Unbekannte veröffentlichen Daten von Spionagesoftwarefirma

6. Juli 2015

Spiegel.de

Unbekannte haben die italienische IT-Firma Hacking Team angegriffen, angebliche Geheimdaten des Herstellers von Überwachungssoftware veröffentlicht. Nun wird die Firma über den eigenen Twitter-Kanal verspottet.

Reporter ohne Grenzen zählt sie zu den Feinden des Internets, jetzt ist die italienische IT-Firma The Hacking Team offenbar selbst Opfer eines Dateneinbruchs geworden. Unbekannte haben nach eigener Darstellung rund 400 Gigabyte Daten aus den Firmennetzen kopiert und im Internet veröffentlicht. Das Datenpaket bietet erstaunliche Einblicke in die Arbeit eines Unternehmens, das bislang Vorwürfe bestritt, Überwachungs-Software an Unterdrückerstaaten zu liefern.

Die Enthüllungsaktion begann mit einem Scherz in der Nacht zum Montag: Der Name des Twitter-Kontos des Unternehmens wurde von Hacking Team (das Hacker-Team) in Hacked Team (das gehackte Team) geändert.

Gleich darauf veröffentlichten die Hacker über den gekaperten Twitter-Account mehrere Nachrichten. Die erste: "Weil wir nichts zu verheimlichen haben, veröffentlichen wir all unsere E-Mails, Dateien und Quellcodes." In den Text eingebettet waren Links, die zum Download der kopierten Firmendaten führen sollen.

Es folgten weitere Tweets, manche enthüllend, manche verhöhnend. So zeigt ein Foto angeblich den Desktop eines Hacking-Team-Mitarbeiters, der nicht verstehe, dass ihm "gerade 5 Megabyte pro Sekunde aus dem Firmennetzwerk entwendet" werden. Auf dem linken Arbeitsmonitor des Mitarbeiters für Netzwerk-Sicherheit ist ein YouTube-Video über Weinfälschungen zu sehen, rechts das Facebook-Konto von Matteo Salvini, dem Parteivorsitzenden der rechten italienischen Partei Lega Nord.

Kunden aus aller Welt

Kurz nachdem die Aktion bekannt wurde, haben sich Aktivisten daran gemacht, die veröffentlichten Daten auszuwerten. Dabei soll unter anderem eine Liste der bisher sorgsam geheimgehaltenen Kunden von The Hacking Team aufgetaucht sein.

Sie soll unter anderem die Regierungen von Südkorea und Kasachstan, Saudi-Arabien, Ägypten, Oman, Libanon und der Mongolei enthalten. Auch drei amerikanische Behörden seien darauf zu finden: So sei das amerikanische Verteidigungsministerium als "inaktiv", ein Vertrag mit der amerikanischen Drug Enforcement Agency (DEA) als "Erneuerung in Gange" markiert. Bis zum 30. Juni 2015 habe auch das FBI einen Vertrag mit dem Hacking Team gehabt.

Russland und Sudan wurden auf dieser Liste als "nicht offiziell unterstützt" markiert. Die Bemerkung könnte als Hinweis gewertet werden, dass The Hacking Team seiner selbst

auferlegten Beschränkung möglicherweise nicht folgt, keine Produkte an Kunden zu liefern, die auf einer schwarzen Liste "von U.S., E.U., U.N., NATO oder ASEAN" stehen.

Warnung vor Viren

Vielleicht ist alles aber auch ganz anders? Hacking-Team-Mitarbeiter Christian Pozzi versucht die unbekannten Angreifer via Twitter zu diskreditieren. "Vieles von dem, was die Hacker über unsere Firma behaupten, ist unwahr", schreibt er beispielsweise. "Bitte verbreitetet diese unwahren Lügen über unsere Dienstleistungen nicht weiter."

Man arbeite eng mit der Polizei zusammen, informiere alle Kunden und äussere sich nicht weiter zum Datenklau. Allerdings, warnt Pozzi, solle man lieber die Finger vom Download der veröffentlichten Dateien lassen, da diese virenverseucht seien. Eine durchaus ernstzunehmende Warnung.

Keine Reaktion auf Anrufe

Unser Versuch The Hacking Team telefonisch um Stellungnahme zu bitten, endet im Sekretariat. Das Unternehmen werden nur auf schriftliche Anfragen reagieren, heisst es. Die Aufregung erscheint angemessen. Die Veröffentlichung der Daten ist nicht nur peinlich, sondern könnte das Unternehmen und dessen Kunden nachhaltig schaden, sofern diese authentisch ist.

Ohnehin wird im Netz darüber gelästert, The Hacking Team würde die interne Sicherheit nicht ernst genug nehmen. Darauf sollen mangelhafte Passwörter und fehlende Datenverschlüsselung hindeuten.

Kritik von Menschenrechtlern

Das Hacking Team offeriert seine Dienste als Spezialist für Internet-Aufklärung: "Wir bieten effektive, leicht nutzbare Angriffstechnik für Strafverfolger und Geheimdienste weltweit an. Technologie muss ermächtigen, nicht behindern", heisst es auf der Firmen-Website.

Menschenrechtsorganisationen ist The Hacking Team zusammen mit Firmen wie der Gamma Group ("FinFisher") ein Dorn im Auge. So warf das amerikanische Citizen Lab der University of Toronto dem Unternehmen vor, der äthiopischen Regierung bei der Bespitzelung von Journalisten geholfen zu haben. Man wolle die Vorwürfe untersuchen, erklärte The Hacking Team am 10. März dieses Jahres.