-Methodik, mit denen ohne konkrete Zielrichtung große Datenmengen gesammelt werden, zeigt deutlich, dass Unternehmen auch dann um die Vertraulichkeit ihrer Informationen fürchten müssen, wenn sie nicht explizit von einem Angreifer ins Visier genommen werden. Das bekannte Argument „Warum sollte es jemand ausgerechnet auf uns abgesehen haben?“ ist damit widerlegt.

4.3 Welche Lösungen eigenen sich noch für den Datenaustausch?

Übliche Methoden zur Datenübertragung, beispielsweise unverschlüsselte E-Mails oder FTP, sind also endgültig indiskutabel geworden, wenn sensible Informationen im Spiel sind. Auch das Image der Cloud-Dienste hat schwer gelitten, nicht zuletzt, weil die meisten großen Anbieter in den USA ansässig sind. Dabei gilt noch immer: Die Cloud ist dank flexibler Zugriffsmöglichkeiten gut für den Datenaustausch geeignet und sollte auch nicht generell verteufelt werden. „Die allerwenigsten Unternehmen können Daten auch nur annähernd so gut sichern, wie dies ein spezialisierter Cloud-Anbieter kann“, so Bitkom-Präsident Dieter Kempf. Empfohlen wird allerdings, auf Dienste aus dem eigenen Land zurückgreifen: Cloud-Daten sollten möglichst in der Heimat bleiben, so der britische Datenschutzaktivist Caspar Bowden. Dieser Meinung ist auch Christian Schaaf von der Sicherheitsberatung Corporate Trust: Ein deutscher Speicherort senke "die Wahrscheinlichkeit, dass ausländische Geheimdienste sich Zugang zu Firmendaten verschaffen können, erheblich." [20]

Doch ein europäischer Standort allein bietet noch keine ausreichende Sicherheit für hochschutzbedürftige Daten: Denn auch das Europäische Institut für Telekommunikationsnormen (ETSI), dem eine Reihe großer Technologiekonzerne angehören, arbeitet in der Arbeitsgruppe „TC Lawful Interception“ an Schnittstellen, über die Sicherheitsbehörden im Rahmen geltender Gesetze Cloud-Daten in Echtzeit überwachen können [21].

Letzten Endes muss der Kunde also auch bei einem europäischen Cloud-Anbieter selbst die Vertraulichkeit seiner Daten sicherstellen. Dies ist möglich, wenn nicht nur die Übertragung der Daten verschlüsselt wird, sondern auch die Daten selbst – und zwar, bevor sie das eigene Netzwerk verlassen. Bleibt der Schlüssel zu den Daten im Unternehmen, bestimmt allein deren Eigentümer, wer Zugriff zu den Klartextdaten erhält. Nur so lässt sich die volle Kontrolle auch in der Cloud aufrechterhalten.

5 Quellen

[1] NSA, GCHQ – Prism, Tempora: So überwachen uns die Geheimdienste über das Internet. In: Fokus Online, unter http://www.focus.de/digital/internet/tid-32065/nsa-gchq-prism-tempora-so-ueberwachen-uns-die-geheimdienste-ueber-das-internet_aid_1027694.html (abgerufen am 01.08.2013).

[2] GCHQ: Engineering and Technology. Unter http://www.gchq.gov.uk/AboutUs/Pages/Engineering-and-Technology.aspx (abgerufen am 01.08.2013).

[3] MacAskill, Ewen et al.: GCHQ taps fibre-optic cables for secret access to world's communications. In: The Guardian (Online-Ausgabe), unter: http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (abgerufen am 01.08.2013).

[4] Greenwald, Glenn; MacAskill, Ewen: NSA Prism program taps in to user data of Apple, Google and others. In: The Guardian (Online-Ausgabe), unter http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (abgerufen am 01.08.2013).

[5] Lau, Oliver: Bericht: PRISM überwacht in Echtzeit. In: heise online, unter http://www.heise.de/newsticker/meldung/Bericht-PRISM-ueberwacht-in-Echtzeit-1908878.html (abgerufen am 01.08.2013).

[6] Rushe, Dominic: Technology giants struggle to maintain credibility over NSA Prism surveillance. In: The Guardian (Online-Ausgabe), unter http://www.theguardian.com/world/2013/jun/09/technology-giants-nsa-prism-surveillance?INTCMP=SRCH (abgerufen am 01.08.2013).

