

# Was nationalstaatliche Cyberkriminelle antreibt

Wenn man Angriffe im Cyberraum verstehen und bekämpfen will, muss man nicht nur die Techniken und Taktiken, sondern ebenso die Motivation der Cyberkriminellen kennen. Auch solche Informationen sind Bestandteil von Threat Intelligence.

Von Sascha Herzog und Jörg Schauff

■ Unter Threat Intelligence versteht man sämtliche Informationen zu Cyberbedrohungen und -angriffen nebst Kontext [1]. Sie reicht von automatisiert erfassten kriminell genutzten IP-Adressen oder bekannten Hashwerten bis hin zu Informationen, welche Bedrohungsakteure auf welche Art gegen welche Ziele vorgehen. Das führt zur Motivation und Absicht, die die Angreifer zu ihren Taten

bewegen. Unter Motivation versteht man den übergeordneten Antrieb, das Warum hinter einer Handlung – was bewegt jemanden grundsätzlich dazu, aktiv zu werden? Die Absicht, also das konkrete Ziel, bei einer spezifischen Aktion oder Kampagne dagegen erschließt sich durch die Frage: „Was soll erreicht werden?“ Die Absicht führt dann zu einer konkreten Handlung.

## TRACT

- ▶ Informationen über Angreifer sind genauso wichtig für Verteidiger wie Informationen zu Angriffen – insbesondere bei nationalstaatlichen Akteuren etwa aus China oder Russland lohnt sich ein genauer Blick.
- ▶ Zwar verfolgen nationalstaatliche Cyberkriminelle in der Regel eher langfristige Ziele, dennoch spiegeln sich tagespolitische Ereignisse häufig in spontanen Angriffen wider.
- ▶ Die größte Cyberbedrohung für die westliche Welt geht von den „Big Four“ aus, von nationalstaatlichen APT-Gruppen aus China, Russland, Nordkorea und dem Iran. Bedrohungsinformationen sind daher in strategische Entscheidungen einzubeziehen, damit man Risiken realistisch einschätzen und reduzieren kann.

Die Motivation staatlich gelenkter Cyberakteure besteht in der Regel aus geopolitischen und strategischen Interessen, Machtprojektion, nationaler Sicherheit und einem Informationsvorsprung gegenüber potenziellen und tatsächlichen Feinden. Das führt die Akteure zu der Absicht, Spionage zu betreiben, geistiges Eigentum oder Unterlagen zu Industrieanlagen zu stehlen oder Sabotageakte durchzuführen, um gegnerische Staaten und politische Feinde einzuschüchtern oder zu schwächen. Ihr Handeln ist langfristig geplant und dient dem Staatsinteresse, etwa der Informationsbeschaffung für militärische, diplomatische oder wirtschaftliche Vorteile.

Allerdings führen solche Akteure auch immer wieder Ad-hoc-Angriffe durch, die durch tagespolitische Ereignisse oder persönliche Beziehungen zwischen einflussreichen Personen (in Russland: Politiker und Oligarchen) und den Geheimdiensten ausgelöst werden. Als beispielsweise russische Sportler bei Olympischen Spielen wegen Dopings ausgeschlossen wurden, kam es unmittelbar danach zu Cyberangriffen durch Sandworm, eine Einheit des russischen militärischen Geheimdienstes GRU, auf die Veranstalter und Dopinglabore. In einem anderen Fall wurde die Anwaltskanzlei, die einen deutschen Baukonzern in einem Rechtsstreit mit einem Vertragspartner aus den GUS-Staaten vertrat, von Fancy Bear, einer weiteren regierungsnahen Hackergruppe, ausspioniert.

