Server der Telekom-Tochter T-Systems in Bördeland, Sachsen-Anhalt

Im Zeichen des Totenkopfs

Überwachung Nach streng geheimen Dokumenten der NSA und des britischen GCHQ versuchen die Dienste, das gesamte Internet auszuspionieren und zu kartografieren – bis zum letzten Computer oder Smartphone. Dafür zapfen sie auch die Deutsche Telekom und Netcologne an.

Bei der Wahl der Codenamen für ihre Geheimoperationen dürfen amerikanische und britische Agenten ihre Fantasie spielen lassen. Gern machen sie Anleihen in Flora und Fauna wie „Üble Olive“ und „Egoistische Giraffe“, manchmal lassen sie sich von Filmen made in Hollywood inspirieren. Ein Programm namens „Schatzkarte“ (Treasure Map) wird dann durch ein internes Geheimdienst-Logo geschmückt, das einen Totenschädel vor einer Windrose zeigt. Dessen Augenhöhlen schimmern dämonisch in Rot – in Anlehnung an Plakate der populären Spielfilmreihe „Pirates of the Caribbean“ mit Johnny Depp in der Hauptrolle.

Tatsächlich handelt es sich bei Treasure Map um alles andere als harmlose Unterhaltung, sondern um den Auftrag zu einem gewaltig anmutenden Raubzug in der digitalen Welt. Es geht darum, das Internet zu kartografieren – und zwar nicht nur seine großen Verkehrsverbindungen, beispielsweise Glasfaserkabel, sondern auch die Geräte, über die unsere Daten vermittelt werden, sogenannte Router.

Sogar jedes einzelne Endgerät, das irgendwo auf der Welt mit dem Internet verbunden ist, soll damit sichtbar gemacht werden können, jedes Smartphone, jedes Tablet und jeder Rechner. Eine solche Karte zeigt nicht nur einen Schatz, sondern Abermillionen.

Der atemberaubende Auftrag geht aus einer Treasure-Map-Präsentation hervor, die sich in den Unterlagen des ehemaligen Geheimdienstmitarbeiters Edward Snowden findet und die der SPIEGEL einsehen konnte. Darin werden die Analysten angewiesen: „Kartografiert das komplette Internet – jedes Gerät, überall, jederzeit.“

Mit Treasure Map lasse sich eine „interaktive Karte des globalen Internets“ herstellen, in „nahezu Echtzeit“, heißt es darin weiter. Auch Mitarbeiter der eng mit der NSA kooperierenden „Five Eyes“-Geheimdienste Großbritanniens, Kanadas, Australiens und Neuseelands können das Programm auf ihre Rechner laden und nutzen. Man kann es sich als eine Art Google Earth des globalen Datenverkehrs vorstellen, eine Luftaufnahme der digitalen Lebensadern des Planeten.

Neben der aktuellen Lagebeobachtung in den eigenen Netzen und jenen der „Gegner“ geht es bei Treasure Map um die „Planung von Computerattacken und Spionageaktionen“. Das Programm liefert damit so etwas wie die Generalstabskarte für den Cyberwar.

Über die Existenz von Treasure Map berichtete die *New York Times* im November. Wie brisant diese „Schatzkarte“ auch aus deutscher Perspektive ist, geht nun aus weiterem Material des Snowden-Archivs hervor, das der SPIEGEL auswerten konnte.

Treasure-Map-Grafiken zeigen nicht nur detaillierte Ansichten deutscher Kabel- und Satellitennetzwerke. Die Schaubilder machen den Spionen durch rote Markierungen auch klar, zu welchen Unternehmen und firmeneigenen Netzwerken sich die Five-Eyes-Geheimdienste nach eigener Darstellung bereits Zugänge verschafft haben. Besonders interessant sind dabei aus deutscher Perspektive zwei „Autonome Systeme“ (AS), beziehungsweise Netzwerke, mit rotem Kern – beschriftet mit Deutsche Telekom AG und Netcologne.

Die Legende zu den Grafiken erklärt die roten Punkte so: „Innerhalb dieser AS gibt es Zugangspunkte für die technische Überwachung.“ Im Klartext: Sie sind geknackt, hier sind die Spione drin.

