ZEIT ONLINE

IT-Sicherheit

Außenministerium will Internet sicherer machen, BND nicht

In der Bundesregierung wird gestritten, wie mit IT-Sicherheitslücken umzugehen ist: Der BND möchte sie heimlich nutzen; das Auswärtige Amt die Nutzung weltweit ächten.

Von **Kai Biermann**

9. Oktober 2017, 9:53 Uhr / 50 Kommentare

BND-Zentrale in Berlin © Hannibal Hanschke/Reuters

Das Auswärtige Amt versucht, die digitale Welt sicherer zu machen. Diplomaten des Außenministeriums arbeiten im Rahmen einer Expertengruppe der Vereinten Nationen daran, sogenannte Zero-Day-Exploits – Schadsoftware, die bislang unbekannte Sicherheitslücken ausnutzt – international zu ächten. IT-Sicherheitsexperten halten diesen Plan für notwendig und wichtig, doch stößt er auch auf heftigen Widerstand, vor allem in der eigenen Regierung. Denn der Bundesnachrichtendienst will Zero Days nutzen, um in andere Computersysteme einzudringen.

Zero Days sind so etwas wie die Biowaffen der digitalen Welt: Wer als erster Lücken und Mängel in Software oder Hardware entdeckt, kann sie mit Viren und Trojanern angreifen, gegen die es noch keine Gegenwehr, keine Impfung gibt, da nicht einmal die Hersteller von ihnen wissen. Sie haben null Tage Zeit – daher der Name – eine Abwehr zu entwickeln. Ohne die Chance auf ein Update aber sind die Opfer schutzlos, weswegen Kriminelle und Geheimdienste solche Zero Days für hohe Summen handeln [http://www.zeit.de/digital/internet/2014-11/bnd-zero-day-exploit-sicherheit].

Gleichzeitig wird genau deswegen die Nutzung solcher Lücken weltweit kritisiert. Denn werden die Probleme heimlich ausgenutzt, statt sie zu beseitigen, bleiben die Programme und Computer unsicher. Schließlich könnte auch jemand anderes die Schwachstellen finden, wodurch schlimmstenfalls Daten, Geld und im Zweifel das Leben von Millionen Menschen gefährdet werden könnte. Wie bedrohlich Angriffe auf die IT-Infrastruktur sein können, hat nicht zuletzt die Ransomware belegt [http://www.zeit.de/digital/internet/2017-05/hackerangriff-deutsche-bahn-ransomware-weltweit], mit der im Frühjahr weltweit Firmen, Krankenhäuser und Ministerien attackiert worden waren.

Eine Expertengruppe der Vereinten Nationen hatte daher mit deutscher Beteiligung bereits 2015 dringend empfohlen, dass alle Staaten IT-Sicherheitsprobleme, die sie entdecken, offenlegen und alle Betroffenen informieren (hier der Bericht der Gruppe als PDF [http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174]). Im englischen Original lautet der entsprechende Absatz: *"States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities, in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure"*. Die UN-Generalversammlung hat diese Empfehlung anschließend einstimmig verabschiedet. Denn die Welt ist abhängig von der Sicherheit ihrer IT-Infrastruktur.

Moratorium wie bei Giftgas oder Atomwaffen

Zero Days stellen eine Bedrohung der Internet- und der Computersicherheit dar, die so gravierend ist, dass niemand sie verwenden sollte, finden die Diplomaten. Das Internet sollte vielmehr sicher sein vor Zugriffen und Manipulationen. So wie der Einsatz von Giftgas, Streubomben oder Atomwaffen international geächtet ist, sollten sich daher alle Staaten der Welt verpflichten, auch Zero Days nicht auszunutzen. Wer Fehler und Mängel in Soft- und Hardware finde, müsse umgehend alle betroffenen Firmen und Länder informieren.

Bis ein solches Moratorium weltweit verhandelt und anerkannt ist, können Jahrzehnte vergehen. Die Empfehlung der UN sei aber bereits ein erster, wichtiger Schritt, heißt es beim Auswärtigen Amt. Sie sei zwar keine völkerrechtlich bindende Vereinbarung, wohl aber eine sehr starke politische Verpflichtung.

Doch Geheimdienste, auch deutsche, wollen sich dieser politischen Verpflichtung nicht unterwerfen. Vor allem der Bundesnachrichtendienst (BND) ist an Zero Days interessiert und möchte nicht darauf verzichten, sie zu kaufen und einzusetzen. Mehrere Millionen Euro sind dafür in seinem geheimen Etat reserviert. BND-Präsident Bruno Karl sagte gerade in einer öffentlichen

Bundestagsanhörung [http://www.zeit.de/politik/deutschland/2017-10/bnd-bfv-mad-geheimdienste-anhoerung-bundestag], es sei wichtig, dass der BND im Ausland aufklären könne und dazu seien auch Lücken in Informationssystemen geeignet. "Daher haben wir keinen Grund, solche Aufklärungsmöglichkeiten auszuschlagen."

