Bundesamt für
Verfassungsschutz

Cyberangriffe

Gefahren, Risiken und Schutz vor
staatlich gesteuerten Attacken

Cyberangriffe

Gefahren, Risiken und Schutz vor
staatlich gesteuerten Attacken

Vorwort

Sicher. Digital. Geschützt.

Die digitale Welt bietet uns viele und immer wieder neue Möglichkeiten – aber sie birgt auch vielfältige Gefahren. Cyberangriffe gehören heute zu den größten Herausforderungen für unsere Sicherheit. Besonders staatlich gesteuerte Angriffe zielen darauf ab, Kritische Infrastrukturen (KRITIS) zu schwächen, Daten aus Politik, Wirtschaft und Wissenschaft zu stehlen oder demokratische Prozesse beispielsweise durch gezielte Desinformation zu destabilisieren.

Diese Broschüre zeigt, was Cyberangriffe sind, welche Bedrohungen von staatlichen Akteuren ausgehen und wie das Bundesamt für Verfassungsschutz (BfV) dagegen vorgeht.

In einer vernetzten Welt bedeutet Sicherheit nicht nur den Schutz Einzelner, sondern die Verteidigung unserer gesamten Gesellschaft. Gemeinsam können wir diese Herausforderung meistern.

Bleiben Sie informiert, wachsam und sicher!

Inhalt

Kapitel 1

Cyberangriffe: eine Einleitung

Cyberangriffe sind gezielte Versuche, durch unbefugten Zugriff auf Netzwerke, Computersysteme oder digitale Geräte, Daten, Anwendungen oder andere Ressourcen zu stehlen, offenzulegen, zu manipulieren, zu deaktivieren oder zu zerstören. Die Auswirkungen erfolgreicher Cyberangriffe können schwerwiegend sein: Störung von Betriebsabläufen, Abfluss von Informationen, Zugangsverweigerungen, Manipulation, Beschädigung oder Zerstörung von Hardware, Daten, Netzwerken, KRITIS oder technischen Systemen. Dabei besteht für die Cyberakteure ein geringes Enttarnungsrisiko bei gleichzeitig relativ hoher Erfolgswahrscheinlichkeit, da Cyberangriffe über eine Vielzahl möglicher Angriffsmuster erfolgen.

DECODIERT

KRITIS ist die Abkürzung für **Kritische Infrastrukturen**. Damit sind Anlagen, Systeme und Organisationen gemeint, die eine wichtige Bedeutung für die Aufrechterhaltung gesellschaftlicher Funktionen haben. Ihr Ausfall hätte erhebliche Auswirkungen auf das Gemeinwesen, zum Beispiel in Form von Versorgungsengpässen und einer Gefährdung der öffentlichen Sicherheit. In Deutschland zählen die Sektoren Energieversorgung, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Siedlungsabfallentsorgung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur zu KRITIS.

Operationen im Cyberraum bieten den Akteuren entscheidende Vorteile:

- Sie sind orts- und personenunabhängig durchführbar.
- Sie erfordern in vielerlei Hinsicht einen geringen Aufwand (zum Beispiel keine persönliche Kontaktaufnahme, keine aufwendige Anbahnungsphase und keine komplexe → *Legendierung* beziehungsweise Verschleierung der Urheberschaft).
- Sie ermöglichen nicht nur den reinen Informationsabfluss, sondern stellen darüber hinaus eine effektive Methode zur Informationssteuerung und -verbreitung bei → *Desinformationskampagnen* und → *Einflussnahmeoperationen* dar.
- Ein einzelner gelungener Angriff kann den Zugriff auf enorme Datenmengen ermöglichen.
- Das Entdeckungsrisiko ist gering.

Cyberangriffe treten in unterschiedlichen Formen auf und richten sich sowohl gegen Privatpersonen als auch gegen Unternehmen oder staatliche Einrichtungen. Zu den häufigsten Formen von Cyberangriffen zählen → *Phishing-Angriffe*, bei denen durch manipulierte E-Mails sensible Daten wie beispielsweise Passwörter entwendet werden. Ebenfalls verbreitet sind → *Malware-Angriffe*, bei denen → *Schadsoftware* genutzt wird, um Systeme zu infiltrieren und Daten zu stehlen oder zu verschlüsseln. → *„Denial of Service" (DoS)-* beziehungsweise → *„Distributed Denial of Service" (DDoS)-Attacken* zielen darauf ab, Netzwerke und Server durch eine massive Überlastung lahmzulegen. Weitere Methoden wie → *Ransomware* oder → *„Man-in-the-Middle"-Angriffe* verdeutlichen die Vielschichtigkeit der Bedrohung.

Diese Formen von Cyberangriffen vermischen sich zunehmend mit Einflussnahmeoperationen staatlich kontrollierter Medien fremder Mächte und ihrer Ableger, um propagandistische Narrative und Desinformation in Umlauf zu bringen.