Der Kölner Anbieter Netcologne betreibt ein eigenes Glasfasernetz und versorgt über 400 000 Kunden mit Telefon und Internet; das ehemalige Staatsunternehmen Telekom, an dem der Bund noch 31,7 Prozent der Anteile hält, gehört zu dem runden

FOTO: THOMAS TRUTSCHEL/PHOTOTHEK.NET

Dutzend internationaler Telekommunikationsunternehmen, die ein weltweites Netzwerk betreiben (Tier1-Anbieter). Allein in Deutschland versorgt die Telekom rund 60 Millionen Kunden mit Mobilfunk, Internet und Festnetzanschlüssen.

Aus der Logik der undatierten Treasure-Map-Unterlagen ergibt sich, dass die NSA und ihre Partner damit möglicherweise nicht nur die Leitungen und den darüber laufenden Verkehr bei den Firmen überwachen können, sondern auch Endgeräte von deren Kunden. Wo genau die NSA sich Zugang zu den Netzen der Firmen verschafft, geht aus den Grafiken nicht hervor; das dort rot markierte Netzwerk der Deutschen Telekom umfasst allein mehrere Tausend Router in aller Welt.

Das deutsche Unternehmen ist auch in den USA und Großbritannien auf dem Markt; zudem gehört die Telekom zum Betreiberkonsortium des Glasfaserkabelnetzes Tat-14, das über Großbritannien an die Ostküste der USA führt. „Der Zugriff ausländischer Geheimdienste auf unser Netz“, so ein Telekom-Sprecher, „wäre völlig inakzeptabel.“

Da es sich bei Netcologne um einen regionalen Anbieter handelt, ist es gut vorstellbar, dass die NSA oder einer ihrer Treasure-Map-Partner in diesem Fall von Deutschland aus in das System eingebrochen ist. Das wäre ein klarer Rechtsbruch und möglicherweise ein weiterer Fall für den Generalbundesanwalt, der bislang nur in der Sache des abgehörten Mobiltelefons der Bundeskanzlerin ermittelt.

Der SPIEGEL hat beide Unternehmen vor einigen Wochen mit einem GCHQ-Dokument konfrontiert, um ihnen Gelegenheit zu geben, Nachforschungen anzustellen. Die Sicherheitsabteilungen beider Firmen haben dies nach eigenen Angaben mit großem Aufwand getan, aber bisher keine verdächtigen Vorrichtungen in beziehungsweise Datenverkehr aus ihren Netzwerken festgestellt. Bei der Telekom und Netcologne handelt es sich nicht um die einzigen deutschen Unternehmen, die von den angloamerikanischen Geheimdiensten ausweislich ihrer eigenen Unterlagen erfolgreich gehackt wurden. Bereits im März hatte der SPIEGEL über den groß angelegten Angriff des britischen GCHQ auf die deutschen Satelliten-Teleport-Betreiber Stellar, Cetel und IABG berichtet (14/2014). Das Geschäftsmodell dieser Teleport-Firmen besteht darin, über Satellitenverbindungen Internet in entlegene Weltgegenden zu bringen. Alle drei Firmen, die bei Bonn (Cetel), in Ottobrunn bei München (IABG) und in Köln-Hürth (Stellar) residieren, sind in Treasure-Map-Darstellungen rot markiert, NSA und Co. verfügen also nach eigener Darstellung auch hier über interne „Collection Access Points“.

Der SPIEGEL hat auch elf in den Unterlagen entsprechend markierte ausländische Betreiber kontaktiert und um Stellungnahmen gebeten. Vier antworteten, sie hätten keine Auffälligkeiten feststellen können. „Wir wären sehr besorgt“, erklärte ein Sprecher des australischen Telekommunikationskonzerns Telstra, „wenn irgendeine ausländische Regierung versucht hätte, sich unautorisierten Zugang zu unseren globalen Netzwerken und unserer Infrastruktur zu verschaffen.“

Wie weit insbesondere der britische GCHQ und die NSA gehen, um ihre geheimen Karten vom Netz und von dessen Nutzern zu erstellen, zeigt das Beispiel des Hürther Unternehmens Stellar.