## Staatliche Interessen oder Geld – oder doch lieber beides?

Klassische Cyberkriminelle dagegen haben primär eine finanzielle Motivation. Sie wollen Firmen mit Ransomware erpressen oder Geld, Zugangsdaten oder Kryptowährungen stehlen und für Profit verkaufen. Es gibt jedoch Ausnahmen: Sowohl iranische als auch nordkoreanische nationalstaatliche Gruppen betätigen sich als Spione und verfolgen gleichzeitig cyberkriminelle Aktivitäten. Die nordkoreanische Lazarus-Gruppe etwa agiert offiziell als staatlich gelenkte APT-Gruppe (Advanced Persistent Threats), verfolgt aber mit Bankraub und Kryptohacks vorwiegend finanzielle Ziele. Die Motivation ist für den Iran, aber auch für Nordkorea identisch: Finanzierung des Regimes, da politische Sanktionen den regulären Außenhandel behindern.

Für Analysten ist das in Abbildung 2 dargestellte wissenschaftliche Modell „Diamond Model of Intrusion Analysis“ (siehe [ix.de/zdxm](http://ix.de/zdxm)) der Sicherheitsexper-



**Die Beantwortung der Fragen nach Motivation (warum?), Absicht (wozu?) und Handlung (wie?) verrät viel über Angreifer (Abb. 1).**

ten Christopher Betz, Sergio Caltagirone und Andrew Pendergast ein gutes Hilfsmittel, um die Zusammenhänge zwischen einem (möglichen) Angreifer und der eigenen Organisation zu verstehen. Die Frage, die ein Analyst zur vorausschauenden Bedrohungsanalyse an das Modell stellen sollte, lautet: Welcher Angreifer hat sowohl die Absicht als auch die Fähigkeiten, eine bestimmte Infrastruktur erfolgreich anzugreifen? Rückblickend ist die Frage zu stellen, welcher Angreifer sowohl die Absicht als auch die Fähigkeiten hatte, die besagte Infrastruktur erfolgreich anzugreifen, und wie die Infrastruktur des Angreifers zum Tatzeitpunkt aussah.

Im Folgenden soll das Beispiel aus Abbildung 2 mit den vorher behandelten Kategorien weiter angereichert und analysiert werden. Die Motivation besteht aus dem geopolitischen Ziel, dass ein Staat politischen Druck auf ein Nachbarland ausüben möchte, ohne eine offene militärische Eskalation zu riskieren. Der strategische Nutzen besteht in der Demonstration von Macht und der Destabilisierung

des Gegners, auch lassen sich neue Cyberfähigkeiten testen.

Die Absicht, also das konkrete Ziel, besteht darin, die Stromversorgung in der Hauptstadt des Zielstaates zu unterbrechen. Ein Sekundärziel könnte die Destabilisierung sein, außerdem soll Misstrauen in die Regierung des Opfers gesät werden. Die eigentliche Handlung besteht aus verschiedenen technischen Schritten. Zunächst wird der initiale Zugang über eine Phishingkampagne gegen IT-Mitarbeiter des Energieversorgers erlangt. Um sich im Zielnetz zu bewegen (Lateral Movement), nutzt der Angreifer Schwachstellen in OT-Netzwerken und Steuerungssystemen (SCADA). Die Ausführung schließlich besteht in der Manipulation von Steuerbefehlen, um Teile des Stromnetzes abzuschalten. Dazu wird eine Command-and-Control-Infrastruktur (C2) auf kompromittierten Servern in Drittländern genutzt.

**Unterschiedlich organisierte Kriminelle**

Organisatorisch unterscheiden sich nationalstaatliche und kriminelle Angreifer deutlich. Nationale Cybereinheiten arbeiten meist hierarchisch in Geheimdiensten oder Militärstrukturen. Sie haben staatliche, oft sehr hohe Budgets, umfangreiche Ressourcen und genießen im eigenen Land Immunität. Die Operationen der

Nationalstaaten werden fast immer sorgfältig geplant, oft über Jahre vorbereitet und technisch und organisatorisch verschleiert – über ausgeklügelte C2-Netzwerke und Briefkasten- oder Tarnfirmen.