Deutschland ist ein attraktives Ziel für staatlich gesteuerte Cyberangriffe. Die zentrale geografische Lage in Europa sowie seine politische Rolle in der EU und der NATO rücken es in den Fokus von Aufklärungsaktivitäten. Aber auch als führende Industrienation weckt der Wirtschaftsstandort Deutschland mit zahlreichen Spitzentechnologieunternehmen, dem Know-how des Mittelstands und seiner Innovationsfähigkeit in Wissenschaft und Forschung das Interesse für Wirtschafts- und Wissenschaftsspionage.

Besonders im Fokus stehen KRITIS-Sektoren wie Energieversorgung, Wasserwirtschaft, Verkehrssysteme/Logistik und das Gesundheitswesen. Diese Bereiche bilden das Rückgrat des täglichen Lebens sowie der Wirtschaft – eine Störung oder ein Ausfall hätte gravierende Konsequenzen.

Kapitel 2

Akteure im Cyberraum

Cyberangriffe sind nicht mehr nur das Werk einzelner Hacker oder krimineller Gruppen – sie werden zunehmend von staatlichen oder staatlich beauftragten Akteuren initiiert, koordiniert oder durchgeführt. Abgrenzend zu kriminellen Hackern verfolgen solche Angriffe unter anderem das Ziel, sensible Daten und innovatives Know-how zu stehlen, KRITIS zu sabotieren, politische Destabilisierung zu erzeugen oder wirtschaftliche und militärische Vorteile zu erlangen. Dabei werden oft hoch entwickelte Technologien genutzt, weshalb sie häufig lange unentdeckt bleiben.

Bedrohungsakteure können Teil eines offiziellen Staatsapparats sein, Mitglieder einer – mit einer Regierung verbündeten oder von ihr beauftragten – Cybercrime-Organisation, „Freiberufler", die gezielt für eine bestimmte Operation angeheuert werden oder eigenmotivierte Personen.

2.1 Eigenmotivierte Cyberakteure

Eigenmotivierte Cyberakteure haben weder einen genauen Auftrag noch unbedingt einen finanziellen Vorteil durch ihr Handeln. Die Cyberoperationen sind häufig politisch, ideologisch oder aber religiös motiviert. Ihre Attacken schließen ein breites Spektrum von einfachen Überlastungsangriffen (DoS-/DDoS-Angriffe) bis hin zu „Hack and Leak"- oder „Hack and Publish"-Operationen ein.

TATORT CYBERSPACE

Das **Hackerkollektiv Anonymous** ist eine der bekanntesten Gruppierungen, die sich dem → *Hacktivismus* zuordnen lässt. Sie übernahm die Verantwortung für einige der größten derartigen Cyberangriffe der jüngeren Vergangenheit. Unter anderem erklärte Anonymous, mit Beginn des umfassenden russischen Angriffskriegs gegen die Ukraine am 24. Februar 2022 in einen „Cyberkrieg gegen die russische Regierung" getreten zu sein. Aber auch auf prorussischer Seite traten im Zuge des Angriffskriegs Hacktivistengruppierungen auf den Plan und greifen fortlaufend westliche Ziele – auch in Deutschland – an.

2.2 Staatliche Cyberakteure

Zu den staatlichen Cyberakteuren gehören staatliche oder staatlich gelenkte Einrichtungen, die im Auftrag einer Regierung Cyberoperationen durchführen. Dabei verfolgen sie die politischen Ziele ihres jeweiligen Landes. Im nachrichtendienstlichen Kontext nutzen fremde → *Nachrichtendienste* Cyberangriffe in großem Umfang mit der Absicht, unbefugt und verdeckt an Informationen zu gelangen. Neben Spionageaktivitäten können solche Cyberangriffe auch zur Vorbereitung von → *Sabotageakten* genutzt werden – insbesondere KRITIS stehen dabei im Fokus fremder Nachrichtendienste. Auch Einflussnahme- oder Desinformationsaktivitäten werden im Rahmen von „Hack and Leak"- oder „Hack and Publish"-Operationen unterstützt.

DECODIERT

Bei **„Hack and Leak"**-Operationen versuchen Cyberakteure mittels Cyberangriffen in Computersysteme vorzudringen („Hack"), um beispielsweise diskreditierendes oder belastendes Material über das Opfer zu erlangen. Dieses wird anschließend im Original oder in verfälschender Form zum Beispiel in Onlineforen oder über Social-Media-Kanäle veröffentlicht („Leak").

