LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/5982**

28.05.2014

Kleine Anfrage 2343

des Abgeordneten Daniel Schwerd PIRATEN

NSA-Implantate in Hard- und Software

Aus den Veröffentlichungen von Dokumenten des Whistleblowers Edward Snowden geht hervor, dass der amerikanische Nachrichtendienst NSA in seiner Abteilung ANT sogenannte „Implants“, also Implantate für IT- und Kommunikationsmittel und –Infrastruktur entwickelt hat. Dazu haben sie Sicherheitslücken von verschiedenen Geräten, Protokollen und Herstellern gesammelt und nicht etwa zur Behebung der Sicherheitslücken an die Hersteller weitergegeben, sondern geheim gehalten, und auf dieser Basis solche Implantate entwickelt.

So existieren beispielsweise (nicht abschließend) die folgenden Implantate:

- IRATEMONK: Ein Implantat, das sich in der Firmware von Festplatten der Hersteller Western Digital, Seagate, Maxtor und Samsung verbirgt;
- SWAP: Ein Bios-Implantat, welches das Nachladen von Steuerungssoftware der NSA für diverse Betriebssysteme (Windows, FreeBSD, Linux, Solaris) und Dateisysteme (FAT32, NTFS, EXT2, EXT3, UFS 1.0) auf PC ermöglicht;
- HOWLERMONKEY: Ein Funksender und Empfänger, der zusammen mit einem anwendungsspezifischen Modul Daten aus IT-Komponenten schmuggelt, beziehungsweise es erlaubt, Geräte fernzusteuern;
- HEADWATER: Eine permanente Backdoor (PBD) für Huawei Router, die resistent gegenüber FirmwareUpdates im Boot-ROM verbleiben und so die Fernsteuerung des Geräts ermöglichen soll;
- SCHOOLMONTANA: Software-Implantat für Serie-J-Router der Firma Juniper;
- SIERRAMONTANA: Software-Implantat für Juniper-Router der M-Serie, das sich laut des NSA-Dokuments resistent gegenüber Softwareupdates im Bios einnistet;
- STUCCOMONTANA: Offenbar ein Implantat für Juniper T-Series-Router, das als Bios-Modifikation auch Softwareupdates überstehen soll;
- JETPLOW: Ein Software-Implantat für Cisco PIX- und ASA-Firewalls, das dauerhafte Hintertüren installiert;
- HALLUXWATER : Offenbar eine Hintertür (Backdoor) für Huawei Eudemon Firewalls in Form eines Software Implantats, das im Boot-Rom verborgen wird;
- FEEDTROUGH: ein Software-Implantat, das Fremdzugriffe auf die Juniper Firewall Modelle N5XT, NS25, NS50, NS200, NS500, ISG1000 ermöglichen soll;

Datum des Originals: 27.05.2014/Ausgegeben: 28.05.2014

Die Veröffentlichungen des Landtags Nordrhein-Westfalen sind einzeln gegen eine Schutzgebühr beim Archiv des Landtags Nordrhein-Westfalen, 40002 Düsseldorf, Postfach 10 11 43, Telefon (0211) 884 - 2439, zu beziehen. Der kostenfreie Abruf ist auch möglich über das Internet-Angebot des Landtags Nordrhein-Westfalen unter www.landtag.nrw.de

