Bundesamt für Verfassungsschutz

Warnmeldung

22. September 2016

Der Cyberabwehr des Bundesamtes für Verfassungsschutz liegen Erkenntnisse zu einem versuchten Cyberangriff der Angreifergruppierung APT 28 auf ein deutsches Medienunternehmen vor.

Der Angriff erfolgte über eine Spear-Phishing Mail mit einem darin enthaltenen Link zu einer mit Schadcode infizierten Seite. Der gespoofte („gefälschte") Absender lautete heinrich.krammer@hq.nato.int. Diese Absenderadresse wurde auch bei den im August und September 2016 erfolgten Cyberattacken auf den Deutschen Bundestag sowie gegen Parteien genutzt. Beide Angriffswellen weisen starke technische Überschneidungen auf.

Alle bislang festgestellten Angriffsversuche erfolgten zwischen dem 15. August und dem 15. September 2016.

Bei einem der Angriffe wurde statt eines schadhaften Links ein maliziöses Office-Dokument als Anlage verwendet. Viele der von den Akteuren der APT 28 Kampagne versandten Spear-Phishing Mails sind in der Regel in englischer Sprache verfasst und nehmen Bezug auf ein aktuelles tagespolitisches Ereignis. Das Opfer wird in diesen E-Mails aufgefordert, für weiterführende Informationen einen maliziösen Link oder ein schadhaftes Office-Dokument zu öffnen. Klickt das Opfer auf den Link, wird er auf eine legitime Nachrichtenseite weitergeleitet, während sich im Hintergrund die Schadsoftware automatisch auf seinem Rechner installiert.

Die Cyberabwehr des Bundesamtes für Verfassungsschutz empfiehlt eine Überprüfung der E-Mail Postfächer nach der Absenderadresse heinrich.krammer@hq.nato.int. Zudem wird eine Prüfung empfohlen, ob empfangene E-Mails (z. B. von internationalen Organisationen) tatsächlich von ihnen auch bekannten Absendern stammen.