Bundesamt für Verfassungsschutz

Sicherheitshinweis für Politik & Verwaltung | 01/2022 | 11. April 2022

Betreff | Krieg in der Ukraine

Ausgangslage

Das militärische Vorgehen Russlands in der Ukraine wird durch Versuche der Einflussnahme und durch Cyberangriffe insbesondere von prorussischer Seite begleitet. Gemeinsam mit weiteren Staaten beteiligt sich Deutschland weiterhin an Sanktionsmaßnahmen gegen Russland und liefert Waffen und Ausrüstung an die Ukraine. Politische Entscheidungsträgerinnen und -träger in Deutschland, ihre Mitarbeiterinnen und Mitarbeiter oder Beschäftigte in der Verwaltung können deshalb – direkt oder indirekt – zu Zielen werden. Darüber hinaus kommen zahlreiche Geflüchtete auch nach Deutschland. Proteste gegen den Krieg haben einen hohen Zulauf. Allerdings nimmt die Zahl gemeldeter Veranstaltungen ab.

Sachverhalte

Fakeanrufe bei britischen Politikerinnen und Politikern

Laut Medienberichten wurde der britische Verteidigungsminister Ben Wallace von einem Mitglied des russischen und in Russland populären Komikerduos „Vovan und Lexus“ per Videoanruf kontaktiert. Der Anrufer gab sich als ukrainischer Premierminister aus. Gesprächsgegenstand war unter anderem ein angebliches Nuklearprogramm der Ukraine. Die Inhalte wurden anschließend in Auszügen veröffentlicht und durch russische Fernsehsender aufgegriffen. Zuvor wurden bereits die Innenministerin sowie die Kultusministerin Großbritanniens entsprechend adressiert.

Das russische Außenministerium griff diesen Videoanruf auf und führte ihn als vermeintlichen Beleg für angebliche Planungen der NATO und der Ukraine an, die Ukraine atomar zu bewaffnen. Die britischen Bemühungen, das Video von der Plattform *YouTube* löschen zu lassen, wurden als Versuch einer Vertuschung dargestellt.

„SOS“-Postfächer und #StopHating Russians

Die Russische Botschaft hat auf der Homepage ein „SOS“-E-Mail-Postfach zur Meldung von Fällen von „Mobbing, Belästigung, Drohungen, Angriffen oder physischer Gewalt“ gegen russische Staatsangehörige eingerichtet. Auch alle russischen Konsulate bieten eine entsprechende E-Mail-Erreichbarkeit oder nehmen Hinweise über ihren regulären Posteingang an. Die gemeldeten Fälle werden auf der Website unter dem Hashtag #StopHatingRussians öffentlich aufgelistet. Auch die thematischen Beiträge in den offiziellen Social-Media-Kanälen der Russischen Botschaft sind in jüngerer Zeit stark auf eine vermeintlich zunehmende „Russophobie“ in Deutschland ausgerichtet.

Hohes Maß an Cyberaktivitäten

Das militärische Vorgehen Russlands wird auch durch Cyberangriffe begleitet. Nach Schätzungen von IT-Sicherheitsforschern sind die Cyberaktivitäten gegen ukrainische Ziele zehnmal so hoch wie in Friedenszeiten. Am 28. März 2022 kam es nach Angaben des größten ukrainischen Telekommunikationsdienstleisters infolge eines Cyberangriffs zu den bislang umfangreichsten Störungen des Internetbetriebs seit Kriegsbeginn.

GHOSTWRITER

Die Cybergruppierung GHOSTWRITER, die bereits in der Vergangenheit deutsche Ziele angegriffen hatte, ist erneut aktiv geworden. So wurden Anfang März private *t-online.de*-E-Mail-Adressen Ziel eines Phishing-Angriffs. Außerdem konnte dem Akteur die neu registrierte Domain *dienste-email.eu* zugeordnet werden. Kürzlich wurde darüber hinaus bekannt, dass kompromittierte E-Mail-Accounts ukrainischer Militärangehöriger genutzt würden, um Phishing-Angriffe gegen Politikerinnen und Politiker verschiedener europäischer Regierungen durchzuführen. Die dabei verwendete Schadsoftware weist laut Analysen Ähnlichkeiten zur GHOSTWRITER-Kampagne auf.