Das Dokument, das den Angriff auf den deutschen Mittelständler beschreibt, stammt aus dem „Netzwerk-Analyse-Zentrum“ des britischen GCHQ am Standort Bude an der Nordküste Cornwalls. Aufgelistet sind „entscheidende Mitarbeiter“ der Firma. Es gelte, sie zu identifizieren und dann zu „tasken“, heißt es in dem Dokument – „to task somebody“ ist im Slang der Dienste der Befehl zur zielgerichteten Überwachung, zum elektronischen Angriff. Neben dem Geschäftsführer Christian Steffen werden neun Mitarbeiter namentlich genannt.

Die Attacke zeigt damit auffällige Parallelen zum GCHQ-Angriff auf den halbstaatlichen belgischen Anbieter Belgacom, den der SPIEGEL im Sommer 2013 enthüllte; auch dort verschaffte sich die Abteilung „Netzwerk-Analyse“ der Briten über gehackte Mitarbeiterrechner tiefen Zugang in Belgacom-Netzwerke und die der Tochterfirma Bics – wo sie Router für Cyberangriffe präparierte.

Der SPIEGEL hat Stellar in Hürth bei Köln besucht und dem Geschäftsführer sowie drei der von den Briten aufgeführten Mitarbeitern die sie betreffenden Passagen vorgeführt. Ein Video des Besuchs ist über den QR-Code am Ende dieses Textes zu sehen, es ist vom Wochenende an auch bei SPIEGEL ONLINE abrufbar.

In dem GCHQ-Dokument erkannten Steffen und seine Mitarbeiter unter anderem eine Liste ihrer zentralen Server, darunter auch der Mailserver der Firma – den die Angreifer offenbar gehackt haben.

Zudem enthält das Dokument Spionageergebnisse wie eine interne Tabelle, welche Stellar-Kunden über welche Satellitentransponder versorgt werden. „Das sind Geschäftsgeheimnisse und sensible Informationen“, so der sichtlich schockierte Stellar-IT-Chef Ali Fares, der in dem GCHQ-Dokument namentlich als Zielperson aufgeführt ist.

Endgültig vorbei ist es mit der Gelassenheit der Stellar-Leute, als sie in den Geheimdienstunterlagen die Kennwörter für einen zentralen Server eines wichtigen Kunden sehen. Die Tragweite dieses Diebstahls sei immens, so Fares: Mit dieser Information könnten die Geheimdienste sogar gezielt Internetverbindungen zum Beispiel in Afrika abschalten. Zudem wäre es Fares zufolge damit möglich, Links zu fälschen und E-Mails zu manipulieren. Und eine für Geheimdienste besonders heiße Information könnte abgerufen werden:

TOP SECRET STRAP1

Employees:

Christian Steffen [redacted]@stellar-pcs.com or .de - CEO of Stellar DBS
[redacted]@stellar-pcs.com - Engineer
Stellar-DBS NOC noc@stellar-dbs.com - NOC
[redacted]@stellar-pcs.com
Christoph Sommer [redacted]@stellar-pcs.com
Ali Fares [redacted]@stellar-pcs.com
Richard Grave [redacted]@stellar-pcs.com
[redacted]@stellar-pcs.com
Simona Steffen [redacted]@stellar-pcs.com
[redacted]@stellar-pcs.com
Oliver Skaletz [redacted]@stellar-pcs.com

GCHQ-Geheimdokument mit Mitarbeiterliste der ausspionierten Telekommunikationsfirma Stellar in Hürth, Stellar-IT-Chef Fares

FOTO: MARCEL ROSENBACH/DER SPIEGEL

„Der Kunde XYZ sitzt in dem Punkt der Welt mit der Geolocation das und das."

Firmenchef Steffen kommentierte die Seite mit einem knappen „Fuck". Für ihn ist sie der endgültige Beleg für ein rechtswidriges Eindringen: „Der gehackte Server stand hinter unserer unternehmenseigenen Firewall. Daran kann man wirklich nur herankommen, wenn man vorher erfolgreich elektronisch bei uns eingebrochen ist." Die betroffene Firma ist aus anderen Gründen nicht mehr Kunde bei Stellar.

