Neue Snowden-Dokumente: Die NSA rüstet zum Cyber-Feldzug

Von Jacob Appelbaum, Aaron Gibson, Claudio Guarnieri, Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Leif Ryge, Hilmar Schmundt und Michael Sontheimer

DPA

Die Geheimdienste betreiben nicht mehr nur Überwachung und Spionage. Dokumente aus dem Fundus von Edward Snowden, die dem SPIEGEL vorliegen, zeigen: Sie wollen die Herrschaft im Internet und bereiten digitale Kriege vor.

Sonntag, 18.01.2015 – 14:00 Uhr

Drucken | Senden | Merken

Nutzungsrechte | Feedback

Kommentieren | 196 Kommentare

Normalerweise müssen Praktikanten imposante Lebensläufe vorlegen, ehrenamtliche Arbeit in Sozialprojekten macht sich immer gut. Bei "Politerain" verlangt die Ausschreibung andere Neigungen: "Praktikanten gesucht, **die Dinge kaputt machen wollen**", heißt es da.

Aber Politerain ist auch nicht das Projekt einer konventionellen Firma, sondern des US-Geheimdienstes NSA. Oder genauer: das Projekt der NSA-Scharfschützen, der Truppe **für maßgeschneiderte Computereinbrüche mit Namen TAO** (Tailored Access Operations). (Der Artikel stammt aus dem SPIEGEL. Lesen Sie sie auch hier im digitalen SPIEGEL.)

Zum Ausforschen fremder Rechner, so wurden Bewerber weiter aufgeklärt, komme die "Manipulation und Zerstörung gegnerischer Computer". Mit dem Programm Passionatepolka beispielsweise soll man "Netzwerkkarten schrotten". Programme wie Berserkr und Barnfire ("Scheunenbrand") sollen Computer mit einer Hintertür versehen oder zentrale Daten löschen. Und TAO-Praktikanten sollten auch fremde Festplatten unbrauchbar machen. Ziel der Ausbildung sei es, "zu **lernen, wie ein Angreifer denkt**".

Die Job-Ausschreibung ist schon acht Jahre alt, inzwischen ist die "Denkweise eines Angreifers" für die Datenjäger der NSA zum Leitbild geworden. Der Geheimdienst hat es nicht nur auf die totale Überwachung der Kommunikation im Internet abgesehen. Die

Digitalspione der sogenannten Fünf-Augen-Allianz aus USA, Großbritannien, Kanada, Australien und Neuseeland wollen mehr.

Sie planen **Schlachten im Internet**, um Computernetzwerke lahmlegen zu können - und damit potenziell alles, was die steuern: Strom- und Wasserversorgung, Fabriken, Flughäfen oder Zahlungsverkehr. So zeigen es **streng geheime Dokumente aus dem Archiv des NSA-Whistleblowers Edward Snowden**, die der SPIEGEL exklusiv einsehen konnte und die SPIEGEL ONLINE teilweise veröffentlicht.

Hinweis: Die dem Artikel beigefügten Dokumente sind aus technischen Gründen nicht auf Android-Geräten abrufbar.

Netzwerkbasierte Angriffe und Datenerbeutung

Dokument über eine Erweiterung des Remote Operations Center (ROC)
Dokument über die Rolle des Remote Operations Center (ROC)
Interview mit einem NSA-Mitarbeiter der Abteilung für maßgeschneiderte Angriffe
Angriffe auf dem Versorgungswege
Klassifizierungsrichtlinie für Computernetzwerk-Operationen
NSA-Schulungsmaterial zu aktiven Computernetzwerk-Operationen
Methodische Übersicht über Cyber-Operationen der NSA
NSA-Projektbeschreibung für Datengewinnung aus Angriffen von Drittparteien
NSA-Programm BADASS zum Erforschen und Ausnutzen von Apps auf Smartphones
Codewort GENIE / Auszug aus dem geheimen NSA-Budget für Computernetzwerk-Operationen
Übersicht über Projekte zur Fern-Zerstörung von Netzwerkkarten
Analyse von Zielen und Datenauswertung mit Apples Geräte-Identifikation
Bericht eines NSA-Mitarbeiters über die Gestaltung einer Backdoor im OpenSSH Daemon
NSA-Dokument über das Implantat QUANTUMSHOOTER

Im 20. Jahrhundert entwickelten ruchlose Wissenschaftler sogenannte ABC-Waffen, atomare, biologische und chemische. Es dauerte Jahrzehnte, bis ihr Einsatz reguliert und teilweise geächtet wurde. Für den Krieg im Netz sind nun digitale Waffen entwickelt worden: Für diese **D-Waffen gibt es keine internationalen Konventionen**. Es gilt das Recht des Stärkeren.

