Mut zur Lücke

Geheimdienste Der Bundesnachrichtendienst will Geld für das Wissen über Softwareschwachstellen zahlen, um Verschlüsselungen im Internet zu knacken. Er befördert damit einen dubiosen Markt.



Neue BND-Zentrale in Berlin

Der Mann aus New York war Stargast auf dem Cybersicherheits-Gipfel in Bonn: Ben Wizner, 42, Rechtsanwalt. Sein prominentester Klient ist der NSA-Whistleblower Edward Snowden.

Wizner, ein unaufgeregter Mann von eher kleiner Statur, richtete eine unmissverständliche Botschaft an die Experten aus Wirtschaft, Politik und Behörden. Mehr Sicherheit in der Informations- und Kommunikationstechnik könne es nur geben, wenn die Geheimdienste endlich ihr Treiben beendeten: Die Dienste würden Verschlüsselungsstandards unterwandern und Softwareschwachstellen ausnutzen – und damit die Risiken für sämtliche Nutzer des Netzes erhöhen.

Auch Klaus-Dieter Fritsche, 61, lauschte Wizners Ausführungen in der Zentrale der Deutschen Telekom am Anfang voriger Woche. Er ist als Staatssekretär im Kanzleramt zuständig für die Nachrichtendienste des Bundes. Die Berichte über deren Schalten und Walten bezeichnete Fritsche als maßlos übertrieben. Allerdings zitierte er seine Dienstherrin, Kanzlerin Angela Merkel: „Nicht alles, was technisch möglich ist, sollten die Nachrichtendienste auch machen."

Wo die Grenze verlaufen soll, führte Fritsche nicht näher aus. Womöglich aus gutem Grund: Der Bundesnachrichtendienst (BND) plant, seine technischen Fähigkeiten auszuweiten – und setzt auf problematische Methoden.

Teil seiner „Strategischen Initiative Technik" ist ein Projekt mit dem Codenamen „Nitidezza" (italienisch: Bildschärfe). Von 2015 bis 2020 will BND-Präsident Gerhard Schindler 4,5 Millionen Euro dafür ausgeben, verschlüsselte Signale zu knacken und auswertbar zu machen. Durch die digitale Aufrüstung soll der Auslandsnachrichtendienst „künftig auf Augenhöhe mit führenden westlichen Nachrichtendiensten kooperieren" können, heißt es in den geheimen Planungsunterlagen.



Behördenchef Schindler
4,5 Millionen Euro für „Nitidezza"

Dafür will der BND das Wissen um Schwachstellen in Computerprogrammen einkaufen. Ausdrücklich erwähnt wird in den Plänen die gängige Transportverschlüsselung SSL, die unter anderem große Shoppingportale und Banken für vermeintlich sichere Onlinegeschäfte nutzen.

Mit seinen bislang streng unter Verschluss gehaltenen Plänen findet sich der BND nun in einer durch die Snowden-Enthüllungen aufgeheizten Debatte: Schwächen ausgerechnet Geheimdienste, welche die Bürger schützen sollen, deren Sicherheit im Netz? Fördern sie durch ihre Neugier und den Kauf von Know-how über Softwareschwachstellen einen Markt, auf dem es vor windigen Gestalten wimmelt?

Manche Experten glauben, dass es den Umschlagplatz ohne die Geheimdienste in diesem Umfang nicht gäbe.

In der Vergangenheit waren es oft Hacker, die Sicherheitslücken in Software entdeckten. Handelte es sich um eher wohlmeinende Tüftler – in der Szene „White Hats" genannt –, so informierten sie die betroffenen Unternehmen, in der Hoffnung auf eine Belohnung.

Einige große Anbieter wie Microsoft, Google oder Facebook richteten sogar „Bounty"-Programme mit festen Prämienversprechen ein. Andere Hacker dagegen

FOTOS: KAY NIETFELD / DPA (O.); THOMAS TRUTSCHEL / PHOTOTHEK / GETTY IMAGES (U.)



Machthaber Ahmadinedschad (M.), Nuklearforscher 2008: Hunderttausend Computer infiziert

versuchten, Firmen mit dem Wissen um Schwachstellen zu erpressen.

Für die Unternehmen sind Einfallstore in ihre Programme, etwa sogenannte Zero Day Exploits, ein großes Sicherheitsproblem. Wer sie kennt, kann in die Programme eindringen, Informationen absaugen oder Systeme manipulieren. Auch das berüchtigte Computerschadprogramm „Stuxnet“ wurde 2009 und 2010 in Steuerungsanlagen des iranischen Atomprogramms eingeschleust, indem gleich mehrere Schwachstellen ausgenutzt wurden. Anschließend infizierte „Stuxnet“ weltweit rund hunderttausend Computer.

Geschäftsleute witterten spätestens seit diesem Zeitpunkt, dass sich mit dem Wissen über Sicherheitslücken riesige Profite erzielen lassen. Zu den Vorreitern gehört die französische Firma Vupen. Sie präsentiert sich als „Weltmarktführer für Schwachstellenforschung“ und verspricht, Regierungen und Geheimdiensten „bei kritischen Netzwerkoperationen zu helfen“. Gut im Geschäft sind zudem Firmen aus Malta, Kanada und den USA, etwa Netragard aus Massachusetts, deren Motto lautet: „Wir schützen Sie vor Leuten wie uns.“

Daneben hat sich ein Schwarzmarkt etabliert. Dort shoppen Autokraten und Diktatoren, „aber auch Konzerne, die das Wissen um eigene Schwachstellen einkaufen“, wie der Regierungsberater Sandro Gaycken, IT-Experte der Freien Universität Berlin, sagt. Die Nachfrage ist groß, wie die Entwicklung der Preise zeigt. Microsoft erhöhte 2013 die Belohnung für das Finden einer Schwachstelle in den eigenen Systemen auf bis zu 150 000 Dollar. Für Apple-Schwachstellen sollen auf dem Markt bis zu 500 000 Dollar aufgerufen werden, Tendenz steigend. Die *New York Times* spricht von einem „Goldrausch“.

