07.06.2011, 21:32

Weltweite Angst vor Hackern

Diebstahl beim Sicherheitskonzern RSA, Attacken auf Sony-Datenbanken: Noch nie waren Großunternehmen von Hackern so bedroht wie heute. Laut Experten ist das nur der Anfang - sie sprechen vom Beginn einer neuen Ära. *von Annika Graf, Hamburg*

Die jüngste Welle von Hackerangriffen auf Großkonzerne hat einen neuen Höhepunkt erreicht. Am Dienstag kündigte RSA, einer der führenden Anbieter von IT-Sicherheitstechnologie, eine groß angelegte Überprüfung seiner sogenannten Token an. Die elektronischen Schlüssel erzeugen Zahlenfolgen, mit denen sich Angestellte in Firmennetzwerke einwählen können. Bei gut 25.000 Kunden sind nach Schätzungen mehr als 40 Millionen im Umlauf.

Zuvor war bekannt geworden, dass das US-Unternehmen im März Opfer von Hackern geworden war. Sie hatten Daten für die Token entwendet, mit denen sie wiederum Ende Mai ins Computersystem des US-Rüstungskonzerns Lockheed Martin eingedrungen waren.

Cyber-Diebstahl: Hackerwelle hat Höhepunkt erreicht

Der Fall zeigt, wie verletzlich Unternehmen durch die wachsende Digitalisierung von Informationen und die zunehmende Vernetzung geworden sind. "Die Industriespionage ist im digitalen Zeitalter angekommen", sagte Candid Wüest vom Sicherheitssoftwareanbieter Symantec. Das Eindringen bei Lockheed Martin falle in die gleiche Kategorie wie die Stuxnet-Attacke, sagte Gartner-Analyst Mark Diodati. "Die Angriffe werden immer aggressiver, das ist definitiv eine neue Ära." Die Stuxnet-Schadsoftware hatte 2010 Steuerungscomputer in den Atomanlagen des Iran befallen. Neben amerikanischen Firmen und Behörden gehören auch deutsche Banken und Konzerne zu den RSA-Kunden. Namen wollte die Konzernmutter EMC, ein US-Speicherspezialist, nicht nennen.

Dass sowohl Lockheed als auch RSA Hackerangriffe öffentlich machen, verdeutlicht, für wie gefährlich Unternehmen sie mittlerweile halten. Bislang wurden solche Bedrohungen meist verschwiegen, um den eigenen Ruf zu schützen und keine Nachahmer anzulocken. Welche Ausmaße das annehmen kann, zeigt der Fall Sony: Seit der ersten Attacke auf das Playstation-Netzwerk im April sabotieren Hacker immer neue Server des japanischen Konzerns.

Teil 2: "Noch nie dagewesene Welle von Attacken"

RSA-Chef Arthur Coviello sprach in einem offenen Brief von einer "noch nie da gewesenen Welle von Cyberattacken" in den vergangenen Wochen. Angriffe auf Sony, Nintendo oder Google hätten zwar nichts direkt mit der Attacke auf RSA zu tun, schrieb Coviello. Sie deuteten aber auf eine veränderte Gefährdungslage hin und hätten für große Verunsicherung gesorgt. RSA prüfe nun, ob Token ausgetauscht oder durch zusätzliche Vorkehrungen abgesichert werden müssten.

Der Hersteller ist Marktführer bei der bislang als sicher geltenden Technologie. Jeder Schlüssel ist mit Benutzername und Passwort ausgestattet, zusätzlich erzeugt er für jeden Einwählversuch eine Nummer, die nur eine begrenzte Zeit haltbar bleibt. Der Server, auf dem sich der Nutzer anmelden will, weiß, welche Nummern ein Token verwenden soll. Mikko Hyppönen, Forschungsleiter bei der Sicherheitssoftwarefirma F-Secure, vermutet, dass dort die Schwachstelle bei Lockheed Martin lag.

Außer diesem Fall seien bislang keine Spähversuche bekannt geworden, schrieb Coviello. Dass ein großer Rüstungskonzern angegangen worden sei, bestätige zudem seine Vermutung, wonach die Hacker auf Betriebsgeheimnisse aus waren und keine finanziellen Interessen verfolgten oder Aufmerksamkeit erregen wollten. Lockheed konnte die Hacker nach eigenen Angaben rechtzeitig abwehren. Allein die Massenüberprüfung der Token zeigt aber, dass RSA ihren Missbrauch nicht ausschließen kann.

Welche Kosten dem Anbieter nun drohen, hängt davon ab, wie viele Kunden den Austausch ihrer elektronischen Schlüssel fordern. Dass komme auf den Einzelfall an, sagte ein Sprecher von EMC. Die Technologie sei aber nach wie vor sicher.

Mehr zum Thema

Angriff auf "SecureID" Sicherheitsfirma tauscht elektronische Schlüssel
(http://www.ftd.de/it-medien/it-telekommunikation/:angriff-auf-secure-id-sicherheitsfirma-tauscht-elektronische-schluessel/60062231.html)

Cyberattacke Hacker stören Website von Versorger EDF
(http://www.ftd.de/unternehmen/industrie/:cyberattacke-hacker-stoeren-website-von-versorger-edf/60061446.html)

Kanonen auf Nerds USA erklären Hackern den Krieg
(http://www.ftd.de/politik/international/:kanonen-auf-nerds-usa-erklaeren-hackern-den-krieg/60061034.html)

Neuer Datendiebstahl Hacker verhöhnen Sony
(http://www.ftd.de/it-medien/computer-technik/:neuer-datendiebstahl-hacker-verhoehnen-sony/60060461.html)

Cyberkriminalität USA besorgt wegen Hacker-Attacke auf Google
(http://www.ftd.de/it-medien/medien-internet/:cyberkriminalitaet-usa-besorgt-wegen-hacker-attacke-auf-google/60060444.html)

Internetstrategie USA wollen Cyberattacken militärisch vergelten
(http://www.ftd.de/politik/international/:internetstrategie-usa-wollen-cyberattacken-militaerisch-vergelten/60059465.html)

Mehr zu: Hacker, Internetkriminalität

Aus der FTD vom 08.06.2011