2018/42 Ausland

https://www.jungle.world/artikel/2018/42/wenn-agenten-schlampen

Der niederländische Geheimdienst hat wahrscheinlich einen Hackerangriff russischer Agenten verhindert

Wenn Agenten schlampen

Von **Elke Wittich**

Anfang Oktober wurde bekannt, dass der niederländische Geheimdienst einen Hackerangriff auf die Organisation für das Verbot chemischer Waffen in Den Haag vereitelt hat. Russische Agenten sollen versucht haben, Ermittlungen in mehreren Fällen zu behindern.

Wie jeder andere Arbeitnehmer auf Dienstreise auch, bewahrte Aleksej Morenets die Taxiquittung für die Fahrt zum Flughafen ordentlich auf. Nur zwei Tage später sollte der Zettel als Beweisstück gegen ihn und seine drei Kollegen gelten. Begonnen hatte die Taxifahrt am 10. April ganz in der Nähe des Moskauer Komsomolski Prospekt 20, wo die »Einheit 26165« des russischen Militärgeheimdiensts GRU residiert. Zu Sowjetzeiten war dort der Sitz der Dechiffrierabteilung des GRU, deren Aufgabe es unter anderem war, abgefangene Nachrichten zu entschlüsseln. Nach rund dreieinhalb Stunden Flugzeit landeten die Cyberexperten Morenets und Ewgenij Serebriakow sowie ihre beiden zur Unterstützung mitgereisten GRU-Kollegen Oleg Sotnikow und Aleksej Minin auf dem Amsterdamer Flughafen Schiphol.

Ein halbes Jahr später veröffentlichte Bilder einer Überwachungskamera zeigen, dass die vier Männer von einem russischen Botschaftsmitarbeiter abgeholt wurden, der neben ihnen herläuft. Er brachte die Geheimdienstler zum 30 Kilometer entfernten Palace Hotel in Noordwijk aan Zee. Am nächsten Tag mieteten die Agenten ein Auto und fuhren nach Den Haag, wo sie die nächsten zwei Tage in der Nähe des Gebäudes der Organisation für das Verbot chemischer Waffen (OPCW) verbrachten. Die unabhängige Organisation ist in die Untersuchung eines Kriminalfalls in Großbritannien involviert: Knapp einen Monat zuvor waren der ehemalige russische Spion Sergej Skripal und seine Tochter Julia bei einem Anschlag mit dem Nervengift Nowitschok vergiftet worden. Die OPCW ermittelt zudem zum Giftgasangriff im syrischen Douma, für den Truppen des Diktators Bashar al-Assad verantwortlich gemacht werden, Russlands Verbündeter in Syrien.

> »Man sollte wirklich denken, dass solche Spione ein neues, leeres Notebook mitgegeben bekommen, wenn sie eine Hacking-operation im Ausland

ausführen sollen.« *Frank Groenewegen, Fox-IT*

Seit dem 10. April wurden die Männer bereits vom niederländischen Militärgeheimdienst MIVD überwacht, nach einem Tipp des britischen Geheimdiensts, aber auch aufgrund »eigener Erkenntnisse«, wie es nun heißt. Möglich ist, dass die Papiere der Russen bereits bei der Einreisekontrolle aufgefallen waren, da sie fortlaufende Seriennummern aufwiesen. Die vier Männer wurden der Spionage verdächtigt, aber was sie genau ausspionieren wollten, war dem MIVD zunächst nicht klar.

Am 13. April parkten sie ihr Mietauto auf dem Parkplatz des Marriott-Hotels gegenüber dem OPCW-Gebäude so, dass das Heck des Wagens genau auf dieses ausgerichtet war. Minin begann, die Umgebung des OPCW ausgiebig zu fotografieren. Als sie anfingen, ihre Hacker-Ausrüstung im Kofferraum in Betrieb zu nehmen, ging alles sehr schnell. Noch bevor die Observierten Daten abgreifen konnten, seien sie verhaftet worden, so Onno Eichelsheim, der Leiter des MIVD, auf einer Pressekonferenz am 4. Oktober, bei der es um die Vereitelung des Angriffs auf die OPWC ging. Dabei geholfen hatten britische Dienste. Als die Russen bemerkten, dass sie aufgeflogen waren, versuchte einer von ihnen noch, sein Mobiltelefon zu zerstören. Wahrscheinlich ist es das Modell, das den niederländischen Ermittlern zufolge am 9. April in Moskau zum ersten Mal aktiviert wurde und Verbindung zum dem Komsomolski Prospekt nächstgelegenen Funkmast aufnahm. Die gesamte Ausrüstung der Männer, darunter Laptops, Smartphones, eine Tasche mit Batterie, Wandler, Antenne und Wifi-Router, wurde beschlagnahmt, des Weiteren eine Plastiktüte mit leeren Bierdosen und anderem Müll, die sie aus dem Hotel mitgenommen hatten, um keine Spuren zu hinterlassen. Ein ebenfalls bei ihnen gefundenes Zugticket zeigt, dass sie offenbar noch weitere Pläne hatten: Das Ticket war für eine Zugfahrt am 17. April von Utrecht nach Basel vorgesehen. Dort in der Nähe befindet sich das eng mit der OPCW zusammenarbeitende Labor Spiez des Schweizerischen Bundesamts für Bevölkerungsschutz. Es forscht unter anderem nach der Herkunft des im Fall Skripal verwendeten Gifts Nowitschok und untersucht in Syrien verwendete Kampfstoffe.

