Quelle: https://www.nzz.ch/international/dass-eine-gewisse-anzahl-von-angriffen-durchkommt-entspricht-der-technischen-realitaet-dieses-katz-und-maus-spiels-ld.1361895

Neue Zürcher Zeitung

«Dass eine gewisse Anzahl von Angriffen durchkommt, entspricht der technischen Realität dieses Katz-und-Maus-Spiels»

Cybersecurity-Experte Florian Egloff erklärt, warum der Hackerangriff auf die deutsche Regierung nicht unbedingt ein Zeichen mangelhafter IT-Sicherheit ist und wieso so wenig darüber bekannt ist.

Esther Widmann 1.3.2018, 15:32 Uhr

Das deutsche Innenministerium hat bestätigt, dass Informationstechnik und Netze des Bundes angegriffen wurden. Wie konnte das passieren?

Florian Egloff: Da muss man zunächst mal sagen: Man weiss ja im Moment noch sehr wenig über den Vorfall, und es ist nicht mal klar, wer alles davon betroffen ist. Klar ist bisher nur: Es hat einen Vorfall von grösserer Tragweite gegeben. Hypothetisch gesprochen, also falls es sich wie berichtet tatsächlich um ein Eindringen in das Datennetz der obersten Bundesverwaltung, den Informationsverbund Berlin-Bonn (IVBB), handeln sollte: Netzwerke, auch wenn sie nicht mit dem Internet verbunden sind, sind infiltrierbar.

Hacker können in einen vom Internet getrennten Bereich eindringen?

Ja. Erstens: Netzwerke, die vermeintlich vom Netz getrennt sind, sind es oft gar nicht. Schnittstellen werden übersehen oder sind trivial nicht erkennbar. Zweitens: Es gibt eine Lieferkette von Software und Hardware, und über die kann auch Schadsoftware ins System gelangen. Der Computerwurm Stuxnet zum Beispiel wurde über USB-Sticks verbreitet. Im vorliegenden Fall ist das aber unwahrscheinlich.

Die russische Gruppe APT28 wird als Hauptverdächtiger gehandelt.

Sollte der Angriff von APT28 ausgehen, wäre es nicht verwunderlich, dass das Auswärtige Amt betroffen ist. Man weiss, dass diese Gruppe, wie auch andere Cyber-Spionage Gruppierungen, diplomatische und Verteidigungseinrichtungen von Nato-Mitgliedsländern zum Ziel hat.

APT28 verschickt nach Erkenntnissen eines amerikanischen Sicherheitsunternehmens unverdächtige Mails mit Links und installiert so Malware auf dem Computer der Nutzer. Gibt es überhaupt irgendeinen Schutz vor dieser Methode?

Das ist eine gute Frage mit einer schwierigen Antwort. Die Antwort heisst: Ja, man kann sich schützen, aber der Schutzmechanismus kann umgangen werden. Oft ist der beste Schutz die Multi-Faktor-Authentifizierung, also die Identifikation des Nutzers mit mehr als einem Merkmal. Wichtig ist zudem, dass infiltrierte Computer schnell erkannt werden, damit der Angreifer sich nicht im Netzwerk festsetzen kann. Aber wir wissen nicht, ob solche Mails in diesem Fall involviert waren.

Warum gibt es denn überhaupt so wenig offizielle Informationen?

Wenn es einen Cyber-Angriff auf Regierungseinrichtungen gibt, wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) aktiv. Die wollen erst untersuchen, was los ist, wie gross das Ausmass des Vorfalls ist. Dann isolieren sie den Angreifer im System und entscheiden über das weitere Vorgehen. Das kann auch eine ganze Weile gehen. Zudem kann der Eindringling weiter beobachtet werden, um mehr herauszufinden. Die Öffentlichkeit nicht sofort zu informieren, gehört zu einer guten Reaktion auf einen Angriff. Man sollte deshalb nicht das BSI beschuldigen, die Öffentlichkeit zu spät informiert zu haben. Für mich ist eher erstaunlich, dass die Information offenbar ungewollt an die Öffentlichkeit gedrungen ist.