Der kanadische Medientheoretiker Marshall McLuhan hat es kommen sehen, er schrieb bereits 1970: "Der Dritte Weltkrieg wird ein Guerilla-Informationskrieg sein, ohne Trennung zwischen Militärs und Zivilisten." Die Spione bereiten sich genau darauf vor.

"Der nächste größere Konflikt wird im Internet beginnen"

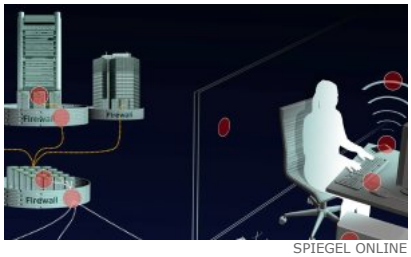
Die U.S. Army, die Navy, das Marine Corps und die Air Force haben eigene Cybertruppen aufgebaut; doch die NSA, die eine militärische Behörde ist, hat längst die Führungsrolle inne. Nicht umsonst trägt ihr Leiter - seit April 2014 Admiral Michael Rogers - neben dem Titel DIRNSA für "Director of the NSA" den des Chefs des **"Cyber Command" der US-Streitkräfte**. Der ranghöchste Überwacher ist in Personalunion also Chef der Cyberkrieger. Die rund 40.000 NSA-Mitarbeiter sind für Spionage und zerstörerische Netzangriffe und deren Abwehr gleichzeitig zuständig.

In der militärischen Sicht auf das Netz ist die Überwachung nur die **"Phase 0" in der Cyberkrieg-Strategie** - und internen Unterlagen zufolge die Voraussetzung für alles Folgende: Durch sie sollen die Schwachstellen der gegnerischen Systeme ausspioniert werden. Wenn sie mit "verborgenen Implantaten" infiltriert und mit "permanenten Zugängen" kontrollierbar sind, ist Phase drei erreicht, die mit "Dominieren" überschrieben ist: "Durch die in Phase 0 gelegten Zugänge kritische Systeme nach Belieben kontrollieren/zerstören." Als kritische Infrastruktur gilt alles, was eine Gesellschaft am Laufen hält: Energie, Kommunikation, Transport. Ziel, so interne Unterlagen, sei schließlich die **"kontrollierte Eskalation in Echtzeit"**.

In einer NSA-Präsentation heißt es: "Der nächste größere Konflikt wird im Internet beginnen." Die US-Regierung treibt die **Aufrüstung mit enormem Aufwand** voran. Laut dem unveröffentlichten Haushalt für

NSA-Programm Quantumtheory: Wie der US-Geheimdienst weltweit Rechner knackt

Interaktive Grafik



SPIEGEL ONLINE

Hier sitzen die Spähwerkzeuge der NSA

Mehr auf SPIEGEL ONLINE

The Digital Arms Race: NSA Preps America for Future Battle (17.01.2015)

Spionage-Software: USA und Briten sollen Trojaner Regin entwickelt haben (25.11.2014)

Trojaner Regin: Super-Software spioniert Russland und Saudi-Arabien aus (24.11.2014)

Snowden-Dokumente: Was die NSA knacken kann - und was nicht (29.12.2014)

Neue Dokumente: Der geheime Werkzeugkasten der NSA (30.12.2013)

In eigener Sache: Samstag ist jetzt SPIEGEL-Tag (16.01.2015)

SPIEGEL-Artikel zu NSA-Überwachung: Kontrollierte Eskalation

Neuer digitaler SPIEGEL: Ausgabe 4/2015

NSA-Geheimdokumente

Zur Quantum-Familie gehört auch QFIRE. Das ist ein im Jahr 2011 ausgearbeitetes Pilotprojekt der NSA, um eine weltweite Struktur zum aktiven Angreifen von Internetverbindungen zu schaffen. Das System soll der NSA erlauben, Internetverbindungen zu unterbrechen und umzuleiten sowie die Kontrolle über Botnetze zu übernehmen.