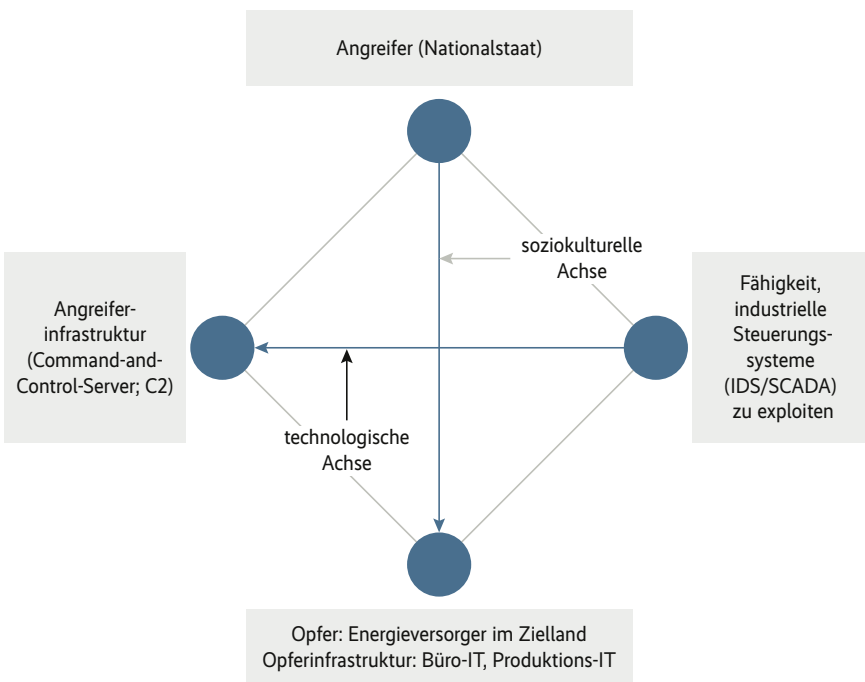
Kriminelle Hackergruppen sind dagegen privatwirtschaftlich organisiert. Viele operieren nach dem „Ransomware-as-a-Service“-Modell (RaaS) als Söldner am Cybermarkt: Sie bieten Malware-Infrastruktur und Unterstützung an (Geldzurück-Garantie, Hotline), rekrutieren Affiliates auf Darknet-Plattformen und nehmen an lukrativen Erpressungen teil. Dennoch können diese „Unternehmen“ riesige Strukturen aufbauen: Im Fall der Conti-Ransomware hatten etwa hundert Mitglieder feste Gehälter, Manager, Codeteams und einen „Big Boss“. Fast wie ein reguläres Softwareunternehmen.

Ein weiterer Unterschied besteht in der Rechtssicherheit. Während staatliche Akteure im eigenen Land nicht mit Strafverfolgung rechnen müssen, riskieren Cyberkriminelle Gefängnis und Vermögenszug.

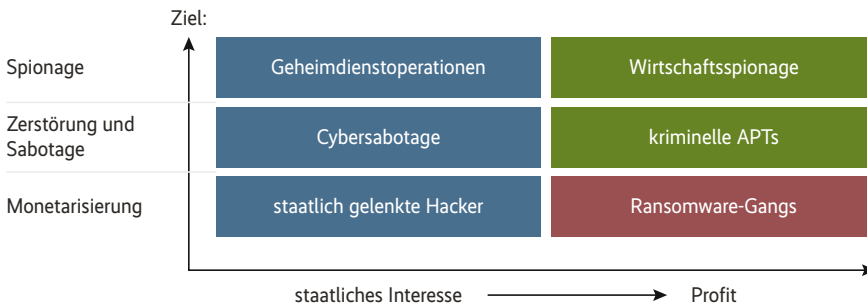
**Nationale Cyberakteure und ihre Vorgehensweisen**

In den letzten Jahren haben immer mehr Staaten eigene Cyberspionagfähigkeiten entwickelt und verfügen über APT-Gruppen, beispielsweise die Türkei mit Cosmic Wolf (alias Marbled Dust), Südkorea mit Shadow Crane (alias ZigZag Hail) oder Kasachstan mit Comrade Saiga. Eine Liste der in Deutschland aktiven APT-Gruppen ist auf der Website des BSI veröffentlicht (siehe ix.de/zdxm). Dieser Artikel konzentriert sich auf die im kürzlich veröffentlichten Microsoft Threat Intelligence Report wieder einmal bestätigten „Big Four“ unter den Nationalstaaten: China, Russland, Iran und Nordkorea.

