



«Allsehendes Internet-Auge»: Durch «XKeyscore» haben US-Spione Zugriff auf jede beliebige Netzkommunikation – auch in der Schweiz.

Spionage

Wo sind die Lecks im Schweizer Datenbunker?

Von Urs Gehriger — Die Schweiz profitiert vom Snowden-Effekt. Wer seine Daten sichern will, bevorzugt unser Land als Server-Paradies. Doch das digitale Netzwerk hat etliche Schwachstellen, die der US-Geheimdienst als Einfallstor nutzen kann. Im Fokus stehen amerikanische IT-Firmen.

«Daten sind das neue Geld der Schweiz», titelte die *Financial Times* Anfang 2011. Ein strenges Datenschutzgesetz mache unser Land zum Server-Paradies, konstatierte das Wirtschaftsblatt. Offenbar hat sich seither der Trend vom Bank- zum Datengeheimnis rasant fortgesetzt. Insbesondere seit den Enthüllungen von Edward Snowden, der rigorose Spionagepraktiken des US-Geheimdienstes National Security Agency (NSA) aufgedeckt hat, verzeichnen Rechenzentren in der Schweiz einen veritablen Boom.

«Die Schweiz wird zum Datenbunker», berichtete die «Tagesschau» letzte Woche. Die Palette an Dienstleistungen mit hoher Nachfrage ist offenbar breit: E-Mail-Verkehr, Internetseiten-Hosting, externe Rechenleistung, Speicherung von Kundendaten und Geschäftsunterlagen. Der Beitrag endete mit einer Warnung: «Es ist durchaus möglich, dass die NSA versucht, auf solche Unternehmen Einfluss zu nehmen», mahnte Internet-Sicherheitsexperte Ueli Maurer von der Uni Zürich. Je mehr Informationen in der Schweiz gebunkert würden, desto stärker könnte sie ins Visier von Geheimdiensten geraten.

Könnte? Nach den Enthüllungen Snowdens muss davon ausgegangen werden, dass der US-Geheimdienst auch in der Schweiz längst am Absaugen ist. Wie systematisch die elektronische Spionagetechnik der Amerikaner ausgestaltet ist, zeigt die Spionagesoftware «XKeyscore», die der *Guardian* aus Snowdens Fundus vor einigen Wochen dokumentiert hat. XKeyscore ist eine Art allsehendes Internet-Auge. Es bietet weltweit Zugriff auf beliebige Netzkommunikation in Echtzeit. Was XKeyscore besonders auszeichnet: Es erlaubt unspezifische Suchvorgänge. Ein

Analyst kann mit Hilfe der Software auf bislang völlig unbekannte Internetnutzer aufmerksam gemacht werden, weil die sich plötzlich für bestimmte Themen interessieren oder ein bestimmtes Verhalten an den Tag legen.

Wie dicht XKeyscore eingesetzt wird, belegt eine Standortgrafik. Ein Teppich von Abschöpfungspunkten erstreckt sich über ganz Europa. Obwohl die Auflösung der im *Guardian* veröffentlichten Karte unscharf ist, wäre es vermessen, anzunehmen, die Schweiz sei eine Insel im Spionagenetzwerk der USA. Trotz Rund-um-die-Uhr-Überwachung in den boomenden Schweizer Datenzentren bietet das elektronische Netzwerk genügend Angriffsfläche für ausländische Nachrichtendienste.

Wer zu viel weiss, muss lügen

Logistisch betrachtet zählen erstens Mietleitungen und zweitens Netzwerkknoten zu den neutralen Stellen, an welchen US-Spione Daten abgreifen können. Bei Mietleitungen handelt es sich um Datenbahnen zwischen Firmen, Internet Providern et cetera und Internet-Knoten. Die Netzwerkknoten (sogenannte Internet Exchange Points) wiederum dienen als Austauschpunkte für den Datenverkehr des Web. An einem Knoten sind oft mehrere hundert Provider so zusammengeschlossen, dass sie den Datenverkehr zwischen ihren jeweiligen Netzen austauschen können.

«Ein Angreifer wird mit Vorzug den Weg des geringsten Widerstandes beziehungsweise des grössten Nutzens bei kleinstem Entdeckungsrisiko wählen», schätzt Informatikprofessor Hannes Lubich von der Fachhochschule Nordwestschweiz. Am einfachsten und sichersten ist

der Zugriff dort, wo eine Firma mit dem Angreifer kooperiert. Dabei fällt der Verdacht in erster Linie auf US-Firmen. Aufgrund der Dokumente, die Snowden enthüllt hat, ist bekannt, dass viele US-Unternehmen zum Datenklau verpflichtet respektive gezwungen werden. In Fachkreisen ist man deshalb weitherum überzeugt, dass der US-Geheimdienst auch in der Schweiz amerikanische Firmen als Einfallstor benutzt, um sich Zugang zu Internetdaten zu verschaffen.