Fotostrecke: "Vorwärtsverteidigung" mit QFIRE

NSA-Überwachung

National Security Agency (NSA)

GCHQ

Geheimdienste

Computersicherheit

Alle Themenseiten

Netz-Selbstschutz: Verschlüsseln, Anonymisieren, Verstecken

die US-Geheimdienste wurde 2013 für die Stärkung des Angriffspotenzials in Sachen Computer-Netzwerk-Operationen über eine Milliarde Dollar veranschlagt. Allein für "unkonventionelle Lösungen" wurden zusätzlich 32 Millionen in den Etat gestellt.

Jeder Netznutzer kann einen Kollateralschaden erleiden

Zuletzt tauchten Schadprogramme auf, die Experten aufgrund etlicher Indizien der NSA und der Fünf-Augen-Allianz zugeschrieben haben: **Stuxnet** beispielsweise zum Angriff auf das Atomprogramm Irans. In Deutschland machte gerade **Regin** Furore, ein leistungsfähiger Schnüffeltrojaner, der auf dem USB-Stick einer **ranghohen Mitarbeiterin von Bundeskanzlerin Angela Merkel** gefunden worden war. Auch beim Angriff auf die EU-Kommission 2011 und auf die belgische Telekom-Firma Belgacom war Regin im Einsatz.

Schadsoftware und Implantate

Dokument des CSEC zur Erkennung von Trojanern und anderen "netzwerkbasierten Abnormalien"

Formalisiertes Verfahren für Analysten zur Wahl der passenden Werkzeuge

QUANTUMTHEORY / Verschiedene Möglichkeiten von Seitenangriffen auf TCP/IP-Verbindungen

Code-Beispiel einer Schadsoftware von den Five Eyes

Der Gefahr, nichts ahnend Opfer eines Datenangriffs zu werden, ist jeder Internetnutzer ausgesetzt. Denn Spione können routinemäßig fast jede Firewall knacken; auf manchen Rechnern herrscht ein munteres Kommen und Gehen diverser Eindringlinge; auch **in Facebook-Chats wird eingebrochen und kopiert** mithilfe von Programmen wie "Quantumdirk"; und zum Abtransport brisanter Daten können die Mobiltelefone Unbeteiligter missbraucht werden.

In diesem **Guerilla-Krieg um Informationen** wird, wie die Snowden-Dokumente zeigen, kaum zwischen zivil und militärisch unterschieden. **Jeder Nutzer des Internets** kann mit seinen Daten und seinem Rechner einen Kollateralschaden erleiden. Und sollte eine D-Waffe wie Barnfire aufgrund eines Programmierfehlers die Steuerzentrale eines Krankenhauses "schrotten", wären selbst jene betroffen, die nicht einmal ein Mobiltelefon besitzen.

Die Geheimdienste haben für ihre Netzoperationen die Devise der "plausible deniability" ausgegeben, **die Attacken müssen sich glaubwürdig leugnen lassen**. Wer für einen Angriff verantwortlich ist, soll nicht nachweisbar sein.

Ein atemberaubender Ansatz, denn die Digitalspione unterlaufen damit vorsätzlich das Fundament aller Rechtsstaaten. Sie machen das **Internet zu einem rechtsfreien Raum**, in dem die Großmächte und deren Geheimdienste nach Gutdünken operieren, ohne dafür zur Verantwortung gezogen werden zu können.

"Deine Daten sind unsere Daten"

Die Zuordnung von Angriffen erfordert detektivische Anstrengungen. Aber in den jetzt von SPIEGEL ONLINE veröffentlichten Dokumenten finden sich ein paar Hinweise. Querty zum Beispiel ist ein Spitzelprogramm, das heimlich alle Eingaben in den Rechner eines Opfers aufzeichnet. Querty ist ein alter, nicht sonderlich raffinierter Keylogger, aber er arbeitet mit Programmbibliotheken ("libraries"), welche die Fünf-Augen-Dienste gemeinsam nutzen. Es gibt Hinweise, dass Querty zu dem Fünf-Augen-Programm Warriorpride gehört, das zum Beispiel zum **Einbrechen in iPhones** eingesetzt wurde. In den veröffentlichten Dokumenten aus dem Snowden-Archiv findet sich ein Musterstück aus dem Querty-Quellcode - es könnte bei der forensischen Analyse anderer Schadprogramme und bei der Entwicklung von Abwehrmethoden hilfreich sein.