Ein zentraler Begriff im Zusammenhang mit Threat Intelligence und der Angriffsanalyse sind die Tactics, Techniques and Procedures (TTPs). Darunter versteht man die detaillierten Vorgehensweisen der Angreifer in allen Phasen eines Angriffs. Die **Taktik** beschreibt, was ein Angreifer erreichen möchte, zum Beispiel initialen Zugang zu einem Netzwerk oder Persistenz, das dauerhafte Verweilen im kompromittierten System. Verschiedene **Techniken** führen den Angreifer ans Ziel, etwa das Umgehen von Benutzerzugangskontrollen (UAC; User Access Control) oder das Manipulieren von Zugriffstoken. Die **Prozeduren** schließlich beschreiben die konkreten Aktionen, mit denen die taktischen Ziele erreicht werden. Eine bekannte Wissensdatenbank, die TTPs



**Die durch Kanten verbundenen Merkmale Angreifer, Infrastruktur, Fähigkeiten und Opfer geben dem Modell seinen Namen: Das Diamantmodell lässt sich mit weiteren Informationen anreichern und etabliert eine standardisierte Vorgehensweise zur Analyse von Einbrüchen in ein Netzwerk (Abb. 2).**



**Angreifermatrix: In ihren kriminellen Motiven und Zielen unterscheiden sich die nationalstaatlichen von anderen Angreifergruppen (Abb. 3).**

auflistet und im Einzelnen beschreibt, ist MITRE ATT&CK (siehe ix.de/zdxm).

### China – bekannt für Industriespionage

Chinesische APT-Gruppen agieren vorrangig im Dienste der wirtschaftlichen und militärischen Entwicklung Pekings. Sie führen seit über zwanzig Jahren groß angelegte Industriespionage durch und konzentrieren sich dabei auf strategische Sektoren wie Verteidigung, Technologie, Telekommunikation, Fertigung und kritische Infrastrukturen. Die Ziele lassen sich von Außenstehenden aus den offiziell bekannt gegebenen staatlichen Programmen der chinesischen Regierung ableiten. Die chinesische Regierung definiert in ihren Fünfjahresplänen und anderen Papieren kritische Wirtschaftssektoren und die Zielvorgaben für die heimischen Industrien. Diese Zielvorgaben sind teilweise nicht durch inländische Forschung und Entwicklung zu erreichen, weshalb noch immer Wirtschaftsspionage betrieben wird. Daher muss der wirtschaftliche Entwicklungsvorsprung anderer Staaten durch Wirtschaftsspionage aufgeholt werden.

Die staatlichen Stellen, denen man die chinesischen APTs zuschlägt, sind das Ministerium für Staatssicherheit, das Ministerium für öffentliche Sicherheit, die Volksbefreiungsarmee und staatlich kontrollierte Forschungsinstitute und Unternehmen.

Das „Täteruniversum“ des Threat-Intelligence-Anbieters CrowdStrike bringt mehr als die Hälfte aller nationalstaatlichen Gruppen mit China in Verbindung. NSA, CISA und FBI warnen, dass chinesische Hacker sensitive Daten, Schlüsseltechnologien und geistiges Eigentum weltweit abgreifen, um Chinas strategische Ziele zu unterstützen. Diese Ziele sind definiert in Programmen wie „Made in China 2025“, „Healthy China 2030“, „National Rejuvenation“ et cetera. Diese Programme sind nicht isoliert zu betrach-

ten, sondern stehen in engem Zusammenhang und beeinflussen sich gegenseitig. Sie sind Ausdruck der ambitionierten Ziele der chinesischen Regierung, ihre Wirtschaft zu modernisieren, ihren Einfluss in der Welt zu stärken und eine führende Rolle in der globalen Arena einzunehmen. Und all dies unterstützt durch offensive Maßnahmen im Cyberspace.