Dass Geheimdienste die besten Kunden auf dem legalen wie dem illegalen Markt seien, wurde lange vermutet, ließ sich aber kaum beweisen. Im Zuge der Snowden-Enthüllungen wurde jedoch bekannt, dass der US-Geheimdienst NSA jährlich einen zweistelligen Millionenbetrag dafür ausgibt. 2012 soll er sogar ein Jahresabo bei Vupen abgeschlossen haben.

Laut Snowden-Dokumenten arbeiten die NSA und der britische Geheimdienst GCHQ daran, Verschlüsselung im Internet zu knacken. In Fachkreisen löste die Shoppingtour in der Halbwelt Empörung aus – zumal IT-Experten sich darüber einig sind, dass diese Lücken keineswegs nur von den eigenen Geheimdiensten ausgenutzt werden können. Niemand wisse, ob die windigen Händler ihre Kenntnisse nicht auch an gewöhnliche Onlinekriminelle oder andere Cyberspione verhökerten.

Der Erfinder des World Wide Web, Tim Berners-Lee, sprach von einem „erschreckenden und dummen“ Vorgehen der Sicherheitsbehörden. Bei der Bürgerrechtsorganisation Aclu heißt es: Jeder Versuch, Verschlüsselung zu schwächen, mache persönliche und geschäftliche Informationen verwundbar für Hackerangriffe von ausländischen Regierungen und Kriminellen.

Sogar jenes handzahme Prüfgremium, das im Auftrag von US-Präsident Barack Obama das Vorgehen der US-Dienste untersuchte, sah Handlungsbedarf. Es sei im Interesse der nationalen Sicherheit, Softwareschwachstellen zu eliminieren, statt sie zur Spionage einzusetzen, hieß es in seinen Handlungsempfehlungen an die US-Regierung. Ausnahmen seien nur in engen Grenzen akzeptabel.

Tatsächlich befinden sich NSA und GCHQ in einem Dilemma. Beide Dienste haben neben ihrer Spionagemission den Auftrag, kritische Infrastrukturen in der Heimat zu schützen – also gegen Angriffe von außen abzusichern. Gleichzeitig argumentierte zuletzt etwa FBI-Chef James Comey, die Sicherheitsbehörden seien darauf angewiesen, weiter und sogar verstärkt auf verschlüsselte Kommunikation zugreifen zu können.

Das BND-Projekt „Nitidezza“ zeigt, dass sich die Bundesregierung im gleichen Konflikt befindet. Gleichwohl scheint man nun entschlossen, Geld für das Wissen über Schwachstellen auszugeben – wenn auch die bislang für das Jahr 2015 eingeplanten 80 000 Euro weit unter den Summen der Amerikaner und Briten liegen. Auf Anfrage wollte sich der BND zu den Plänen nicht äußern.

Die Bundesregierung weiß, dass es sich um ein verfängliches Thema handelt, wie ein Vorgang aus dem Herbst 2013 zeigt. Die *Zeit* fragte beim Innenminister an, ob sein Ministerium oder eine ihm unterstellte Behörde Geschäftsbeziehungen zu Anbietern von „Zero Day Exploits“ unterhalte. Die Anfrage wurde intern als „sehr heikel“ eingestuft, die Antwort fiel ausweichend aus. Tatsächlich hatte das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu diesem Zeitpunkt einen Vertrag mit den Schwachstellen-Spürhunden von Vupen abgeschlossen.

Die französische Firma sorgte erst jüngst wieder für Empörung: Beiläufig gab Vupen bekannt, eine im März 2014 gemeldete Schwachstelle in Microsofts Internet Explorer bereits drei Jahre zuvor entdeckt zu haben. Ob Vupen sein Wissen in der Zwischenzeit zu Geld machte, ist nicht bekannt. Das BSI erklärte auf Anfrage, es habe „bis September 2014“ einen Vertrag mit Vupen gehabt. Zweck dieses Vertrages sei „ausschließlich der Schutz der Regierungsnetze“ gewesen. Das Amt unterhalte auch keine geschäftlichen Beziehungen zu anderen Anbietern von Sicherheitslücken.

Nach Ansicht von Michael Waidner, dem Leiter des Fraunhofer-Instituts für Sichere Informationstechnologie, ist das auch gut so. „Den Markt für Schwachstellen zu unterstützen ist aus staatlicher Sicht eine extrem schlechte Idee.“ Jede Lücke sei für die eigenen Bürger, Behörden und Unternehmen ein großes Risiko, sagt Waidner. „Das einzig Vernünftige, das man mit Schwachstellen tun kann, ist, sie zu beseitigen.“

Maik Baumgärtner, Marcel Rosenbach, Jörg Schindler

FOTO: ABACA / PICTURE-ALLIANCE / DPA