Zur Kerntruppe der NSA zählen jene Männer und Frauen, die in Fort Meade im Bundesstaat Maryland unter dem **Codenamen S321** im Remote Operations Center (ROC) arbeiten, dem Zentrum für ferngesteuerte Einsätze. Der ROC-Trupp sitzt in der dritten Etage eines der NSA-Hauptgebäude. Angefangen hätten sie als "ein Haufen Hacker", erinnert sich ein NSA-Mann in einem Bericht aus dem Snowden-Archiv. "Spontan improvisiert" habe man zunächst; inzwischen gestalteten sich die Abläufe "systematischer". Schon bevor die NSA-Führung die ROC-Mannschaft im Sommer 2005 massiv verstärkte, hieß deren Motto:

REUTERS

Tor-Router zum Selberbauen: Internet-Tarnkappe für 65 Euro

Schutz gegen Internet-Spione: So verschlüsseln Sie Ihre E-Mails

Schutz gegen Internet-Spione: So chatten Sie verschlüsselt

E-Mails, Kurznachrichten, Dateien: Fünfmal Gratis-Sicherheit im Netz

"Deine Daten sind unsere Daten, deine Geräte sind unsere Geräte."

Die Agenten mit diesem erstaunlichen Eigentumsbegriff sitzen rund um die Uhr im Schichtbetrieb vor ihren Monitoren. Wie nahe die NSA der angestrebten "globalen Netzvorherrschaft" schon gekommen ist, zeigt sich vor allem in der Arbeit der **Abteilung Transgression**. Das kann man mit dem deutschen Wort "Überschreitung" übersetzen; im religiösen Kontext aber auch mit "Sünde".

Die NSA nutzt Angriffe anderer Staaten für eigene Zwecke

Die Aufgabe der Abteilung ist das Aufspüren und Analysieren fremder Cyberattacken - und im besten Fall das Abschöpfen der Erkenntnisse konkurrierender Geheimdienste. Diese Form der "Cyber-Gegenspionage" **gehört zum Delikatesten im Agentenwesen**.

Das Archiv von Edward Snowden gewährt nicht nur Einblicke in das digitale Angriffspotenzial der USA selbst, sondern auch in das von anderen Staaten. Die Transgression-Mitarbeiter können dafür auf jahrelange Vorarbeit und Erfahrungen zurückgreifen - und auf Datenbanken, in denen sie die Schadprogramme und Angriffswellen anderer Staaten katalogisieren.

Den Snowden-Unterlagen zufolge haben die NSA und ihre Fünf-Augen-Partner in den vergangenen Jahren **eine Vielzahl von Cyberattacken aus anderen Staaten für ihre eigenen Zwecke genutzt**. Schon 2009 galt es, fremde Angriffe "zu entdecken, zu verstehen, zu bewerten". In einem anderen Dokument heißt es: "Stehlt ihre Werkzeuge, ihr Know-how, ihre Opfer und ihre Ergebnisse."

Im Jahr 2009 bemerkte eine NSA-Einheit einen Dateneinbruch bei Mitarbeitern des US-Verteidigungsministeriums. Die Abteilung spürte daraufhin eine IP-Adresse in Asien auf, die als Kommandozentrale der Angriffe fungierte. Am Ende der detektivischen Arbeit gelang es den Amerikanern nicht nur, China als Ausgangspunkt der Ausspähung zu lokalisieren: Sie griffen auch die Spionageergebnisse aus anderen chinesischen Raubzügen ab - darunter die elektronische Beute bei den Vereinten Nationen. Seither las man in Fort Meade mit, was die Chinesen an Interna aus der Uno abzweigten. **"Die NSA kann sich in die chinesische Aufklärung einklinken",** heißt es in einer internen Erfolgsmeldung aus dem Jahr 2011.

Die Praxis, andere Dienste spionieren zu lassen und sich deren Erkenntnisse anzueignen, wird **"Fourth Party Collection"** genannt. Alle Länder, die nicht zur Fünf-Augen-Allianz gehören, gelten als potenzielle Ziele für diese "nicht traditionelle" Methode - also **auch Deutschland**.

