Angriff auf Raiffeisen

IT-Sicherheit Die Bank hat Hacker beauftragt, Schwachstellen in ihrem System zu finden. Bei Erfolg winkt eine Prämie.

BERNHARD FISCHER

FOTOS: FABIAN HUGO FÜR HZ

Angriff auf Raiffeisen: Das Sextett der Hacker-Truppe von Bug Bounty Switzerland in Bern beim Hack auf die Genossenschaftsbank.

Es ist Donnerstagnachmittag im Berner Matte-Quartier, zwischen Flusskraftwerk und Jazzclub, in einer aufgelassenen Industriehalle. In der Mitte der Halle stehen ein Konferenztisch, ein paar Stühle und ein Dutzend Computer und Laptops, die erst noch an den Strom angeschlossen werden müssen. Es sieht aus wie in einer Kommandozentrale. Die Aufbauten für den nächsten grossen Banken-Hack der IT-Söldner von Bug Bounty Switzerland (BBS) laufen.

Zwei Wochen haben die «ethischen» Hacker von BBS Zeit – also legal, mit Auftrag und für die gute Sache – von ihrem Basislager aus drei ausgewählte Systeme von Raiffeisen auf Lücken zu prüfen. Sie suchen nach Schlupflöchern und Mängeln im System, wollen herausfinden, ob es Sicherheitslücken gibt, die von Cyberkriminellen ausgenutzt werden könnten. Wer eine findet, wird belohnt.

Auslobungen von 10 000 Franken für einen kritischen Fund sind durchaus üblich. Swisscom und die Schweizerische Post zum Beispiel bezahlen solche Beträge für das Auffinden kritischer Schwachstellen.

Erste Schwachstellen wurden gefunden

In böser Absicht und mit ausreichend krimineller Energie könnten Banken wie auch Raiffeisen schlimmstenfalls um viele Millionen Franken erpresst werden. Allfällige Hacker-Prämien sind nichts dagegen. Besonders dann, wenn es den Hackern gelingt, Vertragsdokumente, Konten- und Kundendaten zu klauen. Oder Ransomware auf den Servern zu installieren. Ganz zu schweigen vom Reputationsschaden, wenn es zu Ausfällen kommen sollte oder vertrauliche Daten abgesaugt und der Öffentlichkeit zugänglich gemacht würden. Das versuchen die Bounty-Hunter in diesem Hack aufzuzeigen und für die Zukunft zu verhindern.

Florian Badertscher, das Security-Genie der Truppe mit der meisten Erfahrung, hackt in die Tasten. Er versucht, ins System der Raiffeisen vorzudringen. Und hat bereits erste Schwachstellen gefunden. Nach einigen Zeilen Code im Split-Screen-Modus ist ihm auf einen Blick klar: «Das System hat eine sehr hohe Maturität. Man merkt, dass dieses System schon sehr oft und intensiv getestet wurde.»

Er berät sich mit seinem Compagnon und Chef, Sandro Nafzger. Die beiden stellen fest, diesmal werde es nicht so einfach sein wie beim letzten Hack. Badertscher gähnt, er ist erschöpft vom Hack auf eine Schweizer Grossfirma vor wenigen Tagen und holt sich erst einmal Kaffee und einen Apfel vom Buffet. «Der Test bei dieser Firma hatte bereits nach vier Stunden voll durchgeschlagen auf ihrem Kernsystem, mit der maximalen Kritikalitätsstufe 10. Das ist echt wüst.» Auf ihn wartet eine arbeitsreiche Nacht, die Kernzeit in der Hacker-Welt.

Derweil steckt das restliche Team die Köpfe zusammen. Das Fazit: Es braucht mehr Power. Nafzger gibt seinem Sicherheitschef und «Feldmarschall» Lukas Heppler die Order: «Wir brauchen sofort sechzig weitere Hacker.» Heppler kümmert sich darum, welche Hacker in die Startformation kommen. Er überwacht die Operation und die eingehenden Schwachstellen, entscheidet, ob es noch mehr Leute braucht, und stellt sicher, dass die Programme beendet werden, wenn das Auftragsbudget für die Belohnungen ausgeschöpft wurde. Er tippt in den Laptop und ruft Verstärkung.

