

BfV CYBER INSIGHT

Im Schatten des Cyberspace



Teil 2: Die Welt der APTs

Im Schatten des Cyberspace

Teil 2: Die Welt der APTs

Inhalt

1. Einleitung..... 2

2. Staatliche Cyberakteure 3

3. Cyberakteur: Russische Föderation 3

4. Cyberakteur: Volksrepublik China 7

5. Cyberakteur: Islamische Republik Iran11

6. Cyberakteur: Demokratische Volksrepublik Korea15

7. Anhaltende Bedrohungen im Cyberraum17

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

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 FSB² führen auch der zivile Auslandsnachrichtendienst SWR³ und vor allem der militärische Geheimdienst GRU⁴ 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 Engineering⁶ 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.



APT28

SOFACY – FANCY BEAR – PAWNSTORM – SEDNIT

Seit mindestens 2004 einer der aktivsten und gefährlichsten Cyberakteure weltweit.	ZUGEHÖRIGKEIT: wird dem russischen Militärgeheimdienst GRU zugeordnet	ANGRIFFSVEKTOREN: Spear-Phishing, Credential-Phishing, Brute-Force-Attacken, False-Flag-Operationen
Cyberangriff auf die SPD Der Angriff auf die SPD ab Dezember 2022 war Teil einer weltweiten Kampagne gegen Hochwertziele aus Politik und Wirtschaft, bei der eine bis dahin unbekannte IT-Schwachstelle ausgenutzt wurde. Zur Verschleierung seiner Angriffsinfrastruktur nutzte APT28 weltweit kompromittierte Router.	Cyberangriff gegen deutsche Stiftung Mitte 2024 wurde eine deutsche Stiftung Opfer einer Brute-Force-Attacke. Innerhalb weniger Tage gelang APT28 die vollständige Kompromittierung der IT-Infrastruktur. Der Vorfall steht in einer Reihe ähnlicher Angriffe gegen weitere deutsche Organisationen mit identischem Angriffsvektor, Vorgehen und Tooling.	

TATORT CYBERSPACE



APT29

COZY BEAR – THE DUKES – NOBELIUM

Ein seit mindestens 2008 aktiver, äußerst klandestiner Cyberakteur.

ZUGEHÖRIGKEIT:
wird dem russischen Auslandsnachrichtendienst SWR zugeordnet

ANGRIFFSVEKTOREN:
Spear-Phishing, Supply-Chain-Angriffe, Zero-Day-Exploits, Nutzung von Clouddiensten als C2-Server

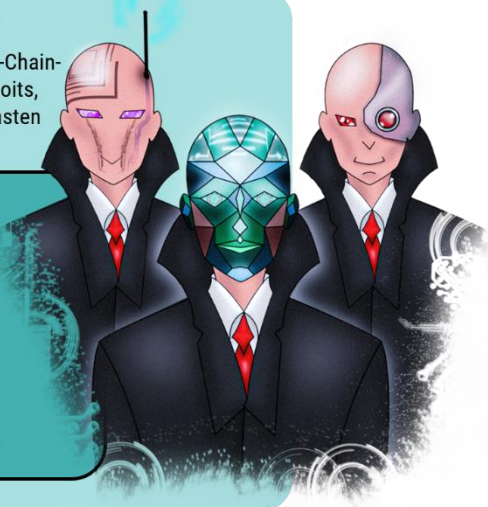


Cyberangriff gegen TeamViewer

Mutmaßlich im Sommer 2024 kam es zu einem Angriff von APT29 gegen den Anbieter für Fernwartungssoftware TeamViewer, bei dem sich der Cyberakteur mittels kompromittierter Anmeldedaten Zugang zur IT-Umgebung verschaffte. Produktumgebung und Kundendaten waren vermutlich nicht betroffen.