Zugriff auf Viertparteien

Abhandlung eines NSA Mitarbeiters über Zugriff auf fünfte Parteien

Sammlung über Viertparteien / Vorteilsnahme aus Netzwerk-Angriffen von Nicht-Partnern

Abwehr und Angriff / Erläuterung der Angriffsmethoden auf vierte Quellen

Übersicht über das Programm TRANSGRESSION zur Ausnutzung fremder Angriffe auf Computernetzwerke

NSA-Fallbeispiel SNOWGLOBE / Ein der französischen Regierung zugeschriebener Trojaner wird entdeckt und zu eigenen Zwecken analysiert

NSA-Zugriff auf vierte Parteien / "Ich trinke deinen Milchshake"

Präsentation über das NSA-Programm TUTELAGE / Instrumentalisierung der Angriffswerkzeuge von Drittparteien

BYZANTINE HADES / Präsentation zu den Angriffen der NSA auf chinesische Angriffswerkzeuge

Dokument des CSEC zur Problematik, beim Angriff mit einem Trojaner andere laufende Trojaner zu erkennen

Analyse der Vorgehensweise und Erfolge chinesischer Angriffsmethoden

Dank der Fourth Party Collection konnte die NSA, Snowden-Dokumenten zufolge, in den vergangenen zehn Jahren **zahlreiche Fälle der Datenspionage aufspüren, viele davon aus China und Russland**. So enttarnte die Abteilung TAO mit der Hilfe von IP-Adressen zunächst die Steuerungsrechner in China und arbeitete sich von dort aus zu den Drahtziehern in der Volksbefreiungsarmee vor. Ihre Gegner hätten es ihnen dabei durchaus schwer gemacht, berichten die US-Spione: Sie hätten mit wechselnden IP-Adressen gearbeitet, "schwierig

zurückzuverfolgen, schwer anzugreifen". Letztendlich sei es ihnen dennoch gelungen, "zentrale Router auszubeuten".

Kniffliger war es wohl, den Spieß umzudrehen und die Angreifer selbst zu attackieren. Erst nach langem "Waten durch uninteressante Daten" drangen die Amerikaner **auf einen Rechner eines hochrangigen chinesischen Militärs vor** - und ergatterten sogar Angaben zu geplanten Zielen in der US-Regierung, weiteren internationalen Regierungen und den Quellcode chinesischer Schadsoftware.

Diesen Operationen stehen allerdings auch chinesische gegenüber. Aus den Snowden-Unterlagen geht die **NSA-interne Schadensbilanz** von vor ein paar Jahren hervor. Demnach gab es mehr als 30.000 erkannte Zwischenfälle allein im Bereich des US-Verteidigungsministeriums; mehr als 1600 seiner Netzwerkrechner seien gehackt worden. Der Aufwand für die Schadensabschätzung und den "Wiederaufbau" des Netzwerks wird mit einer erstaunlich hohen Summe angegeben: **mehr als hundert Millionen Dollar**.

Zu den betroffenen "sensiblen Militärtechnologien" gehörten Zeitpläne für die Luftbetankung von Flugzeugen, das militärische Logistikplanungssystem, Raketen-Navigationssysteme der Marine, Informationen zu Atom-U-Booten, Raketenabwehr und weitere hochgeheime Rüstungsprojekte.

Selbst die Verteidigung lässt sich in einen Angriff verwandeln

Von der Gier, alles wissen zu wollen, sind freilich nicht nur Chinesen und Amerikaner, Russen und Briten getrieben: Schon vor Jahren fielen den US-Diensten **auch Dateneinbrüche aus Iran** auf - sie analysierten sie unter dem Codewort Voyeur. Hinter der Angriffswelle Snowglobe **dürften Franzosen gesteckt haben**.

Mittlerweile läuft die Suche nach fremden Cyberattacken und deren Abwehr bei der NSA und den Fünf-Augen-Partnern weitgehend automatisiert. Das **System Tutelage** kann Angriffe erkennen und dafür sorgen, dass sie das Opfer gar nicht erreichen.

In den Snowden-Unterlagen werden nicht nur chinesische Angriffe genannt, sondern auch die relativ simple Low Orbit Ion Cannon (LOIC). So heißt eine Schadsoftware, mit der etwa die **Bewegung Anonymous** missliebige Websites unerreichbar macht. In diesem Fall, heißt es in einem Dokument, könne Tutelage die IP-Nummern der Rechner erkennen, von denen die Überlastungsangriffe ausgingen, und diese wiederum blockieren.

