WIRTSCHAFTSSPIONAGE

Operation Pferderennen

Ein deutsch-israelischer Programmierer soll mit einer Spezialsoftware Großunternehmen ausgespäht haben – der bislang spektakulärste Computerangriff.

Die Attacke begann mit einem Anruf: Geheimnisvoll meldete sich ein Unbekannter bei der Reporterin Gitit Pincas von der israelischen Wirtschaftszeitung „Globes“ und offerierte eine brisante Enthüllung, die alsbald per E-Mail eintreffen werde. Die Dokumente, die tatsächlich als Anhang einer Mail kamen, ließen sich aber nicht öffnen. Und da sich der Mann nicht mehr meldete, vergaß Pincas die Geschichte wieder.

Erst vor zwei Wochen erfuhr die Reporterin durch Fahnder, dass just über jene Mail das weltweit bislang ausgereifteste Spionageprogramm in ihr System eingeschleust wurde: ein sogenanntes Trojanisches Pferd, Codename „Pinka“ – geschrieben, um ganze Netzwerke auszukundschaften. Fast ein Jahr lang, eröffneten die Beamten der Journalistin, habe eine Privatdetektei nicht nur Manuskripte mitlesen, sondern auch ihre Korrespondenz verfolgen können.

Das Spionageprogramm hat eine breite Spur in Israels Geschäftswelt hinterlassen. Bis zu 60 Firmen wurden mit „Pinka“ ausspioniert – darunter die Importeure von VW und BMW.

Rund ein Dutzend Unternehmen stehen im Verdacht, vom Datenklau profitiert zu haben. Abgewickelt wurde der Deal offenbar über Privatdetekteien. In einer international koordinierten Aktion nahmen israelische, deutsche und britische Fahnder rund 20 Verdächtige fest, darunter 11 Detektive und jenen Mann, der „Pinka“ programmiert haben soll: den deutsch-israelischen Computerspezialisten Michael Haephrati, 41.

AMIT SHABI / LAIF

Verdächtiges Ehepaar Haephrati: *Ausgefeilter Code*

Der Wirtschaftskrimi ist der bislang spektakulärste Fall von Computerspionage, der öffentlich wurde. „Ein Trojanisches Pferd mit so vielen Möglichkeiten hatten wir noch nie“, sagt Michael Dickkopf vom Bundesamt für Sicherheit in der Informationstechnik.

Der Fall offenbart, dass Computernetze für Experten oft weit offen sind – auch deutsche. „Viele Unternehmen verwenden zu wenig Energie auf den Schutz ihrer Firmengeheimnisse“, warnt der deutsche Verfassungsschutzchef Heinz Fromm. Und der Lüneburger Wirtschaftsprofessor Egbert Kahle sagt: „Alle großen Unternehmen haben damit leidvolle Erfahrung gesammelt.“ Nach einer Untersuchung Kahles sollen deutsche Unternehmen bislang durch Computerspionage pro Jahr um mehrere Milliarden Euro geschädigt worden sein.

Vielleicht wäre der Coup nie aufgeflogen, hätte Haephrati „Pinka“ nicht für einen Rachefeldzug eingesetzt: Er spionierte die Eltern seiner Ex-Frau aus. Die merkten den Angriff, und so kam die Polizei an den Code – und den Namen des Hackers. Die „Operation Pferderennen“ begann.

Im April sprachen die Israelis im Landeskriminalamt (LKA) Baden-Württemberg vor. Sie kamen mit einem Rechtshilfeersuchen, denn Haephrati und seine Ehefrau Ruth wohnten seit Mitte Februar in Deutschland, in einem idyllischen Schwarzwald-Städtchen namens Baiersbronn. Ende Mai durchsuchten die Beamten des LKA Haephratis Apartment und fanden Festplatten sowie eine Tasche mit CD-Roms.

Nach dem bisherigen Stand der Ermittlungen hatte Haephrati die Namen der auszuspähenden Unternehmen von Wirtschaftsdetekteien erhalten. Gegen Honorar soll der Meisterhacker zusammen mit seiner Frau dann das Trojanische Pferd in fremde Rechner eingeschleust haben.

Die Opfer sind zum Teil Firmen aus der Beletage der israelischen Wirtschaft, darunter ein Rüstungsunternehmen und börsennotierte Bluechips wie die Telekommunikationsunternehmen Bezeq und Orange. Unter Tatverdacht stehen renommierte Unternehmen wie zwei Mobilfunkanbieter, eine Satelliten-TV-Firma sowie der Importeur eines schwedischen Autokonzerns, der sich für VW-Interna interessiert haben soll. Mehrere Geschäftsführer beteuern nun, sie hätten sich versichern lassen, dass sich die Detekteien an die Gesetze hielten.

Von wegen: Bei dem israelischen BMW-Importeur Kamor beispielsweise ging eine CD mit Werbung ein. Ein Angestellter schob sie in den Computer, und als er ihn am nächsten Morgen wieder anschaltete, hatte „Pinka“, das auf der CD versteckt war, bereits diverse Dateien weitergeleitet.

„Pinkas“ Code ist derart ausgefeilt, dass das Programm in fremden Computernetzwerken von außen steuerbar bleibt, flexibel anpassbar an den Informationsbedarf der Kunden. Selbst in einen israelischen Polizeicomputer soll die Software eingedrungen sein.

„Solche Programme fallen Virenscannern nur auf, wenn sie sich verbreiten – und das sollten sie in diesem Fall nicht“, sagt der Hamburger Computerexperte Peter Franck. „Pinka“ sendete seine Informationen nach Erkenntnissen der Fahnder nach London, wo Haephrati und seine Frau Ruth ein Unternehmen namens Target Eye Limited betrieben. Von dort sollen die Firmen-Interna dann über die Detekteien an die Auftraggeber gelangt sein.

Haephrati, der zurzeit in Haft sitzt, bestreitet die Tat, nicht aber seinen Programmiererfolg. Er lässt mitteilen, er habe „Pinka“ für „gute Zwecke entwickelt“ – um „Verbrechen verhindern“ zu können.

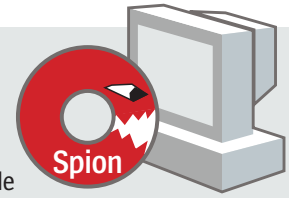
ANNETTE GROSSBONGARDT, HOLGER STARK

Ausgeforschter VW-Importeur (bei Tel Aviv): *Leidvolle Erfahrung*

AMIT SHABI / LAIF

Spion im Gepäck

Gefahr durch Trojanische Pferde



1 Ein scheinbar harmloses Programm aus dem Internet oder von einem Datenträger, das auf dem Computer installiert wird, startet heimlich ein Spionageprogramm, das unbemerkt im Hintergrund läuft.

2 Dieses sogenannte Trojanische Pferd späht vertrauliche Informationen aus, z. B. Passwörter, technische Daten oder Kontonummern. Die Daten kann das Programm dann löschen, verändern oder per Internet an den Angreifer verschicken.

DER SPIEGEL