CYBER-KRIMINALITÄT

Diebe im Haus

Ein Spionage-Angriff auf das Zentrum für Luft- und Raumfahrt alarmiert die Bundesregierung. Die Hacker kaperten Computer und hinterließen kaum Spuren.

Das deutsche Tor zum Weltall befindet sich in Oberpfaffenhofen. Nahe der Autobahn München–Lindau liegt das Areal des Deutschen Zentrums für Luft- und Raumfahrt (DLR). Mit acht wissenschaftlichen Instituten gehört der Standort zu den größten Forschungseinrichtungen des Landes. Im Mittelpunkt der Anlage steht das Raumfahrtkontrollzentrum mit einer direkten Verbindung zum Columbus-Labor der internationalen Raumstation ISS.

Die Elite-Wissenschaftler auf dem Gelände beschäftigen sich mit den großen Hightech-Themen: Sie waren maßgeblich an der Entwicklung der „Ariane"-Trägerrakete beteiligt und schicken im europäischen Verbund Satelliten ins All.

Das DLR ist so etwas wie der Diamant der technischen Forschung in Deutschland – und damit auch ein bevorzugtes Ziel für Spionage-Operationen. Unter Wissenschaftlern gelten die sensiblen Forschungsergebnisse dort als ähnlich gut gesichert wie die Goldreserven in Fort Knox – vielleicht ist das aber nicht gut genug.

Seit Monaten wehren sich die Computerspezialisten des Zentrums gegen einen Angriff, hinter dem mutmaßlich ein ausländischer Geheimdienst steht. Eine Reihe von DLR-Rechnern wurde bereits erfolgreich mit Spionage-Programmen infiltriert. Herkömmliche Anti-Viren-Programme und Firewalls versagten. Deshalb alarmierten die IT-Spezialisten das 2011 von der Bundesregierung eingerichtete Nationale Cyber-Abwehrzentrum in Bonn. Die Regierung stuft den Angriff als äußerst ernst ein, weil er unter anderem auf Rüstung und Raketentechnologien zielt.

Semiprofessionelle Angriffe sind die IT-Fachleute des DLR seit Jahren gewöhnt. Doch die jüngsten Cyber-Attacken haben das ausgeklügelte Immunsystem des Raumfahrtzentrums überwunden. Seit November greifen Schadprogramme, die auf das DLR-System zugeschnitten sind, gezielt Rechner von Wissenschaftlern und Administratoren an. Ist ein Computer mit einem Trojaner infiziert, kann er zum Ausgangspunkt für weitere Operationen gegen andere Mitarbeiter werden.

Neu an der aktuellen Welle sind die offenbar langfristige Planung der Operation und die Perfektion der eingesetzten Trojaner. In einigen Rechnern entdeckten IT-Spezialisten in den Log-Einträgen nur noch ihre flüchtige Spur, sie waren so programmiert, dass sie sich selbst zerstörten, sobald sie entdeckt wurden.

THOMAS ERNSTING / DLR

Raumfahrtkontrollzentrum Oberpfaffenhofen: *Chinesische Schriftzeichen und Tippfehler*

Andere Trojaner sind mit einer Schläferfunktion ausgestattet und aktivieren sich erst nach Monaten des Wartens selbst, wie Diebe, die sich unbemerkt im Haus versteckt halten, um im geeigneten Moment zuzuschlagen.

Wer Urheber der gekonnten Attacken gegen das Raumfahrtzentrum ist, dafür haben die Ermittler bislang allenfalls Indizien. Sie deuten in Richtung China. Die Angriffe erfolgten koordiniert und systematisch, alle vom DLR eingesetzten Betriebssysteme sind betroffen. In den frühen Morgenstunden, wenn in Asien der Arbeitstag beginnt, greifen die feindlichen Hacker an. Ab mittags und an chinesischen Feiertagen herrscht Ruhe.

IT-Forensiker des ebenfalls eingeschalteten Bundesamts für Sicherheit in der Informationstechnik (BSI) entdeckten im Code einiger Trojaner zudem chinesische Schriftzeichen und wiederkehrende Tippfehler, die auf Angreifer aus Fernost hindeuten. „Es könnte sich aber auch um eine simple Tarnung handeln", sagt ein Insider, der einen Angriff aus dem Westen, etwa durch den US-Geheimdienst NSA, nicht völlig ausschließen mag. „Es ist wie ein Schachspiel. Sie reagieren auf jeden Zug, den wir unternehmen, mit einer neuen Finte."

Die Spezialisten des DLR geraten in diesen Abwehrschlachten an ihre Grenzen. Im Januar identifizierten sie einen „Drop-Server" in Wiesbaden, der von den Trojanern angesteuert wurde, um die Daten, die sie gestohlen hatten, über mehrere Stationen zum Urheber der Attacke zu bringen. Wer das war, lässt sich durch die Verschleierung kaum mehr feststellen.

Über die Spur nach Wiesbaden informierten die DLR-Techniker das Bundeskriminalamt (BKA). Doch die Kriminalisten dort sahen sich zunächst außerstande zu ermitteln: Dem DLR sei kein nachweisbarer Schaden entstanden, weil man nicht wisse, ob überhaupt Daten von Rechnern des Zentrums abgesaugt wurden. Deshalb verstrich kostbare Zeit, bevor die BKA-Spezialisten aktiv werden konnten.

Auf Anfrage wollte sich das DLR nicht zu den Einzelheiten des Falls äußern. Die Handlungsfähigkeit des Bundeskriminalamts müsse allerdings „generell verbessert werden", sagt IT-Manager Hans-Joachim Popp, der für die Sicherheit von 12 000 DLR-Computern verantwortlich ist. Es gehe vor allem um die „Reaktionsgeschwindigkeit" der Ermittler. BKA und BSI lehnten eine Stellungnahme ab.

Die Drop-Server, deren Besitzer meist gar nicht wissen, dass sie für Spionage-Operationen missbraucht werden, können binnen weniger Sekunden gewechselt werden. Trotzdem sind sie oft die beste Chance, die Hintermänner der Attacken zu identifizieren. Der Drop-Server in Wiesbaden, auf den die DLR-Leute gestoßen waren, kann den Ermittlern nicht mehr weiterhelfen. Er ist inzwischen abgeschaltet. HUBERT GUDE