Bundesamt
für Sicherheit in der
Informationstechnik

Cyber-Angriff auf den Bundestag abgewehrt: Stellungnahme des BSI

Ort Bonn
Datum 29.03.2017

Nach dem Cyber-Angriff auf den Deutschen Bundestag im Jahr 2015 wurden einige Schutzfunktionen, die das BSI für die Regierungsnetze etabliert hat, vom Deutschen Bundestag auch für dessen eigene Netze übernommen. Seit Anfang Januar 2017 ist das BSI als die nationale Cyber-Sicherheitsbehörde aufgrund von Auffälligkeiten im Netzwerkverkehr des Deutschen Bundestags im engen Austausch mit dem Bundestag. Auf Wunsch des Deutschen Bundestags hat das BSI diese Auffälligkeiten im Netzwerkverkehr analysiert. Die technischen Analysen sind abgeschlossen. Die Webseite der Jerusalem Post war manipuliert und hat auf eine schädliche Drittseite verlinkt. Im Rahmen der Analysen hat das BSI jedoch keine Schadsoftware entdeckt, auch Infektionen sind dem BSI nicht bekannt.

BSI-Präsident Arne Schönbohm erklärt dazu: "Cyber-Angriffe mithilfe von manipulierten Webseiten gehören zum Standard-Repertoire von Cyber-Angreifern und sind aus technischer Sicht nichts Besonderes. Das BSI geht davon aus, dass die Abwehrmechanismen des Deutschen Bundestags die Zugriffe auf diese Webseite detektiert und abgefangen haben. Der Angriff wurde somit abgewehrt."

Schutz der Regierungsnetze

Die Manipulation von Webseiten ist ein weit verbreitetes Mittel, Cyber-Angriffe durchzuführen. Angreifer verstecken dazu schädliche Programme auf Webseiten, die sich durch eine Sicherheitslücke beim Besuch der Webseite selbst auf den Rechner des Anwenders aufspielen. Häufig wird derartige Schadsoftware verwendet, um Daten auszuspionieren oder Schaden auf dem Zielrechner zu verursachen. Eine der Hauptursachen für diese sogenannten Drive-by-Angriffe sind schädliche Werbebanner. Diese werden von unbekannten Dritten bereitgestellt oder von Agenturen vermarktet und werden häufig ohne Überprüfung oder Qualitätskontrolle in eine Webseite eingebunden. Auf diese Weise werden auch populäre und ansonsten gut abgesicherte Webseiten Ausgangspunkt von Cyber-Angriffen.

Kernaufgabe des BSI als nationale Cyber-Sicherheitsbehörde ist die Abwehr von Gefahren für die IT des Bundes. Eine Schutzkomponente im Regierungsnetz blockiert daher derartige Angriffsversuche, indem ausgehende Netzverbindungen auf infizierte Webseiten, die Schadprogramme verteilen sowie Verbindungsversuche von bereits aktiven Schadprogrammen zu Kontrollservern verhindert werden. Allein in der ersten Jahreshälfte 2016 wurden im Regierungsnetz mit dieser Methode täglich rund 3.600 Verbindungsversuche zu Schadcodeservern verhindert.

Mehr Informationen zu Drive-by-Angriffen sowie zu den Schutzmaßnahmen hat das BSI im "Bericht zur Lage der IT-Sicherheit in Deutschland 2016" veröffentlicht.

Pressekontakt:

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
53133 Bonn
Telefon: +49 228 99 9582-5777
Telefax: +49 228 99 9582-5455
E-Mail: presse@bsi.bund.de

Seite teilen

© Bundesamt für Sicherheit in der Informationstechnik