2018/10 Inland

https://jungle.world/artikel/2018/10/ein-netz-voller-baeren-und-schlangen

Ist eine russische Hackergruppe verantwortlich für den Angriff auf Computernetze deutscher Regierungsstellen?

Ein Netz voller Bären und Schlangen

Von **Enno Park**

Hacker sind in das Kommunikationsnetz der Bundesregierung und anderer Behörden eingedrungen. Die Verantwortlichen zu ermitteln, gestaltet sich schwierig.

Ein anonymer Informant aus dem Bundesinnenministerium hatte das monatelang gehütete Geheimnis kürzlich den Medien verraten. Am 28. Februar bestätigte das Bundesinnenministerium, dass der »Informationsverbund Berlin-Bonn« (IVBB) gehackt worden sei. Dieses Netzwerk wird von dem Ministerium verwaltet und verbindet Bundesrat, Kanzleramt, Ministerien, Rechnungshof und verschiedene andere Institutionen miteinander. Zunächst klingt das wie der größte anzunehmende IT-Unfall, allerdings dient der IVBB nur dem Informationsaustausch der Behörden untereinander, wobei verschlüsselt kommuniziert wird. Jede ans IVBB angeschlossene Behörde verwendet intern ein eigenes Netz. Ob und in welchem Ausmaß die Hacker Daten einzelner Behörden erbeuten konnten, ist völlig unklar. Bisher bestätigte lediglich das Außenministerium, dass die Hacker Zugriff auf einige wenige Dokumente gehabt hätten. Um welche Informationen es sich handelt, ist nicht bekannt.

Neben dem Außenministerium nennen verschiedene Medien das Verteidigungsministerium sowie die Stiftung Wissenschaft und Politik als Angriffsziele. Letztere berät die Bundesregierung und den Bundestag in außenpolitischen Fragen. Die Hacker nutzten offenbar die Bundesakademie für öffentliche Verwaltung als Einstiegspunkt. Einige Medien nennen in diesem Zusammenhang auch einen Angriff auf das in Bonn ansässige paralympische Komitee. Einem Delegierten soll in einem Moskauer Hotel über ein gehacktes W-Lan eine Schadsoftware auf sein Smartphone gespielt worden sein. In welchem Zusammenhang dies allerdings mit dem Hack des IVBB stehen soll, bleibt unklar.

Die Mehrheit der Medien verbreitete von Beginn an, dass die Spezialeinheit APT28 des russischen Militärgeheimdienstes hinter dem Angriff stecke, die auch unter dem Namen Cozy Bear bekannt ist. Die US-amerikanische Sicherheitsfirma Fire Eye verfolgt seit längerem das Vorgehen von APT28. Der Leiter der Abteilung für Spionageanalyse der Firma, Benjamin Read, wird in zahlreichen deutschen Medien mit der Aussage zitiert, dass der Angriff auf das IVBB zu einer größeren und längerfristigen Angriffswelle Russlands auf verschiedene Regierungen der EU und anderer Staaten gehöre. Die Sache hat nur einen Haken: Bisher gibt es keine öffentlich bekannten Belege oder Anhaltspunkte, die auf APT28 hinweisen, weshalb Fachleute vor

vorschnellen Mutmaßungen warnen. Die russische Regierung hat die Anschuldigungen dementiert.
Mittlerweile wird eine Hackergruppe für den Angriff verantwortlich gemacht, die unter dem Namen Snake, Turla oder Uroburos bekannt sein und in enger Verbindung zur russischen Regierung stehen soll. Auch bei dieser Meldung gibt es ein Problem: Snake beziehungsweise Turla oder Uroburos ist keine Hackergruppe, sondern eine Software, mit der man in fremde Computersysteme eindringen kann. Wer immer sich eine Kopie des Programms besorgt, kann es benutzen. Ob also Russland, eine andere Regierung oder nichtstaatliche Gruppen hinter dem Hack stehen, lässt sich derzeit nicht sagen.

Mehr ist über die Angriffe bisher nicht bekannt. Der Bundesnachrichtendienst und der Verfassungsschutz haben mitgeteilt, an dem Vorfall »mit hoher Priorität und erheblichen Ressourcen« zu arbeiten, nannten aber keine Details. Der Hack sei bereits im Dezember entdeckt worden. Die Angreifer seien bis zuletzt noch im System unterwegs, aber »unter Kontrolle« gewesen. Offenbar wollten die deutschen Geheimdienste sie nicht gleich auffliegen lassen, um herauszufinden, was die Hacker im Netz anstellen. Das ist bei solchen Angriffen eine übliche Vorgehensweise, bei der die monatelange Geheimhaltung durchaus Sinn ergibt. Dennoch sind die Parlamentarier aus den einschlägigen Fachausschüssen des Bundestags verärgert darüber, erst aus den Medien von der Attacke erfahren zu haben. Doch auch hier ergibt die Geheimhaltung Sinn. Denn als der Bundestag 2015 gehackt wurde, war das oberste Ziel der Hacker offenbar, an Informationen von Abgeordneten zu gelangen, die im Vertrauensgremium zur Kontrolle der deutschen Geheimdienste sitzen.

Wegen der dürftigen Faktenlage kann derzeit niemand sagen, wie sich solche Hacks in Zukunft verlässlich verhindern lassen. Der IVBB und die Regierungssysteme sind wesentlich besser abgesichert als das Bundestagsnetz. So fordert auch Frank Rieger vom Chaos Computer Club eher vage, dass sämtliche Systeme von Grund auf neu aufgebaut werden müssten, um ein hinreichendes Maß an Sicherheit herzustellen. Eines ist allerdings klar: Für den Hack wurden höchstwahrscheinlich sogenannte zero-day exploits verwendet. Das sind Sicherheitslücken in Programmen und Betriebssystemen, die den Herstellern noch nicht bekannt sind und die somit auch noch nicht geschlossen werden können. Alle großen Geheimdienste sammeln solche exploits, ohne die Softwarehersteller zu informieren, um damit selbst in fremde Rechner eindringen zu können. Sie riskieren so permanent die Sicherheit der eigenen und der von der Bevölkerung genutzten Systeme.