Köln, August 2025

Bundesamt für Verfassungsschutz

# BfV CYBER INSIGHT
# Im Schatten des Cyberspace

## Teil 1: Cyberangriffe – Wer? Wie? Was?


SN-25137820.0*1**0

# Im Schatten des Cyberspace

## Teil 1: Cyberangriffe – Wer? Wie? Was?

## Inhalt



9 020031317961



SN-25137820.0*1**0

## 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,
- 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.

[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.

## 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.<br>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.<br>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;<br>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.<br>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“). |


SN-25137820.0*1**0

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

**Bildnachweis**
© BfV

**Stand**
August 2025


SN-25137820.0*1**0


SN-25137820.0*1**0

Köln, August 2025

Bundesamt für Verfassungsschutz

# BfV CYBER INSIGHT
# Im Schatten des Cyberspace

## Teil 2: Die Welt der APTs


SN-25137821.0*1**0

# Im Schatten des Cyberspace

## Teil 2: Die Welt der APTs

## Inhalt



9 020031317978



SN-25137821.0*1**0

## 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 Angriffe 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 und welche Methoden nutzen Akteure für ihre Angriffe? Wer sind die Akteure und welche konkreten Ziele verfolgen die Angreifenden?

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

9 020031317978



SN-25137821.0*1**0

## 2. Staatliche Cyberakteure

Staatliche Cyberakteure sind Organisationen oder Gruppen, die im Auftrag ihrer Regierungen Operationen im Cyberraum durchführen. Länder wie Russland, China, Iran und Nordkorea nutzen diese Fähigkeiten, um ihre politischen und wirtschaftlichen Interessen zu fördern. Diese Akteure sind oft gut finanziert und verfügen über umfangreiche technische Fähigkeiten und Ressourcen, was sie zu ernstzunehmenden Bedrohungen macht. Sie führen Cyberangriffe durch, um Informationen zu stehlen, Kritische Infrastrukturen zu sabotieren oder Einfluss auf politische Prozesse in anderen Ländern zu nehmen.

Russische Cyberakteure sind bekannt für ihre Desinformationskampagnen und Angriffe auf Wahlen und Politik. Chinesische Akteure konzentrieren sich neben dem politischen Raum häufig auf Wirtschaftsspionage, um technologische Vorteile zu erlangen. Iranische Cyberakteure nutzen ihre Fähigkeiten, um Dissidenten zu überwachen und geopolitische Rivalen zu destabilisieren. Nordkoreanische Cyberoperationen zielen oft darauf ab, finanzielle Ressourcen zu erschließen, um das Regime zu unterstützen, und streben an, geschütztes Forschungswissen zu erlangen.

Die Gefahren, die von diesen staatlichen Akteuren ausgehen, sind vielfältig. Sie können zu erheblichen wirtschaftlichen Schäden führen, das Vertrauen in demokratische Institutionen untergraben und durch den Abfluss vertraulicher Informationen die nationale Sicherheit gefährden. Zudem besteht die Gefahr von Cybersabotage: Angriffe auf Kritische Infrastrukturen wie Energieversorgung oder Gesundheitswesen können weitreichende Folgen haben.

## 3. Cyberakteur: Russische Föderation

Die Russische Föderation versteht sich als bedeutende Weltmacht und strebt danach, ihren Einfluss in der Welt zu bewahren und auszubauen. Insbesondere die geopolitische Konzeption des „Russkij Mir“ (dt. „Russische Welt“) ist ein zentraler Baustein für

die als imperialistisch zu bewertende Außenpolitik Russlands und vereint antiwestliche, antiliberale und neoimperiale Denkweisen. Die ehemaligen Sowjetstaaten vom Baltikum bis nach Zentralasien werden als Teil der russischen Einflusssphäre betrachtet. Die Strategie ist darauf ausgerichtet, Russlands Macht und Einfluss zu sichern. Der russische Angriffskrieg gegen die Ukraine ist ein konkretes Mittel, um diese Ziele zu verfolgen. Vor dem Hintergrund des anhaltenden Krieges gegen die Ukraine hat die Stärkung der äußeren und inneren Sicherheit sowie die Ausweitung des strategischen Einflusses in Asien und Afrika für Russland oberste Priorität. Insbesondere die NATO-Erweiterungspolitik und die Ausrichtung der EU auf das transatlantische Bündnis mit den USA werden von der russischen Führung als Gefährdung der nationalen Sicherheit angesehen.

Die Nachrichtendienste der Russischen Föderation nutzen Cyberangriffe in großem Umfang zur Verfolgung der russischen geopolitischen Interessen, zur Informationsbeschaffung, für Desinformation und Propaganda sowie zur Planung, Vorbereitung und Durchführung von Sabotageakten. Damit reihen sich die Aktivitäten im Cyberraum nahtlos in die strategischen Methoden Russlands und seiner Nachrichtendienste gegen Deutschland und andere westliche Demokratien ein.[1]

Dabei liegt der Fokus der Informationsbeschaffung mittels Cyberangriffen, analog zur Aufklärung mit traditionellen Spionagemethoden, auf allen Politikfeldern, die russische Interessen berühren können. Dies sind u.a.:

- außenpolitische Fragen (EU-, Zentralasien-, Nahost-Politik),
- Militärpolitik (insb. westliche Unterstützung der Ukraine),
- Energiepolitik und -sicherheit,
- Sanktionen,
- Ausforschung von Spitzentechnologien mit Schwerpunkt auf den Bereichen Energie-, Militär-, Röntgen- und Nukleartechnik sowie Luft- und Raumfahrt.

Neben dem russischen Inlandsgeheimdienst FSB[2] führen auch der zivile Auslandsnachrichtendienst SWR[3] und vor allem der militärische Geheimdienst GRU[4] offensive

[1] Vgl. „‘Toolbox Russland‘ – Russlands nachrichtendienstlicher Werkzeugkasten gegen Deutschland“ unter: www.verfassungsschutz.de.

[2] Federalnaja Slushba Besopasnosti (Föderaler Dienst für Sicherheit).

[3] Slushba Wneschnej Raswedki (Dienst der Außenaufklärung).

[4] Glawnoje Raswedywatelnoje Uprawlenije (Hauptverwaltung für Aufklärung).

