**So arbeiten Nordkoreas Hackertruppen**

# Kims Dotcom

**Kaum ein Nordkoreaner kommt ins Netz, zugleich hat das Land eine schlagkräftige Cyberarmee: Rund 7000 Hacker stehen in den Diensten Kim Jong Uns. Wie die Truppen vorgehen.**

*Von Sonja Peteranderl*

REUTERS/ KCNA

Kim Jong Un

Freitag, **08.03.2019** 10:23 Uhr



Etwa 25 Millionen Nordkoreaner teilen sich 1,2 Millionen Festnetzanschlüsse, nur wenige haben Zugang zum Internet. Das Reich von Kim Jong Un ist ein telekommunikatives Entwicklungsland. Doch seine Cyberarmee kann sich mit den erfolgreichsten staatlichen Hackertruppen weltweit messen, warnen Experten:

- "Nach verfügbaren Informationen gehört Nordkorea sicherlich zu den Top 15 der Staaten mit offensiven Cyberfähigkeiten, möglicherweise sogar zu den Top 10", sagt der Cybersicherheitsexperte Sven Herpig von der Stiftung Neue Verantwortung (SNV), die sich als Technologie-Thinktank einen Namen gemacht hat.

- Nordkorea spiele nicht in der gleichen Liga wie Russland, China, Israel oder die USA, "aber auf einem sehr guten zweiten Rang", sagt auch der Asien-und Cybersicherheitsexperte Nigel Inkster vom Londoner Thinktank International Institute for Strategic Studies (IISS). "Sie sind technisch nicht extrem ausgefeilt, aber gut genug, um das zu tun, was sie tun müssen."

Während die USA mit Nordkorea über die Aufgabe des Atomprogramms verhandeln und der Westen über den möglichen Wiederaufbau einer stillgelegten Raketenanlage spekuliert, gehen Kims Hacker im Verborgenen auf Beutezug.

**Bitcoin-Beutezüge für den Staat: Was die Hacker erreichen wollen**

Die Attacken sind nicht nur darauf ausgerichtet, geheime Dokumente zu erbeuten oder Gegner zu schwächen - es geht oft einfach ums Geld. Mit Angriffen auf Banken, aber auch auf Bitcoin-Börsen soll die marode Staatskasse des Landes aufgebessert werden. "Sie erwirtschaften durch Computerbetrug Einkommen für den Staat und müssen Quoten erfüllen oder bestimmte Ziele angreifen", so Inkster.

Mehrere größere Attacken werden Nordkoreas Hackertruppen zugerechnet: vom Hack des Filmstudios Sony Pictures Entertainment bis zur WannaCry-Erpressersoftware-Attacke. Sie operieren zum Teil aus dem Ausland und infiltrieren im Staatsauftrag weltweit Computersysteme.

Das Land verfüge über "relativ viele offensive Kapazitäten", sagt Inkster. In Südkorea haben die Hacker sich bereits Zugriff auf Netzwerke der Metro von Seoul verschafft, Militärdokumente gestohlen oder versucht, ins Computersystem eines Atomkraftwerks einzudringen.

Solange im aktuellen Konflikt um Nordkoreas Abrüstung noch eine Option auf Verhandlungen bestünde, werde Nordkorea aber nicht die USA angreifen, glaubt Inkster. Dass es den Hackern gelingen könnte, kritische Infrastruktur oder militärische Einrichtungen in den USA lahmzulegen, hält er zudem für unwahrscheinlich. "Aber sie werden weiter Ziele wie Südkorea oder Japan attackieren und auch die kriminellen Aktivitäten der staatlichen Hacker werden weitergehen", so der Sicherheitsexperte.

**Industriespionage auf der ganzen Welt: Welche Branchen die Hacker ins Visier nehmen**

Eine als "Sharpshooter" bezeichnete Spionageoperation, die auf nordkoreanische Hacker deutet, lief etwa auch während der Verhandlungen zwischen den USA und Nordkorea in den vergangenen Monaten weiter. Laut einem Sprecher der IT-Firma McAfee, deren Sicherheitsforscher Code vom Angriffsserver ausgewertet haben, ist die Operation bereits seit September 2017 in Gang.

Rund 90 Organisationen und Firmen verschiedener Branchen sind betroffen, darunter Energie und Verteidigung. "Auf die aktuellen diplomatischen Aktivitäten zwischen den USA und Nordkorea ist die Operation aber nicht direkt zurückzuführen", sagte ein Sprecher von McAfee zum SPIEGEL.

Zuerst seien vor allem Ziele in den USA, der Schweiz und Israel infiltriert worden, dann wechselten die Angreifer den Fokus. "Die jüngsten Angriffe scheinen sich vor allem auf Finanzdienstleister, Regierungs- und andere Organisationen mit kritischer

Infrastruktur in Deutschland, der Türkei, Großbritannien und den USA zu konzentrieren", so der Sprecher.

Die Operation nutzt ihm zufolge Schadcode, der bereits 2016 von der nordkoreanischen Lazarus-Gruppe verwendet wurde. Die technischen Indizien müssten aber von klassischer Ermittlerarbeit gestützt werden, damit sich die Attacken eindeutig zuordnen ließen.