In der Schweiz ist eine Reihe von namhaften US-Firmen vertreten, die in substanziellem Ausmass technische Infrastruktur anbieten. Dazu gehören Verizon Business, AT&T, Sprint, Cogent Communications, GTT und Level 3. Dabei handelt es sich um sogenannte Carrier, die Mietleitungen (hauptsächlich Glasfaser) vermieten.

Unter den US-Firmen mit Ableger in der Schweiz verfügt namentlich Equinix über eine herausragende Position. Equinix ist ein Gigant im globalen Datennetzwerk. Weil viele illustre Internetgesellschaften ihre Server bei Equinix stehen haben, ist das Unternehmen, gemessen am digitalen Datenverkehr, der weltweit zweitgrösste kommerziell betriebene Internet-Knoten. «Mehr als 90 Prozent aller Internet-Routen führen durch Equinix-Datenzentren», heisst es auf der Firmen-Website.

Der börsenkotierte Konzern hat letztes Jahr global 1,9 Milliarden Dollar umgesetzt und rund 750 Millionen Dollar investiert, vor allem in neue Rechenzentren, wie Marco Dottarelli, Generaldirektor von Equinix Schweiz, auf Anfrage erklärt. Weltweit verfügt die Firma über 99 Standorte. In der Schweiz sind es sieben, zwei in Genf und fünf in Zürich. In einem Zür-

cher Equinix-Datencenter wird auch der Server für den Aktienhandel der Schweizer Börse Six Swiss Exchange betrieben, wodurch diese zur schnellsten Börse der Welt aufgestiegen ist.

«Auch wir verspüren den Boom», sagt Dottarelli. «Negative Auswirkungen durch die Enthüllungen Snowdens habe man keine registriert. In den letzten achtzehn Monaten stelle man ungebrochen hohe Zuwachsraten von 20 Prozent und mehr fest, begünstigt durch die exzellenten Standortbedingungen in der Schweiz. Für die ausländischen Kunden seien ganz traditionelle Schweizer Werte wichtig. Dazu gehörten der hohe Qualitätsstandard, die niedrigen Steuern sowie die grosse Sicherheit. Auch die politische Stabilität und das strenge Datenschutzgesetz seien positive Standortfaktoren, so Dottarelli, der selbst Schweizer Staatsbürger ist.

Neben SwissIX und dem Cern stellt Equinix auch einen der drei Internet-Knotenpunkte in der Schweiz. Auch hier hat Equinix eine Ausnahmestellung. Ihr Knoten ist nicht nur der zweitgrösste, sondern auch der einzige in der Schweiz, der von einer US-Firma kontrolliert wird. «Natürlich sind Internet-Knotenpunkte für Aufklärungsdienste von grossem Interesse, schon alleine deshalb, weil sich dadurch der Aufwand für den Erhalt des Zugriffs auf die Daten mehrerer Provider stark reduzieren lässt», sagt Informatikprofessor Lubich.

In IT-Kreisen herrscht weitem der Verdacht, dass auch Equinix zu jenen Firmen gehört, die vom US-Geheimdienst dazu gezwungen werden, Daten für die nachrichtendienstliche Analyse zugänglich zu machen. «Eine der weltweit grössten Firmen, die durch die US-Regierung einfach ansprechbar ist – da ist praktisch garantiert, dass sie dazu angehalten wird, abzuhören», sagt ein IT-Experte, der über langjährige Berufserfahrung in und mit amerikanischen IT-Firmen verfügt.

Im Namen seiner Firma widerspricht Marco Dottarelli diesem Generalverdacht. «Equinix Schweiz untersteht der Schweizer Gesetzgebung», betont der Chef von Equinix Schweiz. «Wenn der US-Geheimdienst Zutritt zu unseren Rechenzentren verlangen und Equinix diesen gewähren würde, würden wir uns strafbar machen.» Von einer Abhöraktion seitens von US-Geheimdiensten im Firmenbereich von Equinix habe er keine Kenntnis, und er sei auch nie vom amerikanischen Nachrichtendienst diesbezüglich angegangen worden.

IT-Experten überraschen solche Dementis nicht. Entweder wüssten die Mitarbeiter von amerikanischen IT-Firmen gar nicht, dass der Geheimdienst bei ihnen Daten abschöpft, oder sie würden zu Stillschweigen verpflichtet. «Wer von den Tätigkeiten des Nachrichtendienstes weiss, wird genötigt, zu lügen», so ein Kenner der amerikanischen IT-Branche.