„Hack and Publish" bezeichnet die Kompromittierung legitimer Nachrichtenportale oder Social-Media-Konten beziehungsweise Blogs etwa von Journalisten oder Politikern, um diese Kanäle zu missbrauchen („Publish"). Der Zweck besteht darin, erbeutete Informationen, manipulierte Inhalte oder andere Daten zur gezielten Desinformation zu verbreiten. Damit verschleiert der Akteur seine Urheberschaft und nutzt die Reputation des kompromittierten Veröffentlichungskanals für sich aus. Gerade gezielte Falschnachrichten sind damit nur schwer bis gar nicht von seriösen Inhalten zu unterscheiden. Oft werden sie auch parallel über weitere Verbreitungswege wie zum Beispiel Blogs, soziale Medien oder E-Mails an Medienunternehmen gestreut.

2.3 Staatlich beauftragte Cyberakteure

Staatlich beauftragte Cyberakteure werden durch einen fremden Nachrichtendienst oder sonstige staatliche Stellen gelenkt, ohne diesen selbst anzugehören. Sie führen Cyberattacken und Vorbereitungshandlungen für Spionage sowie Sabotage durch, sammeln Informationen, stehlen vertrauliche Daten oder stören bedeutsame Infrastrukturen anderer Regierungen.

Dabei kann es sich auch um Einzelpersonen handeln, organisierte Gruppierungen, die für einzelne Operationen angeheuert werden, aber auch privatwirtschaftliche Unternehmen, die im staatlichen Auftrag Cyberangriffe verüben.

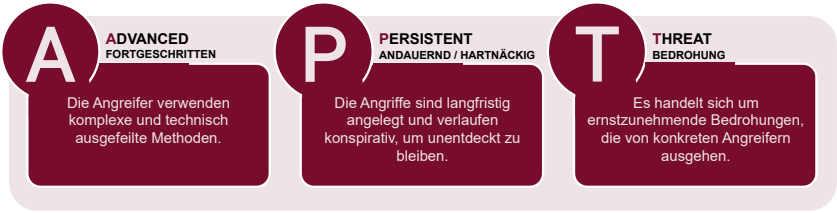
TATORT CYBERSPACE

Am 16. Februar 2024 veröffentlichten Unbekannte auf der Plattform GitHub einen Datensatz, der Details zur Kooperation des chinesischen **Cybersecurity-Unternehmens i-Soon** mit der chinesischen Regierung beziehungsweise deren Nachrichtendiensten enthält. Die Auswertung der Daten belegt eine Industrialisierung von Cyberspionage durch privatwirtschaftlich organisierte Unternehmen, die im staatlichen Auftrag Cyberangriffe verüben. Wenngleich die Daten keine Hinweise auf betroffene Stellen in Deutschland enthalten, bieten sie doch tiefe Einblicke in die Arbeitsweise privater Hackerfirmen sowie in die Verbindungen von Schadsoftwareanbietern zum chinesischen Staat. Sie verdeutlichen, wie APT-Gruppierungen agieren und mit staatlichen Stellen zusammenarbeiten.

Über die enge Verknüpfung privater und staatlicher Akteure informiert die vierteilige Reihe „Die i-Soon Leaks: Industrialisierung von Cyberspionage“. Sie ist auf der Website des BfV (www.verfassungsschutz.de) abrufbar.

DECODIERT

Unter **Advanced Persistent Threats (APT)** werden komplexe und zielgerichtete Bedrohungen verstanden, die sich gegen ein oder wenige Opfer richten. In der Praxis handelt es sich um ressourcenstarke Cyberangreifergruppen, die in der Regel staatlich gesteuert sind. Die konkreten Angriffe im Rahmen dieser Bedrohungen („threats“) werden von den Angreifern aufwendig vorbereitet, sind hochentwickelt („advanced“) und dauern lange an („persistent“).



Ein APT-Angriff soll nach Möglichkeit unentdeckt bleiben, um vertrauliche Daten beispielsweise von Behörden und Unternehmen über einen längeren Zeitraum auszuspähen oder anderen Schaden zu verursachen. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz sowie erhebliche technische Fähigkeiten und Methoden aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.

Cyberangriffe staatlicher oder staatlich beauftragter Akteure zielen insbesondere auf außenpolitische Fragestellungen und Informationen zu Themen der Verteidigungspolitik und des Militärs, der Sicherheits- sowie der Energiepolitik ab. Aber auch Informationen über Spitzentechnologien aus den Bereichen Energie-, Sicherheits- und Verteidigungswirtschaft, Nukleartechnologie, Luft- und Raumfahrt wie auch Biotechnologie, Chip- und Halbleiterfertigung sind von großem Interesse. Darüber hinaus nutzen staatliche oder staatlich beauftragte Akteure Cyberangriffe für die Ausspähung von Dissidenten, Oppositionellen oder von durch ihre Regierungen als „unerwünscht“ oder „terroristisch“ diskreditierten Organisationen.

