BfV-Newsletter 01/2016

Beitrag Spionageabwehr

Nachrichtendienstlich gesteuerte Elektronische Angriffe aus Russland

Deutschland steht im Fokus fremder Nachrichtendienste. Die geostrategische Lage im Zentrum Europas, der Einfluss in der EU, die Mitgliedschaft in der NATO, die große Wirtschaftskraft mit vielen innovativen Unternehmen und die weltweite Anerkennung deutscher Wissenschafts- und Forschungsleistungen öffentlicher und privater Stellen rücken die Bundesrepublik ins Zentrum nachrichtendienstlicher Aufklärungsbestrebungen. Um Regierungsstellen, Unternehmen oder Forschungseinrichtungen auszuforschen, werden von einer Vielzahl fremder Nachrichtendienste Cyber-Angriffe eingesetzt.

Russische nachrichtendienstliche Elektronische Angriffe gegen deutsche Ziele sind meist Teil mehrjähriger, international ausgerichteter Cyberspionage-Operationen im Rahmen einer umfassenden strategischen Informationsgewinnung. Deren Angriffskampagnen zeichnen sich durch eine hohe technische Qualifikation aus, verdeutlichen starke finanzielle Ressourcen und lassen in Art und globalem Umfang der Operationen außergewöhnliche Operativ- und Auswertefähigkeiten erkennen. Elektronische Angriffe der russischen Dienste bedrohen in erheblichem Maße die Informationssicherheit deutscher Stellen in Regierung und Verwaltung, Wirtschaft, Wissenschaft und Forschung.

Einige dieser Operationen lassen sich über eine Zeitspanne von sieben bis zehn Jahren zurückverfolgen. Viele dieser Angriffskampagnen weisen untereinander technische Gemeinsamkeiten wie zum Beispiel Schadsoftwarefamilien und Infrastruktur auf – dies sind wichtige Indizien für dieselbe Urheberschaft. Es ist davon auszugehen, dass sowohl der russische Inlandsnachrichtendienst FSB als auch der militärische Auslandsnachrichtendienst GRU Cyberoperationen ausführen.

Ziele der Angriffe russischer Dienste sind vor allem die Stärkung der äußeren und inneren Sicherheit, die Sicherung strategischen Einflusses sowie die Förderung russischer Militär- und Energieexporte und russischer Spitzentechnologie. Die beobachteten Kampagnen sind in aller Regel auf Informationsbeschaffung, also Spionage, gerichtet. Im Einzelfall zeigten russische Nachrichtendienste aber auch die Bereitschaft zu Sabotage und Datenveränderung, wie beispielsweise die Löschung einer Datenbank bei einem deutschen Opfer gezeigt hat.

Ähnlich der Aufklärung mit traditionellen Spionagemethoden liegt bei der Informationsgewinnung mittels Elektronischer Angriffe der Fokus der russischen Dienste auf allen Politikfeldern, die russische Interessen berühren können. Angriffe auf staatliche Stellen betreffen insbesondere Energiepolitik und -sicherheit, außenpolitische Fragen wie Abstimmungsprozesse in der Europäischen Union (EU), die Zentralasien- und die Nahost-Politik sowie die Militär- und Rüstungspolitik, die Verteilung von EU-Geldern sowie humanitäre Fragen.

Die NATO-Erweiterungspolitik und die Ausrichtung der EU auf das transatlantische Bündnis mit den USA werden von der russischen Führung als Gefährdung der nationalen Sicherheit angesehen.

Die russische Wirtschaft und auch der Staatshaushalt sind in hohem Maße von der Entwicklung der Einnahmen aus dem durch Preisverfall gekennzeichneten Öl- und Gasgeschäft abhängig. Staatsunternehmen sind in strategischen Bereichen wie dem Energie- und Rohstoffsektor, im Flugzeugbau und teilweise im Bereich der Informations- und Kommunikationstechnik dominierend. Angriffe auf ausländische Unternehmen und Forschungseinrichtungen dienen der Abschöpfung von Know-how und Förderung der eigenen Wirtschaft und Forschung.

Russische Angriffskampagnen richten sich unter anderem gegen supranationale Organisationen, Regierungsstellen, Streitkräfte, Politiker und Parlamente, deutsche und internationale Wirtschaftsunternehmen sowie Wissenschafts- und Forschungseinrichtungen. Sie zielen auf die Ausforschung von Spitzentechnologien. Dabei sind Schwerpunkte in den Bereichen Energie-, Militär-, Röntgen- und Nukleartechnik sowie Luft- und Raumfahrt zu beobachten. Zudem stehen Regierungskritiker, Journalisten und NGOs sowie internationale Großbanken und Fernsehanstalten im Fokus russischer Angreifer.

