Informationen zum Cyberangriff auf den Bundestag – hier: Abschlussbericht BSI
Bezug: Beauftragung des BSI am 15.5.2015
Datum: 03.11.2015

Ausgangslage

Anfang Mai 2015 informierte das Bundesamt für Verfassungsschutz den Deutschen Bundestag und das Bundesamt für Sicherheit in der Informationstechnik (BSI) über Hinweise, dass mindestens zwei Rechner aus dem Netz des Deutschen Bundestages kompromittiert seien. Das BSI nahm daraufhin mit dem Deutschen Bundestag Kontakt auf, wo man ebenfalls bereits Anomalien im Netz festgestellt hatte. Diese Auffälligkeiten im Netz des Deutschen Bundestags deuteten bereits zu diesem Zeitpunkt darauf hin, dass zentrale Systeme des internen Bundestagsnetzes kompromittiert waren. Gemeinsam mit einem externen Dienstleister untersuchte das BSI daraufhin im Auftrag des Deutschen Bundestags und im Rahmen seines gesetzlichen Beratungsmandats den Vorfall, um das Ausmaß der Kompromittierung festzustellen.

Ergriffene Maßnahmen

Die Bearbeitung des Vorfalls erfolgte in drei Phasen:

- Analyse,
- abgesicherter Übergangsbetrieb und
- Konzeption sicherer Neustart.

In Phase 1 (Analyse) wurden die auffällig gewordenen Systeme forensisch untersucht, um die Methoden und Ziele der Täter abzuleiten. Hierfür wurden alle Arbeitsplatzsysteme und Server mit einem Detektionstool untersucht, das auf derartig hochwertige Angriffe zugeschnitten ist. Infizierte Systeme konnten hierdurch erkannt werden. Zudem wurden die Logdaten der zentralen Internetübergänge daraufhin untersucht, ob sie Verbindungen zu Kontrollservern der Täter aufwiesen.

Eine besondere Herausforderung bei den Analysen war die Tatsache, dass durch die Berichterstattung in der Presse der Angreifer frühzeitig über das Entdecken seines Angriffes informiert war. Der Angreifer konnte so bestimmten Gegenmaßnahmen ausweichen und seine Aktivitäten frühzeitig Verschleiern, indem er beispielsweise Ausweich-Kontrollserver registrierte.

In Phase 2 (abgesicherter Übergangsbetrieb) wurden auffällige Rechner unverzüglich abgeschaltet und neu aufgesetzt, kompromittierte Accounts deaktiviert und Rückmeldewege für den Datenabfluss gesperrt, sobald darüber Kenntnis erlangt wurde. Der Bundestags-Webverkehr wurde zeitweise über die Sicherheitskomponenten des Regierungsnetzes IVBB geleitet, um Angreiferverkehr zu detektieren und diesen zu sperren.
Das Ziel dieser Maßnahmen, Datenabfluss zu verhindern, wurde eine Woche nach Beginn der Gegenmaßnahmen erreicht. Darüber hinaus konnten ab Ende Mai 2015 keine Täteraktivitäten mehr beobachtet werden.

In Phase 3 (Konzeption sicherer Neustart) wurden die aus der Analyse gewonnenen Erkenntnisse über die Methoden der Angreifer in die Konzeption eines sichereren Netzwerks eingebracht. Zentrale technische Prämisse bei der Konzeption war und ist, dass ein einzelner kompromittierter Arbeitsplatz-PC nicht dazu führen darf, dass das gesamte Netzwerk kompromittiert wird. Beim Neuaufsetzen wurde seitens der Bundestagsverwaltung ein weiterer externer Dienstleister beteiligt. In die Konzeption sind die aus der Analyse gewonnenen Erkenntnisse über die Angreifermethoden eingeflossen. Weitere Maßnahmen sind in der Umsetzung mittelfristig zu ergreifen, um das Netz des Deutschen Bundestages gegenüber künftigen Cyber-Angriffen zu härten.

Bewertung

Die Täter haben beim Cyber-Angriff zunächst einen einzelnen Arbeitsplatzrechner mit einer Schadsoftware infiziert. Diese Erstinfektion erlaubt es typischerweise, Dateien hoch- und herunterzuladen. Die genaue Analyse der Erstinfektion in den Logdateien war durch die kurze Speicherfrist von maximal sieben Tagen nicht möglich. Die Täter nutzten diese Funktionalität, um auf dem infizierten System weitere Tools nachzuladen, darunter auch öffentlich verfügbare und von vielen Tätergruppen genutzte Werkzeuge. Die nachgeladene Software diente unter anderem dazu, die Zugangsdaten eines Systemkontos für die Software-Verteilung herauszufinden und dies für die weitere Ausbreitung im internen Netz zu verwenden. Die Analyse ergab, dass auf einzelnen Systemen ein Backdoor-Schadprogramm installiert worden war, das den Angreifern jederzeit erlaubt, auf das System zuzugreifen. Daneben wurden weitere Angriffstools und Schadprogramme wie Keylogger, die Tastatureingaben mitschneiden und Bildschirmfotos erstellen, sowie selbst geschriebene Skripte zum Sammeln von Dokumenten bestimmter Dateitypen gefunden. Aufgrund der Analyse des Vorfalls war davon auszugehen, dass es die Täter unter anderem auf ausgewählte E-Mail-Postfächer im politischen Bereich abgesehen hatten.
Hinsichtlich der methodischen Einordnung des Cyber-Angriffs ist folgendes festzustellen: Der Angriff entspricht dem klassischen APT-Muster, das von nahezu allen bekannten Cyber-Spionagegruppen angewandt wird. Bei der Ausbreitung im internen Netz („Lateral Movement“) setzten die Angreifer auf gängige Methoden und öffentlich verfügbare Tools, wie sie auch von weniger professionellen Tätern verwendet werden. Dies kann dadurch begründet sein, dass man eine Zuordnung des Angriffs erschweren wollte. Allerdings führten einige Fehler der Angreifer dazu, dass ihre Aktivitäten im Netz nachzuvollziehen und zu detektieren waren.
Im Rückblick kann aufgrund der Analysen festgestellt werden, dass die Angreifer nur ein relativ kurzes Zeitfenster von drei Wochen hatten, Daten zu exfiltrieren. Die Nutzung von IT-Systemen im Bundestag war ab Ende Mai 2015 wieder abgesichert.
Mit freundlichen Grüßen
Im Auftrag

Dr. Häger