



Interne Folien aus einer als „streng geheim“ eingestuften NSA-Präsentation mit dem Titel „Hat Ihr Ziel ein Smartphone?“*

DATENSCHUTZ

iSpy

Der US-Geheimdienst NSA nutzt den Smartphone-Boom für eigene Zwecke und kann geheimen Unterlagen zufolge neben dem iPhone sogar die als abhörsicher geltenden BlackBerrys auslesen. Eine nachrichtendienstliche Goldgrube.

Über das iPhone kann Michael Hayden eine hübsche Geschichte erzählen. Er habe vor einiger Zeit mit seiner Frau einen Apple-Laden in Virginia besucht, berichtete der ehemalige Chef des US-Geheimdienstes NSA bei einer Tagung in Washington kürzlich. Ein Verkäufer habe ihn dort angesprochen und vom iPhone geschwärmt: „Mehr als 400 000 Apps“ gebe es bereits. Hayden erzählte, wie er sich amüsiert zu seiner Frau umgedreht und leise gefragt habe: „Der Junge hat wirklich keine Ahnung, wer ich bin, oder? 400 000 Apps, das bedeutet 400 000 Angriffsmöglichkeiten.“

Hayden hat wohl nur unwesentlich übertrieben. Denn wie aus internen NSA-Unterlagen hervorgeht, die der SPIEGEL einsehen konnte, verwanzt der US-Geheimdienst nicht nur Botschaften und schöpft nicht nur den Datenstrom aus Unterseekabeln ab, um an Informationen zu kommen.

Die NSA interessiert sich natürlich auch intensiv für jene Kommunikationsgeräte, die in den vergangenen Jahren einen atemberaubenden Siegeszug angetreten haben: Smartphones.

In Deutschland beträgt der Anteil der Smartphone-Nutzer unter allen Handybesitzern bereits mehr als 50 Prozent, in Großbritannien machen Smartphones mehr als zwei Drittel aller Handys aus, und in den Vereinigten Staaten besitzen rund 130 Millionen Menschen ein solches Gerät. Die digitalen Alleskönner sind längst zu persönlichen Kommunikationszentralen geworden – digitale Assistenten und Lebensberater, die mehr über ihre Nutzer wissen, als diese meist ahnen.

Für eine Behörde wie die NSA sind die kleinen Datenspeicher eine Goldgrube, weil sie nahezu alle Informationen, die einen Geheimdienst interessieren, in einem Gerät vereinen: soziale Kontakte, Details über das Nutzungsverhalten und den Aufenthaltsort, Interessen (etwa über Suchbegriffe), Fotos, manchmal auch Kreditkartennummern und Passwörter.

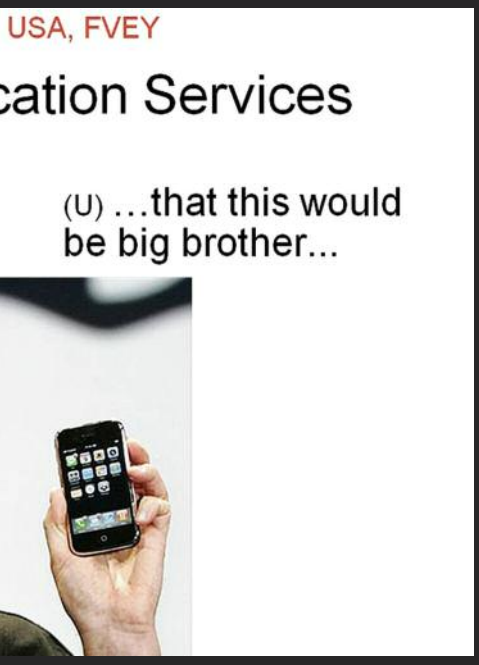
Eine technische Innovation wird zu einer grandiosen Schnüffel-Chance, sie öffnet Tore, die bislang selbst einer so mächtigen Behörde wie der NSA verschlossen waren.