Nach möglichen Ursachen für das aggressive Vorgehen des EU-Partnerlands Großbritannien gegen seine Firma befragt, zuckt Steffen ratlos mit den Schultern. „Die Verkehre unserer Kunden laufen eben nicht über die herkömmlichen Glasfaserleitungen", sagt Steffen, „wir sind aus Sicht der Geheimdienste deshalb offenbar schwer zugängliches Gelände." Das gebe aber „niemandem das Recht, bei uns einzubrechen". Der Gründer und Geschäftsführer von Stellar will sich damit indes nicht zufriedengeben. „Ein solcher Cyberangriff ist nach deutschem Recht eindeutig strafbar", sagt er. „Ich will wissen, warum wir zum Ziel wurden und wie der Angriff auf uns genau erfolgt ist – schon um mich und meine Kunden vor einer Wiederholung zu schützen." Steffen bat vor sechs Wochen in einem Brief an die britische Regierung um Aufklärung, eine Antwort bekam er nicht. Die NSA und der GCHQ wollen die Voränge auch nicht kommentieren.

Die Sicherheitsabteilung der Telekom hat wichtige Router in Europa mit gerichtsfesten Methoden überprüft, bislang ohne Befund. Der Leiter der Sicherheitsabteilung, Thomas Tschersich, hält es für möglich, dass der rote Kern in Treasure Map durch Zugriffe auf das sogenannte Tat-14-Kabel, in dem die Telekom einen Frequenzbereich belegt, in Großbritannien und den USA zu erklären ist. Ende voriger Woche unterrichtete das Unternehmen das Bonner Amt für Sicherheit in der Informationstechnik über die SPIEGEL-Recherchen.

Es gibt ausweislich der geheimen Unterlagen noch weitere Daten aus Deutschland, die permanent zur Aktualisierung der globalen Schatzkarte beitragen. Von den insgesamt 13 Servern, welche die NSA weltweit eigens zu dem Zweck betreibt, den aktuellen Datenverkehr im Internet zu verfolgen, steht einer in Deutschland.

Wie die übrigen Maschinen arbeite das Gerät, das im Zeichen des Totenkopfs Daten ins geheime NSA-Netz schickt, dort „gut getarnt" und „unauffällig" in einem Datencenter.

Andy Müller-Maguhn, Laura Poitras, Marcel Rosenbach, Michael Sontheimer

Video: „Chokepoint" by Katy Scoggin and Laura Poitras

spiegel.de/app382014telekom
oder in der App DER SPIEGEL

Ständig unter Strom

Unternehmen Bislang ist der Aufstieg von Tesla eine Erfolgsstory, doch kann der Hersteller von Elektroautos auf Dauer gegen die Branchenriesen bestehen?

Elon Musk steht im Ruf, er könne Wunder vollbringen. Der Mann, der einst das Internetbezahlsystem PayPal entwickelte und dann für 1,5 Milliarden Dollar verkaufte, gilt als eine Art Messias unter den Unternehmern, als „neuer Steve Jobs" *(Wall Street Journal)*, als Mann, der „das Unvorstellbare in Realität verwandelt".

So zumindest kündigte der Gouverneur von Nevada, Brian Sandoval, den Unternehmer Musk kürzlich an, als der bekannt gab, dass er in diesem Bundesstaat eine „Gigafactory" bauen werde, die größte Batteriefabrik der Welt. Musk sagte: „Alle Batteriefabriken der Welt produzierten voriges Jahr weniger als die Gigafactory."

Wow. Das war mal wieder ein Auftritt, wie er typisch ist für Musk. Bescheiden sein mögen andere. Musk ist der Mann für das Spektakel. Mit einer seiner Firmen (SpaceX) schickt er Raketen ins All, mit einer anderen (Tesla Motors) produziert er ein Elektroauto, das sich in den USA besser verkauft als die Spitzenmodelle von Mercedes-Benz und BMW.