**Attacke auf Hollywood: Warum die Hacker auch symbolische Ziele auswählen**

Über Hackeraktivitäten aus Nordkorea wurde nach dem Sony-Hack von 2014 weltweit diskutiert - auch er wird der Lazarus-Gruppe zugeordnet. Die Angreifer erbeuteten interne Dokumente der US-Filmtochter des japanischen Sony-Konzerns wie Gehaltsabrechnungen, Strafregister, Gesundheitsdaten von Mitarbeitern, E-Mails sowie damals unveröffentlichte Filme wie "The Interview", eine Komödie über ein Mordkomplott der CIA gegen Nordkoreas Staatsoberhaupt Kim Jong Un. Das Material veröffentlichten sie im Internet - ein Imageschaden, der Entschädigungszahlungen an Mitarbeiter in Millionenhöhe nach sich zog.

Technisch sei der Sony-Hack nicht aufwendig gewesen, sagte der US-Verteidigungsexperte Eric Rosenbach von der Harvard Kennedy School im vergangenen Jahr bei einem Vortrag. Zudem sei die IT-Sicherheit des Unternehmens schlecht gewesen. Die Angreifer seien aber "clever" vorgegangen und hätten monatelang Daten und Dokumente abgegriffen.

"Die Nordkoreaner haben gezeigt, was man mit einem Hack im zivilen Sektor anrichten kann", so Rosenbach, der zur Zeit des Sony-Hacks für das Verteidigungsministerium arbeitete. Seitdem hätten sich Nordkoreas Hacker professionalisiert. "Sie sind raffinierter geworden. Kim Jong Un hat erkannt, dass Cyberoperationen ein wichtiger Bestandteil der nationalen Strategie sind."

Nordkorea setze Hackerangriffe ein, um militärische Provokationen und Propaganda zu verstärken, heißt es in einer Analyse von Boo Hyeong Wook vom Korea Institute for Defense Analysis (KIDA). Die Operationen seien bisher nicht die "Topwaffe im Arsenal" Nordkoreas, würden aber für Unannehmlichkeiten sorgen und der Abschreckung dienen, schränkt Inkster vom IISS ein. Auch als alternative Geldquelle stützen sie das Regime.

**Ausgebildet in Pjöngjang: Wer die Hacker sind**

Im vergangenen Jahr haben die USA einen 34-jährigen Hacker aus Nordkorea wegen Computerbetrugs angeklagt, der sich der Most-wanted-Liste des FBI zufolge derzeit wohl in Nordkorea aufhält. Der Mann wurde an der Kim Chaek University of Technology in Pjöngjang ausgebildet und arbeitete zur Tarnung in der IT-Firma Chosun Expo Joint Venture, die dem nordkoreanischen Staat gehört und deren Mitarbeiter in Nordkorea, China und anderen Ländern aktiv waren.

Als Mitglied der Lazarus-Truppe wird ihm und weiteren Hackern zur Last gelegt, am Sony-Hack sowie an globalen Angriffen auf Banken beteiligt gewesen zu sein. 2016 versuchten die Hacker fast eine Milliarde Dollar von der Zentralbank Bangladeschs zu erbeuten, es gelang ein Transfer von umgerechnet 81 Millionen Dollar.

Auch die WannaCry-Attacke im Jahr 2017, der bisher aufsehenerregendste Lösegeldtrojaner-Angriff überhaupt, geht den Amerikanern zufolge auf das Konto der Hackertruppe. Schadsoftware hatte die Computer von Krankenhäusern, Banken und anderen Firmen auf der ganzen Welt verschlüsselt. Der Schaden war groß, Lösegeld zahlten allerdings relativ wenige Opfer.

Zwischen 2017 und 2018 haben die Lazarus-Hacker einem Bericht der IT-Sicherheitsfirma Group-IB zufolge Kryptowährungen im Wert von 571 Millionen Dollar abgegriffen, bei Angriffen auf diverse Kryptobörsen. "Nordkoreas Hackinggruppe ist heute die Haupteinnahmequelle für Fremdwährungen", sagt Kim Seungjoo, ein südkoreanischer Professor für IT-Sicherheit, dem SPIEGEL.

Dem südkoreanischen Verteidigungsministerium zufolge verfügt Nordkorea inzwischen über knapp 7000 Hacker, etwa 1800 davon sollen Teil der Abteilung Bureau 121 sein, einer auf Spionage und Sabotage fokussierten Spezialeinheit.

"Nordkorea hat ein Programm, um die schlauesten und besten Nachwuchshacker zu identifizieren", sagt Sicherheitsexperte Inkster. Die Ausbildung erfolge in Nordkorea, aber auch in anderen Ländern wie China, Russland oder Indien.

**Abgeschottet, aber online: Wie die Hacker ins Netz kommen - und wenig Angriffsfläche bieten**

"Nordkoreas größte Beschränkung ist, dass das Land keinen eigenen internationalen Internetzugang hat", sagt Inkster. "Aber man braucht gar nicht so viel Infrastruktur, um jemandem diese Art von Cyberattacken beizubringen."