In der ethischen Hacker-Welt kennt jeder jeden. Die meisten im Schweizer Bug-Bounty-Team haben sich beim Aufbau von Bounty-Programmen bei Swisscom und der Post kennengelernt. Die Truppe will einen Zahn zulegen, lässt ihre Beziehungen spielen und trommelt gewiefte Programmierer zusammen, die nur darauf warten, mit (legalen) Auftragshacks nicht nur eine Menge Spass zu haben, sondern auch Geld zu verdienen.

Hacker-Genius Florian Badertscher (links) und BBS-Chef Sandro Nafzger.

Um die 20 000 ethische Hacker sind für das Team auf Knopfdruck abrufbar. Jener Hacker, der als Erster etwas findet, bekommt die volle Belohnung. Es gilt: first come, first served. Wer eine Sekunde später dieselbe Schwachstelle findet, geht leer aus.

Der Hacker wächst am Widerstand

Badertscher läuft auf Hochtouren. Er scrollt durch Computerscripts, malt mit dem Filzstift Quadrate, Pfeile und Zahlen ans Board, die nur Insider verstehen. Und bespricht mit dem Team die neue Lage. Der Ehrgeiz ist geweckt.

Solcher Eifer macht Eindruck. Nicht nur bei Banken und Firmen. Auch das Nationale Zentrum für Cybersicherheit (NCSC) unter der Führung von Florian Schütz ist auf die Hacker aufmerksam geworden und hat BBS als strategischen Partner ausgewählt, um die Zusammenarbeit mit ethischen Hackern in der Schweiz zu etablieren. Der Start eines gemeinsamen Pilotprojekts steht kurz bevor. Auch dafür laufen die Vorbereitungen auf Hochtouren. Keine Firma, keine Regierung und kein Geheimdienst solle glauben, vor Cyberattacken ausreichend geschützt zu sein. «Aber wir können helfen», sagt Nafzger mit einem Augenzwinkern, «mit uns hat man meist nach 48 Stunden begriffen, dass die bisherige Risikoeinschätzung falsch war und man trotz allen bisherigen Massnahmen ein sehr leichtes Ziel für Cyberattacken ist.»

Der Sicherheitsbericht für Raiffeisen ist noch nicht geschrieben, der Hack läuft noch. Nafzger darf darüber auch nicht zu viel verraten. Er formuliert es vorsichtig: «Falls uns ein Zugriff auf ein System gelingen sollte, dokumentieren wir, wie uns das gelungen ist und ob wir die Kundendaten einsehen und hätten herunterladen können. Dafür muss man das nicht effektiv tun. Es genügt, zu beweisen, dass wir so weit gekommen sind.»

Genau für diese Sicherheitsüberprüfungen hat Raiffeisen die BBS-Leute engagiert. Erste Erfolge haben die IT-Cracks bereits gefeiert. Das ist gut fürs Ego und den Kunden: «In einigen Tagen oder Wochen wird man wissen, wie viele der gefundenen Schwachstellen unsere Begleitung brauchen werden. So ein Reality-Check ist meist der Anfang einer langjährigen Zusammenarbeit», sagt Nafzger.

UNTER KONTROLLE

Vorteile und Kosten eines Bounty-Hacks

Die Vorteile Im Zuge der Digitalisierung sind Sicherheitsexperten die neuen Rockstars in den Organisationen. Informationssicherheit ist zur Schlüsseldisziplin geworden, damit die digitale Transformation gelingt. Bug-Bounty-Programme sollen dabei helfen, Softwarefehler zu identifizieren. Die Hacker, die dafür von Unternehmen und Privatpersonen, Militärs und Regierungen beauftragt werden, erhalten eine Prämie, wenn sie Fehler finden. Der Auftraggeber kann die Fehler korrigieren und das IT-System sicherer machen. Hacker wiederum werden dadurch entkriminalisiert – und handeln somit «ethisch», mit klaren Vorgaben, nach dem Gesetz und nur gegen vordefinierte Bereiche und Systeme.

Die Kosten In der Schweiz üblich sind Kosten für einen ersten Auftrags-Hack zwischen 20 000 und 50 000 Franken; sie orientieren sich an der Unternehmensgrösse – ein KMU zahlt weniger als ein Grosskonzern. Wenn es weitere Hacker-Dienstleistungen braucht, kann es teurer werden. In der Branche sind sechs- bis siebenstellige Beträge im ersten Jahr keine Seltenheit.