Bei zurückliegenden Cyberangriffen von GHOSTWRITER gegen deutsche Abgeordnete zeigte sich, dass es im Vorfeld des eigentlichen Angriffs Vorbereitungshandlungen gab, wie breit angelegtes Credential-Phishing über Phishing-Mails. GHOSTWRITER hat in der Vergangenheit erfolgreich Daten von Mandatsträgerinnen und Mandatsträgern und sonstigen politischen Zielen erbeutet, um damit möglicherweise „Hack and Leak“-Operationen (erbeutete Daten werden – teils in manipulierter Form – öffentlich gemacht) und/oder „Hack and Publish“-Operationen (Falschinformationen werden über gekaperte reichweitenstarke Kommunikationskanäle veröffentlicht) vorzubereiten.

Bewertung

Manipulative Anrufe zum Zweck von Desinformation

Manipulative Anrufe können als wesentliche Elemente von Desinformations-Kampagnen eingesetzt werden. Auch wenn in Deutschland gleichgelagerte Aktivitäten nicht bekannt geworden sind, sind vergleichbare Aktionen, insbesondere gegen exponierte politische Entscheidungsträger, einzukalkulieren.

Mobilisierung der russischen und ukrainischen Communitys

Die Russische Botschaft überhöht auf Ihrer Homepage („SOS“-Postfach) und in den sozialen Netzwerken (#StopHatingRussians) offenbar bewusst das tatsächliche Ausmaß von Übergriffen oder Diskriminierungen zum Nachteil russischstämmiger Menschen in Deutschland und greift dabei auf nicht überprüfbare Behauptungen zurück. Dieses Agieren kann dazu beitragen, die ohnehin emotional aufgeladene gesellschaftliche Situation, insbesondere innerhalb der russischen und ukrainischen Communitys in Deutschland, zusätzlich anzuheizen. Aktionen wie der prorussische Autokorso durch Berlin sowie Berichte und Bilder von mutmaßlichen Kriegsverbrechen wie aktuell aus dem Kiewer Vorort Butscha, wo russische Truppen gezielt Zivilisten erschossen haben sollen, könnten für zusätzliche Spannungen sorgen.

Mögliche Nutzung zu operativen und Propaganda-zwecken

Es ist außerdem möglich, dass die russischen Nachrichtendienste die über das „SOS“-Postfach erhaltenen Informationen gezielt für operative Zwecke, etwa der Anbahnung, nutzen. Auch kann nicht ausgeschlossen werden, dass Äußerungen oder Entscheidungen von politischen Entscheidungsträgerinnen und -trägern in Deutschland, ihren Mitarbeiterinnen und Mitarbeitern oder von Beschäftigten in der Verwaltung als russlandfeindlich ausgelegt und für Propagandazwecke verwendet werden. Dies gilt auch für Äußerungen von russischen Mitarbeiterinnen und Mitarbeitern sowie Gesprächskontakten, die als russlandfeindlich gedeutet werden könnten.

Gesteigerte Gefährdung durch GHOSTWRITER

Wortwahl und Endung der von GHOSTWRITER neu verwendeten Domain *dienste-email.eu* lassen es wahrscheinlich erscheinen, dass diese Domain für zukünftige Angriffe gegen deutsche und europäische Ziele angelegt wurde. Möglicherweise wird sie auch bereits verwendet.

Handlungsempfehlungen

Telekommunikation

Vergewissern Sie sich immer vorab, dass Ihre Gesprächspartnerin bzw. Ihr Gesprächspartner die Person ist, mit der Sie sprechen wollen. Kündigen Sie im Zweifelsfall einen Rückruf an, um die Authentizität prüfen zu können.

