Diebesgrüße aus Moskau

IT-Sicherheit Die Hacker, die den Bundestag attackierten, greifen weitere Regierungen von Nato-Ländern an. Analysten glauben: Dahinter stecken Russen.

Die E-Mail hatte einen ehrenwerten Absender, es gab keinen erkennbaren Grund, ihr zu misstrauen. Am 30. April landete die Nachricht mit der Endung „un.org“ in den Postfächern deutscher Bundestagsabgeordneter; sie stammte vermeintlich von den Vereinten Nationen. Wer jedoch den Link zu einem „News Bulletin“ der Uno anklickte, öffnete unwissentlich Cyberspionen Tür und Tor zum digitalen Nervensystem des Bundestags. In mehr als einem Dutzend Abgeordnetenbüros tauchte die Mail im Postfach auf.

Auf diese banale Weise begann der bislang offenbar schwerste Hackerangriff auf ein deutsches Verfassungsorgan. Er führte, nach seiner Entdeckung, zu heftigen Debatten über den Schutz der Netze im Berliner Regierungsviertel. Und darüber, wie arg- und ahnungslos Abgeordnete, die auch Gesetze zur IT-Sicherheit beschließen, bisweilen mit eigenen Computern und Daten umgehen. Die Aufklärung der Hintergründe der Attacke gestaltete sich unterdessen zäh.

Nun liegt der Abschlussbericht des Bundesamts für Sicherheit in der Informationstechnik (BSI) vor, der teilweise als „vertraulich“ eingestuft ist. Er beschreibt nicht nur, wie virtuos die Hacker ihren Angriff inszenierten. Er wirft auch ein peinlich grelles Licht darauf, wie dürftig der Bundestag seine Kommunikationssysteme in der Vergangenheit geschützt hat.

Die mutmaßlichen Urheber des Angriffs, eine Hackergruppe namens „Sofacy“ oder „APT28“, sind bereits seit fast zehn Jahren aktiv. Aus dem BSI-Bericht geht hervor, dass die Gruppe mindestens zwei osteuropäische Regierungen attackierte, bevor der Bundestag ihr Ziel wurde. Parallele Analysen der russischen IT-Sicherheitsfirma Kaspersky Lab ergaben, dass Sofacy seitdem ihr Arsenal verfeinert und die Zahl der Angriffe erhöht hat. In diesem Jahr hat die Gruppe demnach mehrere weitere Regierungen ins Visier genommen.

In Berlin gruben sich die Angreifer seinerzeit in Windeseile von den befallenen Rechnern der Parlamentarier aus weiter durchs Netz. Am Ende fanden sie Zugang zu 14 Servern des Parlakom-Netzes, darunter auch der Hauptserver, auf dem sämtliche Zugangsdaten zum Bundestag gespeichert sind.

Für Hacker ist das ein Glücksfall, für Betroffene der größte anzunehmende Unfall. Es ist, als ob ein Bankräuber den Generalschlüssel für sämtliche Räume und Tresore eines Geldhauses in Händen hielte.

Mitte Mai, kurz nachdem der Angriff bekannt geworden war, hatten die Hacker bereits 12,5 Gigabyte an Daten erbeutet. Was folgte, war ein wochenlanger Hickhack über die Frage, ob das Netz sofort heruntergefahren werden müsse oder noch Zeit bis zur Sommerpause sei. Und darüber, wer helfen dürfe, den Schaden zu beseitigen: nur der auf Autonomie pochende Bundestag selbst? Die Fachleute des BSI? Oder gar der Verfassungsschutz? Derweil flossen weitere 3,5 Gigabyte an Daten ab.

Das BSI mühte sich seither, die Spuren der Schadcodes und Angriffsinstrumente mit so kryptischen Namen wie „Coreshell“ und „Xtunnel“ nachzuverfolgen, parallel machten Mitarbeiter von Kaspersky Lab in Moskau dasselbe. In den vergangenen Monaten beobachteten diese erneut massive Attacken der Gruppe, gegen Regierungen anderer Nato-Staaten, aber auch gegen Rüstungsfirmen, insbesondere aus der Luft- und Raumfahrtbranche.

Die Gruppe arbeite hoch professionell, arbeitsteilig mit diversen Teams und verfüge über erhebliche personelle und finanzielle Mittel, sagt Kaspersky-Analyst Costin Raiu. „Allein im vergangenen Jahr hat Sofacy fünf verschiedene Zero Days eingesetzt, das ist ein Rekord.“ „Zero Day“-Attacken machen sich Wissen um bislang unbekannte Schwachstellen in Computerprogrammen zu eigen. Die Schlüssel für solche Hintertüren werden auf Graumärkten gehandelt, auf denen sich auch Geheimdienste tummeln. Sofacy attackierte in der Vergangenheit unter anderem Ziele in Frankreich, Großbritannien, Griechenland und Belgien.

Die Gruppe verfolge offenbar langfristige Aufklärungsziele, urteilt Raiu, von finanziellen Interessen sei bislang nichts bekannt. All das spreche für eine „state-sponsored attack“, also einen Staat als Urheber. Kaspersky Lab hat zudem festgestellt, dass die Schadsoftware augenscheinlich auf Rechnern mit russischen Spracheinstellungen programmiert wurde.

Im Fall des Bundestags stellte das BSI quasi nebenbei fest, dass sich auch gewöhnliche Cyberkriminelle für die Abgeordneten interessieren. Bei der Spurensicherung im Parlakom-Netz stieß die Behörde auf etwa hundert Banking-Trojaner – kleine digitale Schnüffler, dazu angetan, die Bankdaten von Volksvertretern auszukundschaften, um ihre Konten plündern zu können.

Wie es scheint, haben sich die Abgeordneten mit arglosen Klicks transparenter gemacht, als ihnen für gewöhnlich lieb ist.

Maik Baumgärtner, Sven Röbel, Marcel Rosenbach, Jörg Schindler

KATRIN DINKEL / IMAGETRUST

Bundestagsgebäude in Berlin: Transparenter als gewollt