Darüber berichtet hat ja zuerst die Nachrichtenagentur DPA. Woher könnte die die Information denn bekommen haben?

Das kann man nicht sagen. Generell gilt: Je nach Ausmass, und wie die Reaktion auf den Vorfall betrieben wird, wissen mehr oder weniger Leute davon.

Welches Ziel könnten die Hacker denn haben? Wollen die Daten ausspähen oder Staatsgeheimnisse? In früheren Fällen hat APT28 erbeutete Informationen als Propaganda-Waffe genutzt.

Eine kriminelle Motivation ist nicht auszuschliessen, ist aber unwahrscheinlich, weil Kriminelle vor allem Daten abgreifen, die einen direkt verwendbaren monetären Nutzen hätten. Das spricht für einen staatlich gelenkten Angriff. Informationen zu Propaganda-Zwecken zu nutzen, ist allerdings keine häufige Taktik – auch bei den früheren Kampagnen von APT28 ist das nur in den wenigsten Fällen passiert. Die haben viele verschiedene Ziele infiltriert, nicht nur Regierungen.

Lässt sich überhaupt jemals herausfinden, welche Informationen mitgelesen oder abgegriffen wurden?

Das kommt extrem darauf an, in welcher Phase das BSI aktiv wurde und wie genau der Angreifer vorgegangen ist. Je nachdem, wann man die Attacke bemerkt, kann man die Bewegungen des Angreifers im Netzwerk verfolgen und sehen, worauf er zugreift.

Der Bundestag wurde ja 2015 in grossen Stil gehackt, die ganze IT musste ausgetauscht werden. Ist die deutsche Cybersecurity so schlecht?

Das wäre der falsche Schluss. Die meisten Organisationen können Opfer werden, auch die deutsche Regierung ist davon nicht befreit. Es ist logisch, dass sie ein interessantes Ziel ist, und deshalb ist sie auch stark exponiert. Dass dann auch eine gewisse Anzahl von Angriffen durchkommt, entspricht der technischen Realität dieses Katz-und-Maus-Spiels.

Florian Egloff ist Senior Researcher in Cybersecurity am Center for Security Studies (CSS) der ETH Zürich, einem Kompetenzzentrum für schweizerische und internationale Sicherheitspolitik.

Die Hackergruppe APT 28 – ein alter Bekannter auf dem Cyber-Schlachtfeld

Der Hackerangriff auf die deutsche Bundesverwaltung geht angeblich auf das Konto der Gruppe APT 28. Diese ist einschlägig bekannt – hinter ihr steht mit hoher Wahrscheinlichkeit der russische Geheimdienst.

Andreas Rüesch / 28.2.2018, 21:56

Hacker sind in das Computersystem der deutschen Regierung eingedrungen – der Angriff dauerte bis Mittwoch

Auch wenn das Ausmass der Cyberattacke noch unklar ist, wirft dies ein schlechtes Licht auf die IT-Sicherheit der deutschen Regierung. Das Datennetz des Bundes galt bisher als besonders sicher. Der Angriff ging vermutlich von Russland aus und soll auch andere EU-Länder betreffen.

Christoph Eisenring, Berlin / Christian Weisflog / 1.3.2018, 10:04

Newsletter International

Bleiben Sie mit unserem Newsletter auf dem Laufenden. Die internationalen News mit Analysen und Reportagen von NZZ-Korrespondenten aus aller Welt erhalten Sie Montag bis Freitag um 17 Uhr in Ihr Postfach. Hier können Sie sich mit einem Klick kostenlos anmelden.

Copyright © Neue Zürcher Zeitung AG. Alle Rechte vorbehalten. Eine Weiterverarbeitung, Wiederveröffentlichung oder dauerhafte Speicherung zu gewerblichen oder anderen Zwecken ohne vorherige ausdrückliche Erlaubnis von Neue Zürcher Zeitung ist nicht gestattet.