Serebriakows Notebook verriet überdies, dass es weitere Auslandsaufenthalte in Brasilien, der Schweiz und Malaysia gab. Ausdrucke von Google Maps zeigten Adressen russischer Vertretungen in der Schweiz. Bei der Pressekonferenz Anfang Oktober ging es auch um weitere mögliche Hackerangriffe. In Malaysia sollten mutmaßlich die Ermittlungen zum Absturz der Passagiermaschine MH17 in der Ukraine behindert werden. Bislang wird davon ausgegangen, dass eine aus Russland stammende Flugabwehrrakete für den Absturz verantwortlich war.

Der MIVD setzte die russischen Spione umgehend in ein Flugzeug zurück nach Russland. »Wir eskortierten sie zum Flughafen. So handhaben wir solche Operationen«, sagte Eichelsheim. Dabei wäre vermutlich auch eine Inhaftierung der Männer juristisch möglich gewesen, denn sie hatten zwar Diplomatenpässe, waren aber nicht von den niederländischen Behörden als Diplomaten akkreditiert. In diesem Fall hätte die Staatsanwaltschaft die Ermittlungen übernommen und der militärische Geheimdienst keine Chance mehr gehabt, die beschlagnahmten Gegenstände und Geräte zu untersuchen.

Der renommierte Strafrechtler Geert-Jan Knoops geht davon aus, dass die Niederlande kein Interesse an einer Verschlechterung der Beziehungen zu Russland hatten und es bei einer bloßen Demonstration der weiterhin engen Zusammenarbeit zwischen dem bald womöglich nicht mehr zur EU gehörenden Großbritannien und den anderen europäischen Staaten belassen wollten. Ko Colijn vom unabhängigen Think Tank Clingendael Institute sieht das auch so. Es sei definitiv kein Zufall gewesen, dass der britische Botschafter bei der Pressekonferenz des MIVD anwesend gewesen sei.

Bleibt die Frage, warum die russischen Spione derart viele Beweise mit sich herumschleppten. Frank Groenewegen vom Sicherheitsunternehmen Fox-IT sagte dem niederländischen Fernsehsender NOS: »Man sollte wirklich denken, dass solche Spione ein neues, leeres Notebook mitgegeben bekommen, wenn sie eine Hacking-Operation im Ausland ausführen sollen.« Vermutlich habe es sich um eine in letzter Minute angesetzte Reise gehandelt, »sie hatten es anscheinend supereilig«. Dafür spreche auch, dass einer der Männer während der Festnahme versucht habe, sein Handy zu zerstören: »Wenn das Mobiltelefon ordentlich verschlüsselt gewesen wäre, hätte er sich wahrscheinlich keine Sorgen gemacht.« Andererseits könne das Forensische Institut der Niederlande auch aus einem Telefon, das drei Wochen auf dem Meeresboden gelegen habe, noch Daten holen, »Geheimdienste können bestimmt noch viel mehr«.

Auffällig sei, so niederländische Experten, dass über die vier Spione des geheimsten russischen Geheimdienstes viele, teils sogar private Informationen im Internet zu finden gewesen seien. Morenets hat beispielsweise nicht nur ein Profil auf der russischen Datingseite mylove.ru, sein dort veröffentlichtes Bild zeigt ihn sogar vor dem Moskauer Panasonic-Gebäude, das ganz in der Nähe des Komsomolski Prospekts 20 liegt. Serebriakow ist auf Fußball-Websites zu finden, er spielte nämlich in der Amateurliga – und das wohl, so die *Moscow Times*, für ein Team, das als Mannschaft der Geheimdienste gilt.

Sico van der Meer vom Clingendael Institute geht davon aus, dass es den Geheimdienstlern eher egal gewesen sei, ob sie auffliegen. »Wenn wir geschnappt werden, können wir damit auch umgehen«, habe ihre Devise offenbar gelautet. »Sie machen solche Sachen einfach in aller Öffentlichkeit«, so van der Meer. Der Geheimdienstforscher Paul Abels von der Universität Leiden fragt: »Sind die Russen so dumm oder sind wir so schlau? Sie machten alle nur möglichen Anfängerfehler – das kann auf Unterschätzung hindeuten, auf mangelndes Bewusstsein – oder auf Brutalität. Der GRU ist schließlich dafür bekannt, dass er besonders dreist zu Werke geht.«

Russland wies die Vorwürfe der niederländischen Regierung wegen russischer Cyberangriffe auf die OPCW am Montag voriger Woche als unbegründet zurück. Die Niederlande hätten keine ausreichenden Belege präsentiert.

© Jungle World Verlags GmbH