Die NSA vermag inzwischen auch die Verteidigung in einen Angriff zu verwandeln: "Umnutzen und nachbauen" heißt diese Methode. Dabei geht es um sogenannte Botnetze, die mitunter aus Millionen Rechnern von Privatpersonen bestehen, auf denen eine Software eingeschmuggelt wurde. So lassen sie sich als **Teil einer "Zombie-Armee"** fernsteuern, um etwa Firmen lahmzulegen und zu erpressen. Statt diese Botnetze zu stoppen und die ahnungslosen Opfer zu warnen, versklaven NSA-Programme wie **Quantumbot** und**Defiantwarrior** ("Trotziger Krieger") sie teils für eigene Zwecke.

Diese Zombie-Rechner seien ideal als "nicht zurückverfolgbare Wegwerfknoten für Netzangriffe". Statt private Internetnutzer zu schützen, missbraucht Quantumbot sie als **menschliche Schutzschilde**, um eigene Attacken zu tarnen.

Botnetze: Übernahme und Datengewinnung

Überblick über die Nutzung von Botnetzen durch die NSA und das Programm DEFIANTWARRIOR

HIDDENSALAMANDER / Programm zur Erkennung von Botnetz-Aktivitäten und Optionen zur Übernahme von Clients und Daten

---

Die Spezialisten des Remote Operations Center besitzen eine **ganze Palette von digitalen Nachschlüsseln und Brechstangen**, um selbst in die bestgeschützten Rechenzentren einzudringen. Sie geben ihren Werkzeugen brachiale Namen, als böte man sie in einem App-Store für Cyberkriminelle an: Hammerchant erlaubt das Mitschneiden von Internettelefonaten (VoIP), Warriorpride bietet eine Art universelles Software-Esperanto, das alle fünf Partnerdienste verwenden, unter anderem für Einbrüche in iPhones.

Und mit Foxacid lassen sich kleine Schadprogramme, sobald sie sich auf

fremden Rechnern eingenistet haben, aus der Ferne mit immer neuen Funktionen aufrüsten. Als Projektlogo dient ein Fuchs, der schreiend in einem Säurebad aufgelöst wird. Die NSA will sich, wie üblich, zu operativen Details nicht äußern, beteuert aber, dass man sich strikt an die Gesetze halte.

Doch so raffiniert die Waffen des Cyberkriegs auch sein mögen - im Durchleuchten und Knacken fremder Netze lauert ein Paradox: Wer garantiert, dass nicht auch die Geheimdienste selbst **Opfer ihrer eigenen Methoden** werden können, zum Beispiel durch **private Hacker, Kriminelle oder andere Geheimdienste?**

Auf manchen Servern geht es zu wie in einem Taubenschlag

Um die Schadprogramme zu steuern, sind die ROC-Spione mit ihnen verbunden - und das geschieht über eigene, abgeschottete Netze, durch welche hochsensible Telefonmitschnitte, Angriffsprogramme und Passwörter schwappen.

Der Anreiz, hier einzubrechen, ist enorm. Wo immer geheimes Herrschaftswissen konzentriert liegt, diese Zugangsinformationen und VPN-Schlüssel sind sein hochpotentes Konzentrat. Wer über sie verfügt, kann **Konten plündern, militärische Aufmarschpläne durchkreuzen, Jagdbomber nachbauen, Kraftwerke abschalten**. Globale Netzvorherrschaft eben.

Aber die Welt der Geheimdienste ist schizophren: Die NSA soll das Netz verteidigen und gleichzeitig seine Sicherheitslücken ausnutzen; Räuber und Gendarm sein, Bock und Gärtner. Nach dem unter Spionen gängigen Motto: "Enthülle ihre Geheimnisse, schütze deine eigenen."

Auf einigen gehackten Servern geht es deshalb zu wie in einem Taubenschlag, Agenten geben sich die Klinke in die Hand, es herrscht ein Kommen und Gehen, von dem die rechtmäßigen Besitzer keinen Schimmer haben. Als würden die Privatdetektive eines Supermarkts ungerührt bei dessen Plünderung zusehen.

Es ist absurd: Die Spitzel werden bei ihren Raubzügen ständig **von anderen Spitzeln beim Spitzeln bespitzelt**. Also versuchen sie routinemäßig, ihre Spuren zu beseitigen oder falsche zu legen.

"Ahnungslose Datenmaultiere"

Technisch gesehen läuft das Legen falscher Spuren durch die ROC-Mitarbeiter unter anderem so ab: Nach dem Eindringen in fremde Rechner folgt die Exfiltration, also der Rücktransport der erspitzelten Daten. Dabei wird die Beute nicht direkt an die Internetadresse des ROC geleitet, sondern an einen sogenannten **Sündenbock-Empfänger** (Scapegoat). Geklaute Informationen können so auf den Servern von Gegnern landen, womit diese dann am Pranger stehen.