Cyberoperationen gegen politische bzw. wirtschaftliche Ziele und Kritische Infrastrukturen durch. Die Ausforschungsaktivitäten und Cyberangriffe richten sich unter anderem gegen supranationale Organisationen, Regierungsstellen, Streitkräfte, Parlamente, Parteien, Politikerinnen und Politiker, internationale Wirtschaftsunternehmen sowie Wissenschafts- und Forschungseinrichtungen. Zudem stellen regierungskritische und für die Presse tätige Personen, die für den russischen Staat als „unerwünscht“ oder „extremistisch“ eingestuften Organisationen, Nichtregierungsorganisationen (NGO) und Medienunternehmen weitere Ziele dar.

Um prorussische Propaganda zu verbreiten nutzen russische Akteure gezielt Desinformationskampagnen, die vor allem über soziale Medien verbreitet werden. Ziel dabei ist die Schwächung der internationalen Gemeinschaft und die Einschüchterung bzw. Diskreditierung von regimekritischen Strömungen. Politische und gesellschaftliche Spannungen sollen erzeugt oder das Vertrauen in staatliche Stellen bzw. westliche Demokratien unterminiert werden. Zudem werden mit Hilfe von Cyberangriffen Sabotageakte vorbereitet bzw. auch durchgeführt.



Zusammenfassend zeichnen sich russische Cyberangriffe durch einen hohen Professionalisierungsgrad aus. Die Angriffskampagnen finden im Rahmen einer umfassenden taktischen und strategischen Informationsgewinnung statt. Art und Umfang der Operationen weisen auf außergewöhnliche Operativ- und Auswertefähigkeiten sowie starke finanzielle Ressourcen hin. Aufgrund langjähriger Erfahrungen – einige russische APTs sind bereits seit über 20 Jahren aktiv – gehören nahezu alle erdenklichen Angriffsvektoren zu ihrem Repertoire.[5] So zeichnen sich beispielsweise russische Spear-Phishing-Angriffe durch gutes Social Engineering[6] der auf das Opfer zugeschnittenen E-Mails aus: Auf den ersten Blick handelt es sich um gut recherchierte,

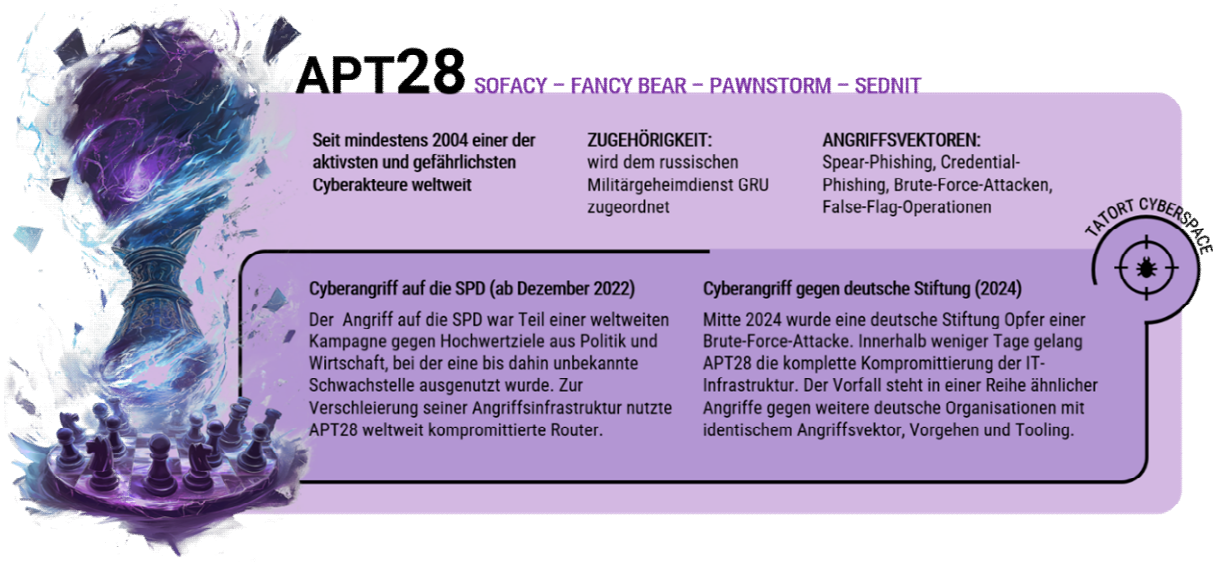
[5] Advanced Persistent Threats (APTs): komplexe und zielgerichtete Angriffe, gegen einzelne Opfer. Dahinter stehen ressourcenstarke Cyberangreifergruppierungen, in der Regel staatlich gesteuert. Angriffe im Rahmen dieser Bedrohungen („threats“) werden aufwändig vorbereitet, sind hochentwickelt („advanced“) und dauern lange an („persistent“). Sie sollen unentdeckt bleiben, um vertrauliche Daten über einen längeren Zeitraum auszuspähen (Cyberspionage) oder anderen Schaden zu verursachen (Cybersabotage). Vgl. „Im Schatten des Cyberspace, Teil 1: Cyberangriffe – Wer? Wie? Was?“.