Aus Sicht der Computerexperten aus Fort Meade, dem Hauptsitz der Behörde, war der Siegeszug der mobilen Minicomputer den Unterlagen zufolge zunächst eine enorme Herausforderung. Die kleinen Kommunikationswunder eröffneten viele neue Kanäle. Es schien, als könnten die Nachrichtendienstler den Wald vor lauter Bäumen nicht mehr erkennen.

Die Verbreitung von Smartphones vollziehe sich „extrem schnell“, heißt es in einem internen NSA-Bericht aus dem Jahr 2010, der mit „Smartphone-Ausbeutung – aktuelle Trends, Ziele und Techniken“ überschrieben ist. Dies erschwere die „klassische Analyse von Zielen“.

Die NSA nahm sich des Themas mit demselben Tempo an, mit dem die Geräte das Nutzungsverhalten der Menschen veränderten. Den Unterlagen zufolge rich-

* Übersetzung des Inhalts: „Wer hätte 1984 geahnt, dass Steve Jobs einmal Big Brother sein würde und dass die Zombies zahlende Kunden sein würden?“





tete sie eigene Arbeitsgruppen für die führenden Smartphone-Hersteller und Betriebssysteme ein. Spezialisierte Teams begannen, Apples iPhone und dessen iOS-Betriebssystem intensiv zu studieren, ebenso Android, das mobile Betriebssystem von Google. Eine weitere Arbeitsgruppe beschäftigte sich mit Angriffsmöglichkeiten gegen BlackBerry, das bislang als uneinnehmbare Festung galt.

Anhaltspunkte für eine massenhafte Ausspähung von Smartphone-Besitzern finden sich im Material nicht. Doch lassen die Dokumente keinen Zweifel daran, dass der Geheimdienst, wenn er ein Smartphone als Ziel definiert, dazu auch Zugang findet.

Dabei ist bereits die Tatsache delikat, dass die NSA Geräte dieser Unternehmen ins Visier nimmt: Bei Apple und Google handelt es sich immerhin um US-Firmen. Kaum weniger sensibel ist der Fall bei BlackBerry, das in Kanada beheimatet ist, einem Partnerland aus dem „Five Eyes"-Verbund der NSA. Die Mitglieder dieses erlesenen Kreises haben sich verpflichtet, keinerlei Spionagemaßnahmen gegeneinander zu unternehmen.

Zumindest in diesem Fall scheint die No-Spy-Politik nicht zu gelten. In den Unterlagen zum Thema Smartphones, die der SPIEGEL einsehen konnte, gibt es keine Hinweise, dass die Unternehmen von sich aus mit der NSA kooperierten.

BlackBerry sagte auf Anfrage, es sei nicht Aufgabe des Unternehmens, zu der angeblichen Überwachung durch Regierungen Stellung zu nehmen. „Wir haben immer wieder öffentlich betont, dass es keine Hintertür in unsere Plattform gibt." „Wir haben keine Kenntnisse von solchen Arbeitsgruppen und öffnen keiner Regierung den Zugang zu unseren Systemen", heißt es in einer Stellungnahme von Google. Die NSA ließ die Fragen des SPIEGEL unbeantwortet.

Bei seiner Ausbeutung macht sich der Geheimdienst den sorglosen Umgang vieler Anwender zunutze. Bei den Smartphone-Besitzern herrsche „Nomophobia", heißt es in einer NSA-Präsentation, ein Kunstwort aus „no mobile phobia". Das Einzige, wovor die Kunden sich fürchteten, sei, den Empfang zu verlieren. Wie umfangreich die Abschöpfmethoden beispielsweise gegenüber Nutzern von Apples populärem iPhone sind, zeigt eine ausführliche NSA-Präsentation mit dem Titel „Hat Ihr Ziel ein Smartphone?"