Natürlich hat das NSA-System, bevor die Daten als Ablenkungsmanöver beim Sündenbock landen, die Daten unterwegs abgefangen, kopiert und zum ROC geschickt. Derlei Vertuschungstaktiken bergen das Risiko einer kontrollierten oder unkontrollierten Eskalation zwischen den Diensten.

Exfiltrationsverfahren

Erläuterung des APEX Ansatzes / Kombination aus passiven und aktiven Methoden zum Herausschleusen von Daten aus angegriffenen Netzwerken

Erläuterung des APEX shaping, um den aus Netzwerken ausgeleiteten Datenverkehr zu legendieren

Präsentation zum FASHIONCLEFT Protocol, mit dem Trojaner die Daten aus angegriffenen Computern zur NSA schleusen

Verfahren für die heimliche Ausleitung von Daten aus angegriffenen Computern, auch wenn diese eigentlich offline sind

Project SPINALTAP / Kombination von Erkenntnissen aus aktiven Operationen mit Erkenntnissen aus passiven Überwachungsvorgängen

Technische Erläuterung zum FASHIONCLEFT Protocol

Freilich müssen es gar nicht unbedingt die Rechner sein, die systematisch geknackt, ausgespäht oder für Botnetze missbraucht werden. Auch **Mobiltelefone werden für den Datenklau am Arbeitsplatz benutzt**. Das unwissende Opfer, dessen Handy mit einem Spionageprogramm infiziert worden ist, schmuggelt dann die Beute aus dem Büro hinaus, woraufhin sie **auf dem Heimweg per Funk** abgegriffen wird. Die Digitalspione verhöhnen die Schmuggler wider

Willen im Slang von Drogendealern als "ahnungslose Datenmaultiere".

Sie fühlen sich sicher dabei. Weil sie für die mächtige NSA arbeiten und weil sie praktisch keine Spuren hinterlassen, die gerichtsfest wären. Und wo es **keinen Schuldbeweis** gibt, kann es auch **keine Strafjustiz** geben, keine parlamentarische Kontrolle der Geheimdienste, keine internationalen Abkommen. Bislang sind die Risiken und Nebenwirkungen der neuen D-Waffen noch kaum bekannt und gesetzlich kaum reguliert.

Edward Snowden hat enthüllt, wie die Geheimdienste der Welt, allen voran die NSA, sich bemühen, das **Internet zu einem rechtsfreien Raum** zu degradieren. Der Aussteiger macht sich inzwischen große Sorgen, dass für die NSA die "Verteidigung eine viel geringere Priorität hat als der Angriff" - so formulierte er es in einem vorige Woche veröffentlichten Interview mit dem US-Sender PBS.

Snowden will das nicht hinnehmen und forderte schon vor Monaten: "Wir müssen einen **neuen internationalen Verhaltenskodex** schaffen."

An English version of this article can also be read on SPIEGEL International.

Die Geschichte stammt aus dem SPIEGEL. Den neuen SPIEGEL finden Sie hier. Den digitalen SPIEGEL gibt es für das iPhone, iPad, Android und Windows 8 sowie als Web-App.

Mehr zum neuen Erscheinungstag des SPIEGEL lesen Sie hier.

NSA in Deutschland ▶

Snowdens Deutschland-Akte: Die Dokumente im PDF-Format

Karte mit Standorten: Hier sitzt die NSA in Deutschland

Abkürzungen erklärt: So lesen Sie die NSA-Dokumente

Zur Startseite

Das könnte Sie auch interessieren

SPIEGEL-Veröffentlichung

Experten enttarnen Trojaner "Regin" als NSA-Werkzeug

Telekom-Unternehmen, die EU-Kommission und eine Mitarbeiterin des Kanzleramts - alle wurden zum Opfer der Schadsoftware "Regin". Die Analyse eines vom SPIEGEL veröffentlichten Codes zeigt nun: "Regin" ist ein NSA-Werkzeug. mehr...

Bettina Wulff bei Sarah Kuttner

Sülze mit der Ex

mehr...

Abendnachrichten

Sprecherin der Schweizer "Tagesschau" kollabiert in der Sendung

Die Sprecherin der Schweizer "Tagesschau" ist während der abendlichen Hauptausgabe zusammengebrochen. Die Sendung musste beendet werden. Später klärte sich der Fall bei Twitter auf. mehr...