KAI BIERMANN

Redakteur im Ressort Investigativ/Daten, ZEIT ONLINE

ZUR AUTORENSEITE [HTTP://WWW.ZEIT.DE/AUTOREN/B/KAI_BIERMANN/INDEX.XML]

Ein Verbot von Zero Days würde gleich mehrere Arbeitsbereiche der Sicherheitsbehörden erschweren. Zum Beispiel den sogenannten Staatstrojaner und die Quellen-Telekommunikationsüberwachung [http://www.zeit.de/digital/datenschutz/2017-06/staatstrojaner-gesetz-bundestag-beschluss]. Unter anderem das Bundeskriminalamt soll diese Spähprogramme nutzen, um Computer von Verdächtigen zu durchsuchen. Softwarelücken machen es einfacher, sie aus der Ferne zu installieren. Ohne sie müssten die Beamten versuchen, den Rechner des Verdächtigen in die Finger zu bekommen, was leichter entdeckt werden kann. Aber auch das Cyberkommando [http://www.zeit.de/digital/internet/2017-04/cyber-armee-bundeswehr-ursula-von-der-leyen] der Bundeswehr ist an Zero Days interessiert. Die Soldaten wollen daraus digitale Waffen entwickeln, um die Server von Angreifern attackieren zu können. Der BND schließlich will sie, um damit heimlich zu spionieren, ohne dass die ausgespähten Systeme Alarm schlagen.

Die Folge: In der Bundesregierung wird derzeit darum gestritten, wie mit bislang unbekannten Schwachstellen in Computersystemen umgegangen werden soll.

Offiziell äußert sich die Bundesregierung nur sehr vage zu diesem Streit und ihren Plänen. Der BND selbst schweigt, wie immer in solchen Fällen: Zu "geheimhaltungsbedürftigen Angelegenheiten" äußere man sich nur "gegenüber der Bundesregierung und den zuständigen parlamentarischen Gremien".

ZITiS soll über Nutzung von Zero Days künftig entscheiden

Doch auch gegenüber Parlamentariern ist die Auskunft nicht viel gehaltvoller. Die SPD-Bundestagsabgeordnete Saskia Esken hat gerade versucht, eine Antwort darauf zu bekommen. "Der (...) Kauf, die Entwicklung und die Nutzung von Schwachstellen und Exploits durch Strafverfolgungsbehörden ist ein für die Bundesregierung relevantes Thema", heißt es in der Antwort des Innenministeriums, die ZEIT ONLINE vorliegt. Man setze sich derzeit

"inhaltlich intensiv mit dieser Problematik auseinander". Und weiter: "Die Überlegungen sollen in einen Prozess münden, sind allerdings nicht abgeschlossen und bedürfen noch einer Konkretisierung."

Klarer wird die Auskunft nicht. Doch ist mit "ein Prozess" nach Informationen von ZEIT ONLINE das Verfahren gemeint, das die US-Regierung für den amerikanischen Geheimdienst NSA vorgeschrieben hat. Es heißt "Vulnerabilities Equities Process" (VEP). Die Regierung untersucht dabei, wie gefährlich eine technische Lücke ist und entscheidet anschließend, ob die eigenen Geheimdienste sie für ihre Zwecke ausnutzen dürfen, oder ob besser die Hersteller und Betreiber der Systeme gewarnt werden, damit sie sie schließen können. Bestehen Zweifel, solle eher für eine verantwortungsbewusste Offenlegung entschieden werden als dagegen, so die Idee.

Ein Nutzungsverbot ist das nicht. Es ist auch keine Garantie dafür, dass die Interessen der Techniknutzer wichtiger genommen werden als die Wünsche der Geheimdienste. In den USA wird VEP daher durchaus kritisiert. [https://epic.org/privacy/cybersecurity/vep/] Denn der Prozess der Auswahl ist nicht transparent. Und er sorgt für eine Verzögerung, die allein schon genügen kann, um riskante Lücken zu einer Bedrohung für sehr viele Menschen zu machen.

BND und Bundeswehr sollen beteiligt werden

Die Bundesregierung möchte sich bei ihrer Regelung trotzdem daran orientieren. Noch ist nicht ganz geklärt, wie genau der Prozess zur Bewertung der Lücken aussehen soll, doch scheint bereits klar zu sein, welche Behörde die Prüfung vornehmen wird: die neu gegründete ZITiS [http://www.zeit.de/digital/datenschutz/2017-08/zitis-eroeffnung-thomas-de-maiziere-bundeshacker], die Zentrale Stelle für Informationstechnik im Sicherheitsbereich. Auf die schriftliche Frage von ZEIT ONLINE, ob ZITiS sich mit Zero Days befassen wird, antwortete das Bundesinnenministerium: "ZITiS soll Expertise in allen technischen Fragestellungen mit Cyberbezug für die Sicherheitsbehörden bündeln." Das kann als Ja verstanden werden.

Da Zero-Day-Exploits so viele Bereiche betreffen, sollen an dem Bewertungsprozess aber auch der BND, das Bundesamt für Sicherheit in der Informationstechnik und die Bundeswehr beteiligt werden, ist von Beteiligten zu hören. Priorität solle dabei wie in den USA die Prävention haben, also die Sicherung der Systeme. Schließlich müsse ja auch die eigene IT sicherer werden.

Genau deswegen haben IT-Fachleute etwa aus dem Chaos Computer Club schon seit langer Zeit eine eindeutige Haltung zu Zero Days. Mit ihnen sollen "kritische Sicherheitslücken missbraucht werden, die auch anderen

Kriminellen einen Angriffspunkt bieten. Gleichzeitig wird es Bürgern und Unternehmen erschwert, sich vor technischen Angriffen auf persönliche Daten oder Geschäftsgeheimnisse zu schützen", so der CCC [https://www.ccc.de/de/updates/2014/0days-an-den-bnd]. Vor allem aber befeuere dieses Verhalten den Anreiz, aufgespürte Sicherheitslücken im Geheimen zu handeln, statt sie zu beseitigen.