Darin ziehen die Verfasser in drei aufeinanderfolgenden Folien einen Vergleich mit George Orwells Überwachungsklassiker „1984", der die aktuelle Sichtweise der Behörde auf Smartphones und deren Nutzer entlarvt: „Wer hätte 1984 geahnt, dass dies einmal ‚Big Brother' sein würde …", fragen die Geheimdienst-Mitarbeiter zu einem Bild von Steve Jobs (siehe Folien oben). Und Bilder begeisterter Apple-Kunden und iPhone-Besitzer kommentiert die NSA: „… und dass die Zombies zahlende Kunden sein würden?"

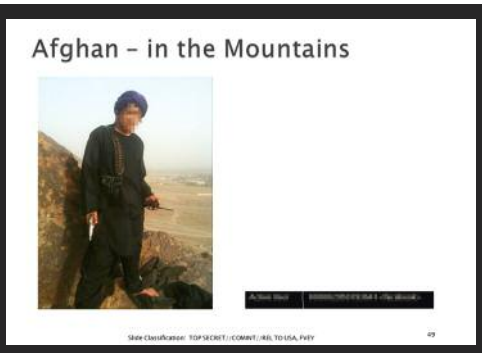
Tatsächlich kann die NSA bei den von ihr definierten Zielen ein breites Spektrum an Nutzerdaten von Apples umsatzträchtigstem Produkt auslesen – zumindest wenn man ihren eigenen Darstellungen Glauben schenkt.

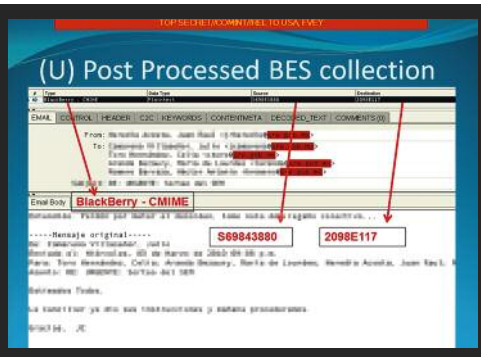
Die Ergebnisse, die der Geheimdienst anhand mehrerer Beispiele dokumentiert, sind jedenfalls beeindruckend. Zu sehen ist etwa das Bild des Sohnes eines früheren Verteidigungsministers, der eine junge Frau im Arm hält und sich dabei mit seinem iPhone aufnimmt. Eine Bilderleiste zeigt junge Männer und Frauen in Krisenländern, einen Bewaffneten in den afghanischen Bergen, einen Afghanen mit Freunden und einen Verdächtigen in Thailand.

Alle Bilder stammen offenbar von Smartphones. Ein Bild aus dem Januar 2012 ist besonders pikant: Es zeigt einen ehemaligen hochrangigen Beamten eines Landes, der laut NSA auf seiner Couch vor dem Fernseher entspannt und sich dabei selbst fotografiert – mit einem iPhone. Der SPIEGEL verzichtet aus Rücksicht auf die Persönlichkeitsrechte darauf, Namen und weitere Details zu veröffentlichen.

Der Geheimdienst macht sich den sorglosen Umgang vieler Anwender zunutze.

Die Zugänge zu derlei Material sind unterschiedlich, laufen aber häufig über eine Abteilung der NSA, die für maßgeschneiderte Überwachungsoperationen gegen Ziele von besonders hohem Interesse verantwortlich ist. Dabei machen sich die US-Agenten beispielsweise die sogenannten Backup-Dateien zunutze, die Smartphones anlegen. Einem NSA-Dokument zufolge enthalten sie diejenigen Informationen, die für Analysten von besonderem Interesse seien. Kontakte etwa, die Anrufhistorie, aber auch SMS-Entwürfe. Um derlei auszulesen, brauchten die Analysten nicht einmal Zugriff





