

# Grüße aus Fernost

## Chinas Spähangriff auf die Bundesregierung

Die E-Mail verhielt Inhalte von weltpolitischer Bedeutung. Ihren Empfängern gaukelte sie einen Informationsaustausch unter den wirtschaftspolitischen Beratern der mächtigsten Politiker der Welt vor, und zwar Anfang September 2013, unmittelbar vor dem Gipfeltreffen der G-20-Staaten im russischen St. Petersburg. Die sogenannten Sherpas waren gerade in der heißen Phase der Konferenzvorbereitung. Doch die E-Mail enthielt keine Informationen, die bei ihren Verhandlungen halfen.

Die gesamte Nachricht war nach Erkenntnissen deutscher Sicherheitsbehörden gefälscht – statt Informationen enthielt sie Spionagesoftware, die die Rechner der Empfänger infizieren sollte. Nach Angaben aus Sicherheitskreisen gingen diese und ähnliche E-Mails an hochrangige Entscheidungsträger in mehreren Bundesministerien und bei Banken. Offenbar gehörte auch der wirtschaftspolitische Berater von Kanzlerin Angela Merkel, Lars-Hendrik Röller, zu jenen, die der Spionageangriff treffen sollte.

Eine Regierungssprecherin bestätigt Versuche, „die Informationssicherheit im Bundeskanzleramt auf dem beschriebenen Weg zu kompromittieren“. Zu Röller als möglichem Ziel äußerte sie sich nicht. Der Angriff sei abgewehrt worden.

Nach internen Erkenntnissen des Verfassungsschutzes kann die Attacke „nachrichtendienstlichen Urhebern zugeordnet“ werden. Die Spähsoftware sollte ihre Ergebnisse nach China liefern. Chinesische Geheimdienste spähden demnach nicht mehr nur die hiesige Hightech-Industrie oder Oppositionelle im Exil aus. Sie haben auch die deutsche Politik im Visier.

Weltweit beobachten westliche Nachrichtendienste, dass in den chinesischen Botschaften die Zahl mutmaßlicher Geheimdienstmitarbeiter kontinuierlich steigt. Zudem registrieren sie, dass Chinas Geheimdienste vermehrt dort Zuträger gewinnen wollen, wo internationale Politik gemacht wird – etwa in Brüssel.

Noch auffälliger aber ist die Vielzahl elektronischer Attacken, die die

Sicherheitsbehörden staatlich gesteuerter Spionage aus China zuordnen, auch wenn oft Restzweifel über die tatsächlichen Urheber bleiben.

Ein weiteres Beispiel für einen solchen Angriff ist eine E-Mail an die Außenministerien von fünf EU-Mitgliedstaaten – ebenfalls im Vorfeld des G-20-Treffens in St. Petersburg. Darin erhielten die Diplomaten einen Anhang „US military options in Syria“. Bei dem Gipfel sollte tatsächlich über einen möglichen Militärschlag gegen den syrischen Diktator Baschar al-Assad geredet werden. Der Titel des Anhangs sollte die Empfänger wohl verleiten, die Schadstoffsoftware schnell zu öffnen und so zu aktivieren. Auf ähnliche Weise sind nach Erkenntnissen der deutschen



Pressezentrum beim G-20-Gipfel\*  
Spionagesoftware statt Informationen

Sicherheitsbehörden auch deutsche Botschaften im Ausland, Entscheidungsträger in deutschen Ministerien und Ministerien anderer europäischer Regierungen angegriffen worden.

Besonders häufig werden die staatlichen Hacker aus Fernost im Umfeld von internationalen Gipfeln aktiv. Es geht ihnen offenbar nicht nur darum, die Vorbereitungen der Staaten auf die Treffen auszuspionieren, sie wollen allgemein Spähsoftware in die Ministerien einschleusen. „Der Anlass Gipfeltreffen dient vorrangig dazu, die niedrige Aufmerksamkeitsschwelle im Vorfeld auszunutzen“, sagt ein Sicherheitsexperte. Dann herrscht Stress – und Thema und Absender erscheinen zu wichtig, um an Spione zu denken.

FIDELIUS SCHMID

das Amt wohl nicht das gesamte zur Verfügung stehende nachrichtendienstliche Instrumentarium anwenden, also etwa Telefonüberwachung, Quellenanwerbung oder Observationen. Aber zumindest will man alles daransetzen herauszufinden, was insbesondere in Botschaften und Konsulaten vor sich geht, wer dort arbeitet und über welche technischen Möglichkeiten man verfügt. Zum Beispiel, ob deutsche Regierungsstellen von der US-Botschaft in Berlin aus abgehört werden.

Der Chef des Bundesamts für Verfassungsschutz, Hans-Georg Maaßen, ist bereits aktiv geworden. Er hat die US-Botschaft aufgefordert, Namen und Daten diplomatisch akkreditierter Nachrichtendienst-Mitarbeiter in Deutschland zu übermitteln. Zudem verlangte Maaßen Auskunft, mit welchen Privatfirmen die Amerikaner in Deutschland im Bereich Spionage kooperieren. Inzwischen, heißt es in Köln, sei man darüber besser im Bilde als noch vor wenigen Monaten.

Derweil hat auch beim kleinsten der drei deutschen Geheimdienste, dem Militärischen Abschirmdienst (MAD) der Bundeswehr, eine Diskussion über eine Neuausrichtung begonnen. MAD-Chef Ulrich Birkenheier lässt derzeit prüfen, ob der Dienst bei der Spionageabwehr nicht auch stärker in Richtung befreundeter Nachrichtendienste blicken soll.

Neun Monate nach Beginn der NSA-Affäre schwenkt die Bundesregierung damit ernsthaft auf Konfrontationskurs mit Washington. Es wäre ein Bruch mit der jahrzehntelang geübten Praxis, die westlichen Partner in Deutschland weitgehend unbeobachtet schalten und walten zu lassen. Zwar gibt es vor allem im Kanzleramt und im Innenministerium Stimmen, die vor unabwehrbaren Folgen für die geheime Geheimdienst-Kooperation mit den Partnerstaaten warnen. Anders aber, sagen hochrangige Regierungsmitglieder, würden die Amerikaner nicht begreifen, welche nachhaltigen Erschütterungen die NSA-Affäre ausgelöst habe.

Eine endgültige Entscheidung ist noch nicht gefallen. Das Auswärtige Amt, das Innenministerium und das Bundeskanzleramt stimmen sich noch ab. Auch aus diesem Grund verschiebt sich der geplante Besuch von Angela Merkel in Washington nach hinten. Ursprünglich war der März im Gespräch, jetzt verlautet nur noch, die Kanzlerin werde „im Frühjahr“ reisen. Womöglich wird es noch später. Merkel, heißt es in Regierungskreisen, werde erst fahren, wenn es in Berlin eine abgestimmte Linie gebe. Und wenn vorher geklärt sei, dass sie mit einem vorzeigbaren Erfolg zurückkommen werde. Merkel brauche einen „Skalp“. Noch ist unklar, wie er aussehen wird.

HUBERT GUDE, HORAND KNAUP,  
JÖRG SCHINDLER, FIDELIUS SCHMID,  
HOLGER STARK

\* In St. Petersburg 2013.