Süddeutsche Zeitung
SZ.de Zeitung Magazin

6. März 2018, 14:53 Uhr IT-Sicherheit

So schleusten die Hacker Daten aus dem Auswärtigen Amt

Über E-Mails kommunizierten die Hacker mit der Schadsoftware. (Symbolbild) (Foto: Shutterstock/SZ-Grafik)

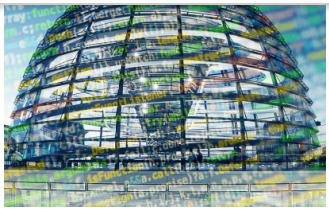
- Über das Mailprogramm Outlook ist es Hackern gelungen, Daten aus den Regierungsnetzen zu kopieren.
- Das Vorgehen beschreibt ein IT-Sicherheitsforscher als "elegant, weil es unauffällig ist."
- Die Technik deutet auf eine Gruppe von Hackern hin, die nach Ansicht von Sicherheitsbehörden im Auftrag der russischen Regierung agieren soll.

Von Hakan Tanriverdi

Im Fall des Hackerangriffs auf die Bundesregierung ist nun klar, wie es den Angreifern gelungen ist, Daten aus dem internen Netzwerk in ihren Besitz zu bringen. Die Angreifer nutzten nach Informationen der *Süddeutschen Zeitung* das Mailprogramm Microsoft Outlook und verstecken codierte Befehle in einem Mail-Anhang.

Die verdächtigte Hacker-Gruppe Turla setzt eine Methode ein, die IT-Sicherheitsforschern zufolge in dieser Form von niemandem sonst verwendet wird. Sie ist also vergleichbar mit einem Fingerabdruck, der am Tatort gefunden wurde. Die Gruppe agiert nach Einschätzung vieler Sicherheitsbehörden und IT-Sicherheitsforschern im Auftrag der russischen Regierung.

IT-Sicherheitsfirmen, die die Vorgehensweise von Hackergruppen genau verfolgen, veröffentlichen Berichte, in denen sie ihr Wissen teilen. Es kommt vor, dass Hackergruppen daraufhin ihre Vorgehensweise ändern. Deshalb behalten Firmen sensible Informationen oft für sich, mit denen sie Angreifer identifizieren können.



Spähaktion

Auch Staaten der ehemaligen Sowjetunion sowie Länder Südamerikas und im Baltikum sollen Ziele gewesen sein. In deutschen Netzen hatten die Hacker wohl Zugriff auf 17 Rechner. *Von Reiko Pinkert und Hakan Tanriverdi, Berlin* **mehr ...**

Elegant und unauffällig

Der Weg, den die Turla-Hacker über Outlook nahmen, wurde in dieser Form bisher öffentlich noch nicht beschrieben. Das soll ausschließen, dass andere Gruppen diese Aktion der Turla-Hacker imitieren. Deren Vorgehen beschreibt einer der IT-Sicherheitsforscher als "elegant, weil es unauffällig ist".

Im Auswärtigen Amt waren insgesamt 17 Rechner infiziert. Auch eine Woche nach Bekanntwerden des Hacker-Angriffs auf das Bundesnetz hält sich die Regierung bedeckt, wenn es darum geht, öffentlich einen Schuldigen zu benennen. Auf Nachfragen reagierte das Bundesinnenministerium bislang nicht. Der Weg der Daten über Outlook wäre eine Spur, die auch unabhängig überprüft werden könnte, etwa wenn die Schadsoftware sich auf öffentlichen Webseiten wiederfindet.

