Ausländische Hacker nehmen Stromversorgung ins Visier

Stand: 09:30 Uhr | Lesedauer: 3 Minuten

Von **Anette Dowideit**, Jan Lindenau

In Deutschland ist die Gefahr stark gestiegen, dass Strom- oder Wasserversorgung durch Hackerangriffe ausfallen könnte.

Die Sicherheitsbehörden verzeichnen deutlich mehr Cyberangriffe als noch vor einem Jahr.

Das Bundesamt für Sicherheit in der Informationstechnik bestätigt, die Angriffe hätten eine „neue Qualität" erreicht.

In Deutschland ist die Gefahr deutlich gestiegen, dass Strom, Wasser oder andere lebenswichtige Versorgung durch Hackerangriffe ausfallen könnte. Die Sicherheitsbehörden verzeichnen Recherchen von WELT AM SONNTAG zufolge deutlich mehr Cyberangriffe als noch vor einem Jahr. Auch die Angriffsart hat sich geändert: Oft geht es nicht mehr darum, Geld zu erpressen, sondern zu sabotieren: den Strom auszuschalten, die Wasserversorgung zu manipulieren, die Kommunikation zu stören. Die Sicherheitsbehörden vermuten, dass hinter solchen Attacken häufig ausländische Nachrichtendienste stecken.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI (https://www.bsi.bund.de/DE/Home/home_node.html)) bestätigt, dass die Angriffe eine „neue Qualität" erreicht hätten. Laut bislang unveröffentlichter Zahlen verzeichnet das BSI auch deutlich mehr Meldungen über solche Attacken.

In der zweiten Jahreshälfte 2018 erfuhr das BSI von 157 Hackerangriffen auf Versorger kritischer Infrastruktur, davon 19 auf das Stromnetz – ein deutlicher Anstieg gegenüber dem vorherigen Berichtsjahr, in dem im Gesamtjahr bei der Behörde 145 Attacken auf die Infrastruktur gemeldet wurden.

Auch der nordrhein-westfälische Verfassungsschutz (https://www.im.nrw/themen/verfassungsschutz/schutz-von-behoerden-und-unternehmen) teilt die Einschätzung, die Qualität der Angriffe habe sich verändert: „Früher handelte es sich bei den Hackerattacken auf die kritische Infrastruktur vor allem um Spionageangriffe. Nun gibt es immer häufiger Sabotageangriffe."

Bei den Behörden vermutet man, dass die wahre Zahl der Hackerangriffe auf die Infrastruktur noch sehr viel höher liegt. Es gebe eine „entsprechende Dunkelziffer", so das BSI. Den Sicherheitsbehörden zufolge halten viele Versorger Cyberattacken geheim, weil sie Imageschäden vermuten. „Wir müssen davon ausgehen, zahlreiche Angriffe bislang überhaupt nicht zu sehen", sagte auch der stellvertretende Fraktionsvorsitzende der Grünen, Konstantin von Notz.

Die meisten Angriffe (/regionales/baden-wuerttemberg/article176424802/EnBW-Tochter-war-2017-Ziel-von-Cyberangriff.html) finden somit unbemerkt von der Öffentlichkeit statt, etwa solche auf mittelgroße Versorger wie Stromverteilzentren und Stadtwerke. Zwar besteht eine gesetzliche Meldepflicht

(https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/Neuregelungen_KRITIS/Meldepflicht/FAQ_zur_Meldepflicht/faq_meldepflicht_node.html#faq8141840) für Angriffe auf Anbieter sogenannter kritischer Infrastruktur, darunter fallen Strom- und Gasversorger oder große Kläranlagen.

Ausnahmen für kleine Anbieter

Viele kleinere Betreiber, darunter etwa auch Krankenhäuser oder Nahverkehrsanbieter, sind jedoch von der Pflicht ausgenommen. Recherchen von WELT AM SONNTAG ergaben, dass es in Deutschland bereits mehrmals Sabotageangriffe von Hackern gab, die spürbaren Schaden verursachten.

Dass so viele Cyberattacken nicht gemeldet würden, liegt nach Ansicht von Grünen-Politiker von Notz (https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/) daran, dass die Aufsichtsbehörde BSI nicht unabhängig, sondern dem Bundesinnenministerium unterstellt ist. „Für ein funktionierendes Frühwarnsystem brauchen wir Vertrauen in die Unabhängigkeit des BSI“, sagte er.

Baden-Württembergs Innenminister Thomas Strobl (CDU) warnte davor, dass die neuartige Bedrohungslage dazu führen könne, „dass die kleineren und mittleren Unternehmen beim digitalen Wandel zurückhaltend werden“. Sein Bundesland – wo mit dem Stromkonzern EnBW ein großer Anbieter Opfer eines Hackerangriffs wurde – habe deshalb eine „Cyberwehr“ eingerichtet: eine Art Feuerwehr, die bei einer Hackerattacke den angegriffenen Unternehmen helfe.

Zum Rechercheblog von WELT-Investigativ geht es hier entlang: www.investigativ.de *(https://investigativ.welt.de/)*