

Teherans Papierdiebe

Spionage Hacker aus Iran griffen weltweit Universitäten und Unternehmen an – und stahlen auch 23 deutschen Hochschulen viele Dokumente.

Als Rod Rosenstein eine Woche vor Ostern in Washington vor die Presse trat, wählte er drastische Worte. Die US-amerikanischen Behörden seien »feindlichen Akteuren« auf der Spur, sagte der Vizechef des Justizministeriums. Diese wollten »von Amerikas Ideen profitieren«.

Rosenstein enthüllte einen groß angelegten Hackerangriff aus Iran. Computerexperten im Dienst der Revolutionswächter hätten weltweit 320 Universitäten attackiert, zudem amerikanische Unternehmen und Behörden und die Vereinten Nationen. Allein die Erkenntnisse, die amerikanischen Universitäten gestohlen worden seien, hätten einen Wert von 3,4 Milliarden Dollar. Das FBI habe neun Iraner zur Fahndung ausgeschrieben, unter anderem wegen Verschwörung.

Kurz vor Rosensteins Auftritt hatten die Umtriebe der Hacker auch in Deutschland Betriebsamkeit ausgelöst – allerdings still und leise, unbemerkt von der Öffentlichkeit.

Das Kanzleramt hatte eilig eine Sonder-sitzung des Parlamentarischen Kontrollgremiums einberufen: Diese Bundestagsabgeordneten tagen geheim und kontrollieren die Arbeit der deutschen Geheimdienste. Und Ermittler des Bundeskriminalamts und des Generalbundesanwalts hatten sich auf den Weg nach Wuppertal gemacht. Im Gepäck: ein Durchsuchungsbeschluss für die Räumlichkeiten eines iranischen Staatsbürgers.

Die Zeit drängte. Informationen, die sorgsam gehütet worden waren, schienen nun im fernen Washington öffentlich zu werden. Die Hacker infiltrierten offenbar auch 23 Universitäten in Deutschland und erbeuteten unter anderem unveröffentlichte Forschungsergebnisse, Dissertationen und Konferenzberichte.

Diese könnten wertvoll für den Geheimdienst sein, selbst wenn es sich nicht um Papiere über Nuklear- und Raketentechnologie handelt – jene Felder, an denen Iran trotz des Atomabkommens mit dem Westen ein intensives Interesse nachgesagt wird. Teile ihrer weltweiten Beute stellten die Täter unter dem Titel »Megapaper« online und warben damit, »wissenschaft-



US-Vizejustizminister Rosenstein*: »Feindliche Akteure«

liche Schätze« von Fachverlagen wie Springer, Nature Publishing Group, Elsevier oder Thieme im Angebot zu haben. Gegen Bezahlung können Nutzer angeblich auf 85 Millionen Dokumente zugreifen, darunter Zigtausende deutsche Forschungsarbeiten.

Ihren Raubzug in der deutschen Wissenschaft betrieben Teherans Papierdiebe mit großem Aufwand und über Jahre. Die Ermittler können erste Attacken bis in den Herbst 2014 zurückverfolgen. Im Januar 2015 bekamen deutsche Behörden erstmals Wind von der Operation. Mitarbeiter der Universität Göttingen erhielten Mails, die auf sie zugeschnitten waren. Die Absender baten zum Beispiel um wissenschaftliche Zusammenarbeit.

Klickten die Empfänger auf einen Link, öffnete sich eine professionell gefälschte Webseite mit ihrem Universitätslogo und der Aufforderung, Benutzernamen und Passwort erneut einzugeben. Allein in Göttingen gelangten die Cyberdiebe so an die Login-Daten von 34 Universitätsmitarbeitern. Das war beachtlich – aber sah noch nicht wie ein flächendeckender Angriff aus.

Zwei Jahre später jedoch erreichte der Hinweis eines Nachrichtendienstes aus den Vereinigten Staaten die Bundesrepublik. Neben Göttingen seien 22 weitere deutsche Hochschulen betroffen, allesamt mit Sitz in Hessen und Nordrhein-Westfalen. Die Angreifer fälschten offenbar die Seite eines Bibliotheksportals, das viele Universitäten benutzen: Eine Mail verleitete die Wissenschaftler dazu, auf dieser

falschen Seite ihre Nutzerdaten einzugeben – ansonsten laufe ihr Online-Bibliothekszugang aus.

Die Behörden konnten nun nachvollziehen, wer hinter dem Angriff steckte. Die Spur führte zu einem Institut in Teheran mit dem Namen Mabna. Zu dessen Auftraggebern sollen die iranischen Revolutionswächter gehören. In Sicherheitskreisen heißt es, das Institut sei eine Tarnfirma der iranischen Spione.

Die Bundesanwaltschaft hat deswegen ein Verfahren wegen des Verdachts auf »geheimdienstliche Agententätigkeit« eingeleitet. Doch Ermittlungen im virtuellen Raum sind schwierig und langwierig – und die Hacker suchen sich immer neue Ziele. »Sie haben nicht aufgehört«, sagt der IT-Spezialist und Ex-FBI-Mann Crane Hassold, »die Attacke läuft weiter.«

Das könnte auch für Deutschland gelten. Inzwischen heißt es, dass auch hierzulande Unternehmen angegriffen worden sein könnten. Ob am Ende ein Täter gefasst wird, ist unsicher.

Ein Ansatzpunkt, den die Fahnder zwischenzeitlich hatten, führte offenbar zunächst zu keinem Erfolg: Bei der Razzia in Wuppertal sahen sie sich einem Mann gegenüber, zu dem die Hacker womöglich eine falsche Spur gelegt hatten. Er soll, als die Fahnder bei ihm auftauchten, verduzt reagiert haben – und nach Einschätzung der Ermittler »eine glaubhafte Erklärung« dafür abgeben haben, nichts mit der Sache zu tun zu haben.

Jörg Diehl, Matthias Gebauer,
Martin Knobbe, Fidelius Schmid,
Wolf Wiedmann-Schmidt

* Auf der Pressekonferenz zum iranischen Hackerangriff im Ministerium in Washington am 23. März.