Bekannte chinesische nationalstaatliche Gruppen sind Winnti (alias Leopard Typhoon oder Wicked Panda), Salt Typhoon (auch GhostEmperor oder Operator Panda genannt) und Volt Typhoon (alias Bronze Silhouette, Vanguard Panda). Volt Typhoon wird offiziell der Volksbefreiungsarmee zugerechnet und begann bereits vor Jahren, kritische US-Infrastrukturen zu infiltrieren. Die Gruppe platziert Schadsoftware in Netzwerken großer Kommunikations-, Energie- und Versorgungsunternehmen (Prepositioning), um im Kriegsfall sofort zuschlagen zu können. Ihre TTPs sind auf hohe operative Sicherheit (Tarnung) ausgelegt: Sie nutzen oft Living-off-the-Land-Methoden [2], also integrierte Windows-Tools (PowerShell, wmic, netsh und so weiter) und legitime Netzwerkverwaltungsprogramme statt Schadsoftware, um Erkennung zu vermeiden.

### Angriffe unterhalb des Radars

Daneben nutzt Volt Typhoon gelegentlich modifizierte Versionen von Open-Source-Tools wie Fast Reverse Proxy (frp) oder EarthWorm, um Command-and-Control-Kanäle (C2) über Proxys einzurichten und den Datenverkehr zu verschleiern. Diese Tools sind besonders effektiv, denn sie werden in der Regel nicht von herkömmlicher Antivirensoftware erkannt, da sie als legitime Systemprozesse erscheinen.

Generell forschen chinesische Angreifer nach neuen Sicherheitslücken – oder adaptieren bekannt gewordene Exploits anderer Angreifer, etwa in Pulse Secure, Microsoft-Produkten oder VPN-Gate-

ways, und nutzen sie binnen Tagen aus. Außerdem verschleiern sie ihre Infrastruktur durch wechselnde VPN-Server und den Einsatz gehackter Heimrouter als verschlüsselte Proxys. Zusammenfassend: China betreibt groß angelegte, anhaltende Cyberspionage zur Informations- und Technologiebeschaffung.

### Die berüchtigten Geheimdienste Russlands

Russland verfügt über mehrere Geheimdienste, die sehr fähige Cyberabteilungen haben: den militärischen Geheimdienst GRU, den Inlandsgeheimdienst inklusive Kriminalpolizei und Grenzschutz FSB und den Auslandsgeheimdienst SVR. Ihre Aktivitäten reichen von Spionage über politisch motivierte Desinformations- und Sabotagekampagnen bis hin zur Zerstörung gegnerischer Infrastrukturen. Ein prominenter Fall von Spionage ist der Cyberangriff auf den Deutschen Bundestag 2015, der der GRU-Einheit APT28 (Fancy Bear) zugeschrieben wird. Dabei wurden E-Mails und Zugangsdaten zahlreicher Abgeordneter kompromittiert und über längere Zeit exfiltriert.

Bei den Desinformations- und Sabotagekampagnen sticht die „Doppelgänger“-Kampagne heraus: Sie bezeichnet eine seit mindestens 2022 aktive Russland zugeschriebene Einflussoperation, bei der täuschend echte Kopien westlicher Medien erstellt und über soziale Netzwerke verbreitet wurden, um prorussische Narrative zu platzieren und Vertrauen in demokratische Institutionen zu untergraben. Ein Beispiel für die Zerstörung gegnerischer Infrastrukturen schließlich ist CrashOverride, auch Industroyer genannt. Diese speziell für industrielle Kontrollsysteme (ICS) entwickelte Malware wurde 2016/2017 bei Angriffen auf das ukrainische Stromnetz eingesetzt. Sie ermöglichte das gezielte Abschalten von Umspannwerken und gilt als erste bekannte Cyberwaffe mit direkter physischer Wirkung auf Strominfrastruktur.