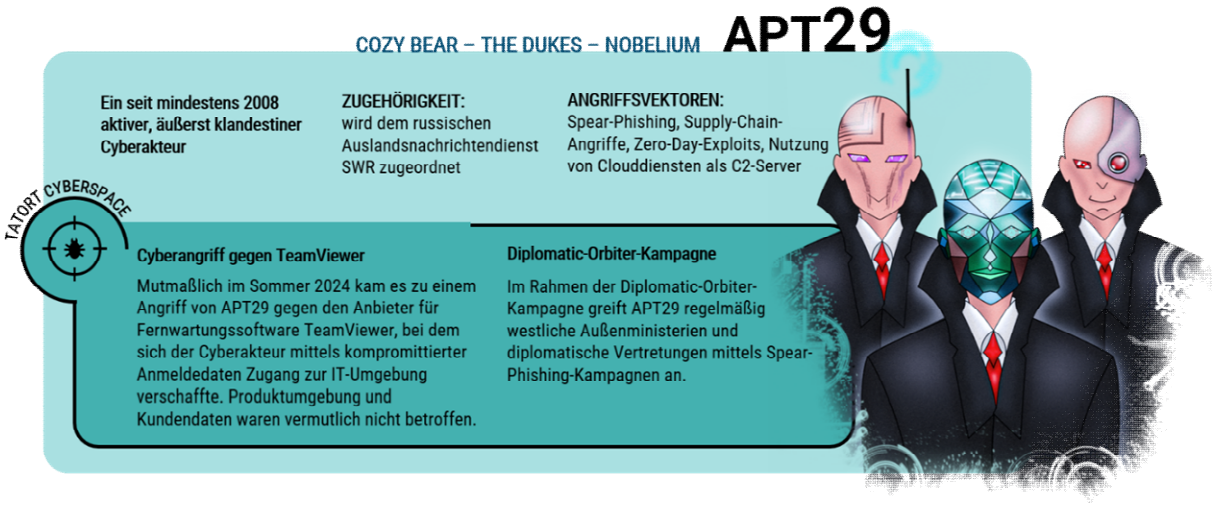
[6] Spear-Phishing: Eine Form des Phishings, bei der eine manipulierte Website oder E-Mail an einen gezielt ausgewählten Empfängerkreis versendet wird. Beispielsweise stehen Personen in Schlüsselpositionen im Fokus der Angreifenden. Durch umfangreichen Hintergrundrecherche (Social Engineering) werden Inhalte speziell auf ein Opfer zugeschnitten und diese zu einem bestimmten Verhalten veranlasst.

glaubwürdige E-Mails mit für das Opfer relevanten Inhalten (teilweise Insiderwissen) und ihm vermeintlich bekannten Absendern.

Russland ist in der Lage, auf außenpolitische Kräfteverschiebungen (insbesondere Spannungen mit EU und NATO) kurzfristig zu reagieren und setzt sowohl Cyberspionage als auch Cybersabotage zielgerichtet ein. Kollateralschäden und Auswirkungen von Aktivitäten auf andere Bereiche, die beabsichtigte oder auch unbeabsichtigte Folgen herbeiführen (auch Spillover-Effekt genannt) werden rücksichtslos in Kauf genommen. Durch die europaweite Ausweisung mehrerer Hundert russischer Nachrichtendienstangehöriger als Konsequenz des russischen Angriffskrieges gegen die Ukraine sind die russischen Nachrichtendienste gezwungen, ihr übliches Vorgehen der Informationsbeschaffung aus Legalresidenturen mit weiteren nachrichtendienstlichen Methoden zu ergänzen. Dadurch gewinnen komplexe Cyberoperationen zur Beschaffung von Informationen sowie für Desinformationskampagnen und Sabotageaktivitäten zunehmend an Bedeutung.











## 4. Cyberakteur: Volksrepublik China

Die Volksrepublik (VR) China strebt die Schaffung einer technologischen und wirtschaftlichen Unabhängigkeit an und will dabei gleichzeitig ihre globale Position stärken. Insbesondere die zwei wirtschaftlichen Strategien „Belt and Road Initiative“ (BRI) und „Made in China 2025“-Initiative der chinesischen Regierung sollen das wirtschaftliche Wachstum und damit den globalen Einfluss Chinas stärken, indem sie sowohl die Infrastrukturentwicklung als auch die technologische Modernisierung vorantreiben. China verfolgt zudem eine aggressive Politik der territorialen Ansprüche, insbesondere im Südchinesischen Meer und gegenüber Taiwan. Es strebt an, seine nationale

Souveränität zu wahren und militärische Präsenz in strategisch wichtigen Regionen auszubauen. Der völkerrechtswidrige russische Angriffskrieg gegen die Ukraine erlaubt dabei der VR China, den Umgang westlicher Staaten mit derartigen militärischen Konflikten zu beobachten. Die NATO-Erweiterungspolitik und die Ausrichtung der EU auf das transatlantische Bündnis mit den USA werden von der chinesischen Führung als Gefährdung der eigenen nationalen Sicherheit angesehen.

Im Zusammenhang mit der geopolitischen sowie außenpolitischen Ausrichtung Chinas nutzt das Land neben traditionellen Spionagemethoden insbesondere Cyberangriffe in großem Umfang zur Beschaffung von Informationen aus unterschiedlichsten politischen und wirtschaftlichen Bereichen, welche die Interessen der VR China berühren. Dazu zählen beispielsweise:

- außenpolitische Themen der EU (EU-, Zentralasien-, Nahost-Politik) mit Bezug zur VR China,
- Militärpolitik,
- Energiepolitik und -sicherheit,
- Ausspähung von Dissidenten,
- Ausforschung von Spitzentechnologien mit Schwerpunkt auf den Bereichen Energie-, Militär-, und Nukleartechnik sowie Luft- und Raumfahrt, Biotechnologie und Chip- und Halbleiterfertigung.



Die VR China ist in der Lage, auf außenpolitische Kräfteverschiebungen – insbesondere Spannungen mit EU und NATO – kurzfristig zu reagieren und setzt Cyberspionage zielgerichtet ein. Cyberangriffe richten sich zunehmend gegen deutsche Unternehmen, Institutionen, Behörden und Privatpersonen. Begleitet werden diese Angriffe durch langfristige Ansätze der Cyberspionage, die auf die digitale Souveränität Europas und somit auch Deutschlands abzielen. Besonders betroffen sind auch Unternehmen, die im Umfeld politischer Stellen tätig sind. Die Angreifer nutzen diese Unternehmen häufig als Zugangspunkt für ihre Attacken, um so an ihr eigentliches, oftmals besser geschütztes Ziel zu gelangen – sogenannte Supply-Chain-Angriffe. Besonders im Fokus stehen Cyberangriffe auf IT-Dienstleister, die für die Betreuung von Behördennetzwerken verantwortlich sind. Oft verschaffen sich die Angreifer durch die Ausnutzung bislang unbekannter Schwachstellen – sogenannter Zero-Day Exploits – Zugriff auf interne Netzwerke und breiten sich dort vorsichtig aus. Durch das Einrichten administrativer Zugänge erhalten sie dann privilegierten Zugriff auf weitere Systeme im internen Netzwerk der IT-Dienstleister (Kern-Netzwerk), um in der Folge ihre Aktivitäten

