Köln, August 2025

Bundesamt für Verfassungsschutz

BfV CYBER INSIGHT
Im Schatten des Cyberspace

Teil 1: Cyberangriffe – Wer? Wie? Was?

Im Schatten des Cyberspace

Teil 1: Cyberangriffe – Wer? Wie? Was?

Inhalt

1. Einleitung

Die Welt des Cyberspace ist ein dynamisches und komplexes Umfeld, das zahlreiche Herausforderungen mit sich bringt. Nahezu täglich finden sich Nachrichten über Datenlecks, Hackerangriffe oder staatlich unterstützte Cyberoperationen. Diese Berichte verdeutlichen, dass Cyberangriffe längst keine Fiktion mehr sind, sondern eine ernstzunehmende Bedrohung für Unternehmen, Regierungen und Privatpersonen darstellen. Hinter diesen Angriffen stehen oft hochprofessionelle Akteure, die gezielt und klandestin vorgehen, um sensible Informationen zu erlangen, Abläufe zu stören und Schaden zu verursachen.

Der Schutz vor solchen Angriffen wird zunehmend komplexer. Im digitalen Raum gibt es keinen physischen Safe, der vor Angriffen schützt – besonders wenn die Angreifer neueste technische Möglichkeiten wie Künstliche Intelligenz (KI) nutzen, um Schwachstellen zu identifizieren oder ausgeklügelte Angriffsoperationen durchzuführen. KI wird heute bereits eingesetzt, um Sicherheitslücken schneller zu erkennen, gleichzeitig aber auch, um immer raffiniertere Angriffsmethoden zu entwickeln. Das macht den Schutz von Daten und sensiblen Infrastrukturen zu einer der größten Herausforderungen im digitalen Zeitalter.

Doch was genau ist eigentlich ein Cyberangriff? Wie ordnet man einen Angriff einem Akteur zu? Wer sind die Akteure und welche konkreten Ziele verfolgen Angreifer? Und welche Methoden nutzen unterschiedliche Akteure für ihre Attacken?

Das Bundesamt für Verfassungsschutz (BfV) beleuchtet diese Fragen in einer CYBER INSIGHT-Doppelserie:

- Im Schatten des Cyberspace, Teil 1: Cyberangriffe – Wer? Wie? Was?
- Im Schatten des Cyberspace, Teil 2: Die Welt der APTs

2. Was sind Cyberangriffe: Definition und Grundlage

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 von erfolgreichen Cyberangriffen können variieren, von geringfügig bis verheerend: Störung von Betriebsabläufen, Abfluss von Informationen, Zugangsverweigerungen, Manipulation, Beschädigung oder Zerstörung von Hardware, Daten, Netzwerken, Kritischen Infrastrukturen oder technischen Systemen. Dabei bergen Cyberangriffe ein geringes Enttarnungsrisiko mit relativ hoher Erfolgswahrscheinlichkeit.

Cyberangriffe sind heute nicht mehr nur das Werk einzelner Hacker, Hacktivistenkollektiven oder krimineller Gruppen. Stattdessen werden sie zunehmend von staatlichen Akteuren oder von ihnen beauftragten Organisationen ausgeführt. Diese gezielten Angriffe werden oft von Regierungen oder anderen staatlichen Stellen wie staatlich unterstützten Gruppen geplant und koordiniert. Im Gegensatz zu (meist finanziell oder persönlich motivierten) kriminellen Hackern verfolgen die Angriffe staatlicher Akteure oft das Ziel, mittels Cyberspionage sensible Daten zu stehlen, Kritische Infrastrukturen durch Cybersabotage zu schädigen oder zu zerstören, politische Destabilisierung durch Einflussnahme- bzw. Desinformationsaktivitäten zu bewirken oder wirtschaftliche und militärische Vorteile zu erlangen. Dabei kommen häufig hochentwickelte Technologien zum Einsatz, die es ermöglichen, Angriffe lange unentdeckt durchzuführen. Durch das geringe Enttarnungsrisiko haben Cyberangriffe eine relativ hohe Erfolgswahrscheinlichkeit, da sie sich einer Vielzahl von möglichen Angriffsmustern bedienen.