Diplomatic-Orbiter-Kampagne

Im Rahmen der Diplomatic-Orbiter-Kampagne greift APT29 regelmäßig westliche Außenministerien und diplomatische Vertretungen mittels Spear-Phishing-Kampagnen an.

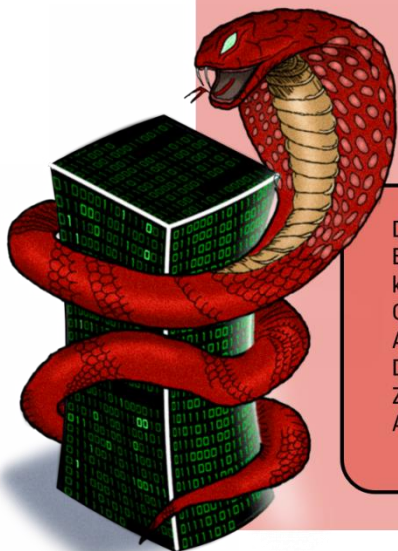


TURLA

SNAKE – UROBUROS – WATERBUG – VENOMOUS BEAR – SECRET BLIZZARD

Ein seit mindestens 2005 aktiver, technisch sehr versierter und äußerst klandestiner Cyberakteur.

ANGRIFFSVEKTOREN:
Phishing-Angriffe, Ausnutzung von Schwachstellen, Eigen- bzw. permanente Weiterentwicklung eingesetzter Schadsoftware



Diplomatische und politische Einrichtungen weltweit stehen kontinuierlich im Interesse der Gruppierung TURLA. Der erfolgreichste Angriff auf Regierungseinrichtungen in Deutschland erfolgte 2018, als TURLA Zugriff auf interne Systeme des Auswärtigen Amtes erlangte.

In Europa ist TURLA besonders aktiv und greift erfolgreich Regierungseinrichtungen in verschiedenen europäischen Staaten an. Darüber hinaus legt TURLA einen besonderen Fokus auf Militäreinrichtungen in Europa. Dies geschieht verstärkt vor dem Hintergrund des russischen Angriffskrieges gegen die Ukraine.



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

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

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.

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.

METUSHY – KE3CHANG – VIXEN PANDA – MIRAGE

APT15

Seit mindestens 2010 einer der derzeit aktivsten und gefährlichsten Cyberakteure.

Technisch sehr versiert, Verschleierung auf hohem Niveau.

ANGRIFFSVEKTOREN:
Zero-Day-Exploits, Supply-Chain-Angriffe, Phishing-Angriffe, Verschleierungsnetzwerke



Angriff gegen eine deutsche Behörde

Im Dezember 2021 wurde eine laufende Cyber-angriffskampagne gegen deutsche Institutionen und Organisationen bekannt, woraus die tiefgreifende Kompromittierung eines Bundesamtes hervorging. Das aus dem Internet erreichbare Netzwerk (DMZ) war vollständig kompromittiert. Auch der Zugriff auf andere Netzbereiche – wie das interne Büro-Netzwerk – war zu diesem Zeitpunkt wahrscheinlich.

Cyberangriff gegen ein deutsches Unternehmen

Im Jahr 2024 führte APT15 einen Angriff gegen ein deutsches Unternehmen durch, dessen Ziel eigentlich ein Kunde des besagten Unternehmens war. Hierfür nutzte der Cyberakteur eine IT-Schwachstelle in einem Netzwerkgerät (Edge Device) aus, um vollumfänglichen Zugriff auf das System zu erhalten.





APT31

JUDGMENT PANDA – ZIRCONIUM – RED KERES

Ein seit mindestens 2014 aktiver und technisch versierter Cyberakteur.

Er nutzte eines der bekanntesten Verschleierungsnetzwerke (TORB).

