WIR SIND DRIN

Als Auftragshacker greift *Timo Kobs* Firma Hisolutions große Dax-Konzerne und öffentliche Einrichtungen an. Hier tobt ein Kampf zwischen Menschen wie Maschinen

Von YVES BELLINGHAUSEN

Ein simpler Hack kostet bei Timo Kob etwa 7000 Euro. Dann ist es aber ein primitiver Angriff, mit vorgefertigten Werkzeugen, die seine Mitarbeiter aus dem Internet herunterladen. Für raffiniertere Attacken, mit selbst geschriebenen Werkzeugen und Viren, die exakt auf das Opfer zugeschnitten sind, verlangt Kob deutlich mehr, bis in die Hunderttausenden.

Kriminelle Energie zu imitieren, ist Timo Kobs Geschäftsmodell. Er ist einer von drei Gründern des Berliner Unternehmens Hisolutions, das öffentlichen Einrichtungen und Firmen hilft, ihre Computersysteme virenfrei zu halten. Seine Kunden tragen große Namen wie etwa Allianz, Commerzbank, aber auch Bundesbank und EZB. Auch Fernsehsener wie der RBB und NDR und die Verkehrswirtschaft suchen die Dienste. Zwar haben auch Lufthansa, Deutsche Bahn oder die Berliner Verkehrsbetriebe eigene IT-Fachleute, um Systeme einzurichten, Software zu pflegen und zu erhalten. Die sind meist aber keine Experten, um die sensiblen Anlagen kaputt zu machen. Darum beauftragen sie damit Hisolutions mit seinen 160 Mitarbeitern. Davon sind 20 Leute fast ausschließlich dabei, sich in die Rechner der Auftraggeber zu hacken, so weit, bis sie theoretisch Schaden anrichten könnten. Dann wissen sie, wo sie verletzlich sind, und Hisolutions bessert diese Systemlücken aus.

Timo Kob, ein stämmiger Mann von 48 Jahren mit dichtem Siebentagebart, hat die Firma mit zwei Kommilitonen von der Technischen Universität Berlin gegründet. Vor 26 Jahren sollten sie eigentlich für ein Uniprojekt eine Marktstudie für Spracherkennungssoftware schreiben. „Total langweilig“, sagt Kob, „aber wir haben gemerkt, dass wir gut miteinander können.“ Seit 24 Jahren sitzt Hisolutions nun im obersten Stock eines sanierten Industriebaus in Berlin-Alt-Treptow, wo AEG früher Elektrogeräte produzierte. Heute tragen hier die älteren Informatiker legere Hemden, die jüngeren T-Shirts mit aufgedruckten Informatikerwitzen, die nur Eingeweihte verstehen.

Kob leitet Hisolutions, er lehrt an einer Wiener Hochschule und berät die CDU. Der studierte Informatiker kann mit seinen Mitarbeitern inzwischen kaum noch mithalten, sagt er. Für gezielte Hacks müsse man auf dem aktuellen Stand sein. „Obwohl“, stockt er, „eigentlich basieren die meisten gezielten Hacks auf einem ähnlichen Prinzip.“

ZUERST SENDEN KOBS LEUTE Anfragen an die IP-Adresse ihrer Opfer und beobachten, wie der Server reagiert. Aus der Antwort, die sie bekommen, lässt sich schließen, welche Software und welchen Server das Opfer einsetzt. „Ich schicke sozusagen ein ‚Hallo‘ an einen Server, und der antwortet dann vielleicht ‚Hallo, ich bin ein Server, auf dem Microsoft Exchange läuft‘“, schildert Kob. Haben sie das herausgefunden, testen sie etwa mittels Fehlerdatenbanken die Schwachstellen der jeweiligen Software. „Das wäre dann beispielsweise, dass eine Mail mit dem Inhalt ‚XY‘ an Microsoft Exchange Verwirrung beim Computer auslöst und dieser uns, also den Eindringling, bittet, das Problem zu lösen“, sagt er. „Das sind dann die berühmten Wir-sind-drin-Momente, die man aus Hollywood kennt.“ Von hier aus kann man das Netzwerk manipulieren, auf andere Server zugreifen und sich im schlimmsten Fall zum Superadministrator machen.

Solche Hacks kommen von extrem spezialisierten Tätern, die wie Scharfschützen ein ganz bestimmtes Opfer treffen wollen: Banken, Verkehrsinfrastruktur, Versicherungen oder die Energie- und Wasserversorgung. Die meisten Viren, die man sich privat einfängt, entsprechen hingegen dem Prinzip Schrotflinte. Hacker führen hierzu denselben Angriff auf Millionen Rechnern aus und hoffen, dass es irgendwo funktioniert.

Noch suchen Menschen nach den Einfallstoren. Aber fast alle großen Sicherheitssoftwarehersteller nutzen inzwischen auch künstliche Intelligenz, um Muster in Hackangriffen zu erkennen, sagt Kob. In wenigen Jahren würden Angreifer keine eigenen Anfragen mehr an Server schicken, sondern schnellere und bessere mittels selbstlernender Systeme. „Gerade sehen wir ein ungeheures Wettrüsten darum, wessen Algorithmen schneller lernen“, sagt Kob. Bald können autonome Computer eines Hackers die Computer einer Firma angreifen, denen dann wiederum Kobs Computer helfen. Die Menschen sehen dann den Angriffen vor dem Bildschirm zu und drücken ihrem Computer die Daumen – ein Game, bei dem viel auf dem Spiel steht.

YVES BELLINGHAUSEN lebt und arbeitet als freier Journalist in Leipzig

Foto: Anja Lehmann für Cicero