- Durch die zunehmende Vernetzung im Cyberraum sind Cyberakteure in der Lage, weltweit zu operieren. Damit sind Cyberangriffe an keinen bestimmten Ort gebunden und global einsetzbar, sodass ein Angriff aus einem Drittland erfolgen kann, in dem weder Angreifer noch Angriffsziel ansässig sind.
- Cyberakteure agieren anonym, personenunabhängig aus der Ferne und durch automatisierte Methoden. Dabei benötigen Cyberangriffe keine aufwendige

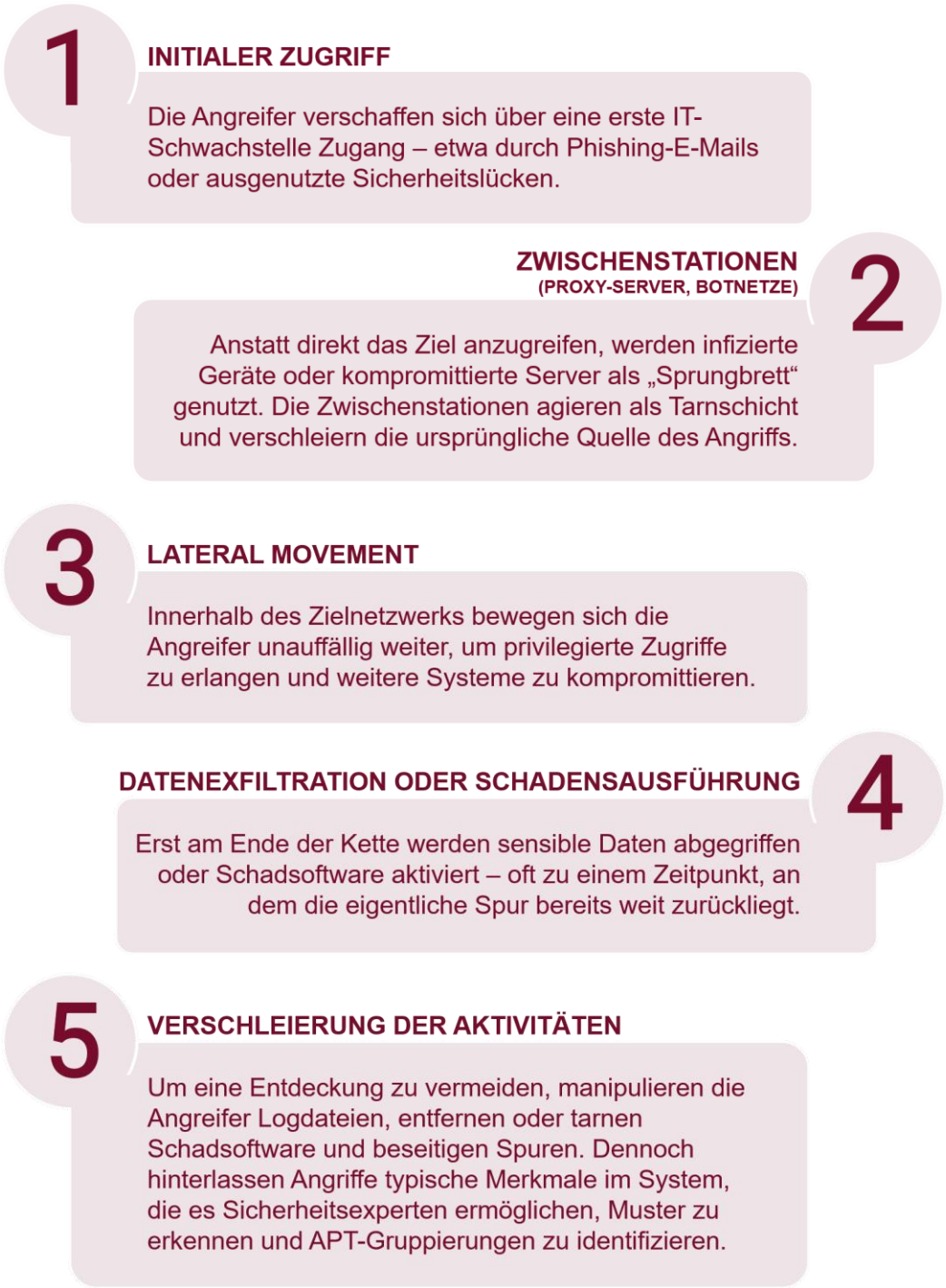
Anwerbungsphase, in der Vertrauen und ein Zugang zum Ziel aufgebaut werden muss. Zudem ist keine komplexe Legendierung notwendig.