Cybersicherheit

- Blocken Sie die Domain *dienste-email.eu*.
- Beschränken Sie Zugriffsmöglichkeiten auf ein Minimum, um mögliche Angriffsvektoren zu reduzieren. Überlegen Sie sorgfältig, welche Vorgänge und Systeme aktuell für die Gewährleistung von Funktionalitäten erforderlich sind.
- Fertigen Sie in regelmäßigen Abständen Backups und bewahren Sie diese anschließend getrennt von den betroffenen Systemen auf.
- Schließen Sie bekannte Sicherheitslücken durch das Einspielen vorhandener Update-Patches.
- Geben Sie Ihrem Intrusion Detection Management System (IDMS) die Berechtigung, das Starten und Ausführen von Malware nicht nur zu protokollieren, sondern die entsprechenden Prozesse auch sofort zu stoppen und Dateien in Quarantäne verschieben zu können.
- Entfernen Sie unbekannte oder nicht mehr verwendete Nutzer und reduzieren Sie die Berechtigungen für Nutzer auf ein Minimum.
- Schützen Sie Ihre Konten nach Möglichkeit mit Multi-Faktor-Authentifizierung vor (Credential-)Phishing-Angriffen.
- Misstrauen Sie allen E-Mails, die Sie zu dringenden Handlungen auffordern. Geben Sie niemals Ihre Passwörter an und klicken Sie niemals auf Links oder Anhänge verdächtiger E-Mails. Dies gilt auch für E-Mails von Familie, Freunden oder dem Arbeitgeber. Deren E-Mail-Konten könnten ebenfalls gehackt worden sein.
- Informieren Sie Mitarbeiterinnen und Mitarbeiter über die aktuelle Bedrohungslage, um ein Gefährdungsbewusstsein zu schaffen.
- Etablieren und kommunizieren Sie Meldeprozesse innerhalb der Organisation sowie die Ansprechbarkeiten der zuständigen Behörden bei Auffälligkeiten und Sicherheitsvorfällen.

IT-Sicherheitsverantwortliche sollten die Entwicklungen weiter aufmerksam verfolgen und ihre Maßnahmen bei Bedarf anpassen. Das Bundesamt für Verfassungsschutz aktualisiert laufend seine Übersicht über die ihm vorliegenden Indicators of Compromise (IoCs). Diese Liste stellt der Präventionsbereich auf Anfrage digital zur Verfügung.

Kommunikation mit Kontakten in Russland

Reduzieren Sie Ihre Kommunikation mit Ansprechpartnerinnen und -partnern in Russland auf ein Minimum. Halten Sie Ihre Kommunikation sachlich. Russische Kontakte sollten nicht in die Lage gebracht werden, sich per Telefon oder E-Mail zum Krieg in der Ukraine äußern zu müssen.

So erreichen Sie uns

Für Informationen zu Bedrohungen für Ihre Branche durch Spionage und Sabotage, Terrorismus oder gewaltbereiten Extremismus sowie für konkrete Sicherheitsanfragen oder Verdachtsfälle kontaktieren Sie den Bereich Prävention:

praevention@bfv.bund.de
+49 (0)30 – 18 – 792 33 22

Für spezifische technische Hinweise oder Rückfragen zu einem konkreten Cyberangriff oder einer bestimmten Kampagne wenden Sie sich direkt an die Expertinnen und Experten der Cyberabwehr:

cyberabwehr@bfv.bund.de
+49 (0)30 – 18 – 792 26 00

Natürlich steht Ihnen auch die Landesbehörde für Verfassungsschutz in Ihrem Bundesland als Ansprechpartner zur Verfügung. Sollte Ihnen der Kontakt nicht bekannt sein, vermitteln wir Ihnen diesen gerne.

Ihre Angaben werden in jedem Fall vertraulich behandelt.

PRÄVENTION
POLITIK UND VERWALTUNG