Kapitel 3

Fremde Staaten und ihre Ziele

3.1 Die Russische Föderation

Russland nutzt Cyberangriffe als geopolitisches Werkzeug, um strategische Vorteile zu erzielen und Einfluss auf globale wie auch nationale Politikprozesse auszuüben. Dazu verfolgt Russland im Cyber- und Informationsraum eine Doppelstrategie aus Cyberangriffen und Desinformationskampagnen. Häufig eingesetzte Methoden sind Phishing und das Ausnutzen von Schwachstellen in IT-Systemen sowie Malware. Dabei sind die Absichten der Cyberakteure vielfältig:

- Politische Destabilisierung
  Russland zielt darauf ab, demokratische Systeme zu untergraben und politische Instabilität zu schaffen. Dies geschieht oft durch das Hacken politischer Institutionen und die anschließende Verbreitung gestohlener Informationen.

TATORT CYBERSPACE

Im Juni 2023 informierte die SPD die Öffentlichkeit darüber, dass ihre Parteizentrale Anfang des Jahres Opfer eines Cyberangriffs geworden war. Unter Ausnutzung einer Sicherheitslücke in Microsoft Outlook kam es dabei möglicherweise zu Zugriffen auf Teile des E-Mail-Systems der Partei. Im Mai 2024 hat die Bundesregierung diesen und weitere Angriffe gegen deutsche Unternehmen aus der ersten Jahreshälfte 2023 der **Gruppierung APT28** (unter anderem auch bekannt als Fancy Bear) zugerechnet – eine staatliche russische Hackergruppe, die dem russischen Militärnachrichtendienst GRU (Glawnoje Raswedywatelnoje Uprawlenije) zuzuordnen ist.

- Spionage
  Russische Cyberakteure stehlen gezielt geheime Informationen von Regierungen, Verwaltungen und internationalen Organisationen, um sich strategische Vorteile zu verschaffen.

- Desinformation
  Russische Cyberakteure setzen ihre Cyberangriffe häufig im Rahmen umfassender Desinformationsoperationen ein. Dabei werden erbeutete Daten zur Verbreitung von Desinformation über soziale Medien oder gefälschte Nachrichtenwebsites genutzt, um das Vertrauen in demokratische Prozesse oder Institutionen zu erschüttern.

TATORT CYBERSPACE

Beim **„Doppelgänger-Netzwerk“** handelt es sich um eine russische Desinformationskampagne, die erstmals im Jahr 2022 identifiziert wurde. Sie hat das Ziel, westliche Regierungen und deren Politik zu diskreditieren – insbesondere im Zusammenhang mit der Reaktion auf den russischen Überfall auf die Ukraine. Die Kampagne startete nach der russischen Invasion in die Ukraine 2022 und zielt darauf ab, Desinformationen über gefälschte Websites zu verbreiten, die seriöse Medien imitieren. Auf diesem Weg sollen gefälschte Nachrichten gestreut werden. Solche nachgebauten Websites konnten für verschiedene Länder festgestellt werden, unter anderem Frankreich, Deutschland, die USA und Polen. Die Inhalte werden oft von Fakeprofilen und Bots in sozialen Medien aufgegriffen und verbreitet.

3.2 Die Volksrepublik China

China verfolgt mit seinen Cyberangriffen primär wirtschaftliche und technologische Ziele. Im Gegensatz zu Russland, das oft auf politische Destabilisierung abzielt, liegt der Fokus Chinas auf dem Diebstahl geistigen Eigentums und strategischen Wissens, um die eigene Wirtschaft und Technologie zu stärken. Gleichwohl spielen auch Ziele in Politik und Behörden eine wichtige Rolle für chinesische Cyberangriffe. Die Absichten Chinas können wie folgt zusammengefasst werden:

- Wirtschaftliche Dominanz
  Chinesische Cyberakteure greifen gezielt Unternehmen in Schlüsselindustrien und strategisch relevanten Zukunftsbranchen an, um sensible Informationen wie zum Beispiel Produktionspläne, Patente und Geschäftsstrategien zu erlangen. Die gestohlenen Daten fließen direkt in die Förderung chinesischer Unternehmen, insbesondere staatlich geführter Konzerne.

- Know-how-Abfluss aus Hochschulen
  Deutsche Hochschulen und Forschungseinrichtungen sind zentrale Ziele chinesischer Cyberangriffe. Chinas Cyberakteure infiltrieren Netzwerke, um Zugang zu innovativen Forschungsprojekten, Patenten und zukunftsweisenden technischen Entwicklungen zu erhalten. Besonders betroffen sind die Bereiche Künstliche Intelligenz, Biotechnologie und Materialwissenschaften.

- Strategische Langzeitziele
  Über langfristige Cyberoperationen versucht China, sich technologische, militärische und politische Vorteile zu verschaffen, um sein Ziel einer dominierenden Weltmachtstellung zu erreichen. Die Angriffe erfolgen oft über Lieferketten, Partnernetzwerke und unzureichend geschützte Systeme.