Was die TTPs angeht, so bedienen sich die russischen Angreifer klassischer und fortgeschrittener Methoden. Die GRU-Einheit 26165, bekannt als APT28 oder Fancy Bear, führt zum Beispiel umfangreicher Spear-Phishing-Kampagnen mit gefälschten Sicherheitswarnungen und Webmail-Seiten aus, um Zugangsdaten zu phishen. Danach setzt sie eigene Linux- und Windows-Tools wie Drovorub ein oder greift mit Brute-Force-Attacken (etwa über Kubernetes-Cluster) Tausende Cloud-Konten an. Die SVR-Gruppe (APT29/Cozy Bear) hingegen nutzt maß-

geschneiderte Malware wie GoldMax oder TrailBlazer und innovatives Credential Hopping; Sie stiehlt Browser-Cookies, um den Multi-Faktor-Schutz zu umgehen. Das US-Justizministerium nennt APT29 als Täter für den SolarWinds-Supply-Chain-Angriff.

Andere Einheiten legen Wert auf Zerstörung. So nutzt die GRU-Einheit 74455 (bekannt als Sandworm Team) etwa DDoS-Attacken und zerstörerische Malware wie BlackEnergy, KillDisk oder NotPetya, um Infrastrukturen lahmzulegen. Auch der FSB, ehemals KGB, beschafft sich über Cyberoperationen Informationen, zum Beispiel über Netzwerksensoren und Brute-Force-Angriffe auf öffentlich erreichbare Dienste. Auffällig ist, dass der FSB wiederholt kriminelle Hacker einspannt. Die amerikanische IT-Sicherheitsbehörde CISA dokumentiert, dass der FSB gezielt Cyberkriminelle für Spionageaufträge anwirbt, während diese Ransomware- und Phishingkampagnen fahren.

So verschwimmen die Grenzen zwischen staatlichem Auftrag und Kriminalität, was Dritte kaum unterscheiden können. Basierend auf Berichten aus öf-

fentlichen Quellen schätzen die Sicherheitsbehörden der USA, Australiens, Kanadas, Neuseelands und Großbritanniens (Five Eyes), dass mehrere mit Russland verbündete cyberkriminelle Gruppen eine Bedrohung für kritische Infrastruktureinrichtungen darstellen. Zu diesen Gruppen gehören The CoomingProject, Killnet, SMOKEY SPIDER, Wizard Spider (der russische Teil nach der Aufspaltung dieser Cybercrimegruppe) und das Xaknet Team. Insgesamt lässt sich sagen, dass russische Gruppierungen hochprofessionell und aggressiv agieren. Sie kombinieren Einbruchs-, Ausspäh- und Sabotagemethoden und arbeiten koordiniert gegen klassische Geheimdienstziele.

## Hacktivismus im Iran

Die Cyberkrieger des Iran, vor allem die iranische Militär- und Sicherheitsorganisation IRGC (Islamische Revolutionsgarden) und der Geheimdienst MOIS, operieren vorrangig für das Regime, setzen aber auch vielfach symbolische Hacktivismus-Aktionen ein. Historische Beispiele sind die Shamoon-Wiper-Attacken von 2012 und 2016 gegen die saudische

Ölindustrie, die zeigen, dass der Iran kritische Infrastrukturen in großem Maßstab angreifen und zerstören kann. Das häufigste Ziel war und ist jedoch Spionage und Einflussnahme: Medien, Regierungseinrichtungen und Unternehmen im Nahen Osten, in den USA und Europa werden von Gruppen wie APT34 alias OilRig oder Helix Kitten und APT35, bekannt als Charming Kitten oder Mint Sandstorm, angegriffen. Diese Akteure finanzieren oft das Regime, stehlen technologische Geheimnisse und sammeln Informationen über Dissidenten.