Russlands Präsident

Glaubt Putin die eigene Propaganda?

Wladimir Putin hat ein taktisches Verhältnis zur Wahrheit: Vor der Krim-Annexion log er, um Zeit zu gewinnen. Doch Russlands Präsident verheddert sich im Netz der Lügen - und wirkt oft schlecht unterrichtet. mehr...

Video-Empfehlungen

Angriff auf Mariupol: Steinmeier warnt vor weiterer Eskalation

Angriff auf Blauhelme: Proteste gegen Luftangriffe in Mali

Angriff auf "Charlie Hebdo": Al-Qaida im Jemen beansprucht...

Forum ▶

Diskutieren Sie über diesen Artikel
insgesamt 196 Beiträge

Alle Kommentare öffnen

Seite 1 von 40

1. Wo sind die europäischen Geheimdienste?
liberalerfr 18.01.2015
Dank Snowden wissen wir wie professionell der US Geheimdienst arbeitet und auch liefert - in vielen Artikeln wird darauf hingewiesen, dass zahlreiche Erkenntnisse zu aktuellen Terrorgefahren und den Hintermännern aus den USA [...]

2. Schon vor der ersten Schlacht verloren...
franxinatra 18.01.2015
Regierungsorganisationen werden organisierter Kriminalität immer hinterher hinken; ein Umstand, der mich so bezeichnete Terrormächte weit aus weniger fürchten fürchten läßt als die unterschiedlichen mafiösen Kreise von [...]

3. einfach nur krass
partey 18.01.2015
Ich hätte nicht gedacht, dass die Zukunft schon Gegenwart ist. So etwas kenne ich nur aus Filmen, welche leider meist Dystopien beschrieben.

4. Digitales Armageddon
bjbehr 18.01.2015
Wenn man die heutige Menschheit betrachtet und die Anzahl der existierenden Smartphones weltweit, kann man getrost darauf schließen, wie dumm und ignorant diese ist und sie sich dank Facebook, Apps und saemtlicher [...]

5. Nicht mitgegangen und trotzdem mitgehangen
dunnhaupt 18.01.2015
Die "Guten", die sich anfangs weigern, die jüngsten technologischen Errungenschaften zu akzeptieren, sind stets die hinterher hinkenden Verlierer, die dann am Ende doch noch nachzuholen suchen, was sie verpasst haben, [...]

Alle Kommentare öffnen

Seite 1 von 40

Ihr Kommentar zum Thema

Bitte melden Sie sich an, um zu kommentieren. Anmelden | Registrieren

Überschrift optional

Beitrag

Kommentar senden

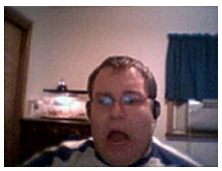
News verfolgen

Lassen Sie sich mit kostenlosen Diensten auf dem Laufenden halten: Hilfe

alles aus der Rubrik Netzwelt	Twitter |	RSS
alles aus der Rubrik Netzpolitik		RSS
alles zum Thema NSA-Überwachung		RSS

MEHR AUS DEM RESSORT NETZWELT

BEST OF WEB



Netz-Fundstücke: Was Sie im Internet unbedingt sehen müssen

SILBERSCHEIBEN

Das lohnt sich: Die besten CD- und DVD-Schnäppchen

BILDERWELTEN

Bessere Fotos: So holen Sie ganz einfach mehr aus Ihren Bildern raus

ANGEFASST

Gadget-Check: Handys und anderes Spielzeug in Matthias Kremps Praxistest

ANGESPIELT

Game-Tipps: Spiele für Computer und Konsole im SPIEGEL-ONLINE-Test

ÜBERSICHT NETZWELT ▶

▲ TOP

DER SPIEGEL

Inhalt
Abo-Angebote
Heft kaufen

Dein SPIEGEL

Inhalt
Abo-Angebote

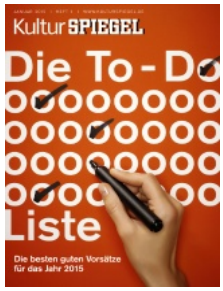
SPIEGEL GESCHICHTE

Inhalt
Abo-Angebote
Heft kaufen

SPIEGEL WISSEN

Inhalt
Abo-Angebote
Heft kaufen

KulturSPIEGEL



Inhalt
Abo-Angebote