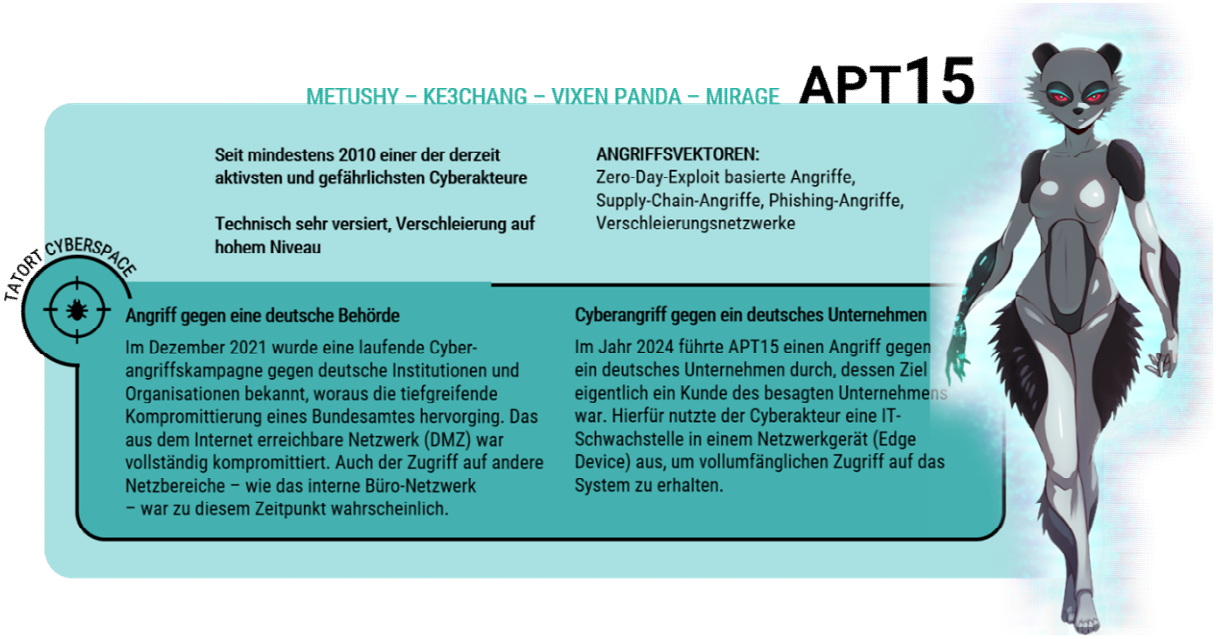
gegen den Kunden des Dienstleisters – das eigentliche Ziel – fortzusetzen. Dabei werden Cyberakteure aktiv durch die VR China und die dortige Gesetzgebung unterstützt.

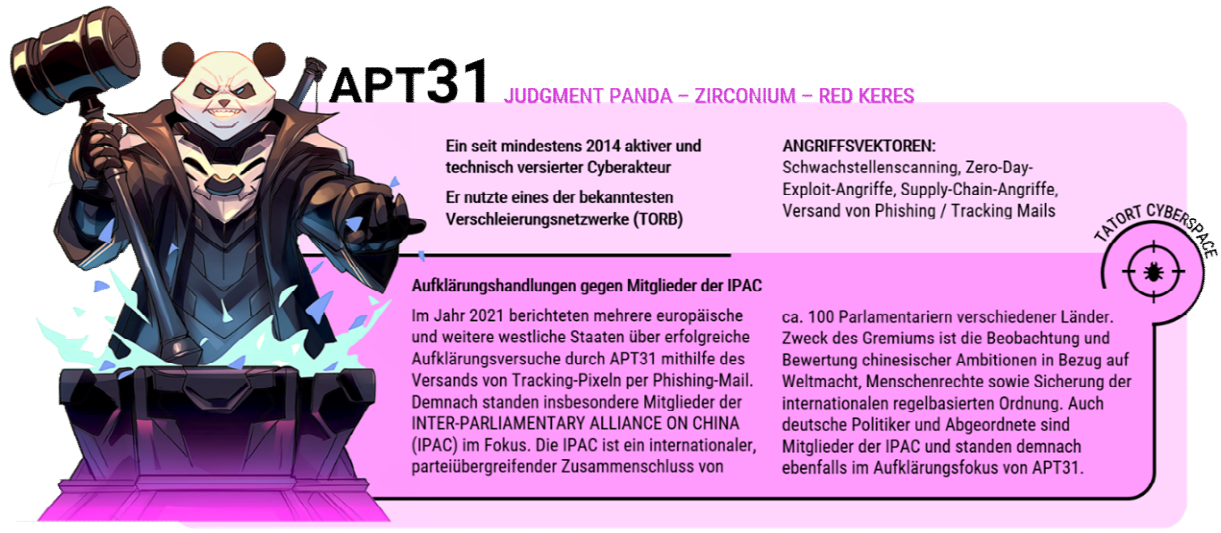
Die umfassende chinesische Cyberpolitik fördert nicht nur die Entwicklung fortschrittlicher Technologien zur Überwachung und Verteidigung, sondern ermöglicht auch eine koordinierte Zusammenarbeit zwischen staatlichen und privaten Akteuren. Dadurch wird die Fähigkeit zur Durchführung und Unterstützung von Cyberangriffen erheblich gestärkt, was die Sicherheitslage sowohl national als auch international beeinflusst. Insbesondere das chinesische Schwachstellengesetz, offiziell bekannt als „Gesetz über die Cybersicherheit von 2021“, welches am 1. September 2021 in Kraft trat, stellt einen bedeutenden Schritt in der Regulierung der Cybersicherheit in China dar. Es verpflichtet alle in China tätigen Unternehmen, einschließlich ausländischer Firmen, zur Meldung von Sicherheitsvorfällen und Schwachstellen. Die Regierung erhält damit Zugang zu sensiblen Unternehmensdaten und Informationen über Schwachstellen, die dann gegebenenfalls für gezielte Cyberoperationen benutzt werden können. Für staatliche Cyberakteure bedeutet das Gesetz eine erweiterte Befugnis zur Überwachung und Kontrolle von Cyberaktivitäten. Dies könnte sowohl staatlich unterstützte als auch kriminelle Akteure stärken, die gezielte Angriffe durchführen, und beeinflusst somit sowohl die nationale Sicherheit als auch die internationale Cybersicherheitslandschaft. Die enge Verknüpfung der staatlichen Stellen mit privaten Stellen im chinesischen Cyberraum verdeutlichen die sogenannten i-Soon-Leaks, die einen Einblick in das chinesische Cyberökosystem geben.[7] Flankierend dazu haben chinesische Cyberakteure eine beachtliche Weiterentwicklung ihrer operativen Sicherheit vorangetrieben, die sich anhand zunehmend komplexerer Techniken und in einem hohen Ressourceneinsatz äußert. Sie verwenden vermehrt sogenannte Verschleierungsnetzwerke, um ihre Aktivitäten weitestgehend zu tarnen. Dabei übernehmen Cyberangreifer in wachsender Zahl Endgeräte wie Heimrouter oder Geräte wie Smart-TVs, die für den Einsatz in kleineren Unternehmen oder von Privatanwendern konzipiert sind, und missbrauchen diese anschließend in Cyberangriffskampagnen gegen staatliche und politische Stellen.



