Presseinformation

Sendesperrfrist: 8. Dezember, 12.00 Uhr

Russische Propaganda und Desinformation

- Seit dem Beginn der Ukraine-Krise erheblicher Anstieg russischer Propaganda- und Desinformationskampagnen in Deutschland
- Breites Instrumentarium und enormer Einsatz finanzieller Ressourcen Russlands zur Steuerung und Verbreitung von Propaganda und Desinformation (staatliche und soziale Medien, Diasporapolitik, Think Tanks)
- Zielgruppen: Russischsprachige Bevölkerung, politische Bewegungen, Parteien und Entscheidungsträger im politischen Raum
- Ziel: Verunsicherung der deutschen Gesellschaft sowie Schwächung oder Destabilisierung der Bundesrepublik
- Ziel: Stärkung extremistischer Gruppierungen und Parteien, um die Arbeit der Bundesregierung zu erschweren und den politischen Diskurs zu beeinflussen

Russische Propaganda- und Einfluss-Operationen im Rahmen der Angriffskampagne APT 28

- Zu den Besonderheiten der Angriffskampagne APT 28 gehören Propaganda und Desinformation, die meist unter „falscher Flagge“ durchgeführt werden. Dieses Vorgehen stellt einen in anderen von Russland gesteuerten Angriffskampagnen bislang nicht beobachteten Modus Operandi dar. Staatliche Stellen verüben in diesen Fällen Cyber-Angriffe unter dem Deckmantel vermeintlicher Hacktivisten.

- In den letzten Monaten ist ein eklatanter Anstieg von Spear-Phishing-Attacken gegen Parteien und Bundestagsfraktionen zu verzeichnen. Sie werden der Angriffskampagne APT 28 zugeschrieben, die auch für den DNC-Hack verantwortlich gemacht wird. Durch APT 28 konnten im Rahmen des Angriffs auf den Deutschen Bundestag im Jahr 2015 bereits erfolgreich Daten abgeschöpft werden.

Der Präsident des BfV, Dr. Hans-Georg Maaßen, erklärt hierzu:

„Propaganda und Desinformation, Cyberangriffe, Cyberspionage und Cybersabotage sind Teil der hybriden Bedrohung für westliche Demokratien. Das geänderte Informationsverhalten der Nutzer in sozialen Netzwerken ist ein ideales Einfallstor für die gezielte Desinformation. Sorge bereitet uns, dass dort Echokammern entstehen, in denen die innenpolitische Meinungsbildung insbesondere durch die automatisierte Stimmungsmache auf fruchtbaren Boden fallen könnte.

Im politischen Bereich stellen wir zunehmend aggressive Cyberspionage fest. Wir sehen eine mögliche Gefährdung von deutschen Regierungsmitgliedern, Bundestagsabgeordneten und von Mitarbeitern der demokratischen Parteien durch Cyberoperationen. Informationen, die bei Cyberattacken abfließen, könnten im Wahlkampf auftauchen, um deutsche Politiker zu diskreditieren. Die Hinweise auf Versuche einer Beeinflussung der Bundestagswahl im kommenden Jahr verdichten sich. Wir erwarten einen weiteren Anstieg von Cyberangriffen im Vorfeld der Bundestagswahl.“