Neben Langzeitoperationen werden auch ereignisorientierte oder anlassabhängige Angriffe festgestellt, die für ein russisches staatliches Aufklärungsinteresse sprechen, so zum Beispiel die Cyberangriffe auf das niederländische Ermittlerteam im zeitlichen Kontext mit der Veröffentlichung des Abschlussberichts im Herbst 2015 zu den Ursachen des Absturzes des Malaysia-Airlines-Fluges MH17 am 17. Juli 2014 über der Ostukraine.

Die russischen Angreifer demonstrieren ihr technisches Know-how unter anderem anhand einer großen Bandbreite schwer zu detektierender Angriffsvektoren. Sie umfasst E-Mails mit Schadanhang oder Links zu Webseiten mit Schadcode, USB-Sticks, Phishing-Seiten, Watering Holes oder infizierte legitime Webseiten.

Spear-Phishing-Angriffe zeichnen sich durch gutes Social Engineering der auf das Opfer zugeschnittenen E-Mails aus. Es handelt sich dabei regelmäßig um gut recherchierte, glaubwürdige E-Mails mit für das Opfer relevanten Inhalten (teilweise Insiderwissen) und ihm vermeintlich bekannten Absendern. Darüber hinaus zeichnen sich die Angreifer durch eine große Sprachkompetenz aus. So wurden verseuchte E-Mails bereits in unterschiedlichen europäischen Sprachen festgestellt.

Eine in den letzten Monaten häufiger beobachtete Methode zur Erlangung privater Zugangsdaten zu Opfersystemen mittels Spear-Phishing-Angriffen beschreibt zum Beispiel das IT-Sicherheitsunternehmen Trend Micro in einem entsprechenden Report:
Dazu registriert der Angreifer Domains, die sich nur durch kleine Änderungen in der Schreibung von legitimen Webseiten unterscheiden (sog. Typosquatting). Dann versendet er eine E-Mail mit Link an ausgewählte Opfer, in diesem Beispiel an Mitarbeiter der amerikanischen Sicherheitsfirma Academi (ehemals Blackwater). Wird der Link angeklickt, erscheint im Vorschau-Fenster von MS-Outlook in einem neuen Reiter eine legitime Nachrichtenseite – in diesem Fall eine Seite, die über Afghanistan

berichtet und mithin den Interessen des Empfängerkreises entsprechen dürfte. Im Hintergrund sorgt jedoch in der Zwischenzeit ein veränderter Java-Script-Befehl dafür, dass die auf dem nun verdeckten Reiter befindliche Seite gegen die neu erstellte Outlook-Seite des Angreifers ausgetauscht wird. Wechselt das Opfer nun von der Vorschau der Nachrichtenseite zurück zu seinem Outlook-Programm, sieht es nur noch die manipulierte Angreiferseite (mit nachgebauter Anmeldemaske), die vortäuscht, die Session sei abgelaufen und ihn auffordert, seine Zugangsdaten erneut einzugeben. Diese Eingabe ermöglicht dem Angreifer dann, mit diesen Daten das Opfer auszuspähen und sich möglicherweise weitere Zugänge zu verschaffen.

Dieser Spear-Phishing-Angriff zeigt die Raffinesse, mit der der Angreifer hier vorgeht. Das Opfer hat in der Regel keine Chance, diesen Angriff als solchen zu erkennen, da kaum jemand auf die genaue Schreibweise einer URL achten wird. Zudem verdeutlicht dieser Vorfall die Zielrichtung mancher nachrichtendienstlich gesteuerter Angriffswellen. So erfolgten die Angriffe gegen Academi im Frühjahr 2014 zeitgleich mit dem Vorwurf des russischen Außenministeriums, das Unternehmen entsende 400 Söldner in die Ukraine.

Bei der Analyse staatlich gesteuerter Elektronischer Angriffe aus Russland zeigt sich deutlich die hohe informationstechnische Qualität dieser Angriffsoperationen – zum Beispiel durch Ausnutzung noch unbekannter Sicherheitslücken. Sichtbar wird auch die Finanzstärke der Täter; zudem lassen Art und globaler Umfang der Operationen immense Operativ- und Auswertekapazitäten erkennen. Die festgestellten Angriffe erfolgen meist sehr zielgerichtet und passgenau: Die jeweiligen Opfer werden gezielt ausgewählt und angegriffen („target list“).

Die Erfolgswahrscheinlichkeit und damit das Schadpotenzial russischer Angriffe sind aufgrund des erkennbar hohen Ressourcenansatzes, der herausgehobenen technischen Fähigkeiten und des guten Social Engineerings groß.