[7] Vgl. „BfV CYBER INSIGHT: Die i-Soon-Leaks: Industrialisierung von Cyberspionage, Teil 1-4“ unter: www.verfassungsschutz.de.

Chinesische Cyberakteure zeichnen sich durch komplexe Techniken und einen hohen Ressourceneinsatz aus, die mit einer sehr hohen operativen Sicherheit einhergehen. Die ohnehin hohe Gefährdungslage durch chinesische Cyberakteure verschärft sich dabei immer weiter. Das besonders vorsichtige und heimliche Vorgehen der Cyberakteure erschwert zunehmend die Detektion, eine der anspruchsvollsten Aufgaben der Cyberabwehr. Diese geht daher von einer erheblichen Anzahl nicht erkannter, qualitativ sehr hochwertiger Cyberangriffe aus.

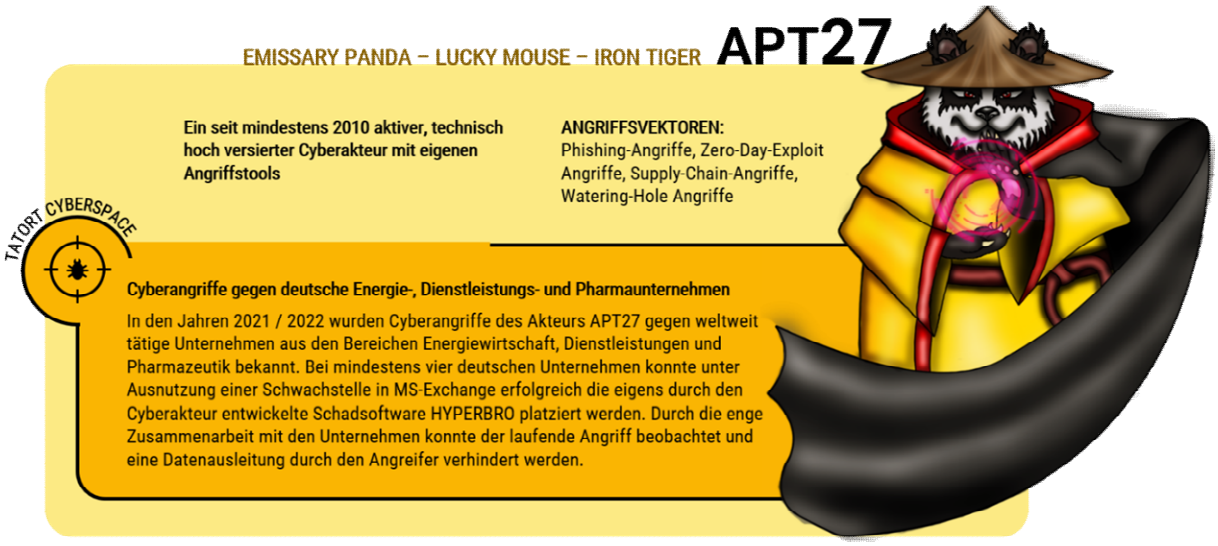



9 020031 317978



SN-25137821.0*1**0




## 5. Cyberakteur: Islamische Republik Iran

Die Islamische Republik Iran versteht sich selbst als Regionalmacht mit einer ausgeprägten antiwestlichen sowie antiisraelischen Stoßrichtung, schon lange vor den israelischen und amerikanischen Angriffen auf iranische Atomanlagen (begründet mit der Gefahr einer nuklearen Bewaffnung Teherans). Eines der vorrangigen Ziele der iranischen Nachrichtendienste ist der Schutz der „Islamischen Republik“ gegen Umsturzversuche. Hierfür ist ein wichtiger Ansatzpunkt sowohl des Ministry of Intelligence and Security[8] (der zivile In- und- Auslandsnachrichtendienst, zumeist MOIS abgekürzt) als auch der nachrichtendienstlich agierenden Islamischen Revolutionsgarde[9] (IRGC) die Überwachung von Regimekritikern und Oppositionellen im In- und Ausland durch Cyberspionage. Sie setzen daher Cyberangriffe vorrangig zur Dissidenten-Ausspähung und zur Informationsbeschaffung ein. Im Zuge des Konfliktes zwischen Israel und Iran im Juni 2025 haben proiranische Hacktivisten-Gruppierungen „Hack and Leak“-Operationen[10] gegen öffentliche und private Stellen in Israel durchgeführt. Diese wurden

[8] In Farsi: Vezerat-e-Ettela’at-e Jomhourt-ye Eslami-ye Iran – VAJA.

[9] Die IRGC, denen rund 125.000 Personen angehören sollen, verstehen sich seit ihrer Gründung nach der Islamischen Revolution 1979 als Hüter dieser Revolution. Anders als die reguläre Armee Irans unterstehen sie unmittelbar dem obersten religiösen Führer Irans Ali Khamenei. Mit der IRGC-Intelligence Organization (in Farsi: Sepah Pasdaran) unterhalten die Revolutionsgarden einen eigenen Nachrichtendienst, der sowohl für Spionage im Ausland als auch für Abwehraufgaben im Inland zuständig ist.

[10] Angreifer dringen mittels cybergestützter Angriffstechniken in Computersysteme ein („Hack“), um diskreditierendes oder belastendes Material über das Opfer zu erlangen. Dieses wird anschließend im Original oder in verfälschter Form bspw. in Onlineforen oder über Social-Media-Kanäle veröffentlicht („Leak“).

durch niedrigschwellige Störaktionen im Cyberraum, wie DDoS-Angriffe und Webseiten-Defacements[11], begleitet. Größere Cybersabotageoperationen iranischer Akteure gegen Israel wurden während des Konfliktes bislang aber nicht bekannt.