- Ein erfolgreicher Cyberangriff kann den Zugriff auf große Mengen sensibler Daten ermöglichen und erlaubt im Erfolgsfall den schnellen und massenhaften Abfluss von Informationen. Innerhalb kurzer Zeit können ganze Datenbanken, Kommunikationsverläufe oder Forschungsergebnisse extrahiert werden – in einem Tempo und mit einer Tiefe, die mit herkömmlichen Mitteln, beispielsweise über das Anwerben menschlicher Quellen, kaum erreichbar sind. Zudem können einmal entwickelte Angriffsstrukturen mehrfach genutzt und angepasst werden, was langfristige Cyberoperationen ermöglicht, die mit geringem Aufwand immer wieder erweitert werden können.
- Cyberangriffe dienen nicht nur dem reinen Abfluss von Informationen, sondern sind auch eine wirkungsvolle Methode zur Informationssteuerung. Durch gezielte Desinformationskampagnen können Angreifer falsche oder manipulierte Informationen und Daten verbreiten, so die öffentliche Meinung beeinflussen und dadurch das Vertrauen in Institutionen des demokratischen Rechtsstaates sowie in die Medien schwächen. Dies geschieht beispielsweise durch das Hacken und Verändern von Nachrichtenquellen, die Verbreitung gefälschter Dokumente oder den Einsatz von Social Bots, um Fehlinformationen gezielt in sozialen Netzwerken zu streuen.
- Cyberakteure agieren häufig über längere Zeit unentdeckt in den angegriffenen Systemen. In vielen Fällen sind die Täter bereits erfolgreich, bevor ein Angriff überhaupt erkannt wird. Die Zuordnung der Angriffe (Attribution) gestaltet sich meist äußerst schwierig und ist manchmal sogar unmöglich. Daher sind Cyberangriffe ein besonders effektives Mittel für fremde Nachrichtendienste, um den Ursprung von Spionage- oder Sabotageaktivitäten zu verschleiern.

3. Angriffsketten im Cyberraum: So funktionieren Cyberangriffe

Cyberangriffe staatlicher Akteure sind komplex und verlaufen häufig über lange Ketten, um ihren Ursprung zu verschleiern. Angreifer haben ein Interesse, möglichst lange und unentdeckt zu agieren und handeln entsprechend vorsichtig. Ihre Angriffsketten bestehen in der Regel aus mehreren aufeinanderfolgenden Schritten, die bewusst über verschiedene Systeme, Netzwerke und oftmals auch über unterschiedliche geografische Standorte verteilt werden. Jeder dieser Schritte dient dazu, die Identität der Angreifer zu verschleiern, die Zuordnung zu erschweren und gleichzeitig das Zielsystem

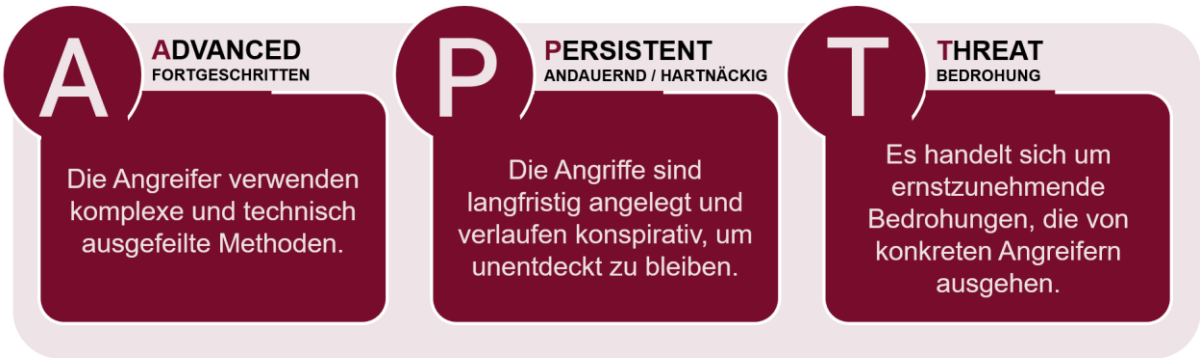
möglichst unbemerkt zu infiltrieren. Der Ablauf einer solchen Kette kann beispielsweise wie folgt aussehen:



Sicherheitsmaßnahmen, die lediglich einzelne Systeme überwachen, erkennen solche Angriffe gegebenenfalls zu spät oder gar nicht, da einzelne Aktivitäten oft harmlos erscheinen. Durch die mehrstufige Vorgehensweise wird die Rückverfolgung eines Cyberangriffs erheblich erschwert.

4. Advanced Persistent Threats (APTs): Merkmale und Hintergründe

Unter Advanced Persistent Threats (APTs) werden komplexe und zielgerichtete Bedrohungen verstanden, die sich gegen ein oder mehrere Opfer richten. Der Begriff APT steht im Einzelnen für folgendes:



Ein APT-Angriff soll nach Möglichkeit unentdeckt bleiben, um vertrauliche Daten angegriffener Stellen in Politik und Verwaltung, Wirtschaft und Wissenschaft oder von zivilgesellschaftlichen Einrichtungen oder Einzelpersonen über einen längeren Zeitraum auszuspähen oder anderen Schaden zu verursachen. APT-Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten und Methoden aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren. In der Praxis werden mit dem APT-Begriff ressourcenstarke Cyberangreifergruppen beschrieben, die in der Regel staatlich gesteuert sind. Je nach staatlichem Akteur und dessen strategischer Zielsetzung unterscheiden sich APT-Gruppen deutlich in ihrer personellen Zusammensetzung und Organisationsstruktur. Einige dieser Gruppen bestehen aus kleinen, hochspezialisierten Einheiten innerhalb staatlicher Nachrichtendienste oder militärischer Organisationen, die gezielte Cyberoperationen gegen ausgewählte Ziele durchführen. Andere sind Teil größerer, umfassend organisierter Strukturen und agieren etwa innerhalb eines komplexen Cyber-Ökosystems mit umfangreichen Ressourcen. Entsprechend reicht das Spektrum staatlich gesteuerter

APTs von kompakten Einsatzteams bis hin zu komplexen Organisationen, die mit nachrichtendienstlicher Präzision und strategischer Ausrichtung agieren.

5. Cyberangreifer benennen: Die Strategien hinter den Bezeichnungen der APT-Gruppierungen

Die Namen der Angreifer-Gruppierungen werden oft anhand von Merkmalen wie der verwendeten Malware, bestimmten Code-Fragmenten oder den ersten beobachteten Angriffen vergeben. Bei dem genutzten Namen handelt es sich um eine Bezeichnung, die IT-Sicherheitsunternehmen vergeben. Ein und dieselbe Gruppierung kann daher durchaus mehrere Namen gleichzeitig haben (wie beispielsweise das auf einer Durchnummerierung basierende Kürzel APT 29 oder die Bezeichnung Cozy Bear).

Bei der Bezeichnung der APTs hat jedes IT-Sicherheitsunternehmen seine eigene Systematik. Die einen nummerieren die von ihnen identifizierten Gruppierungen durch, da sie keine Rückschlüsse auf den Ursprung unmittelbar mitteilen können oder wollen. Andere vergeben Namen von Tieren, die allgemein für die Herkunftsregion der APT stehen sollen. So werden Cybergruppierungen, die mit Russland in Verbindung gebracht werden, häufig als Bären bezeichnet – wie Cozy Bear oder Berserk Bear. Die Katze bei Charming Kitten steht symbolisch für den Iran. Chinesische Gruppierungen werden je nach Analysten Drachen oder Pandas genannt.