Fotoauswertung aus der NSA-Präsentation „Smartphone Analysis“ vom Juni 2012, von der NSA entschlüsselte BlackBerry-E-Mail aus „Mein Ziel nutzt ein BlackBerry – was tun?“ (2010)

auf das iPhone selbst, heißt es. Es reiche aus, wenn der Rechner der Zielperson, mit dem das Smartphone synchronisiert werde, vorher von der Abteilung entsprechend präpariert worden sei. Unter der Überschrift „iPhone-Fähigkeiten“ listen die NSA-Spezialisten auf, welche Daten sie in diesen Fällen auswerten können. Demnach existierten etwa für die Betriebssysteme des iPhone 3 und 4 kleine NSA-Programme („Skripte“), die 38 verschiedene iPhone-Anwendungen ausspionieren können: den Kartendienst, die Voicemail, Fotos sowie die Anwendungen Google Earth, Facebook und den Yahoo Messenger.

Besonders freuen sich Analysten der NSA über die in Smartphones und vielen ihrer Apps gespeicherten Geodaten, mittels derer sie erkennen können, wann sich ein Nutzer wo aufgehalten hat.

So waren einer Präsentation zufolge die Aufenthaltsorte sogar über längere Zeiträume auslesbar, bis Apple diesen „Fehler“ mit der Version 4.3.3 seines mobilen Betriebssystems ausräumte und den Speicher auf sieben Tage begrenzte.

Für die NSA bleiben die „Ortungsdienste“ dennoch nützlich, die viele iPhone-Anwendungen und Apps von der Kamera über Maps bis zu Facebook verwenden. Die „Bequemlichkeit“ der Nutzer werde dafür sorgen, notieren die Analysten, dass die meisten freiwillig zustimmten, wenn sie von Anwendungen gefragt würden, ob diese ihren aktuellen Standort verwenden dürften, heißt es in den Unterlagen der US-Spione.

Ähnlich intensiv wie dem populären iPhone widmeten sich die NSA und ihre Partnerbehörde, das britische GCHQ, einem anderen elektronischen Spielzeug: dem BlackBerry.

Das ist besonders interessant, weil das Produkt der kanadischen Firma eine klare Zielgruppe hat: Unternehmen, die ihre Mitarbeiter damit ausstatten. Tatsächlich galt das Gerät mit dem kleinen Tastenfeld eher als Manager-Spielzeug denn als Gerät, über das mutmaßliche Terroristen ihre Anschlagspläne absprechen.

Diese Einschätzung teilt auch die NSA. Demnach überwogen in extremistischen Foren lange mit großem Abstand Nokia-Geräte, Apple folgte auf Rang drei, BlackBerry lag abgeschlagen auf Rang neun.

Wie mehrere Dokumente belegen, arbeitet die NSA seit Jahren intensiv daran, die besonders geschützte BlackBerry-Kommunikation zu knacken, und unterhält zu diesem Zweck eine spezielle „BlackBerry Working Group“. Die schnellen Entwicklungszyklen dieser Industrie halten allerdings die damit beauftragten Spezialisten gehörig auf Trab, wie ein als „UK geheim“ eingestuftes Papier des britischen Geheimdienstes GCHQ belegt.

Demnach sind im Mai und Juni 2009 plötzlich Probleme mit der Verarbeitung

von BlackBerry-Daten entstanden, die, wie man dann festgestellt habe, auf eine vom Hersteller neu einführte Kompressionsmethode zurückgingen.

Im Juli und August habe man in der zuständigen GCHQ-Abteilung daraufhin recherchiert, dass BlackBerry zuvor eine kleinere Firma übernommen hatte. Parallel habe man begonnen, den neuen BlackBerry-Code zu studieren. Im März 2010 sei das Problem schließlich gelöst gewesen, heißt es in der internen Chronik. „Champagner!“, lobten sich die Analysten selbst.