TATORT CYBERSPACE

Am 31. Juli 2024 ordnete die Bundesregierung öffentlich den 2021 verübten **„schweren Cyberangriff" auf das Bundesamt für Kartographie und Geodäsie (BKG)** staatlichen chinesischen Akteuren zu. Die Netzwerke des BKG wurden damals zu Spionagezwecken infiltriert. Die Angreifer kompromittierten dabei Endgeräte von Privatpersonen und Unternehmen, um diese im Rahmen eines sogenannten Verschleierungsnetzwerks für den Angriff zu nutzen.

Das BKG ist aufgrund seiner Funktion als Kompetenz- und Dienstleistungszentrum für topografische und amtliche Geodaten unter anderem ein wichtiger Dienstleister für andere Stellen. Dazu gehören auch die Bundeswehr und Sicherheitsbehörden sowie privatwirtschaftliche Einrichtungen und Unternehmen aus dem Bereich KRITIS. Die Attribution erfolgte durch die Sicherheitsbehörden des Bundes in Form von umfassenden Analysen und Ermittlungen unter Federführung des BfV.

3.3 Die Islamische Republik Iran

Iran setzt Cyberangriffe strategisch ein, um seine regionalpolitischen Ziele zu erreichen, Gegner zu destabilisieren, Oppositionelle auszuspähen und einzuschüchtern und so die eigene Herrschaft der derzeitigen Machthaber abzusichern. Iranische Cyberakteure nutzen Techniken wie → *Social Engineering*, Phishing und Malware, um Opfer in Wirtschaft, Wissenschaft und Verwaltung zu schädigen.

TATORT CYBERSPACE

Das BfV konnte Ausspähversuche der Cybergruppierung **Charming Kitten** identifizieren, die sich gegen iranische Personen und Organisationen in Deutschland richteten. Die Cyberangriffe zielten vor allem auf iranische Oppositionelle beziehungsweise Dissidentenorganisationen und Exil-Iraner wie beispielsweise Juristen, Journalisten sowie Menschenrechtsaktivisten ab. Dazu verwendeten die Angreifer aufwendiges Social Engineering, das mit großer Ausdauer bis zur erfolgreichen Infektion der Kommunikationssysteme der Opfer durchgeführt wurde. Das BfV hat Betroffenen Hinweise und Empfehlungen zum Schutz vor solchen Ausspähversuchen gegeben.

3.4 Die Demokratische Volksrepublik Korea (Nordkorea)

Nordkorea nutzt Cyberangriffe primär zur finanziellen Bereicherung des Regimes und zur Umgehung internationaler Sanktionen. Nordkoreanische Cyberakteure sind bekannt für Bankraub durch Hacking, Ransomwarekampagnen und Angriffe auf Kryptowährungsplattformen. Darüber hinaus werden Cyberoperationen für politische Zwecke wie Spionage oder Sabotage eingesetzt.

TATORT CYBERSPACE

Der Diebstahl von Kryptowährung hat sich zu einem wichtigen Pfeiler der Staatsfinanzierung Nordkoreas entwickelt. Das erbeutete Geld fließt unter anderem in das Raketenprogramm der Staats- und Militärführung Nordkoreas sowie in die Finanzierung der eigenen Nachrichtendienste und Cybergruppierungen. Im Februar 2025 wurde die Kryptobörse Bybit kompromittiert und Kryptowährung im Wert von über 1,4 Milliarden US-Dollar erbeutet. Es handelt sich um den bisher größten Diebstahl von Kryptowährung weltweit. Der Angriff geht auf nordkoreanische Cyberakteure zurück.

3.5 Weitere Staaten

Neben diesen Staaten gibt es auch andere Länder und nicht staatliche Akteure, die im Bereich der Cyberangriffe tätig sind. Insbesondere mehrere asiatische Staaten sind mit offensiven Cyberoperationen aktiv. Beispiele dafür sind die Republik Indien und die Islamische Republik Pakistan, die seit Jahrzehnten miteinander in Konflikt stehen.

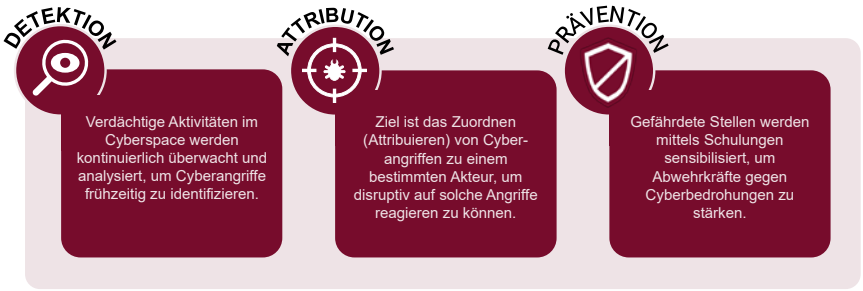
Kapitel 4

Wie das BfV Cyber-angriffen begegnet

4.1 Der Auftrag

Cyberangriffe ausländischer Nachrichtendienste stellen eine bedeutende Gefahr für die Sicherheit Deutschlands dar. Sie richten sich gegen Politik und Verwaltung, Wirtschaft, Wissenschaft sowie gegen KRITIS und haben dabei das Potenzial, erhebliche Schäden zu verursachen – sei es durch Datendiebstahl, Sabotage oder die Beeinflussung von Entscheidungs- und Meinungsbildungsprozessen.

