

# 1 IT-Sicherheitsfirma FireEye wird selbst Ziel von Hackern

dpa/dj

9.12.2020 - 13:35



Die Hacker haben eine Angriffssoftware gestohlen, mit der FireEye üblicherweise die Abwehrsysteme seiner Kunden testet.

dpa

**Wenn amerikanische Behörden oder Unternehmen Ziel von Cyberangriffen werden, sind Experten der Firma FireEye die erste Anlaufstelle. Jetzt brachen Hacker bei ihnen selbst ein. US-Sicherheitskreise vermuten den russischen Geheimdienst dahinter.**

Die IT-Sicherheitsfirma FireEye, die unter anderem US-Behörden oft bei Cyberattacken einschalten, ist selbst Ziel von Hackern geworden. Dabei sei auch Angriffssoftware gestohlen worden, mit der FireEye üblicherweise die Abwehrsysteme seiner Kunden teste, gab das Unternehmen bekannt.

Es sei noch unklar, ob diese Werkzeuge für Hackerangriffe eingesetzt werden sollen. Bisher habe FireEye keine Hinweise darauf gesehen. Man habe aber Gegenmittel entwickelt, die davor schützen sollen.

Ausserdem hätten sich die Angreifer insbesondere für Informationen über Regierungskunden des Unternehmens interessiert, schrieb FireEye-Chef Kevin Mandia in einem Blogeintrag. Es sehe bisher nicht danach aus, als hätten sie Kundendaten aus den Speichersystemen abrufen können.

## 2 Staatliche Hacker vermutet

FireEye gehe davon aus, dass im staatlichen Auftrag agierende Hacker hinter der Attacke stecken, betonte Mandia. Darauf wiesen unter anderem die technischen Fähigkeiten und die Disziplin der Angreifer hin. FireEye habe die Bundespolizei FBI eingeschaltet. Die Aktie der Firma verlor im nachbörslichen Handel gut sieben Prozent.

Das «Wall Street Journal» berichtete unter Berufung auf Ermittlerkreise, als wahrscheinliche Täter würden aktuell Hacker aus dem Umfeld des russischen Geheimdienstes gesehen. Es könne eine der Gruppen sein, die im US-Wahlkampf 2016 E-Mails der Demokratischen Partei gestohlen habe. Die Veröffentlichung der Mails hatte damals Donald Trumps Gegenkandidatin Hillary Clinton geschadet.

## 3 «Schuss eines Scharfschützen»

Den Ermittlern zufolge setzten die Hacker eine ungewöhnliche Kombination von Angriffswerkzeugen ein, von denen einige noch gar in Erscheinung getreten seien. «Es war der Schuss eines Scharfschützen, der durchkam», zitierte die Zeitung einen an der Untersuchung Beteiligten. «Die Angreifer haben ihre Fähigkeiten der Weltklasse speziell zugeschnitten, um FireEye zu attackieren», schrieb Mandia.

Die gestohlene FireEye-Software habe keine Angriffsszenarien für sogenannte «Zero-Day»-Schwachstellen enthalten, versicherte er. So werden Sicherheitslücken genannt, die noch nicht allgemein bekannt sind. Deshalb stehen sie für den Entdecker weit offen und sind besonders gefährlich.

Die Experten von FireEye werden bei besonders grossen oder schwerwiegenden Cyberattacken zur Hilfe gerufen. Das war zum Beispiel der Fall bei dem Angriff auf Sony Pictures Ende 2014, der das gesamte Computer-System des Hollywood-Studios lahmlegte.