Cyberangreifergruppen erhalten Namen, um sie identifizieren und unterscheiden zu können. Da es viele verschiedene Gruppen mit unterschiedlichen Zielen, Methoden und Hintergründen gibt, erleichtert die Benennung die Kommunikation und Analyse innerhalb der Sicherheitsforschung und zwischen (Cyber-)Sicherheitsbehörden. Namen helfen dabei, bestimmte Angreifergruppen zu kategorisieren, ihre Aktivitäten nachzuvollziehen und gezielt Gegenmaßnahmen zu entwickeln.

Für die Cyberabwehr des BfV sind die einzelnen Namen jedoch nicht entscheidend. APT-Gruppierungen führen ihre Angriffe häufig mit denselben Taktiken, Techniken und Verfahrensweisen durch. Das Kürzel dafür lautet TTP, es leitet sich aus dem Englischen „Tactics, Techniques and Procedures“ ab. Diese Elemente des Vorgehens sind wichtige Komponenten im Bereich der Cybersicherheit. Sie stellen die Strategien (Taktiken), Methoden (Techniken) und detaillierten Prozesse (Verfahren) dar, die

Cyberakteure verwenden, um in IT-Systeme einzudringen. In der Analyse der TTPs und der Zielauswahl liegt ein Schlüssel, um Ursprung und Motiv eines Angriffs festzustellen. Mit diesen Informationen können potenzielle Angriffsopfer wie Unternehmen oder Behörden besser vor möglichen Angriffen gewarnt und Schutzmaßnahmen eingeleitet werden, bevor ein Angriff stattfindet.

6. Cyberangriffe zuordnen: Die Attribution und Identifikation der Urheber

In der Welt der Cyberangriffe ist die genaue Identifizierung der Täter – die sogenannte Attribution – eine der größten Herausforderungen. Derzeit gibt es viele APT-Gruppen und auch deshalb ist es herausfordernd, sie treffend zu unterscheiden und ihre Angriffe zu attribuieren, aber es ist nicht unmöglich. Dazu werden verschiedene Aspekte der Angriffskampagne analysiert. Um die nötigen technischen und politischen Hinweise zusammenzuführen, ergreift die Cyberabwehr des BfV verschiedene Maßnahmen, darunter:

- eigene operative Schritte,
- Austausch mit Partnerdiensten,
- Auswertung von Berichten von IT-Sicherheitsunternehmen und
- die Untersuchung offener Quellen.

Die Puzzlestücke eines möglichen Cyberangriffs setzen sich so nach und nach zu einem Gesamtbild zusammen. APT-Gruppierungen führen ihre Angriffe häufig mit denselben TTPs durch. Dazu zählt beispielsweise der Kreis der beabsichtigten Angriffsziele, auf welche Art und Weise die Angreifer eigene Tools entwickeln oder welche einzelnen Schritte eine Gruppierung bei ihren Angriffen macht. Sofern mehrere Angriffe die gleichen TTPs aufweisen, lässt sich ein Muster in der Angriffsweise erkennen. Dann kann in der Regel davon ausgegangen werden, dass es sich um dieselbe Angreifergruppierung handelt. Fortan können entsprechende Angriffe dieser Gruppierung zugeschrieben und unter demselben APT-Namen zusammengefasst werden.

7. Staatliche Cyberakteure: Disruption und Abwehrstrategien

Die Bedrohung durch nachrichtendienstliche Cyberakteure ist eine zentrale Herausforderung für die Cybersicherheit. Die Digitalisierung erweitert das Spektrum möglicher gezielter Angriffe und damit die Risiken für Kritische Infrastrukturen, Unternehmen und Regierungsorganisationen. Staatliche Cyberakteure profitieren von der globalen Vernetzung im Cyberspace, verfügen über enorme Ressourcen sowie eine hohe technische Expertise und verfolgen langfristige Angriffsstrategien.