In Deutschland richten sich die nachrichtendienstlich gesteuerten Cyberaktivitäten des Regimes vorwiegend gegen Exiliraner, Oppositionelle, Regimekritiker, Journalisten und Einzelpersonen aus dem Bereich der Menschen- und Frauenrechtsaktivisten. Daneben begrenzen die umfangreichen internationalen Sanktionen gegen das Land seinen Zugang zu aktuellen wissenschaftlichen Forschungsergebnissen. Iranische Cyberspionageaktivitäten richten sich daher auch gegen akademische Einrichtungen wie Hochschulen, Forschungseinrichtungen sowie Unternehmen in forschungsintensiven Branchen, wie dem Luft- und Raumfahrtsektor. Die Cyberkapazitäten werden gezielt eingesetzt, um Know-how, Informationen und Produkte aus Branchen zu beschaffen, die für die nationale Sicherheit des Landes von Bedeutung sind.

Um an relevante Informationen zu gelangen erstellen iranische APT-Gruppierungen auf die Zielperson zugeschnittene Online-Identitäten, die unter einem glaubwürdig erscheinenden Vorwand mit dem Opfer in Kontakt treten und ein Vertrauensverhältnis aufbauen. Durch dieses im Vorfeld erfolgte Social-Engineering kann zielgerichtet ein scheinbar unbedenklicher Kontakt etabliert werden, indem sich auf Personen bezogen wird, die den Opfern bekannt sind oder Themen angesprochen werden, die den Opfern schlüssig erscheinen. Ziel ist es, an vertrauliche Daten zu gelangen – wie etwa Zugangsdaten zu Onlinediensten und E-Mail-Konten sowie Cloudspeicher- oder Messengerdiensten. Die Anbahnung erfolgt auf fast allen vorstellbaren Kommunikationsebenen. Dazu zählen beispielsweise:

- Spear-Phishing-E-Mails,
- E-Mail-Spoofing,[12]
- Kontaktaufnahme mittels gefälschten Social-Media-Accounts,

[11] Bei einem Defacement (engl. to deface – dt. entstellen / verunstalten) wird eine Webseite oder auch ein Social Media Account durch einen Angreifer unter Ausnutzung von Schwachstellen oder ausgespähten bzw. erratenen Zugangsdaten mutwillig verändert. Der Angreifer manipuliert bestehende Webseiten oder integriert neue Unterseiten mit selbst erstellten Inhalten. Die Motivation des Angreifers besteht darin, die Reputation des Betreibers zu schädigen, Desinformation zu verbreiten und/oder Ansehen in der Defacement-Szene zu erlangen. In einer verschärften Variante kann eine Webseite in Erscheinung und Inhalt komplett verändert und zur Verbreitung von irreführenden Informationen genutzt werden.

[12] Spoofing (von to spoof, auf Deutsch: manipulieren, verschleiern, vortäuschen) nennt man in der IT verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

- klassische Watering-Hole-Angriffe.[13]

Um Opfersysteme mit Schadsoftware zu infizieren setzen iranische Cyberakteure ebenfalls vergleichsweise einfache technische Mittel wie z.B. sogenannte Password Spraying Angriffe[14] erfolgreich ein. Ein weiterer gängiger Angriffsvektor ist zudem die Ausnutzung von Sicherheitslücken in der IT-Struktur, z.B. die Verwendung schwacher Passwörter oder die Verletzbarkeit ungepatchter Systeme gegen bekannte Schwachstellen.

Iranische Cyberakteure setzen eine Vielzahl von Angriffsvektoren ein und nutzen gezielt bekannte Schwachstellen in Software und Hardware aus. Dabei kommen häufig öffentlich zugängliche Schadprogramme zum Einsatz, die gegebenenfalls individuell modifiziert werden. Vereinzelt verwenden iranische Gruppierungen auch selbst erstellte Schadsoftware, die jedoch zumeist ein mittleres technisches Niveau in Bezug auf Programmierung und vor allem Verschleierung und Detektionssicherheit aufweist – insbesondere in Abgrenzung zu russischen und chinesischen Cyberakteuren. Insgesamt verfügen sie über die erforderlichen Ressourcen, um vielfältige technische Aufklärungsmaßnahmen vom Ausland aus gegen deutsche Ziele im Cyberraum auszuführen.

Iranische Cyberakteure werden auch zukünftig bemüht sein, ihre Fähigkeiten weiter auszubauen. Angesichts der umfassenden Sanktionen wird der Iran weiterhin versuchen, Know-how, Informationen und Produkte durch Cyberspionage zu erlangen. Darüber hinaus führt die anhaltend schwierige wirtschaftliche Lage im Iran zu einem hohen Konfliktpotenzial innerhalb der iranischen Gesellschaft. Im Nachgang des Israel-Iran-Konfliktes könnte das iranische Regime aus Sorge um seinen Machterhalt repressive Maßnahmen gegen Oppositionelle verschärfen. Daher wird der Überwachungsdruck der iranischen Nachrichtendienste auf Dissidenten auch durch Cyberspionage aufrechterhalten. Aufgrund der großen iranischen Community in Deutschland ist es sehr

[13] 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.

[14] Password Spraying ist eine spezielle Art eines Brute-Force-Angriffs, bei dem Cyberangreifer versuchen, mittels ein und desselben (Standard-)Passwortes einen erfolgreichen Login bei vielen unterschiedlichen Konten zu erlangen. Im Gegensatz zum „klassischen“ Brute-Force-Angriff wird versucht, durch wenige (verteilte) Anfragen eine geringere Aufmerksamkeit bei den Zielsystemen zu erwecken.

wahrscheinlich, dass Einzelpersonen und Organisationen weiterhin Ziel iranischer Cyberspionage bleiben. Auch hochrangige Personen aus Wissenschaft und Politik, die sich beruflich mit dem Iran beschäftigen, stehen weiterhin im Aufklärungsfokus iranischer Cyberakteure.