Auffallend ist zuletzt eine starke Zunahme politischer Cyberoperationen. Seit dem Krieg zwischen Israel und der Hamas (Oktober 2024) haben iranische Hacker Desinformationskampagnen und „Hack&Leak“-Angriffe, bei denen sie vertrauliche Informationen stahlen und meist über Social Media veröffentlichten, gegen westliche Wahlen und Institutionen gefahren. Zudem greift die iranische Gruppe CyberAv3ngers israelische OT-Produkte an, die bei westlichen Firmen im Einsatz sind, zum Beispiel in der Trinkwassergewinnung in Irland oder Deutschland.

Bei den TTPs setzen iranische Gruppen überwiegend auf Social Engineering und Credential-Angriffe. So fährt beispielsweise APT35 nahezu ununterbrochen aufwendige Spear-Phishing-Kampagnen, die manipulierte E-Mails oder Webseiten (Watering Holes, gefälschte Login-Seiten) einsetzen, um Zugangsdaten zu erlangen. Nach einem erfolgreichen Einstieg laden sie eigene Backdoors wie Sponsor oder BellaCiao und Tools wie Mimikatz oder PsExec nach, um dauerhaften Zugang zu etablieren und Daten zu exfiltrieren. Andere iranische Gruppen wie MuddyWater und APT33/34 verwenden Living-off-the-Land-Techniken – sie nehmen Windows-Tools, etwa Power-Shell, Certutil oder cURL zu Hilfe und nutzen Frameworks wie Cobalt Strike für C2-Kommunikation.

Zudem kommt es häufig vor, dass gestohlene Netzwerkzugänge auf Darknet-Marktplätzen weiterverkauft werden, um Einnahmen zu generieren. Iranische Hacker setzen außerdem nach Einschätzung der CISA massiv auf Brute-Force-Methoden. Seit Ende 2023 kompromittieren sie mit Passwort-Spraying und MFA-Push-Bombing-Attacken Nutzerkonten (auch in kritischen Branchen) und manipulieren Multi-Faktor-Registrierungen, um persistenten Zugang sicherzustellen. Zusammengefasst lässt sich sagen, dass die Cyberkräfte des Iran ideologisch motiviert und vielseitig sind, von konventioneller Spionage über Hacktivismus bis hin zu taktischen Zerstörungsangriffen mit Wipern und Ransomware.

## Sonderfall Nordkorea

Nordkorea stellt einen Sonderfall dar: Das Regime betrachtet Cyberkriminalität als zusätzliche Einnahmequelle. Die Lazarus-Gruppe (auch APT38, Bluenoroff und weitere) ist einerseits ein typischer nationalstaatlicher Player, agiert aber mit einer Kombination aus politischer Spionage und ausgeprägter Profitgier. Ihre bekanntesten Operationen bislang waren 2016 der Cyberbankraub von 81 Millionen Dollar bei der Zentralbank von Bangladesch und 2017 die Verbreitung der WannaCry-Ransomware, bei der weltweit Schäden in Milliardenhöhe entstanden. Seit 2017 wurden dem nordkoreanischen Regime über sechzig Hacks auf krypto-bezogene Unternehmen und Plattformen zugeschrieben.

In Bezug auf die TTPs setzen Lazarus und andere nordkoreanische Gruppen oft auf breit angelegte, aber sehr gezielte Cyberoperationen. Sie entwenden Banking-zugangsdaten, verschleiern Geldtransfers

über Kryptowährungen und verwenden eigene Ransomware wie WannaCry, Niwa oder Manjusaka als Tarnung für Datendiebstahl. Die CISA und das FBI stellten fest, dass diese staatlich geförderte Gruppe neben WannaCry und dem Bangladesch-Bankraub auch für die Angriffe auf Sony Pictures und viele andere Attacken verantwortlich ist. In der Praxis heißt das, Nordkorea mischt Wirtschaftsspionage mit bewaffneter Kriminalität und finanziert so sein Staatsbudget, um einerseits dem Regime seinen luxuriösen Lebensstil zu ermöglichen und andererseits die Entwicklung des militärischen Atomprogramms voranzutreiben.