Mit der rasanten Entwicklung von KI entstehen sowohl neue Bedrohungen im Cyberraum als auch neue Abwehrmöglichkeiten. KI wird bereits jetzt eingesetzt, um Angriffsoperationen noch gezielter, effizienter und schwerer zuordenbar zu machen. Deepfakes, automatisierte Phishing-Kampagnen und selbstlernende Schadsoftware sind nur einige Beispiele für neue Cybertools. Angriffsstrategien können zudem durch Machine Learning angepasst werden, sodass sich APTs dynamisch an neue Sicherheitsmaßnahmen anpassen können.

Auf der anderen Seite bietet KI auch Chancen zur Verbesserung der Datensicherheit und der Aufklärung von Cyberangriffen. Sicherheitslösungen, die KI-gestützt Anomalien im Datenverkehr detektieren, können helfen, APT-Aktivitäten frühzeitiger zu erkennen. Automatisierte Reaktionssysteme können verdächtige Prozesse stoppen, bevor sie größeren Schaden im System anrichten. Zudem sind gut gewartete IT-Systeme, regelmäßige Sicherheitsupdates für Betriebssysteme und Anwendungen sowie Antivirus- und Endpoint-Schutz unerlässlich. Sichere Passwörter und Mehr-Faktor-Authentifizierung sollten Standard sein. Netzwerksegmentierung und eine restriktive Rechtevergabe nach dem „Need-to-know“-Prinzip erschweren die unbemerkte Ausbreitung von Angreifern im System. Regelmäßige Schulungen zu Phishing und dem sicheren Umgang mit E-Mails sind auch künftig erforderlich. Klare Meldewege und Notfallpläne ermöglichen schnelle Reaktionen, und verdächtige Links sowie Anhänge sollten stets kritisch geprüft werden.[1]

[1] Detaillierte Informationen und Tipps zur IT- und Cyber-Sicherheit bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI). Es ist die zentrale Anlaufstelle in Deutschland, zuständig für die Entwicklung von Sicherheitsstandards, die Beratung von Behörden und Unternehmen sowie die Durchführung von Sicherheitsanalysen. Zudem fördert das BSI die Sensibilisierung der Öffentlichkeit für die IT-Sicherheit.

Die Zukunft einer erfolgreichen Cyberabwehr wird maßgeblich von technologischem Fortschritt, internationaler Zusammenarbeit und der Weiterentwicklung von Cyberabwehr-Strategien abhängen. Nur durch kontinuierliche Innovationen und vorausschauende Sicherheitsstrategien kann unsere digitale Welt vor Bedrohungen aus dem Schatten des Cyberspace geschützt werden.

In dem Maße, wie staatliche Cyberakteure immer raffiniertere Techniken entwickeln, geht das BfV als Cyberabwehrbehörde aktiv dagegen vor. Dabei nimmt das BfV eine zentrale Rolle in der Bekämpfung von nachrichtendienstlich gesteuerten Cyberangriffen ein. Die Aufgaben des BfV umfassen:

Das BfV sensibilisiert im Rahmen der Prävention Politik und Verwaltung, Wirtschaft und Wissenschaft wie Zivilgesellschaft mit seinen Erkenntnissen aus Detektion und Attribution und unterstützt so mit gezielten Informationen und Präventionsprodukten, die auf der Webseite des BfV abrufbar sind.[2] Dazu zählen insbesondere:

- Joint Cybersecurity Advisories – in Kooperation mit nationalen und internationalen Partnerdiensten herausgegebene Warnungen und technische Hinweise zu global aktiven Angriffsgruppen und laufenden Kampagnen,
- BfV Cyber-Briefe – kompakte, praxisnahe Hinweise für Unternehmen und Behörden mit konkreten Empfehlungen zu Schutzmaßnahmen,
- Sicherheitshinweise für die Wirtschaft wie für Politik und Verwaltung – das Erscheinen ist anlassbezogen,

[2] Informationen, detaillierte Analysen (BfV CYBER INSIGHT) und aktuelle Warnhinweise (BfV Cyber-Brief) sind auf der BfV-Website www.verfassungsschutz.de oder über den BfV-X-Kanal (@BfV_Bund) abrufbar.