Eine chinesische und seit dem vergangenen Jahr auch eine russische Firma versorgen Nordkorea bisher mit Internetzugang, es gibt allerdings bisher nur wenige funktionierende Verbindungen. Bei ihren Auslandseinsätzen haben Hacker unbegrenzten Zugang zum Internet.

"In den meisten Ländern lernen Studenten aus Programmierbüchern und in Computer-Labs, aber Nordkoreas Hacker verbessern ihre Fähigkeiten durch Praxis - das wirkt sich stark auf ihre Fähigkeiten aus", so IT-Professor Kim Seungjoo.

Im Global Threat Report der IT-Sicherheitsfirma CrowdStrike, der auswertet, wie schnell Hacker sich Zugang zu weiteren Rechnern im Netzwerk verschaffen können, nachdem sie einen Computer infiltriert haben, landeten Nordkoreas Hacker kürzlich hinter Russland auf Platz zwei. CrowdStrike-Mitgründer Dmitri Alperovitch hält Nordkorea für das innovativste Land von weltweit: "Sie mögen nicht die komplexesten Werkzeuge haben, aber was das Erreichen der Ziele ihrer Regierung mithilfe des Internets angeht, sind sie führend."

Mit Cyberkapazitäten können Staaten wie Nordkorea die Machtbalance zu militärisch hochgerüsteten Ländern wie den USA verändern - und sich mit vergleichsweise günstigen Mitteln geheime Informationen sichern, mit Angriffen auf kritische Infrastruktur drohen und mitunter viel Schaden anrichten.

Sven Herpig von der Stiftung Neue Verantwortung sagt: "In die gleiche Kategorie wie Nordkorea gehört auch Iran, also Staaten mit wenig oder weniger Wirtschaftsmacht, die im militärischen Bereich ihre offensiven Cyberfähigkeiten ausbauen, um ihre konventionelle Militärkraft zu unterstützen oder teilweise zu ersetzen."

Dass Nordkorea bisher selbst kaum vernetzt ist, ist dabei für das abgeschottete Land von Vorteil: So bietet es kaum Angriffsfläche für digitale Attacken anderer Staaten.

**Zur Startseite**

**Diesen Artikel...** Drucken | Feedback | Nutzungsrechte

**Mehr zum Thema**

**Nordkorea** **Hacker** **Computersicherheit**
Alle Themenseiten



## Forum ›

**Diskutieren Sie über diesen Artikel**
insgesamt 74 Beiträge

Alle Kommentare öffnen



**pakeha52** gestern, 10:35 Uhr
**1. Die Überschrift ...**
... erweckt den Eindruck das @KimDotCom (alias Kim Schmitz, derzeit in Neuseeland lebend) beteiligt ist ! Solch ein Wortspiel ist meines Erachtens bedenklich und nicht rechtens ! - - - - - - Unseres Erachtens nicht. MfG [...]

**Spiegelleserin57** gestern, 10:38 Uhr
**2. gehackt wird überall!**
sicherlich auch hier. Der normale Bürger der nicht sehr mit der IT verbunden ist wird es kaum bemerken. Viele IT-Artikel berichten schon lange darüber dass immer wieder Firmen und auch Privatleute ausgespäht werden. Daher [...]

**Beat Adler** gestern, 10:40 Uhr
**3. 7000 nordkoreanische Hacker surfen frei im Internet? Wirklich?**

7000 nordkoreanische Hacker surfen frei im Internet? Wirklich? Sollte das so sein, werden sie zur Keimzelle, welche das Ende der Kimdynastie einlaeutet! Diese 7000 Nordkoreaner sind nicht immun gegen das Virus der Freiheit! [...]

**lspring** gestern, 10:42 Uhr

**4. 0 je!**

Da wird aber ein riesiger Popanz aufgebaut.

**oldman2016** gestern, 10:43 Uhr

**5. Wo ist das Problem?**

Cyberkriminalität durch Nordkorea ist ohne den starken Bruder im Norden - der Volksrepublik China - überhaupt nicht denkbar. Diese banale Wahrheit in einem Artikel zu unterdrücken grenzt an Volksverdummung. Offenbar wagen sich [...]

Alle Kommentare öffnen

Seite 1 von 15

## Ihr Kommentar zum Thema

Bitte melden Sie sich an, um zu kommentieren. Anmelden | Registrieren

Das SPON-Forum: So wollen wir debattieren

Überschrift

optional

Beitrag

Kommentar senden



TOP

Firmenwagenrechner
Jobsuche

## FREIZEIT

Eurojackpot
Lottozahlen
Glücksspirale
Sportwetten
Gutscheine
Bücher bestellen
Arztsuche
Ferientermine
Spiele

## SPIEGEL GRUPPE

Abo - Shop - bento - manager magazin - Harvard Business Manager - buchreport - Werbung - Jobs - Planestream

DER SPIEGEL SPIEGEL WISSEN Dein SPIEGEL SPIEGEL GESCHICHTE SPIEGEL CHRONIK

Impressum - Datenschutz - Nutzungsbedingungen - Nutzungsrechte - Kontakt - Hilfe