Warum ist Attribution, also die Zuschreibung einer kriminellen Handlung zu den Tätern, wichtig? Attribution ermöglicht es Organisationen, Cyberangriffe bestimmten gegnerischen Aktivitätsclustern zuzuordnen und dafür die Vertrauensstufe festzulegen. Dadurch kann man bekannte TTPs und Infrastrukturmuster dieser Akteure in der eigenen IT-Sicherheitsplanung berücksichtigen. Dies erlaubt eine priorisierte Absicherung derjenigen Systeme, die für den jeweiligen Gegner strategisch relevant sind, und ein gezieltes Threat Hunting, also ein aktives Suchen nach Sicherheitsvorfällen, ehe es Anzeichen dafür gibt. Attribution unterstützt die Bewertung, ob ein Vorfall Teil einer breiteren Kampagne oder einer isolierten Operation ist. Sie ist damit Grundlage für Lagebilder, Eskalationsentscheidungen und die Koordination mit Partnern. Ohne belastbare Attribution ist weder eine gezielte Suche nach potenziellen Angreifern in der eigenen Infrastruktur noch eine zielgerichtete und wirksame Reaktion möglich.

## Fazit

Nationalstaatliche Cyberakteure unterscheiden sich deutlich von klassischen Cyberkriminellen – sowohl hinsichtlich der Motivation als auch bei Struktur und Vorgehensweise. Während Kriminelle primär finanzielle Interessen verfolgen, agieren staatliche Gruppen mit geopolitischen und strategischen Zielsetzungen: Informationsbeschaffung, Machtprojektion, Sabotage und politische Einflussnahme. Dabei verschwimmen die Grenzen zunehmend, wie die Beispiele Iran und Nordkorea verdeutlichen, bei denen staatliche Akteure zugleich durch kriminelle Aktivitäten ihr Regime finanzieren.

Für die Verteidigung kritischer Infrastrukturen ist daher essenziell, nicht nur technische Indikatoren, sondern auch geopolitische Entwicklungen, organisa-

torische Muster und strategische Zielsetzungen der Angreifer einzubeziehen. Das Diamantmodell bietet hierbei einen hilfreichen Rahmen, um Absicht, Fähigkeiten und Infrastrukturen von Angreifern systematisch zu analysieren.

Die „Big Four“, also China, Russland, Iran und Nordkorea, stehen weiterhin im Zentrum globaler Cyberbedrohungen. Ihre Operationen sind hochgradig professionell, variieren in Taktiken, Techniken und Prozeduren (TTPs) und sind meist langfristig angelegt. Damit stellen sie für Unternehmen und Staaten gleichermaßen eine dauerhafte Bedrohung dar. Entscheidend ist, diese Entwicklungen nicht isoliert, sondern im Kontext geopolitischer Spannungen und wirtschaftlicher Interessen zu betrachten.

Zusammenfassend lässt sich sagen: Cybersicherheit ist längst kein rein technisches Problem mehr, sondern eine Frage nationaler und internationaler Resilienz. Organisationen müssen lernen, Bedrohungsinformationen in strategische Entscheidungen einzubeziehen – nur so lassen sich Risiken realistisch einschätzen und wirksam reduzieren. (ur@ix.de)

## Quellen

- [1] Jörg Schauff, Sascha Herzog; Cyber Threat Intelligence – Angreifer und Angriffe verstehen; iX 5/2025, S. 58
- [2] Frank Ully; Living off the Land: Cyberangriffe ohne Malware; iX 5/2025, S. 44
- [3] Das Diamantmodell, die APT-Liste des BSI und der Microsoft Threat Intelligence Report sind über [ix.de/zdxm](http://ix.de/zdxm) zu finden.

### SASCHA HERZOG

ist technischer Geschäftsführer und Penetrationstester bei der NSIDE ATTACK LOGIC GmbH in München.



### JÖRG SCHAUFF

ist Head of Threat Intelligence bei NSIDE. Seine Erfahrungen mit Threat Intelligence sammelte er unter anderem beim deutschen Bundesamt für Verfassungsschutz in der Abteilung Spionageabwehr.



