Kai Nothdurft

Attribution von „Cyber"-Angriffen durch Politik und Medien

In meinem Vortrag auf der FIfFKon 2017 in Jena habe ich zunächst eine Einführung in die Methoden der IT-Forensik gegeben. Ich habe kurz dargestellt, welche digitalen Spuren ForensikerInnen untersuchen und wie einfach solche Spuren verwischt und manipuliert werden können. Dies sollte veranschaulichen, warum die Attribution eines Hacker-Angriffs eine große Herausforderung und eine klare Identifikation der Angreifenden nur selten möglich ist. Am Beispiel des Bundestagshacks 2015 habe ich dargelegt, auf welcher Informationsbasis die Medien die Täteridentifizierung vornahmen und sich der Narrativ gebildet hat, dass die Angriffe aus Russland stammen würden.

Während ForensikerInnen zumeist professionell einen Vorfall untersuchen und bewerten und ihnen die oben geschilderten Unsicherheiten nur allzu bewusst sind, machen es sich sowohl Politik als auch Medien häufig mit der Zuordnung eines Angriffs zu einer bestimmten Gruppe einfacher. Wir haben es dabei mit einer Meinungs- und Stimmungsmache zu tun, die nur auf einer sehr eingeschränkten Faktenlage basiert. Es muss ein Schuldiger gefunden und der Öffentlichkeit präsentiert werden. Wenn es ins Weltbild passt, wird auch eine dünne Indizien-„Beweis"lage, die eh nur Experten verstehen, als ausreichend für eine Schuldzuweisung angesehen. Dies kann in einer gefährlichen Eskalation münden und muss friedenspolitisch thematisiert und kritisiert werden.

Erstaunlich selten fällt der Verdacht auf Geheimdienste verbündeter oder befreundeter Staaten, obwohl z. B. durch die Snowden Leaks sehr gut dokumentiert wurde, dass sich NSA und GCHQ auch beim Ausspionieren und Hacken von Verbündeten nicht zurückhalten. Das bedeutet nicht, dass Russland, China oder Nordkorea Waisenknaben sind, aber sie sind eben keineswegs die Einzigen, die über militärische Hackereinheiten verfügen. Die NSA dürfte die fortschrittlichste, mit dem größten Etat ausgestattete Einheit unterhalten. Im US-militärisch-wirtschaftlichen Komplex haben die US-Dienste außerdem privilegierten Zugang zu weltweit eingesetzten IT-Produkten inklusive zu deren Schwachstellen und möglicherweise auch Hintertüren. Eine Sicherheitslücke erlaubt dem Hersteller jedoch immer, die Absicht für den Einbau oder das Offenhalten einer Hintertür abzustreiten (plausible deniability).

Im Falle eines russischen Produkts, der Antimalware-Lösung von Kaspersky, wurde eine behauptete, aber nicht nachgewiesene Zugriffsmöglichkeit der russischen Regierung insbesondere in den USA als Risiko betrachtet und das Produkt vom Einsatz in Behörden ausgeschlossen.[1] Dem war ein bizarrer Sicherheitsvorfall vorangegangen. Ein externer Mitarbeiter der NSA hatte unter Verletzung mehrerer Sicherheitsvorschriften auf seinem Privat-PC „dienstliche" NSA-Malware gespeichert.[2] Der auf dem PC installierte Virenscanner von Kaspersky stufte diese Malware völlig korrekt als verdächtig ein und lud diese NSA-Cyberwaffen zur weiteren Analyse zu einem Kaspersky-Server hoch. Angeblich gelangten diese dann zu russischen Geheimdienstkreisen, wobei eine Mitschuld oder gar aktive Beteiligung von Kasperskys Produkt zwar in einem Wallstreet-Journal-Beitrag behauptet, aber nicht näher erläutert oder gar nachgewiesen und von Kaspersky vehement bestritten wurde.[3]

Pikanterweise machte der israelische Geheimdienst, der einen seiner Mitarbeiter bei Kaspersky eingeschleust hatte, die NSA erst auf das Sicherheitsproblem aufmerksam, dass sie die Kontrolle über mehrere ihrer Cyberwaffen verloren hatte.

Am 28.2.2018 meldete dpa einen Hackerangriff auf das Datennetz der Bundesverwaltung und beschuldigte APT28 als Tätergruppe, die auch als Schuldige in dem im Vortrag behandelten Bundestagshack gelten. Dies wurde bereits am Folgetag (1.3.2018) korrigiert, nun soll es die „russische Hackergruppe Snake"[4] gewesen sein. Vielleicht wird der forensische Bericht noch veröffentlicht, dann ließe sich möglicherweise eine fundierte Bewertung treffen, auf welchen Spuren die Behauptung fußt.

Referenzen

1 https://www.heise.de/newsticker/meldung/USA-verbieten-Behoerden-Nutzung-von-russischer-Kaspersky-Software-3831122.html
2 https://www.heise.de/newsticker/meldung/Russland-soll-dank-Kaspersky-Software-NSA-Dokumente-an-sich-gebracht-haben-3851108.html
3 https://www.heise.de/newsticker/meldung/Kaspersky-Keine-Weitergabe-von-NSA-Malware-an-russische-Hacker-3871326.html
4 https://www.heise.de/newsticker/meldung/Bundeshack-Russische-Hackergruppe-Snake-soll-hinter-Angriff-stecken-3984930.html

Kai Nothdurft

Kai Nothdurft arbeitet als *Information Security Officer* in einer großen deutschen Versicherung. Seit 2009 ist Kai Nothdurft im Vorstand des FIfF e. V. aktiv. Seit Jahren hält er Vorträge und schreibt Artikel, die sich kritisch mit seinem Fachgebiet IT-Sicherheit beschäftigen.