Auch Fredy Künzler, CEO des Winterthurer Internetproviders Inet7, sagt, er wäre nicht überrascht, wenn amerikanische Firmen wie Equi-

Globale Daten-Ströme der Firma Equinix

Mehr als 90 Prozent aller Internet-Routen führen durch Equinix-Datenzentren



Unter Verdacht: Equinix, ein Gigant im globalen Datennetzwerk.

nix in der Schweiz für den US-Geheimdienst Daten abschöpfen würden. «Ein Einfallstor für den US-Geheimdienst sehe ich jedoch nicht im Bereich der Datenspeicher oder Internet-Knotenpunkte», so Künzler, der von 2005 bis 2010 als Präsident der SwissIX Internet Exchange amtierte. «Der grösste Teil des digitalen Datenverkehrs läuft via sogenannte Private Network Interconnects (PNI).» Das sei auch einer der grössten Ertragsströme von Equinix.

Ratlosigkeit bei Experten und Behörden

Entlang der Glasfaserleitungen sei ein Abgreifen von Daten relativ problemlos (durch passives *Fiber-wiretapping*) machbar. «Ein Zugriff kann überall dort erfolgen, wo das Glasfaserkabel physikalisch hindurchführt.» Der Kunde merke davon nichts. «Der mit den Überwachungsbehörden kooperationswillige Glasfaserbetreiber kündigt einfach ein Wartungsfenster an, das Kabel wird umgesteckt, und der optische Abgriff ist implementiert.»

Bisher sind offiziell zwar keine Abhöraktionen bekannt. Dennoch drängen sich folgende Fragen auf: Welche Art Straftat würde eine Firma gemäss Schweizer Recht begehen, wenn sie aus der von ihr bereitgestellten Infrastruktur auf Schweizer Boden Daten zuhanden eines ausländischen Geheimdienstes abschöpfen würde? Mit welchen Konsequenzen müsste sie rechnen? Welche Instanz wäre zuständig, um eine entsprechende Untersuchung einzuleiten?

Eine Umfrage der *Weltwoche* bei Fachjuristen löste rundum konsterniertes Sinnieren aus. Auch die kontaktierten Experten in den Bundesämtern für Kommunikation und Informatik, der Melde- und Analysestelle Informationssicherung (Melani) sowie der Datenschutzbeauftragte erweckten nicht den Eindruck, dass über diese Thematik bereits abendfüllend diskutiert worden ist. Die aufgeworfenen Fragen seien sehr relevant, heisst es zwar. Gleichzeitig wird darauf verwiesen, dass es sich um eine komplexe Materie handle und die IT-Welt in rasantem Wandel begriffen sei.

Das Bundesamt für Justiz (BJ) seinerseits verweist auf die entsprechenden Artikel im Strafgesetzbuch (StGB). Wenn ein Host-Provider in der Schweiz angefallene oder gespeicherte fremde Daten unrechtmässig an eine ausländische Behörde weiterleite, mache er sich gemäss Artikel 271 strafbar. Zuständig für die Strafverfolgung sei die Bundesanwaltschaft, sofern die Tat gegen die Interessen der Eidgenossenschaft gerichtet ist. Dies gelte auch für den Fall, dass nicht direkt bundeseigene, sensitive Daten betroffen sind, sondern Datensätze von privaten Personen oder Firmen.

Allerdings liegt offenbar die Hürde für eine Strafverfolgung hoch: «Die Verfolgung von politischen Straftaten bedarf der Ermächtigung durch den Bundesrat», so das BJ. Und um ein entsprechendes Verfahren einzuleiten und durchzuführen, müssten zuerst auf Straftaten hinweisende Verdachtsgründe bekanntwerden.

Wie müsste denn ein solcher Verdachtsgrund beispielsweise aussehen? Reicht die von Snowden enthüllte Praxis der amerikanischen Geheimdienste, US-Firmen zum Datenklau zu zwingen, dafür aus? Die Antwort im BJ ist ein temperiertes Nein. «Die Verdachtsgründe müssen konkretisiert sein.» Ein solch hinreichender Tatverdacht könne sich aus zusätzlichen Hinweisen, zur Verfügung gestellten Dokumenten oder auch aus weiteren (Vor-)Abklärungen der Behörden ergeben.

Man kann sich täuschen, aber, gemessen an den Reaktionen in der Bundesverwaltung, wird man den Eindruck nicht los, dass bisher noch niemand die prominenten IT-Firmen amerikanischer Provenienz gebührend unter die Lupe genommen hat. Einerseits registriert man mit umgreifender Freude den Zustrom ausländischer Firmen in die vermeintlich sichere Daten-Hochburg Schweiz. Andererseits scheinen Politiker und Behörde die Augen vor den Enthüllungen über die NSA-Praxis zu verschliessen. Solange kein «Schweizer Snowden» auftaucht, haben amerikanische Datensauger in der Schweiz offenbar nichts zu fürchten. ○