Rüstungskonzern im Fadenkreuz

28.05.2011, 16:38

# Hacker attackieren Lockheed Martin

**Für Rüstungsfirmen sind Cyber-Attacken ein fast schon schlimmerer Alptraum als eine Welt ohne Konflikte. Als Drahtzieher hinter dem Angriff auf den größten Partner des US-Militärs werden Länder wie China und Russland gehandelt. Bisher laufen aber alle Spuren ins Leere.**

Sicherheitsalarm bei einer der größten Rüstungsfirmen der Welt: Ein Hacker hat einem Bericht der "New York Times" zufolge versucht, in das Computernetzwerk von Lockheed Martin einzudringen. Die Attacke sei am vergangenen Sonntag entdeckt worden, berichtete die Zeitung unter Berufung auf nicht näher bezeichnete Sicherheits- und militärische Kreise.

Demnach ist unklar, wohinter der Eindringling her war. "Eine Möglichkeit ist, dass jemand für einen Staat agiert", zitierte das Blatt den Sicherheitsexperten James Lewis vom Center for Strategic and International Studies in Washington. Es könnten aber auch Kriminelle sein, die versuchten, Kunden des Konzerns zu schaden.

Brisantes Wissen: F-35 Lightning II Joint Strike Fighter von Lockheed Martin

Die US-Regierung vermutet, dass China, Russland und andere Länder Drahtzieher von vergangenen Hacker-Attacken zur Ausspähung militärischer oder auch industrieller Geheimnisse waren.

Lockheed Martin ist der größte Vertragspartner des US-Militärs. Der Konzern stellt unter anderem Kampfflugzeuge, Spionagesatelliten und andere zum Teil hochgeheime sicherheitsrelevante Technologien für die Washingtoner Regierung her. Eine Reihe der von dem Konzern hergestellten Waffensysteme wird derzeit in Auslandskonflikten eingesetzt.

Besonders besorgniserregend: Nach dem Zeitungsbericht könnte die Cyber-Attacke in Verbindung mit einem Hacker-Angriff auf die renommierte US-Sicherheitsfirma RSA im März stehen. RSA beliefert zahlreiche Großunternehmen - darunter Lockheed und andere Produzenten militärischer Ausrüstung - mit dem Sicherheitssystem "SecurID". Es ist ein elektronisches Token mit sich ständig ändernden Pin und soll gewährleisten, dass nur Befugte von außen - etwa auf Dienstreisen - Zugang zum internen Firmen-Computernetzwerk haben.

RSA hatte bestätigt, dass es einen Cyber-Angriff gab, der möglicherweise einige Produkte kompromittiert habe. Zahlreiche Kunden hatten daher zusätzliche Schutzmaßnahmen ergriffen.

Lockheed selbst hat den anonymen Sicherheitskreisen zufolge nach der Attacke vom vergangenen Sonntag den Zugang von außen ins Computernetzwerk weitgehend gesperrt und zahlreichen Mitarbeitern neue Token und Passwörter gegeben.

Industrievertreter weisen unterdessen darauf hin, dass geheime Daten von militärischen Vertragspartnern in der Regel nicht in Computern gespeichert werden, die von außen zugänglich sind, sondern in getrennten Netzwerken.

Sowohl RSA als auch Lockheed äußerten sich zunächst nicht zu den Berichten über die jüngste Hacker-Attacke. Ein Sprecher des Rüstungskonzerns sagte lediglich, das Unternehmen ergreife regelmäßig Maßnahmen zum Schutz des Systems und der Programmdaten: "Wir haben weiterhin Vertrauen in die Integrität unseres robusten vielschichtigen Informationssicherheitssystems."

**Mehr zum Thema**

**Cyberattacken** Wettrüsten für den Krieg im Internet
(http://www.ftd.de/politik/europa/:cyberattacken-wettruesten-fuer-den-krieg-im-internet/60008435.html)

**Krieg im Internet** Wie sich die Staaten gegen Cyberattacken rüsten
(http://www.ftd.de/politik/international/:krieg-im-internet-wie-sich-die-staaten-gegen-cyberattacken-ruesten/60008721.html)

**Cyberwar** Nebulöser Krieg
(http://www.ftd.de/politik/international/:cyberwar-nebuloeser-krieg/60008416.html)

**Sicherheit im Netz** Die neue Angst vorm Datenklau
(http://www.ftd.de/karriere-management/management/:sicherheit-im-netz-die-neue-angst-vorm-datenklau/60022660.html)

Mehr zu: Hacker, Lockheed Martin, US-Regierung

dpa, 28.05.2011