So lässt sich ganz legal hacken

Die Schweiz gerät zunehmend ins Visier krimineller Hacker, etwa aus Russland. Politik und Wirtschaft versuchen daher, den Kampf gegen Cybercrime zu intensivieren. Dabei spielen sogenannte ethische Hacker eine wichtige Rolle – deren Rechtslage ist aber oft unsicher.

Gregory Remez

Daten der Bundesverwaltung sind besonders begehrt. Im Bild: Bundeshaus in Bern. Bild: Gaëtan Bally/Keystone

Die Liste der Cyberangriffe in der Schweiz wächst beinahe täglich. Der jüngste Vorfall, der landesweit für Aufregung sorgte: ein Hackerangriff der russischen Erpresserbande «Play» auf das Interlakner Unternehmen Xplain. Dieses ist laut Bundesrat ein «zentraler IT-Dienstleister für nationale und kantonale Behörden». Nun sind heikle Daten von Verwaltung und Behörden frei im Darknet zugänglich, darunter vom Bundesamt für Polizei.

Ein ähnliches Schicksal ereilte jüngst auch diese Zeitung, als Daten des Herausgeberverlags CH Media erbeutet wurden und im Darknet landeten. Auch damals hiess der Angreifer Play. Gemäss Fachleuten hat sich die Schweiz inzwischen zu einem «Topziel für Cyberattacken» entwickelt, nicht nur für finanziell, sondern auch politisch motivierte Hacker.

«Gute» Hacker gehen grosse Risiken ein

Als Antwort darauf versuchen derzeit Politik und Wirtschaft, den Kampf gegen Cybercrime zu intensivieren. Eine immer wichtigere Rolle spielen dabei auch sogenannte ethische Hacker oder «White Hat Hacker», die sich den Cyberkriminellen in den Weg stellen – oder ihnen zumindest zuvorkommen wollen. Laut dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (Edöb) haben Hinweise zu IT-Sicherheitslücken von dieser Seite zugenommen.

Im Gegensatz zu finanziell oder politisch motivierten Angreifern, versuchen ethische Hacker, Schwachstellen in einem System aufzuspüren und Systembetreibern zu melden, damit diese ihre IT-Sicherheit verbessern können. Handeln sie jedoch auf eigene Faust und ohne Wissen der Verantwortlichen, können sie schnell in Rechtsschwierigkeiten geraten.

Deswegen hat der Edöb jüngst ein Merkblatt veröffentlicht, das sich explizit an ethische Hacker richtet. Das Dokument solle allen, die «das Richtige tun wollen», Denkanstösse geben, damit sie «die Auswirkungen ihrer Aktivitäten besser einschätzen können». Unter anderem heisst es darin, dass die Bekanntgabe einer Sicherheitslücke an die Medien vor deren Schliessung nicht mit den Grundsätzen des Datenschutzgesetzes vereinbar sei.

Grundsätzlich dürfen ethische Hacker Systembetreiber nicht schaden oder diesen nicht in seinen Arbeiten behindern, Sicherheitsmängel zu beheben. Neben zivilrechtlichen Risiken gehen die Hacker ansonsten auch strafrechtliche Risiken ein. So wird laut dem Strafgesetzbuch bestraft, «wer auf dem Wege von Datenübertragungseinrichtungen unbefugterweise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt». Dabei sei es für den Tatbestand unerheblich, mit welcher Motivation die Tat verübt werde.

IT-Experte plädiert für Kulturwandel

Diese Rechtsunsicherheit gab zuletzt auch in der IT-Sicherheitsbranche zu reden. «Mit der heutigen Vernetzung, der Cloud und dem Aufkommen des ‹Internet of Things› ist es gar nicht mehr so einfach zu sagen, was unter ethisches Hacking fällt und was nicht», sagt Luca Cappiello, der bei der Baarer Firma Infoguard den Bereich Sicherheitstests (Penetration Testing & Research) verantwortet. Es sei komplex geworden, entsprechend gebe es einen rechtlichen Graubereich. Mit dem Merkblatt versuche das Edöb nun, etwas Licht ins Dunkel zu bringen, es brauche aber noch eine viel breitere Debatte über IT-Sicherheit in der Schweiz.

Gar für einen Kulturwandel im Umgang mit dem Thema plädiert Sandro Nafzger, CEO der Luzerner Cybersicherheitsfirma Bug Bounty. «IT-Sicherheit ist kein Zustand, der erreicht werden kann, sondern ein kontinuierlicher Prozess, an dem täglich gearbeitet werden muss. Grundsätzlich habe fast jedes System Schwächen und Lücken, die ausgenutzt werden können. «Die Frage ist nur, von wem sie zuerst entdeckt würden, von ethischen oder kriminellen Hackern.»

Laut dem Gesetz sind ethische Hacker nicht verpflichtet, eine Sicherheitslücke an den Edöb zu melden. Im Gegensatz zu den verantwortlichen Firmen, die eine Meldepflicht haben, sobald etwaige Lücken ein «hohes Risiko für betroffene Personen» mit sich bringen. Dies geschehe jedoch nicht immer, monieren die IT-Sicherheitsexperten.

«Immer wieder erleben wir, dass Softwarehersteller oder Firmen nur zögerlich oder gar nicht auf gemeldete Schwachstellen reagieren, denn die Schliessung einer Lücke ist natürlich immer mit Kosten verbunden», sagt Cappiello von Infoguard. Erst kürzlich habe man einen Fall von Babykameras gehabt, über die sich theoretisch jeder Zugang verschaffen und sogar die Sprechanlage übernehmen konnte. «Der Hersteller hat jedoch monatelang nicht auf unsere Meldung reagiert, so blieb die Sicherheitslücke offen. Hier sollte man sich überlegen, ob Firmen in solchen Fällen künftig nicht mehr zur Verantwortung gezogen werden sollten.»

«Ethische Hacker haben zunehmend wichtige Rolle»

Auch bei Bug Bounty kennt man derartige Beispiele zuhauf. «Noch immer werden Fehler und Lücken gerne unter den Teppich gekehrt, dabei wäre ein offener Umgang mit dem Thema wichtig für alle Beteiligten», sagt Nafzger. Eine Firma müsse sich heute genauso um seine IT-Sicherheit kümmern wie um die tägliche Buchhaltung und die Geschäftsstrategie. «Ethische Hacker haben hier eine zunehmend wichtige Rolle, werden aber noch nicht als wichtige Stakeholder erkannt.»

Nafzger wünscht sich deshalb eine Gesetzesanpassung oder zumindest «eine stärkere Etablierung von ethischem Hacking», damit unter definierten Rahmenbedingungen legal gehackt werden kann. Cappiello pflichtet bei: Natürlich gebe es auch vermeintlich gute Hacker, die stümperhaft vorgingen und zu einem falschen Zeitpunkt zu viel preisgeben – zum Nachteil von Nutzerinnen und Nutzer. Kriminell werde es aber erst dann, wenn Hacker «Daten klauen, sich bereichern oder die Privatsphäre von Nutzern missachten».