- GOURMETTROUGH: Ein konfigurierbares Implantat für eine Reihe von Juniper Firewalls, wie das NSA-Dokument zeigt;
- SOUFFLETROUGH: Ein im Bios verborgenes Implantat für Juniper SSG300- und SSG500-Geräte, das eine permanente Hintertür (PBD) herstellen soll;
- DEITYBOUNCE: Eine im BIOS permanente Backdoor für Dell PowerEdge-Server;
- GODSURGE: Ein Hardware-Implantat für Dell PowerEdge-Server;
- IRONCHEF: Ein Implantat für HP-Server;
- DROPOUTJEEP: Ein Implantat für Apples iPhone-Betriebssystem iOS, das die Fernsteuerung über SMS oder Datendienste ermöglichen soll. Laut des NSA-Dokuments soll es diverse Möglichkeiten bieten: Dateien herunter- oder auf das Handy hochladen, SMS auslesen, Adressbuch auslesen, Voicemail abhören, Standortdaten erfassen, Mikrofon und Kamera unbemerkt einschalten, Funkzelle bestimmen. Anfang 2008 war es noch in der Entwicklung;
- GOPHERSET: Ein Implantat für GSM SIM-Karten, das über verborgene Funktionen das Telefonbuch, Kurznachrichten (SMS) und das Protokoll ab- und eingehender Gespräche ausliest;
- MONKEYCALENDAR: Eine Angriffs-Software, die es ermöglicht, SIM-Karten dazu zu bringen, Standortinformationen als verborgene SMS zu versenden;
- TOTEGHOSTLY: Ein Implantat, das die vollständige Fernsteuerbarkeit von Windows Mobile Phones ermöglicht. Es soll diverse Möglichkeiten bieten: Dateien herunter- oder auf das Handy hochladen, SMS auslesen, Adressbuch auslesen, Voicemail abhören, Standortdaten erfassen, Mikrofon und Kamera einschalten, Funkzelle bestimmen;
- ANGRYNEIGHBOR: Eine Familie von Radarwanzen und Werkzeugen zur Auslesung dieser.

Diese Implantate sind teilweise als Software, teilweise als Hardware vorhanden. Bei Software-Implantaten wird die Firmware des Gerätes infiltriert, bei Hardware-Implantaten ist zusätzliche Hardware im Gerät eingebaut.

Software-Implantate werden bei PCs und Komponenten nach einem Angriff über das Internet per QFIRE-Technologie eingepflanzt, ohne das physischer Zugriff auf ein Gerät notwendig ist. Router, Firewalls und Server werden über das Internet direkt angegriffen.

Hardware-Implantate werden physisch in die Geräte eingebracht (die NSA spricht von „Interdiction“), teilweise beim Versand von bestellten Geräten durch Abfangen von Paketen und Kompromittierung der Hardware.

Der veröffentlichte Katalog stammt aus dem Jahre 2008. Es ist davon auszugehen, dass in der Zwischenzeit weitere Implantate für andere Geräte entwickelt worden sind.

Manche der befallenen Geräte sind bereits durch technische Nachfolger der jeweiligen Hersteller ersetzt worden. Die Implantate werden entweder kompatibel sein mit den technischen Nachfolgern, oder aber mit großer Wahrscheinlichkeit von der NSA-Abteilung ANT auf den jeweiligen neueren Stand gebracht worden sein.

Ich frage die Landesregierung:

1. Welche Komponenten (Festplatten, BIOS, Router, Firewalls, Server und Mobiltelefone) der in den veröffentlichten Dokumenten der ANT-Abteilung des NSA genannten Hersteller und Modelle, bzw. der jeweiligen technischen Nachfolger desselben Modells befinden sich in der Landesregierung, Ministerien, Landesbehörden und landeseigenen Betrieben im Einsatz? Nennen Sie Modelle/Geräte und Anzahl pro Behörde bzw. Unternehmen.

2. Wie viele SIM-Karten sind bei der Landesregierung, Ministerien, Landesbehörden und landeseigenen Betrieben im Einsatz? Nennen Sie jeweilige Anzahl pro Behörde bzw. Unternehmen.

3. Welche Maßnahmen wird die Landesregierung unternehmen bzw. hat sie bereits unternommen, um bei jedem dieser Komponenten bzw. Geräte die Firmware nach Befall respektive die Hardware nach einem Hardware-Implantat zu durchsuchen? Nennen Sie jede einzelne Maßnahme für jede Art von Komponente bzw. Gerät mit Zeitplan.

4. Auf welche Weise werden die Ergebnisse von 3.) veröffentlicht? Nennen Sie jeden (ggf. geplanten) Zeitpunkt und Veröffentlichungsort.

5. Welche Hilfestellung wird die Landesregierung Unternehmen, Organisationen, Kommunen und Privatleuten im Land NRW geben, um sie bei der Suche nach und der Entfernung von NSA-Implantaten zu unterstützen?

Daniel Schwerd