## 6. Cyberakteur: Demokratische Volksrepublik Korea

Die Nachrichtendienste der Demokratischen Volksrepublik Korea (Nordkorea) nutzen offensive Cyberoperationen weltweit zur Informationsgewinnung sowie zur Wirtschaftsspionage. Mit Cyberangriffen zur Devisenbeschaffung finanziert das Regime sein Nuklearprogramm. So hat Nordkorea bis heute Kryptowährung in dreistelliger Millionenhöhe erbeutet, vorläufiger Höhepunkt war die Kompromittierung einer Kryptobörse 2025, in deren Zuge über 1,4 Milliarden US-Dollar Schaden entstand.

Aufgrund der weitgehenden internationalen Isolation setzt Nordkorea seine Cyberkapazitäten zudem für die Sammlung politisch, diplomatisch und akademisch wertvoller Informationen ein. Entsprechende Angriffsoperationen zielten in der Vergangenheit darauf ab, Zugriff zu internen Strategiepapieren von Außenministerien oder anderweitige Dokumente mit Forschungswissen/Expertise zu erlangen, von denen das Land aufgrund der verhängten Sanktionen abgeschnitten ist. In diesem Zusammenhang fokussieren sich nordkoreanische Cyberakteure auf:

- akademische und diplomatische Ziele,

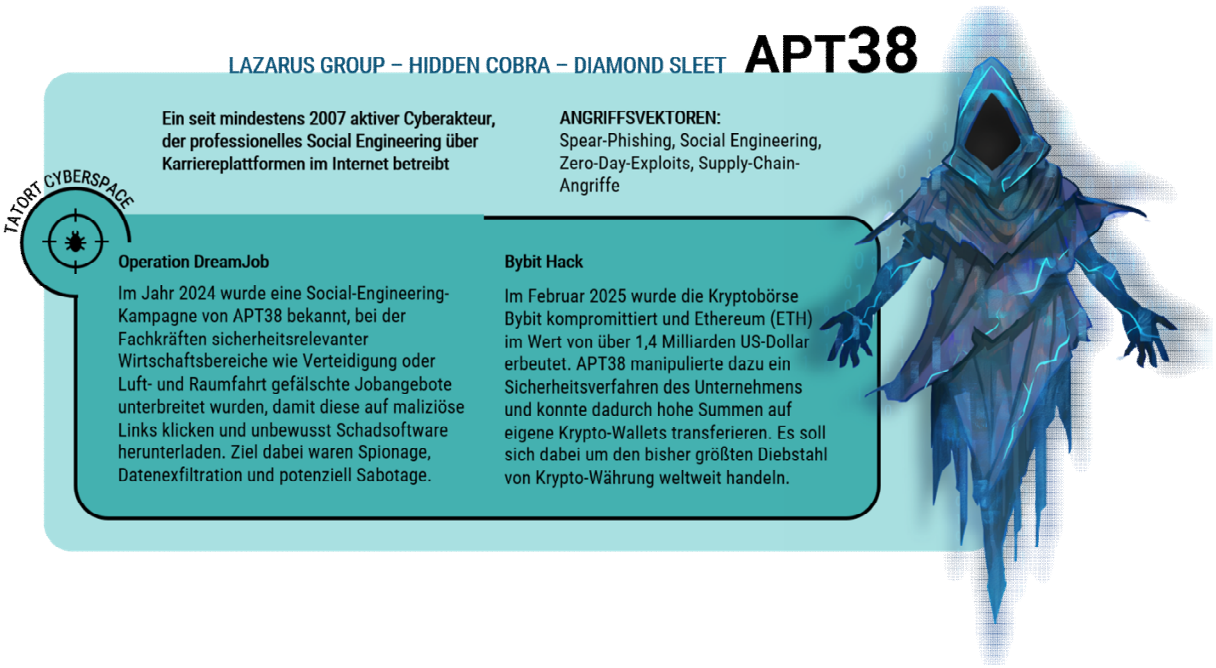
- Nichtregierungsorganisationen und Thinktanks,
- zwischenstaatliche Organisationen wie die Vereinten Nationen, die mit der Verhängung, Durchsetzung und Evaluation internationaler Sanktionen gegen Nordkorea betraut sind,
- Personen, die sich mit der politischen und humanitären Lage auf der koreanischen Halbinsel befassen,
- Akademikerinnen und Akademiker mit entsprechenden Forschungsschwerpunkten.

Darüber hinaus ist Deutschland als Heimat zahlreicher Unternehmen aus dem Verteidigungssektor sowie aus den Bereichen Luft- und Raumfahrt ein attraktives Ziel für nordkoreanische Cyberakteure. Im Jahr 2023 verübten diese weltweit Cyberspionageangriffe zur Erbeutung geschützten Know-hows aus Unternehmen der Luft- und Raumfahrt- sowie der Antriebstechnologie. Als Angriffsvektor wurde dabei mehrfach erfolgreich Social Engineering genutzt.

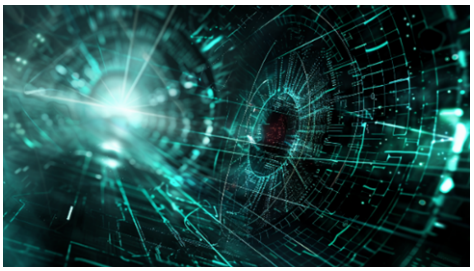
Nordkoreanische Cyberoperationen sind von Kreativität geprägt und besitzen insbesondere angesichts der wirtschaftlichen Lage des Landes ein erstaunlich hohes technisches Niveau. Dabei ist insbesondere die Gruppierung LAZARUS hervorzuheben, die auch eigens entwickelte Schadsoftware einsetzt und in der Lage ist, vorhandene Schwachstellen auszunutzen. Zwischen der ersten Kontaktaufnahme zu einem Angriffsziel bis zur Ausleitung sensibler Daten liegen dabei teilweise nur wenige Tage. Dem eigentlichen Cyberangriff geht häufig eine intensive Phase der Zielaufklärung voraus, in der potentielle Schwachstellen aufgedeckt und anschließend auch mithilfe von Zero-Day-Exploits sowie Supply-Chain-Angriffen ausgenutzt werden. All diese Aktivitäten gehen mit einem erfolgreichen Social Engineering ein.

Nordkoreanische Cyberakteure zeigen seit Jahren eine Professionalisierung ihrer technischen Fähigkeiten und Vorgehensweisen. Dadurch sind auch erfolgreiche Cyberangriffe gegen Unternehmen möglich geworden, die auf dem Gebiet der IT-Sicherheit gut aufgestellt sind. Aufgrund der perspektivisch anhaltenden politischen

Isolation des Landes ist damit zu rechnen, dass Deutschland auch weiterhin im Fokus nordkoreanischer Cyberakteure steht.




