Ein besonders energetischer Bär

Wie Hacker Stromversorger angreifen / Von Justus Bender

FRANKFURT, 6. September. Sollte es der Bundesrepublik eines Tages wie der Ukraine am 23. Dezember 2015 gehen, wäre der Albtraum der deutschen Sicherheitsbehörden eingetreten. An diesem Tag fiel in rund 700 000 Haushalten der Westukraine der Strom aus. Allerdings geschah das nicht, weil Separatisten ein Kraftwerk beschossen hatten oder wegen eines technischen Defekts. Allein einige E-Mails mit Computerviren an Mitarbeiter des Energieversorgers hatten ausgereicht, um die Stromversorgung zu unterbrechen. Vor dem Hintergrund des Ukraine-Konflikts lagen zwei Vermutungen nahe. Erstens, dass es russische Hacker gewesen sein könnten, die den Gegner durch Sabotage schwächen wollten. Zweitens, dass es sich um das spezielle Problem einer früheren Sowjetrepublik handeln könnte, von der westliche Staaten wie Deutschland nicht betroffen sein würden. Letzteres könnte sich als Fehlschluss erweisen.

Zu dem Zeitpunkt, als in der Ukraine die Lichter ausgingen, waren westliche Energieversorger längst von mutmaßlich russischen Angreifern heimgesucht worden. Seit Februar 2013 hatte eine Hackergruppe, die von Sicherheitsfirmen wahlweise „Energetic Bear“ (energetischer Bär) oder „Dragonfly“ (Libelle) genannt wird, westliche Energiefirmen und Stromversorger angegriffen. Sie versandten virenbelastete E-Mails und hackten Internetseiten, auf denen Mitarbeiter der Energiebranche oft verkehrten. Betroffen waren Länder wie Spanien, die Vereinigten Staaten, Frankreich, Italien, Deutschland und andere. Die Angriffe hatten das Ziel, Passwörter zu stehlen, sie installierten aber auch Programme, die eine Fernsteuerung ermöglichten. Eine Analyse der Sicherheitsfirma Symantec ergab damals, dass die Schadprogramme alle zu Uhrzeiten erstellt wurden, die einem Neunstundentag zwischen 9 und 18 Uhr in der Moskauer Zeitzone UTC+4 entsprechen, besonders an Dienstagen wurde viel gehackt, an Wochenenden hingegen nie. Ein unwiderlegbarer Beweis war das allerdings nicht, weil eine Fälschung solcher Uhrzeiten technisch möglich ist.

Das war 2013. Laut einem am Mittwoch veröffentlichten Bericht von Symantec ist die gleiche Gruppe in diesem Jahr wieder besonders aktiv gewesen. Sie griffen Energieversorger in der Schweiz, den Vereinigten Staaten und der Türkei an. Symantec konnte außerdem feststellen, dass auch Mitarbeiter deutscher Energieversorger infizierte Internetseiten der „Dragonfly“-Hacker besucht hatten. Dabei handelte es sich zum Beispiel um Seiten, auf denen eine Registrierung für eine Fachtagung möglich war. Eine tatsächliche Infizierung eines deutschen Energieversorgers konnte bei dieser neuerlichen Angriffswelle nicht nachgewiesen, aber auch nicht ausgeschlossen werden. „Seit Mai 2017 hatten wir eine verstärkte Aktivität gesehen, und die besteht fort. Die Angriffswelle ist noch nicht vorbei, deshalb finden wir es wichtig, dass wir informieren“, sagte der Symantec-Analyst Candid Wüest dieser Zeitung am Mittwoch. „Wir wollen keine unnötige Panik verbreiten, aber wenn Strom aus der Ferne abgeschaltet werden kann, ist das ein großes Druckmittel“, sagte Wüest in Anspielung auf das Kräfteverhältnis zwischen gegnerischen Staaten.

In dem Bericht heißt es, die Gruppe habe „nun potentiell die Fähigkeit, diese Systeme zu sabotieren und zu kontrollieren, sollte sie sich dazu entscheiden“. Wüest zögert, die Hackergruppe eindeutig als russische Gruppe zu identifizieren. „Wie immer bei Cyberattacken ist eine Zuschreibung praktisch unmöglich.“ Bei der Analyse der Programmcodes fanden Wüests Kollegen auch Wörter in russischer Sprache, aber auch solche in französischer.

Amerikanische Regierungskreise scheinen bei der Zuschreibung der Hackergruppe weniger zögerlich zu sein. Sowohl in der Zeitung „Washington Post“ als auch in der „New York Times“ wurde die „Dragonfly“-Gruppe unter Berufung auf amerikanische Sicherheitskreise als Gruppe „russischer Hacker“ bezeichnet. Im Juli dieses Jahres warnten das amerikanische FBI und das Heimatschutzministerium die dortige Energiebranche vor Angriffen. Die Wolf Creek Nuclear Operating Corporation, Betreiberfirma eines Kernkraftwerks in Kansas, war zum Beispiel Opfer eines Angriffs von „Dragonfly“ geworden.

In Deutschland beobachtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) ebenfalls eine „systematische Fortentwicklung von Cyber-Angriffen auf Unternehmen der Energiebranche“, wie BSI-Präsident Arne Schönbohm dieser Zeitung am Mittwoch mitteilte. Erst im Juli habe das BSI deshalb eine „zielgruppengerechte Warnmeldung“ an Betreiber kritischer Infrastrukturen versendet. Leichter soll es für Hacker in Zukunft zumindest nicht werden. Bis zum 31. Januar 2018 müssen deutsche Energiefirmen der Bundesnetzagentur mit einem Zertifikat belegen, dass ihre Sicherheitsmaßnahmen den Mindeststandards genügen – fünf Jahre nach den ersten Angriffen von „Dragonfly“.

„Viel zu

Spä

Erst spät
funden w
der Erinn
Sportler
Olympisc
sischen T
Lange Jal
schlichte
schen Do
woch ist
denkstätt
diese Ges
Geschich

Der isr
Rivlin, de
kam, ließ
schmerzli
Würdigur
empfund
hundert
und der S
gewartet.
Mahnmal
geben we
Menschei
chen als

Vor 45
tember 19

Im Gespräch: Thüringens Ministerpräsident Bodo Ramelow (Linkspa

„Veränderung scheint eine Urang