Um Deutschland vor solchen Angriffen zu schützen, spielt das BfV als Cyberabwehrbehörde eine zentrale Rolle. Die Aufgaben des Verfassungsschutzes umfassen bei Detektion, Disruption und Prävention in der Cyberabwehr diese Felder:



4.2 Die Zuordnung

In der Welt der Cyberangriffe ist die genaue Identifizierung der Täter – die sogenannte Attribution – eine der größten Herausforderungen. Cyberakteure nutzen Verschleierungstechniken, ihre Angriffe sind komplex und verlaufen häufig über lange Ketten. Sie tun zudem alles, um ihren Ursprung zu verbergen: Sie verwenden gefälschte IP-Adressen, → *Proxy-Server* und nutzen Malware aus öffentlich zugänglichen Quellen. Diese und weitere Methoden erschweren häufig die Zuordnung der Angreifer, die ein großes Interesse daran haben, möglichst lange unentdeckt agieren zu können und entsprechend vorsichtig handeln. Andere wiederum legen bewusst falsche Fährten, sogenannte False Flags, um die eigentliche Urheberschaft eines Cyberangriffs zu verschleiern.

DECODIERT

„False Flag“-Operationen sind von Nachrichtendiensten oder anderen Stellen durchgeführte Operationen, die den Anschein erwecken, sie würden von einem Drittstaat oder einer anderen Organisation durchgeführt. Innerhalb der Cyberabwehr werden hierunter die gezielten Bemühungen eines Cyberakteurs, die eigenen Handlungen zur Verschleierung der Urheberschaft einer anderen Stelle zuzuschreiben und eine Attribution zu erschweren, verstanden.

Nur mit einem klaren Bild über die Urheber können gezielte Gegenmaßnahmen ergriffen, Verantwortliche zur Rechenschaft gezogen und politische oder wirtschaftliche Entscheidungen für eine angemessene Reaktion auf belastbare Fakten gestützt werden.

Derzeit existiert eine Vielzahl an APT-Gruppierungen. Diese zu unterscheiden und ihnen entsprechende Cyberangriffe zuzuordnen, ist eine anspruchsvolle Aufgabe. Dabei kommen technische Analysen wie die Untersuchung von Schadsoftware und Netzwerkverkehren zum Einsatz. Ergänzt werden diese durch die Herausarbeitung strategischer Indikatoren wie mögliche Motive und geopolitische Kontexte sowie die Sichtung offener Quellen zur weiteren Einordnung. Auch eigene operative Maßnahmen können zum Einsatz kommen. Ein weiterer wichtiger Aspekt beim Attribuieren von Cyberangriffen ist der fachliche Austausch durch internationale Zusammenarbeit.

Doch die Attribution von Cyberangriffen zu ihren Urhebern bleibt ein Balanceakt: Sie erfordert sorgfältige Analysen und transparente Kommunikation. Cyberangriffe erfolgreich zu attribuieren bedeutet also mehr als technische Kompetenz – es handelt sich um ein Zusammenspiel aus Forensik, Kooperation und gegenseitigem Austausch.

4.3 Der Schutz

Sollten Sie bei einem Cyberangriff einen nachrichtendienstlichen oder extremistischen Hintergrund vermuten, kommen Sie auf uns zu. In derartigen Fällen kann das BfV Sie beraten und gegebenenfalls Ihre Maßnahmen mit zusätzlichen Hintergrundinformationen unterstützen. Der Bereich Prävention (Wirtschafts- und Wissenschaftsschutz) wie auch die Cyberabwehr des BfV stehen betroffenen Stellen als vertrauliche Ansprechpartner zur Verfügung.

Sie erreichen uns jederzeit unter:

Cyberabwehr des BfV
Tel.: 0228 99 792-2600
cyberabwehr@bfv.bund.de

Präventionsbereich des BfV
Tel.: 0228 99 792-3322
030 18 792-3322
wirtschaftsschutz@bfv.bund.de

CODEBREAKER (Begriffserklärungen)

→ *Denial-of-Service (DoS)-/ Distributed-Denial-of-Service (DDoS)-Angriff*

Bei einem Denial-of-Service (DoS)-Angriff senden einzelne Systeme eine hohe Anzahl von Anfragen an einen bestimmten Server. Das Ziel der Aktion besteht darin, diesen derart zu überlasten, dass seine Dienste nicht mehr abrufbar sind. Da moderne Server in der Regel mehr Anfragen verarbeiten können, als ein einzelner Rechner produzieren kann, wird für einen solchen Angriff meistens eine Vielzahl von Rechnern zu einem sogenannten Botnetz zusammengeschlossen, um so die Rechenleistung der Angreifer-Infrastruktur zu vervielfachen. In diesem Fall spricht man von einem Distributed-Denial-of-Service (DDoS)-Angriff.