- BfV CYBER INSIGHTs – ein Lageformat mit Hintergrundanalysen zu strategischen Bedrohungen, aktuellen Angriffskampagnen und relevanten Akteuren,
- Informationsblätter Wirtschaftsschutz – komprimierte Übersichtsdarstellungen und Verhaltenstipps zu Sicherheitsrisiken durch das Agieren fremder Nachrichtendienste.

8. Ausblick

Staatliche Akteure nutzen Cyberangriffe, Cyberspionage und Cybersabotage um ihre strategischen, politischen, militärischen, wirtschaftlichen und technologischen Ziele durchzusetzen. Informationsdiebstahl, das Schwächen von politischen Gegnern, Einflussnahme auf andere Staaten, die Sabotage von Kritischen Infrastrukturen und die Manipulation öffentlicher Meinungen über Desinformation sind schwerwiegende Folgen erfolgreicher Cyberangriffe. Cyberoperationen staatlicher Stellen sind längst fester Bestandteil geopolitischer Auseinandersetzungen und werden zunehmend raffinierter, gezielter und schwerer nachweisbar.

Im zweiten Teil der CYBER INSIGHT-Doppelserie „Im Schatten des Cyberspace, Teil 2: Die Welt der APTs“ beantwortet das BfV wer die Akteure staatlich gesteuerter Cyberangriffe sind und welche konkreten Ziele die Angreifer verfolgen.

Anhang: Angriffsvektoren im Cyberraum / Methoden staatlicher Cyberakteure

Cyberangriffe staatlicher Akteure richten sich meist nach dem Zielspektrum und Aufklärungsinteresse der dahinterstehenden Regierungen. Sie verfügen über effektive Tools, um Daten zu sammeln und relevante Informationen zu gewinnen. Je nach Strategie und Taktik wählt der Cyberakteur seinen Angriffsvektor aus, also die Methode, um in das Opfersystem einzudringen und dort Schadsoftware zu installieren. Die Analyse vergangener Kampagnen zeigt eindrücklich, über welch weitreichendes Arsenal potenter Tools staatliche Cyberakteure verfügen. Dabei hängt der Erfolg des genutzten Angriffsvektors von den im Zielsystem eventuell vorhandenen Sicherheitslücken ab.

In der nachfolgenden Tabelle werden die gängigsten Angriffsvektoren aufgelistet und ihre Funktionsweise erklärt:

Angriffsvektor	Funktionsweise
Brute-Force-Angriff	Mit einem Brute-Force-Angriff (zu Deutsch: „rohe Gewalt“) versucht der Angreifende ein Passwort oder PIN dadurch zu knacken, dass alle möglichen Zeichenkombinationen ausprobiert werden.
Credential-Phishing	Beim Credential-Phishing stehen die Zugangsdaten (Credentials) eines Opfers im Fokus. Der Angreifende gibt sich hierzu als seriöse Instanz aus und fordert das Opfer zumeist per E-Mail auf, seine Nutzerdaten zum Beispiel über ein gefälschtes Kontaktformular zu bestätigen.
Exploit	Ein Exploit ist eine Schadsoftware, die eine oder mehrere Sicherheitslücken in einem System ausnutzt. Hat der Exploit das System erfolgreich infiziert, lädt dieser weitere Schadprogramme nach, um sich möglichst großflächig im Opfersystem auszubreiten.
„Hack & Leak“-Operationen	Angreifer dringen mittels cybergestützter Angriffstechniken in Computersysteme ein („Hack“), um diskreditierendes oder belastendes Material über das Opfer zu erlangen. Dieses Material wird anschließend im Original oder in verfälschter Form bspw. in Onlineforen oder über Social-Media-Kanäle veröffentlicht („Leak“).
„Hack & Publish“-Operationen	Hack & Publish bezeichnet die Kompromittierung von legitimen Nachrichtenportalen, Social-Media-Kanälen oder Blogs z.B. von Personen des öffentlichen Lebens, um darüber Desinformationen zu verbreiten. Sie sind so nur schwer oder gar nicht von seriösen Inhalten zu unterscheiden.
Phishing	Das Wort Phishing leitet sich von dem englischen Wort „fishing“ (dt. angeln) ab. Darunter versteht man den Versuch, in der elektronischen Kommunikation, persönliche Daten illegal zu „angeln“ und für unzulässige Zwecke zu verwenden. Mit vermeintlich authentischen und vertrauenserweckenden E-Mails, Webseiten oder Anrufen sollen Daten (z.B. Zugangsdaten, Passwörter) erlangt werden, ohne dass Opfer die Manipulation erkennen können.
Social Engineering	Beim Social Engineering versuchen die Angreifenden, durch verschiedene psychologische oder soziale Methoden das Vertrauen ihrer Opfer zu erlangen. Der Angreifende versucht mit Hilfe falscher Angaben, das Opfer zu einem bestimmten Verhalten zu bewegen wie etwa dem Anklicken eines Links.