Wenn man den geheimen Unterlagen Glauben schenken kann, blieb es nicht bei diesem einen Erfolg gegen einen Konzern, der damit wirbt, abhörsichere Geräte anzubieten – und der zuletzt wegen strategischer Schwächen erheblich an Marktanteilen verloren hat, wie auch die NSA aufmerksam notiert: Allein zwischen August 2009 und Mai 2012 sei der Anteil von Beschäftigten der US-Regierung, die BlackBerry-Geräte nutzten, von 77 Prozent auf unter 50 Prozent gesunken, heißt in einem internen Dokument unter „Trends“.

Das einzige zertifizierte Regierungs-Smartphone werde zunehmend durch gewöhnliche Verbrauchergeräte ersetzt. Da müsse man sich Gedanken um die Sicherheit machen, notieren die Analysten. Offenbar gehen sie davon aus, dass weltweit nur sie in der Lage sind, BlackBerrys heimlich auszulesen.

Bereits 2009 jedenfalls vermerkten die NSA-Spezialisten, dass sie den SMS-Verkehr von BlackBerrys „sehen und lesen“ könnten, zudem könne man „BIS-Mails sammeln und verarbeiten“. BIS ist der BlackBerry Internet Service außerhalb von Unternehmensnetzen, der anders als die Datenströme über eigene BlackBerry-Server (BES) nur komprimiert, aber nicht verschlüsselt läuft. Offenbar ist aber selbst diese höchste Sicherheitsstufe nicht vor Zugriffen der NSA gefeit. Das belegt jedenfalls eine Präsentation, die mit „Mein Ziel nutzt ein BlackBerry – was tun?“ überschrieben ist.

Demnach erfordere die Erfassung des verschlüsselten „BES“-Verkehrs eine „nachhaltige Operation“ der NSA-Abteilung „Maßgeschneiderte Zugriffsoperationen“, um „das Ziel vollständig zu verfolgen“. Dass dies in der Praxis eingesetzt wird und gelingt, zeigt eine E-Mail aus einer mexikanischen Behörde, die in der Präsentation unter dem Titel „BES-Sammlung“ vorkommt – im Klartext, nach ihrer Entschlüsselung durch die NSA (siehe Folien Seite 146).

Im Juni 2012 hatten die amerikanischen Datenjäger ihr Angriffsarsenal gegen BlackBerry offenbar weiter ausgebaut. Nun listeten sie auch die Sprachtelefonie unter den eigenen „Fähigkeiten“ auf, nämlich die beiden beispielsweise in Europa und den USA gebräuchlichen Mobilfunkstandards „GSM“ und „CDMA“.

Zufrieden war die interne Expertenrunde, die zu einem „Runden Tisch“ zusammengekommen war, dennoch nicht. Laut der Vorlage wurde die Frage diskutiert, welche „zusätzlichen Erweiterungen in Sachen BlackBerry“ gewünscht würden.

Auch wenn alles in den vom SPIEGEL eingesehen Materialien für einen zielgerichteten Einsatz dieser NSA-Abhörmöglichkeiten spricht – die Firmen dürften die Aktivitäten der NSA kritisch sehen.

BlackBerry schwächelt und sucht gerade Übernahmeinteressenten. Sicherheit ist auch bei seinen jüngsten Modellen wie dem Q10 eines der wesentlichen Verkaufsargumente. Wenn nun offenbar wird, dass die NSA Apple- wie auch BlackBerry-Geräte zielgerichtet ausforschen kann, hat das womöglich weitreichende Konsequenzen, sogar für die deutsche Bundesregierung.

Vor nicht allzu langer Zeit hat die Berliner Regierung einen Großauftrag für die sichere mobile Kommunikation in Bundesbehörden vergeben – unter anderem an einen Verschlüsselungsanbieter, der bei der Hardware auf ein vermeintlich an sich schon abhörsicheres Gerät setzt: BlackBerry.

Laura Poitras, Marcel Rosenbach, Holger Stark