Ein Visionär ist Musk zudem. Irgendwann einmal will er Menschen zum Mars befördern. Zuvor möchte er noch einer neuen Form der Mobilität auf Erden zum Durchbruch verhelfen, den Elektroautos. Der Chef von Tesla Motors ist überzeugt: „Die Leute werden in einigen Jahren auf Benzinmotoren zurückblicken so wie wir heute auf Dampfmaschinen und sagen: Es war eine gute Zeit, aber sie ist vorbei."

Die Zahl der Menschen, die an Musk und seine Ideen glauben, ist groß, nicht zuletzt unter den Kapitalanlegern. Tesla Motors verkaufte im vergangenen Jahr gerade mal 22 000 Autos, erwirtschaftete einen Verlust von 55 Millionen Euro und wird an der Börse mit rund 27 Milliarden Euro bewertet. BMW brachte fast zwei Millionen Autos auf den Markt, wies einen Gewinn vor Steuern von acht Milliarden Euro aus und ist nur gut doppelt so viel wert wie Tesla (siehe Grafik).

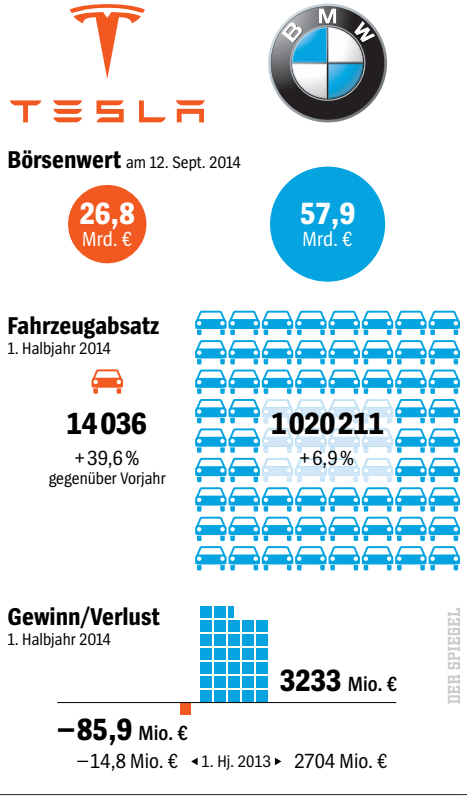
Die Börse spiegelt vor allem die Erwartungen an die Zukunft eines Unternehmens wider. So gesehen ist Tesla einer der größten Hoffnungswerte – mit entsprechend großem Absturzpotenzial.

Elon Musk mag mit seiner Einschätzung richtigliegen, dass sich das Zeitalter der Verbrennungsmotoren dem Ende zuneigt. Aber es ist noch völlig offen, ob künftig rein elektrisch betriebene Fahrzeuge den Verkehr beherrschen oder Hybridautos, die einen Elektro- und einen Verbrennungsmotor an Bord haben, oder Fahrzeuge, die von einer Brennstoffzelle angetrieben werden. Damit ist Tesla Motors, das nur auf den Elektroantrieb setzt, für die Anleger eine Wette auf die Antriebstechnologie der Zukunft.

Die Gefahren werden bislang noch überstrahlt vom Erfolg des Model S, das die gesamte Automobilindustrie blamiert. Da brachte ein ehemaliger Internetunternehmer mal eben ein Elektroauto der Luxusklasse auf den Markt, ein Modell, das die Etablierten für nicht realisierbar hielten und das viele Kunden nun einer S-Klasse von Mercedes-Benz, einem 7er von BMW oder einem A8 von Audi vorziehen.

VW-Boss Martin Winterkorn wollte wissen, wie dies geschehen konnte. Er ließ drei Exemplare des Tesla S kaufen, ausgiebig testen und anschließend auseinandernehmen. Danach sagte Winterkorn zu seinen Entwicklern: „Ein solches Auto hätte ich von Ihnen erwartet."

Dass dieses Fahrzeug nicht in Wolfsburg entwickelt wurde, sondern in Kalifornien, liegt vor allem an Musk. Er war mutiger als die angestellten Automanager, er agierte wie ein Unternehmer. Tesla wartete

Elektro-Hype beflügelt Aktie

Konzernzahlen von Tesla und BMW