→ ***Seite 6***

→ *Desinformation*

Desinformation ist die Verbreitung falscher oder irreführender

Informationen, um Einzelpersonen, Gruppen oder die öffentliche Meinung als Ganzes zu beeinflussen. Eine Desinformation liegt vor, wenn sie nach objektiven Maßstäben inhaltlich unzutreffend ist, der Urheber dies weiß und sie dennoch mit dem Ziel der Beeinflussung verwendet. Gleiches gilt für das Verschweigen wesentlicher Teile einer Information. Desinformationsaktivitäten sollen Emotionen, Wahrnehmungen und Einstellungen verändern. Sie sind ein klassisches Instrument fremder Nachrichtendienste, die damit ihre Regierungen beim Ausbau der politischen, wirtschaftlichen oder strategischen Positionen sowie der internationalen Reputation unterstützen.

→ ***Seite 5***

→ *Einflussnahme*

Einflussnahme kann legitim oder illegitim erfolgen. Staaten verfolgen ihre Interessen über eine Vielzahl zulässiger, meist diplomatischer Aktivitäten. Darüber hinaus gibt es aber auch unzulässige Einflussnahmeaktivitäten. Diese erfolgen eher im Verborgenen, unter Vorspiegelung falscher Tatsachen und teilweise unter Einsatz von Nachrichtendiensten. Sie sollen auf Meinungs- und Willensbildungsprozesse sowie Entscheidungs- und Funktionsträger anderer Staaten einwirken, das Vertrauen der Bevölkerung in die Institutionen und die Mechanismen der Demokratie schwächen oder Bündnisse untergraben.

→ ***Seite 5***

→ *Hacktivismus*

Hacktivismus ist eine Kombination aus „Hacking“ und „Aktivismus“ und bezeichnet den Einsatz von Mitteln und Methoden der Cyberkriminalität, die aber nicht dem kriminellen Gelderwerb dienen. Die Aktionen sind häufig politisch oder ideologisch, aber auch moralisch oder religiös motiviert. Computer und Netzwerke sind gleichzeitig Tatmittel und Angriffsziele. Attacken von Hacktivisten können beispielsweise zur Umgehung der Zensur autoritärer Regime erfolgen, aber auch zur Desinformation oder zur illegalen Ausforschung von schützenswerten Geheimnissen.

→ ***Seite 8***

→ *Legende*

Legende bezeichnet im Sprachgebrauch der Nachrichtendienste die Verwendung ganz oder teilweise

erfundener oder geänderter biographischer Daten, um den nachrichtendienstlichen Auftrag zu erfüllen und für sie tätige Personen gegenüber Dritten zu schützen.
Im Rahmen einer Legende werden Tarnmittel eingesetzt, wie beispielsweise gefakte E-Mail Adressen, Webseiten etc.
→ ***Seite 5***

→ *Malware*

Malware sind Computerprogramme, die entwickelt wurden, um von Benutzern unerwünschte, unautorisierte und gegebenenfalls schädliche Funktionen ausführen zu können. Malware ist ein Oberbegriff, der unter anderem auch den Begriff Computervirus umfasst.
→ ***Seite 6***

→ *„Man-in-the-Middle"-Angriff*

Ein „Man-in-the-Middle"-Angriff schaltet sich zwischen zwei Kommunikationspartner ein. Sendet eines der beiden Kommunikationssysteme Daten an das andere, fangen die Angreifer die Information zunächst ab und verarbeiten sie für ihre Zwecke weiter. Anschließend leiten sie die Daten an den ursprünglich vorgesehenen Empfänger weiter. Je nach Absicht der Angreifer leiten sie entweder die Originaldaten weiter oder manipulieren diese vorher.
→ ***Seite 6***

→ *Nachrichtendienste*

Nachrichtendienste sammeln Informationen über Bestrebungen die die innere oder äußere Sicherheit eines Staates gefährden und werten sie aus. Hierbei können sie verdeckt arbeiten. Die Ergebnisse der Analyse werden in Berichtsform zusammengefasst und den politischen Entscheidungsträgern, den Kontrollgremien sowie teilweise auch der Öffentlichkeit zur Verfügung gestellt. In Deutschland gibt es folgende Nachrichtendienste: Das BfV und 16 Landesämter für Verfassungsschutz für die innere Sicherheit, den Bundesnachrichtendienst (BND) für die Aufklärung des Auslands und das Bundesamt für den Militärischen Abschirmdienst (BAMAD) für die Bundeswehr.