So gingen die Hacker vor

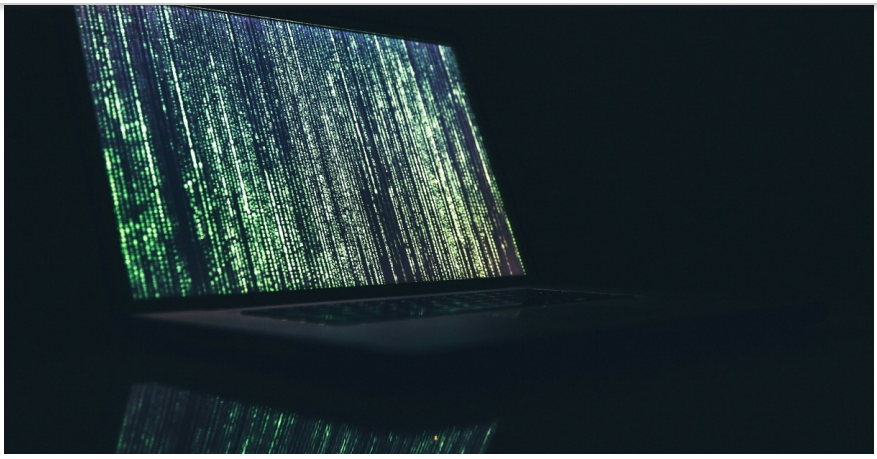
Unbemerkt mit Outlook zu kommunizieren, ist auf vielen Wegen möglich. Die Hacker verwenden das Mailprogramm, um mit ihrer Schadsoftware zu interagieren, wenn die sich bereits innerhalb des angegriffenen Netzwerkes befindet.

So schicken die Turla-Hacker eine E-Mail an einen Rechner, den sie bereits mit Schadsoftware infiziert haben. Denn nach der Infektion müssen die Angreifer die für sie interessanten Daten auch irgendwie aus den abgeschlossenen Netzen herausbekommen. Hackergruppen versuchen in der Regel, über das Internet verschlüsselte Verbindungen zu einem Server aufzubauen und die Daten aus dem geschützten Bereich direkt dorthin zu schicken. Über diese Infrastruktur kommunizieren sie von außen mit ihrer Schadsoftware. In den Netzen des Auswärtigen Amtes sollen nach SZ-Informationen solche Verbindungen aber blockiert werden. Der einzige Weg nach draußen führt demnach über Mails. Also dürfte auch die Kontrolle der Schadsoftware über Mails gelaufen sein.

Die Mail, die die Angreifer an den schon infizierten Rechner schicken, enthält einen Anhang. Solche Anhänge werden von Outlook heruntergeladen, ohne dass der Nutzer mit ihnen interagieren muss. In diesen Dokumenten - es ist unklar, um welchen Typ es sich handelt, etwa PDF oder Doc - sind versteckte Informationen enthalten. Das sind Befehle wie: "Hacke den nächsten Rechner, verschicke ein Dokument!"

Das heißt: Die Schadsoftware, die sich auf dem infizierten Rechner befindet, bleibt zunächst passiv. Sie scannt das Postfach und wartet auf Instruktionen. Eine Sprecherin von Microsoft wollte den Fall auf Nachfrage "zu diesem Zeitpunkt nicht kommentieren."

Die Personen, mit denen die *SZ* über die Schadsoftware gesprochen haben, wollen anonym bleiben, da der Hack der Bundesregierung "ein verdammtes Pulverfass" sei.



Diese Gruppe soll hinter dem Bundeshack stecken

Bei den Hackern von "Turla" handelt es sich um eine der technisch versiertesten Gruppen, die Verbindungen zur russischen Regierung haben sollen. *Von Hakan Tanriverdi* **mehr...**

zur Startseite 〉

Diskussion zu diesem Artikel auf: Rivva
Themen in diesem Artikel: Hacker Bundesregierung IT-Sicherheit

Mehr zum Thema

IT-Sicherheit
Hackerangriff gegen Regierung war Teil weltweiter Spähaktion

IT-Sicherheit
Diese Gruppe soll hinter dem Bundeshack stecken

IT-Sicherheit
Schläfer im Datennetz

Cyber-Angriff
Regierung ließ russische Hacker monatelang gewähren

IT-Sicherheit
Hacker-Angriff auf Außenministerium

Leser empfehlen im Ressort Digital

1 Grünen-Chef Habeck zur AfD **"Die Grenze ist an vielen Stellen überschritten"**

2 Silvio Berlusconi **Der Auferstandene**

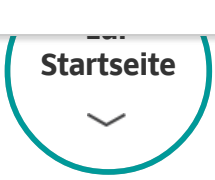
3 Islamfeindlichkeit in Deutschland **2017 gab es mindestens 950 Angriffe auf Muslime und Moscheen**

Meistgelesene Artikel

1 Grünen-Chef Habeck zur AfD **"Die Grenze ist an vielen Stellen überschritten"**

2 Paris-Pleite in der Champions League **Das viele Geld geht in Rauch auf**

3 Welthandel **Donald Trump, Meister der falschen Argumente**


Startseite