[7] Greenwald, Glen et al.: How Microsoft handed the NSA access to encrypted messages. In: The Guardian (Online-Ausgabe), unter http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (abgerufen am 01.08.2013).

[8] Hoffmann, Maren: Sicherheit beim Cloud Computing. „Der Kunde sitzt am kürzeren Hebel“. In: Manager Magazin Online, unter http://www.manager-magazin.de/unternehmen/it/mehr-sicherheit-beim-cloud-computing-a-901110.html (abgerufen am 01.08.2013).

[9] Lubbadeh, Jens: Abhör-Skandal Tempora: Forscher basteln an neuer Internetstruktur . In: heise online, unter http://www.heise.de/newsticker/meldung/Abhoer-Skandal-Tempora-Forscher-basteln-an-neuer-Internetstruktur-1902403.html (abgerufen am 01.08.2013).

[10] Stöcker, Christian; Horchert, Judith: Überwachungsskandale: Alles, was man über Prism, Tempora und Co. wissen muss. In: Spiegel Online, unter http://www.spiegel.de/netzwelt/netzpolitik/prism-und-tempora-fakten-und-konsequenzen-a-909084.html (abgerufen am 01.08.2013).

[11] Sydow, Christoph: NSA-Abhörskandal: Die Datenräuber von der USS "Jimmy Carter". In: Spiegel Online, unter http://www.spiegel.de/politik/ausland/die-uss-jimmy-carter-soll-fuer-die-nsa-glasfaserkabel-anzapfen-a-908815.html (abgerufen am 01.08.2013).

[12] Pfister René et al.: Der fleißige Partner. In: Der Spiegel (22.07.2013), Nr. 30, S. 16–21.

[13] Norton-Taylor, Richard; Hopkins, Nick: UK and US spy chiefs have some explaining to do. In: The Guardian (Online-Ausgabe), unter http://www.theguardian.com/uk/defence-and-security-blog/2013/jul/01/gchq-nsa-eu (abgerufen am 01.08.2013).

[14] Europäisches Parlament (Hrsg.): Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)). Teil 1: Entschließungsantrag. Begründung. Unter http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE (abgerufen am 01.08.2013).

[15] Beuth, Patrick: Massenhaftes Abhören soll der Wirtschaft dienen. In: Zeit Online, unter http://www.zeit.de/digital/datenschutz/2013-06/wirtschaftsspionage-prism-tempora (abgerufen am 01.08.2013).

[16] Kröger, Michael: Prism-Programm: Unternehmen befürchten Industriespionage der NSA. In: Spiegel Online, unter http://www.spiegel.de/wirtschaft/soziales/prism-unternehmen-befuerchten-industriespionage-der-nsa-a-908867.html (abgerufen am 01.08.2013).

[17] Hecking, Claus: Firmen gegen NSA: Wie sich deutscher Mittelstand vor Industriespionage schützt. In: Spiegel Online, unter http://www.spiegel.de/wirtschaft/unternehmen/spionage-deutsche-industrie-soll-sich-besser-schuetzen-a-912066.html (abgerufen am 01.08.2013).

[18] Bundesministerium des Innern (Hrsg.): Verfassungsschutzbericht 2011. Unter http://www.verfassungsschutz.de/embed/vsbericht-2011.pdf (abgerufen am 01.08.2013).

[19] Kröger, Michael: Prism-Programm: Unternehmen befürchten Industriespionage der NSA. In: Spiegel Online, unter http://www.spiegel.de/wirtschaft/soziales/prism-unternehmen-befuerchten-industriespionage-der-nsa-a-908867.html (abgerufen am 01.08.2013).

[20] Kaiser, Arvid: Spionageskandal. Deutsche Cloud-Dienste florieren trotz Prism. In: Manager Magazin Online, unter http://www.manager-magazin.de/unternehmen/it/usa-spionage-laesst-deutsche-cloud-anbieter-kalt-a-909443.html (abgerufen am 01.08.2013).

[21] Kuhn, Johannes: Überwachung in der Wolke. In: Süddeutsche Zeitung (Online-Ausgabe), unter http://www.sueddeutsche.de/digital/cloud-computing-ueberwachung-in-der-wolke-1.1434325 (abgerufen am 01.08.2013).