Ausländische Nachrichtendienste sind in Deutschland aktiv, um Informationen aus allen Bereichen des öffentlichen Lebens zu gewinnen (politische, wirtschaftliche, militärische Entwicklungen und Entschei-

dungen). Hinsichtlich ihrer Organisation und ihrer Befugnisse sind diese Dienste in den verschiedenen Staaten unterschiedlich ausgestaltet.
→ ***Seite 9***

→ *Phishing*
Unter Phishing versteht man den Versuch, in der elektronischen Kommunikation persönliche Daten illegal abzugreifen und für unzulässige Zwecke zu verwenden. Mit gefälschten E-Mails, Websites oder Anrufen sollen Daten (zum Beispiel Passwörter oder Kreditkartennummern) erlangt werden, ohne dass die Opfer die Manipulation erkennen.
→ ***Seite 6***

→ *Proxy-Server*
Proxy (englisch „Stellvertreter“) beschreibt in der Cyberabwehr einen Vermittler in Computernetzwerken. Ein Proxy-Server dient als Stellvertreter für die Anfragen eines Clients beziehungsweise für Anfragen an einen Webserver und leitet diese weiter.
→ ***Seite 19***

→ *Ransomware*
Ransomware beschreibt eine Schadsoftware, welche Dateien auf dem infizierten Rechner eines Opfers verschlüsselt und im Anschluss mit einem Entschlüsselungs-Key sichert. Der Besitzer des Rechners kann diesen dadurch nicht mehr nutzen. Angreifer können dann für die Entschlüsselung ein Lösegeld mit dem Versprechen fordern, den Entschlüsselungs-Key nach Bezahlung zu übersenden. Sie können diesen aber auch zerstören und eine Entschlüsselung somit nahezu unmöglich machen.
→ ***Seite 6***

→ *Sabotage*
Sabotage ist das Einwirken auf Einrichtungen und Prozesse in Politik, Wirtschaft, KRITIS sowie Militär mit dem Ziel, diese zu beschädigen oder zu zerstören. Besonders gefährdet sind Anlagen und Einrichtungen im Bereich KRITIS (zum Beispiel Kraftwerke, Verkehrsverbindungen oder Kommunikationsanlagen).
→ ***Seite 9***

→ *Schadsoftware*
Schadsoftware und Malware werden häufig synonym verwendet und sind

Sammelbegriffe für „bösartige“ Programme. Sie haben zumeist das Ziel, nach der Infektion eines Systems zusätzliche Schadsoftware nachzuladen. Die Software ist üblicherweise für eine bestimmte, oftmals besonders gängige Betriebssystemvariante konzipiert. Die häufigsten Kategorien von Schadsoftware sind Virus, Wurm und Trojaner.

→ ***Seite 6***

→ *Social Engineering*

Social Engineering dient dazu, Informationen über Menschen zu sammeln, um sie zu einem bestimmten (sicherheitskritischen) Verhalten zu verleiten. Social Engineering ist Teil der Vorbereitung von weiterführenden Aktivitäten, wie zum Beispiel Cyberangriffen oder nachrichtendienstlichen Anwerbungsversuchen in der Realwelt wie im Cyber- und Informationsraum. Die zusammengestellten Informationen dienen dazu, bestimmten Menschen gezielt E-Mails zuzusenden, deren Inhalt scheinbar ihren persönlichen Interessen entspricht. Dadurch sollen diese meist zum Öffnen präparierter Dateianhänge verleitet werden, wodurch dann ihre Geräte mit Malware infiziert werden können.

→ ***Seite 16***

Notizen

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Merianstraße 100
50765 Köln
www.verfassungsschutz.de

Cyberabwehr des BfV
Tel.: +49 (0)228 99 792-2600
cyberabwehr@bfv.bund.de

Präventionsbereich des BfV
Tel.: +49 (0)228 99 792-3322
Tel.: +49 (0)30 18 792-3322
wirtschaftsschutz@bfv.bund.de

Layout & Produktion
Bundesamt für Verfassungsschutz
Mediengestaltung und Druck
im ServiceCenter I

Stand
Februar 2026 (B-0048)

Bildnachweis

picture alliance/Science Photo Library, RICHARD JONES (Titelbild) | BfV/KI Generiert (S. 4) | BfV/KI Generiert (S. 7) | picture alliance/HELMUT FOHRINGER/APA/picturedesk.com, HELMUT FOHRINGER (S. 8) | BfV/Broschürentitel (S. 10) | BfV/KI Generiert (S. 12 oben u. unten) | picture alliance/Zoonar, Bruno Coelho (S. 13) | picture alliance/imageBROKER, G. Lenz (S. 15) | BfV/KI Generiert (S. 16) | BfV/KI Generiert (S. 17 oben u. unten) | iStock.com/liulolo (S. 18) | iStock.com/patpitchaya (S. 22).

www.verfassungsschutz.de