## 7. Anhaltende Bedrohungen im Cyberraum



Cyberoperationen sind längst fester Bestandteil geopolitischer Auseinandersetzungen. Die Entwicklung neuer Angriffstechniken, der Einsatz Künstlicher Intelligenz (KI) sowie die zunehmende Industrialisierung von Cyberspionage tragen dazu bei, dass Cyberoperationen immer raffinierter, gezielter und effektiver werden. Langfristig ist zu erwarten, dass Cyberangriffe zunehmend in Verbindung mit anderen Konfliktformen stehen werden, wie beispielsweise wirtschaftlichen Sanktionen, Desinformationskampagnen oder militärischen Auseinandersetzungen.

Sowohl Russland, China, Iran als auch Nordkorea werden weiterhin zu den globalen Drahtziehern im Cyberspace gehören. Dabei verfolgen sie unterschiedliche Ziele. Die Russische Föderation wird ihre Cyberfähigkeiten weiter nutzen, um politische Diskurse zu beeinflussen, Kritische Infrastrukturen ins Visier zu nehmen und geopolitische Interessen durchzusetzen. Die Volksrepublik China legt ihren Fokus weiterhin auf wirtschaftliche und technologische (Cyber-)Spionage, insbesondere mit Blick auf

Schlüsseltechnologien wie Quantencomputing und KI. Daneben ist aber auch ein starkes Aufklärungsinteresse am politischen Raum erkennbar, welches sich in Cyberangriffen widerspiegelt. Der chinesische Staat ist bereits jetzt gewillt und in der Lage, mit enormen finanziellen Ressourcen eine hochprofessionelle APT-Umgebung aufzubauen, die nach marktwirtschaftlichen Prinzipien funktioniert und die staatlichen Cyberspionageinteressen mit den gewinnmaximierenden Bestrebungen der miteinander konkurrierenden Unternehmen koppelt.[15] Die Islamische Republik Iran wird auch im Zuge der aktuellen Entwicklung im Nahen Osten weiterhin auf Cyberangriffe setzen, um geopolitische Gegner zu attackieren und zu destabilisieren. Dazu zählen neben regionalen Rivalen auch westliche Staaten. Social-Media-Plattformen und verschlüsselte Kommunikationsdienste werden auch zukünftig infiltriert oder blockiert werden, um Protestbewegungen und regimekritische Stimmen zu unterdrücken und Dissidenten auszuspähen. Hinzu kommen potentielle Vergeltungsmaßnahmen des iranischen Regimes gegen die Feinde der Republik. Frühere Operationen im Bereich der Cybersabotage könnten verstärkt werden. Nordkorea wird seine Cyberoperationen zur Generierung finanzieller Mittel sowie zur Informationsbeschaffung weiter ausbauen, um sein Rüstungsprogramm zu finanzieren und westliche Sanktionen zu umgehen.

Im Hinblick auf die Gemengelage an Akteuren, Methoden und Zielen sind sichere IT-Systeme unerlässlich und müssen durch regelmäßige Sicherheitsupdates, Antivirus- und Endpoint-Schutz aktuell gehalten werden. Auch sichere Passwörter und Mehr-Faktor-Authentifizierung sollten als Standard zum Einsatz kommen. Netzwerksegmentierung und eine restriktive Rechtevergabe erschweren Angreifern die Ausbreitung im System. Zudem sind regelmäßige Schulungen zu Phishing und dem sicheren Umgang mit E-Mails notwendig, um die Mitarbeitende zu sensibilisieren. Klare Meldewege und Notfallpläne sollten eingerichtet sein, um im Verdachtsfall schnell reagieren zu können. Im persönlichen Umgang ist die bewusste Kontrolle über persönliche und dienstliche Daten ein weiterer Schutzfaktor. Die Reduzierung von Informationen in sozialen Netzwerken und Foren verringert die Angriffsfläche für Social Engineering. Sensible Informationen zu beruflichen Tätigkeiten und internen Abläufen sollten ausschließlich über

[15] Vgl. „BfV CYBER INSIGHT: Die i-Soon-Leaks: Industrialisierung von Cyberspionage, Teil 1-4“ unter: www.verfassungsschutz.de.

geschützte Kanäle geteilt werden. Verdächtige Links und Anhänge sind stets kritisch zu prüfen.[16]

Das BfV ist als Abwehrdienst für Politik und Verwaltung, Wirtschaft und Wissenschaft wie Zivilgesellschaft auch in der Prävention tätig und warnt seit langem vor der anhaltenden Bedrohung durch staatlich gesteuerte Cyberakteure und liefert konkrete Handlungsempfehlungen. Eine enge Zusammenarbeit zwischen staatlichen Stellen wie auch mit Unternehmen auf (inter-)nationaler Ebene ist von entscheidender Bedeutung. Dies gilt sowohl für die Entwicklung neuer Schutzmechanismen als auch für die Identifizierung und Behebung von Schwachstellen – nur so kann die Abwehr akuter Bedrohungen durch staatliche Cyberakteure gelingen.

Zudem unterstützt das BfV Politik, Verwaltung, sowie Wirtschaft und Wissenschaft mit gezielten Informationen und Präventionsprodukten, die auf der Webseite des BfV abrufbar sind.[17] 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,
- 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.

Auch künftig stellt umfassende Cybersicherheit sowohl eine technisch-organisatorische wie auch eine nachrichtendienstliche Herausforderung dar. Das BfV als Cyberabwehrbehörde nimmt auch künftige seine zentrale Rolle bei der Bekämpfung nachrichtendienstlich gesteuerter Cyberangriffe aktiv wahr.

[16] Detaillierte Informationen und viele Tipps zur IT- und Cybersicherheit 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 für Sicherheitsanalysen. Zudem fördert das BSI die Sensibilisierung der Öffentlichkeit für die IT-Sicherheit.

[17] 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.


SN-25137821.0*1**0


SN-25137821.0*1**0


## 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

**Bildnachweis**
© BfV

**Stand**
August 2025

SN-25137821.0*1**0


SN-25137821.0*1**0


SN-25137821.0*1**0