Wie kann man sich vor derartigen Angriffen schützen?

- Phishing-Mails nachrichtendienstlicher Angreifer wirken häufig seriös. Hinterfragen Sie kritisch jede Aufforderung zur Passworteingabe, die Sie per Mail erhalten.
- Öffnen Sie keine Anhänge und klicken Sie nicht auf Links in E-Mails von bislang unbekannten oder nicht vertrauenswürdig erscheinenden Absendern.
- Melden Sie verdächtig erscheinende E-Mails im Arbeitsumfeld Ihrem zuständigen IT-Sicherheitsbeauftragten. Dieser kann die betreffende E-Mail bei Bedarf zur weiteren Analyse an das BfV weiterleiten.
- Auch wenn Sie selbst Ihre Tätigkeit nicht als nachrichtendienstlich relevant einschätzen sollten: der potenzielle Angreifer kann darauf abzielen, Ihr Netzwerk zu missbrauchen, um über dieses in ein weiteres Netzwerk einzudringen.

Wir sichern Ihnen absolute Vertraulichkeit zu!

Weitere Informationen zum Verfassungsschutz finden Sie hier:

www. verfassungsschutz.de

Herausgeber
Bundesamt für Verfassungsschutz
Merianstraße 100, 50765 Köln
Telefon: +49 (0) 30 18 792 - 0
+49 (0) 22 899 792 - 0
Fax: +49 (0) 30 18 10 - 792 - 29 15
+49 (0) 22 899 10 - 792 - 29 15
E-Mail: poststelle@bfv.bund.de

Bildnachweis
© picture alliance - Westend61 - Andrew Brookes
© picture alliance - Jochen Tack - Jochen Tack
© picture alliance - ZB - Z6944 Sascha Steinach
© iStockphoto.com - BrianAJackson

Stand
Juni 2022 (F-0001)

Bundesamt für Verfassungsschutz

Cyberangriffe

Gefahren erkennen – Risiken minimieren

Aktuelles Cyberlagebild

Mandatsträger, Parteien und politische Stiftungen sind wesentliche Instrumente der politischen Willensbildung in Deutschland. Gerade deshalb steht auch ihre Arbeit im Fokus des Aufklärungsinteresses ausländischer Nachrichtendienste. Um an sensible Informationen zu gelangen, setzen diese häufig Cyberangriffe als nachrichtendienstliches Mittel ein. Dabei versuchen sie, verdeckten Zugriff auf relevante IT-Systeme zu erlangen.

Angriffe sind nicht auf technische Systeme beschränkt. Der „Faktor Mensch“ stellt für den Angreifer einen mindestens gleichwertigen Angriffsvektor dar. Auch noch so unbedeutend erscheinende persönliche Informationen können dabei hilfreich für den Angreifer sein, um die Tür zu weiteren sensiblen Daten zu öffnen. Ein hundertprozentiger Schutz vor Cyberangriffen ist derzeit nicht erreichbar; denn selbst jede noch so perfekt gesichert scheinende IT-Umgebung weist zwangsläufig die eine oder andere Schwachstelle auf.

Cyberangriffskampagnen werden aktuell auch dazu genutzt, die politische Willensbildung in der Gesellschaft durch ausgefeilte Desinformationskampagnen gezielt zu beeinflussen. Dabei erscheinen vorab gestohlene Informationen in einem neuen, verzerrten Kontext und werden auf unterschiedlichsten Plattformen für die Öffentlichkeit zugänglich gemacht.

Das Bundesamt für Verfassungsschutz (BfV) geht nach wie vor von einer anhaltenden Gefährdung deutscher Parteien, parteinaher Stiftungen, politischer Institutionen und der Medien durch Cyberangriffe aus. Insbesondere Soziale Netzwerke stellen für fremde Nachrichtendienste immer wieder ein besonders lohnenswertes Ziel dar. Diese dienen einerseits als Quelle für brisante Informationen, andererseits lassen sich solche Netzwerke relativ einfach zur Verbreitung von Propaganda und Desinformation instrumentalisieren.

Wie lässt sich ein möglicher Cyberangriff erkennen?

Das BfV hat zwei Angriffsarten detektiert, die vor dem in diesem Faltblatt behandelten Hintergrund bevorzugt Anwendung finden.

1. Angriffe mit Schadsoftware

International agierende Angriffskampagnen, „Advanced Persistent Threats“ (APT), verwenden in der Regel sogenannte Spear-Phishing-Mails für die Erstinfektion eines Netzwerkes. Derartige E-Mails zeichnen sich unter anderem aus durch

- legitim wirkende Absender (oftmals politische oder mediale Organisationen),
- ein Informationsangebot zu aktuellen politischen Themen,
- eingebaute Links zu unverdächtig wirkenden, jedoch maliziösen Webseiten,
- einen Anhang mit schadhaften Dateien,
- begleitende Telefonanrufe mit der Aufforderung zur Eingabe von Passwörtern.

2. Credential-Phishing-Attacken

Neben den geschilderten Angriffen mit Schadsoftware führen Angreifer auch sogenannte Credential-Phishing-Attacken durch, um beispielsweise an die Zugangsdaten dienstlicher beziehungsweise dienstlich genutzter E-Mail-Accounts oder solche kommerzieller Anbieter zu gelangen. In solchen Fällen werden vom Angreifer E-Mails mit einem eingebauten Link zu einer nachgestellten Login-Seite versandt. Auf solchen Seiten werden potenzielle Opfer dann zur Preisgabe ihrer Zugangsdaten aufgefordert.

Weitere Schwachstellen

Entwicklungen im IT-Sicherheitsbereich zeigen, dass selbst als vermeintlich sicher geltende Betriebssysteme, wie beispielsweise Apple-Systeme (MacOS) oder Linux-Distributionen, vermehrt zum Ziel von Cyberangriffen werden.

Darüber hinaus besteht die Gefahr, dass durch sogenannte Defacements Inhalte der eigenen Webauftritte verändert werden. Hierbei können ungewollte Botschaften platziert oder aber eigene Inhalte gezielt verfälscht werden.

Vor diesem Hintergrund empfehlen wir die von Ihnen genutzte Software immer auf dem aktuellsten Stand zu halten und die Sicherheitsempfehlungen der Hersteller stets zu berücksichtigen. Für entsprechende Hinweise oder Rückfragen steht Ihnen der Präventionsbereich des BfV jederzeit zur Verfügung. Bei Bedarf bieten wir Ihnen zudem gezielte Sensibilisierungsmaßnahmen sowie persönliche Beratung im Zusammenhang mit der Thematik an.

Mail:
wirtschaftsschutz@bfv.bund.de

Telefon:
+49 (0) 30 18 792 - 33 22
+49 (0) 22 899 792 - 33 22