Ressort: Politik

Hackerangriff auf Gaskraftwerk: Neue Vorwürfe Richtung Russland

Riad, 23.10.2018, 18:09 Uhr

GDN - Die IT-Sicherheitsfirma Fireeye geht in einem nicht-öffentlichen Bericht davon aus, dass ein Labor mit Verbindungen zum russischen Militär eine entscheidende Rolle bei einem Hackerangriff auf ein saudisches Gaskraftwerk gespielt hat. Der Angriff werde sehr ernst genommen und die möglicherweise betroffene Unternehmen in Deutschland seien bereits gewarnt, berichten "Süddeutsche Zeitung" (Mittwochsausgabe), NDR und WDR unter Berufung auf das Bundesamt für IT-Sicherheit.

Fireeye ist einer der Marktführer in der Analyse von Hackerangriffen. Die Firma war vom saudischen Betreiber des Kraftwerks mit der Aufklärung beauftragt worden. IT-Sicherheitsexperten weltweit werten die Operation als Eskalation digitaler Angriffe. Öffentlich bekannt wurde diese im Dezember 2017. Seitdem analysieren Forscher das Vorgehen. Die Hacker waren im Sommer 2017 in das Netzwerk eines Gas-Kraftwerks in Saudi-Arabien eingedrungen. Dort versuchten sie gezielt, die Kontrolle über Sicherheitssysteme zu erlangen. Diese Systeme dienen nur dem Zweck, menschliches Leben und die Umwelt zu schützen. Kommt es zum Beispiel zum Überdruck, kann der betroffene Teil einer Anlage sicher heruntergefahren werden. Wer diese Systeme kontrolliert, kann Teile der Anlage manipulieren - und damit unter Umständen eine Explosion herbeiführen. In deutschen Sicherheitsbehörden löste die Fireeye-Analyse Aufregung aus. Auf Nachfrage teilte ein Sprecher des für IT-Sicherheit zuständigen Bundesamts für Sicherheit in der Informationstechnik (BSI) mit, dass man Angriffe auf Sicherheitssysteme sehr ernst nehme. Attacken wie die in Saudi-Arabien seien "als sehr kritisch zu betrachten". Seit Ende 2017 habe man "bereits zwei Warnungen an den Kreis möglicher Betroffener herausgegeben". Das BSI bestätigte, das Thema in das Nationale Cyber-Abwehrzentrum "eingebracht" zu haben, wo es behördenübergreifend analysiert und bewertet werde. Das Bundesamt für Verfassungsschutz sitzt ebenfalls in diesem Abwehrzentrum und teilte auf Anfrage mit, dass der Angriff der Behörde bekannt sei. Über Details wolle man nicht sprechen. Mitarbeiter des BSI trafen sich über Wochen hinweg mit Unternehmen aus der Chemieindustrie. Das Vorgehen wurde im Detail analysiert, um etwaige Angriffsversuche in Deutschland schnell zu erkennen und abzuwehren. In einer eigens eingerichteten Test-Umgebung rekonstruierten die Fachleute zentrale Elemente des Angriffs. Schließlich setzen Hunderte Industrieanlagen in Deutschland ähnliche Systeme ein - und könnten zu Zielen werden. Der Angriff schlug damals fehl. Bis heute ist unklar, an welchem Punkt den Hackern ein Fehler unterlief. Teile der Anlage schalteten sich ab. So wurden die Betreiber des Kraftwerks auf die Schadsoftware aufmerksam. In dem Bericht trifft Fireeye eine außerordentlich präzise Zuschreibung, wer in den Angriff involviert gewesen sein soll. Im Bericht heißt es, die Mitarbeiter des Moskauer Instituts hätten unter anderem die Aufgabe gehabt, Hackern ein unbemerktes Eindringen in das Netzwerk zu ermöglichen. Sind sie erst einmal im Netzwerk, versuchen sie, Administratoren-Rechte zu erlangen, und damit weitreichende Befugnisse. Man habe das Institut und vor allem einen Mitarbeiter aufgrund einer Vielzahl von Indizien enttarnen können, heißt es von Fireeye. Zum Beispiel habe man eine Datei gefunden, in der ein sogenannter PDB-Pfad enthalten gewesen sei. Wenn Programmierer ihren Code testen wollen, sucht der Rechner zusätzliche Informationen über diesen Pfad. Er kann auch den Namen enthalten, unter dem eine Person auf dem Rechner angemeldet ist. Nach Angaben von Fireeye handelt es sich dabei um einen Spitznamen, der einem russischen Hacker zugeordnet wird. Dieser Hacker stehe in Verbindung zum Institut aus Russland. Seinen Namen nennt Fireeye allerdings nicht.

Bericht online:
https://www.germandailynews.com/bericht-113980/hackerangriff-auf-gaskraftwerk-neue-vorwuerfe-richtung-russland.html

Redaktion und Veranwortlichkeit:
V.i.S.d.P. und gem. § 6 MDStV:

allein jeweilige Autor verantwortlich.

Editorial program service of General News Agency:
United Press Association, Inc.
3651 Lindell Road, Suite D168
Las Vegas, NV 89103, USA
(702) 943.0321 Local
(702) 943.0233 Facsimile
info@unitedpressassociation.org
info@gna24.com
www.gna24.com