Industriespionage Deutsches Chemieunternehmen gehackt

tagesschau.de/investigativ/ndr/hackerangriff-chemieunternehmen-101.html

tagesschau

Exklusiv

Stand: 31.01.2020 07:50 Uhr

Eine Hackergruppe hat jahrelang deutsche Konzerne ausgespäht. Nun konnten Reporter von *BR* und *NDR* einen weiteren Fall nachweisen - beim Chemieriesen Lanxess. Experten vermuten, dass der chinesische Staat dahintersteckt.

Von Jan Strozyk (NDR), Hakan Tanriverdi (BR)

Das Chemieunternehmen Lanxess ist Opfer eines Hacker-Angriffs geworden. Nach Recherchen von *BR* und *NDR* steckt hinter der Attacke eine Gruppe mit dem Namen "Winnti". Experten vermuten, dass die Hacker eine Verbindung zur chinesischen Regierung haben. Bereits im Juli hatten *BR* und *ND*R berichtet, dass "Winnti" mehrere Dax-Konzerne gehackt hat, darunter Siemens, BASF und Henkel.

Jan Lukas Strozyk

Lanxess bestätigte den Angriff auf Anfrage. Demnach ist die Schadsoftware in der "zweiten Hälfte des vergangenen Jahres" identifiziert worden, woraufhin man Gegenmaßnahmen eingeleitet habe. Es seien "keine geschäftsrelevanten sensiblen Daten in signifikantem Umfang abgeflossen", sagte ein Sprecher. Auf Nachfrage korrigierte sich der Konzern: Man

habe keine Erkenntnisse zu einem möglichen Abfluss von Daten. Lanxess hat den Vorgang nach eigener Aussage an die Strafverfolgungsbehörden übergeben und möchte sich nicht weiter zu dem Vorfall äußern.

Über Jahre ausspioniert?

Eine Untersuchung der "Winnti"-Schadsoftware durch Reporter von *BR* und *NDR* ergab, dass diese mutmaßlich schon 2015 für den Einsatz bei Lanxess entwickelt wurde. In dieser Zeit hat "Winnti" auch mehrere Konkurrenten von Lanxess attackiert. Daher liegt nahe, dass der Konzern über Jahre ausspioniert wurde. Doch um rückblickend nachvollziehen zu können, ab wann und wie die Hacker sich im Unternehmensnetz bewegten, braucht es umfassende Log-Dateien. Nach Ansicht mehrerer IT-Sicherheitsexperten wäre es ungewöhnlich, wenn Lanxess solche Dateien so lange aufbewahren würde.

Die Schadsoftware landete Anfang des Jahres auf einer Datenbank für Schadsoftware, dort fiel sie Experten auf. Die Hacker schrieben den Namen des gehackten Unternehmens direkt in ihr Programm, in diesem Fall: Rheinchemie, eine Unterabteilung von Lanxess. Die Firma gehört mit einem Jahresumsatz von 7,2 Milliarden Euro (2018) und mehr als 15.000 Mitarbeitern zu den größten Chemiekonzernen Deutschlands. Die Aktien des Unternehmens sind im M-Dax gelistet.

Winnti-Hacker weiter aktiv

Dass "Winnti" weiter aktiv ist, darauf deuten mehrere Fälle in Hongkong und Taiwan hin. Mit Hilfe von sogenannten Command-and-Control-Servern (C2-Server) lässt sich zeigen, dass "Winnti" mehrere Universitäten in Hongkong ins Visier genommen hat. Hacker betreiben derartige Server, um nach einer erfolgreichen Virus-Infektion mit der Schadsoftware kommunizieren zu können und beispielsweise den Befehl zum Kopieren von Daten zu erteilen.

Reporter von *BR* und *NDR* konnten mit Hilfe eines Programms, das verschiedene mögliche Namenskombinationen durchprobiert, die Existenz von mehreren C2-Server nachweisen, deren Namen auf mehrere Universitäten in Hongkong hindeuten. Auf Anfrage teilte eine Universität mit, sie habe bislang keinen "Winnti"-Angriff festgestellt, die übrigen ließen Anfragen zu den mutmaßlichen Attacken unbeantwortet. Die IT-Sicherheitsfirma ESET veröffentlichte an diesem Freitag eine eigene Untersuchung zu Hackerangriffen der "Winnti"-Gruppe in Hongkong. Zu konkreten Universitäten äußert sich ESET nicht.

Verfassungsschutz warnt vor Winnti

Auch in Taiwan hat es mutmaßlich einen neuen "Winnti"-Vorfall gegeben. So soll die Software-Firma Cyberlink Ende 2019 von "Winnti" ausspioniert worden sein. Cyberlink stellt unter anderem Software-Lösungen für Videokonferenzen und Messenger her. Cyberlink äußerte sich auf Anfrage nicht.

Das Bundesamt für Verfassungsschutz (BfV) hatte zuletzt im Dezember vor "Winnti" gewarnt und Unternehmen konkrete Regeln an die Hand gegeben, mit denen ein Angriff der Hacker festgestellt werden kann. Auf Anfrage erklärte BfV-Präsident Thomas Haldenwang nun schriftlich: "Das BfV geht davon aus, dass es weitere unbekannte "Winnti"-Opfer in Deutschland gibt, insbesondere in der Chemie-Branche."

Spur der Hacker führt nach China

Die Frankfurter IT-Sicherheitsfirma Quoscient beschrieb die "Winnti"-Hacker in einer 14-seitigen Analyse. Laut der Expertin Sophie Walther ist die Zuweisung von Angriffen grundsätzlich schwierig. Aber wenn man das Vorgehen der Hacker analysiere, sowohl technisch als auch geopolitisch, gebe es Indizien, die in Richtung China deuten.

Das Land habe "Wirtschaftsstrategien veröffentlicht, in denen bestimmte Industriesektoren aufgelistet sind, in denen China sehr großes Interesse hat, Weltmarktführer zu werden. Und wenn man das vergleicht mit den Konzernen, die in Deutschland und auch weltweit angegriffen wurden, stimmen die auf eine bestimmte Art und Weise überein", sagte Walther *BR* und *NDR*.

Bislang war "Winnti" vor allem durch klassische Ziele für Industriespionage aufgefallen: Unternehmen der Chemiebranche und Hochtechnologiekonzerne. Die mutmaßlichen Attacken auf die Hongkonger Universitäten deuten darauf hin, dass die Gruppe sich vermehrt auch politisch motivierten Angriffszielen zuwendet. Bereits 2019 gab es Hinweise darauf, dass die Gruppe Regierungsstellen in Hongkong angegriffen hatte.

Zurück zur Startseite Zurück