	Ein Beispiel für gutes Social Engineering ist eine exakt auf das Opfer mit seinen sozialen Kontakten und Interessen abgestimmte (Spear-Phishing) E-Mail.
Spear-Phishing	Spear-Phishing stellt eine spezielle Form des Phishings dar, bei der die manipulierte Website oder E-Mail an einen weitaus gezielter ausgewählten Empfängerkreis versendet wird. So stehen z.B. bestimmte Personen mit Schlüsselpositionen in Unternehmen oder Organisationen im Fokus der Angreifenden. Mithilfe einer umfangreichen Hintergrundrecherche stellt der Angreifende einen speziell für das Opfer zugeschnittenen Inhalt zusammen, sodass die Täuschung nur schwer erkennbar ist.
Supply-Chain-Angriff	Große Konzerne und Organisationen stellen für Angreifende ein mitunter schwieriges Angriffsziel dar, da sie in der Regel einen höheren technischen und finanziellen Aufwand betreiben, um ihre Netzwerke zu schützen. Bei einem Supply-Chain-Angriff (zu Deutsch: „Lieferketten-Angriff“) wird zunächst nicht direkt das eigentliche Ziel attackiert, sondern ein schwächer geschütztes Element in der Liefer- oder Versorgungskette. Durch den erfolgreichen Angriff auf diesen schwächer geschützten Zulieferer kann nun das eigentliche Ziel angegriffen werden. Dabei wird auch das Vertrauensverhältnis innerhalb der Lieferkette ausgenutzt.
Watering-Hole-Angriff	Beim Watering-Hole-Angriff nutzen die Angreifenden legitime und beliebte Websites, um ihre Opfer anzugreifen. Durch vorhandene Schwachstellen wird die Website mit Schadcode infiziert oder so verändert, dass unbemerkt eine Weiterleitung auf eine gefälschte Website erfolgt. Dort befindet sich die eigentliche Schadsoftware und infiziert das Opfer. Wie bei Raubtieren, die am Wasserloch („Watering Hole“) auf Beute warten, hat der Angreifende mit der infizierten Website ein Ziel ausgesucht, welches von seinem Opfer früher oder später aufgesucht wird.
Zero-Day-Exploit; Zero-Click-Exploit	Eine Zero-Day-Schwachstelle ist eine bislang nicht öffentlich bekannte Sicherheitslücke und/oder für welche kein Sicherheitsupdate existiert (also seit „Null Tagen“ bekannt ist). Angriffe, die auf solche Schwachstellen setzen, haben daher eine hohe Erfolgswahrscheinlichkeit. Die Ausnutzung von Zero-Days lässt zudem auf große technische oder finanzielle Ressourcen des Angreifers schließen. Zero-Click-Exploits beruhen häufig auf Zero-Day-Schwachstellen. Sie zeichnen sich dadurch aus, dass keine Interaktion des Opfers wie der Klick auf einen Link, die Aktivierung von Makros oder das Starten von ausführbaren Dateien erforderlich sind (eben „Zero Clicks“).

Impressum

Herausgeber
Bundesamt für Verfassungsschutz
Abteilung 4
Merianstraße 100
50765 Köln
poststelle@bfv.bund.de
www.verfassungsschutz.de
Tel.: +49 (0) 228/99 792-0
Fax: +49 (0) 228/99 10 792-2915

Druck
Bundesamt für Verfassungsschutz
ServiceCenter I

Stand
August 2025