ANGRIFFSVEKTOREN:

Schwachstellenscanning, Zero-Day-Exploits, Supply-Chain-Angriffe, Versand von Phishing / Tracking Mails

Aufklärungshandlungen gegen Mitglieder der IPAC

Im Jahr 2021 berichteten mehrere europäische und weitere westliche Staaten über erfolgreiche Aufklärungsversuche durch APT31 mithilfe des Versands von Tracking-Pixeln per Phishing-Mail. Demnach standen insbesondere Mitglieder der INTER-PARLIAMENTARY ALLIANCE ON CHINA (IPAC) im Fokus. Die IPAC ist ein internationaler, parteiübergreifender Zusammenschluss von ca. 100 Parlamentariern verschiedener Länder. Zweck des Gremiums ist die Beobachtung und Bewertung chinesischer Ambitionen in Bezug auf Weltmacht, Menschenrechte sowie Sicherung der internationalen regelbasierten Ordnung. Auch deutsche Politiker und Abgeordnete sind Mitglieder der IPAC und standen demnach ebenfalls im Aufklärungsfokus von APT31.



EMISSARY PANDA – LUCKY MOUSE – IRON TIGER

APT27

Ein seit mindestens 2010 aktiver, technisch hoch versierter Cyberakteur mit eigenen Angriffstools.

ANGRIFFSVEKTOREN:
Phishing-Angriffe, Zero-Day-Exploits, Supply-Chain-Angriffe, Watering-Hole-Angriffe



Cyberangriffe gegen deutsche Energie-, Dienstleistungs- und Pharmaunternehmen

In den Jahren 2021/2022 wurden Cyberangriffe des Akteurs APT27 gegen weltweit tätige Unternehmen aus den Bereichen Energiewirtschaft, Dienstleistungen und Pharmazeutik bekannt. Bei mindestens vier deutschen Unternehmen konnte unter Ausnutzung einer Schwachstelle in MS-Exchange erfolgreich die eigens durch den Cyberakteur entwickelte Schadsoftware HYPERBRO platziert werden. Durch die enge Zusammenarbeit des BfV mit den Unternehmen konnte der laufende Angriff beobachtet und eine Datenausleitung durch den Angreifer verhindert werden.

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 Security⁸ (der zivile In- und- Auslandsnachrichtendienst, zumeist MOIS abgekürzt) als auch der nachrichtendienstlich agierenden Islamischen Revolutionsgarde⁹ (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 Haktivisten-Gruppierungen „Hack and Leak“-Operationen¹⁰ gegen öffentliche und private Stellen in Israel durchgeführt. Diese wurden durch niedrighschwellige Störaktionen im Cyberraum, wie DDoS-Angriffe und Webseiten-Defacements¹¹, 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.

⁸ In Farsi: Vezerat-e-Ettela'at-e Jomhouri-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“).

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.

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,
- 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 Angriffe¹⁴ 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

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.

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.

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 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.

CHARMING KITTEN

APT35 – APT42 – MINT SANDSTORM – PHOSPHORUS – TA453
YELLOW GARUDA – UNC788 – CHARMINGCYPRESS – CALANQUE



Ein seit mindestens 2015 aktiver Cyberakteur.

ZUGEHÖRIGKEIT:
wird gemäß mehrerer IT-Dienstleister den IRGC zugeordnet

ANGRIFFSVEKTOREN:
Spear-Phishing, Credential-Phishing, hochprofessionelles Social Engineering

Cyberspionage gegen Dissidenten

2022 hat die APT-Gruppierung CHARMING KITTEN auch in Deutschland Cyberangriffe gegen Kritiker des iranischen Regimes durchgeführt. Die Aktivitäten richteten sich vor allem gegen Dissidentenorganisationen und Einzelpersonen – wie Juristinnen und Juristen, Journalistinnen und Journalisten oder Menschenrechtsaktivistinnen und -aktivisten.

„Hack and Leak“-Operation vor US-Präsidentenwahl
Vor der US-Präsidentenwahl 2024 kam es zu einer Kompromittierung von E-Mail-Konten der Mitarbeiter von US-Präsident Donald Trump. Die erbeuteten Daten

wurden im Anschluss US-Medien zugespielt. Ziel war die Beeinflussung der Präsidentenwahl im Sinne des iranischen Regimes.

Cyberangriff gegen deutsche Politikerin

Im Jahr 2025 wurde eine deutsche Politikerin Opfer eines Cyberangriffs von CHARMING KITTEN, in dem Schadsoftware mit ausgeklügeltem Social Engineering auf Endgeräten der Politikerin installiert werden sollte. Der Angriff diente wahrscheinlich Spionagezwecken.



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 beauftragt 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.

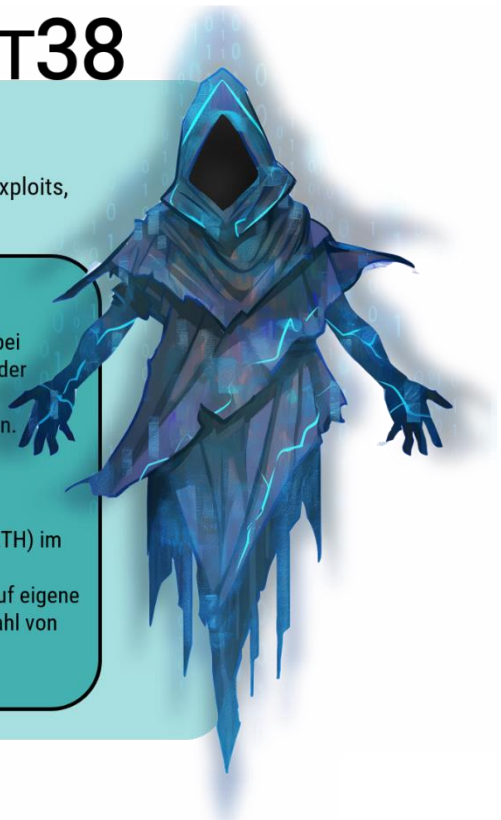
Nordkoreanische Cyberoperationen sind von Kreativität geprägt und besitzen insbesondere angesichts der wirtschaftlichen Lage des Landes ein erstaunlich hohes technisches Niveau. Dabei ist insbesondere die Gruppierung LAZARUS hervorzuheben, die auch eigens entwickelte Schadsoftware einsetzt und in der 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.

LAZARUS GROUP – HIDDEN COBRA – DIAMOND SLEET

APT38



Ein seit mindestens 2007 aktiver Cyberakteur, der professionelles Social Engineering über Karriereplattformen im Internet betreibt.

ANGRIFFSVEKTOREN:
Spear-Phishing, Social Engineering, Zero-Day-Exploits, Supply-Chain-Angriffe

Operation DreamJob

Im Jahr 2024 wurde eine Social-Engineering- Kampagne von APT38 bekannt, bei der Fachkräften sicherheitsrelevanter Wirtschaftsbereiche wie Verteidigung oder Luft- und Raumfahrt gefälschte Jobangebote unterbreitet wurden, damit diese auf maliziöse Links klicken und unbewusst Schadsoftware herunterladen. Ziel dabei waren Spionage, Datenexfiltration und potenziell Sabotage.

Bybit Hack

Im Februar 2025 wurde die Kryptobörse Bybit kompromittiert und Ethereum (ETH) im Wert von über 1,4 Milliarden US-Dollar erbeutet. APT38 manipulierte dazu ein Sicherheitsverfahren des Unternehmens und konnte dadurch hohe Summen auf eigene Krypto-Wallets transferieren. Es soll sich dabei um den bisher größten Diebstahl von Krypto-Währung weltweit handeln.

TATORT CYBERSPACE



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

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

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 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.

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.

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 künftig seine zentrale Rolle bei der Bekämpfung nachrichtendienstlich gesteuerter Cyberangriffe aktiv wahr.

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.

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

