Ethische Hacker – bewusster Eigenbeschuss für mehr Sicherheit

Jedes IT-System hat seine unbekannten Sicherheitslücken. Cyberkriminelle machen sich einen Spass daraus, genau jene zu finden. Dadurch können Schäden in Millionenhöhe entstehen. Sandro Nafzger ist Wirtschaftsinformatiker und CEO von Bug Bounty Switzerland. Er hilft Schweizer Organisationen, mit ethischen Hackern zusammenzuarbeiten und durch deren Hilfe genau diese Sicherheitslücken zu schliessen. Im Interview erklärt er, was ethische Hacker sind, wie diese vorgehen und weshalb die Schweizer Rechtsgrundlage diesbezüglich zu optimieren ist.

Interview: Michelle Guilfoyle; Fotos: zvg

Bist du ein Hacker?

Ich selbst bin kein Hacker. Aber ich helfe Schweizer Organisationen dabei, mit ethischen Hackern zusammenzuarbeiten. Vor rund 20 Jahren habe ich eine vierjährige Berufslehre als Informatiker bei der Ascom und Swisscom absolviert. So bin ich in die IT eingestiegen. Damals habe ich Software entwickelt – vor allem Internetapplikationen –, damals war das noch etwas recht Neues (lacht). Aber ich habe recht schnell gemerkt, dass ich eben kein Hacker bin. In seiner ursprünglichen Bedeutung steht Hacker ja für einen «Tüftler», der alles um sich herum vergisst und richtig in die Technik eintaucht, den Dingen wirklich tief auf den Grund geht und mit viel Geschick und Hingabe beinahe mit der Maschine zusammenschmilzt. Im positiven Sinne kann man so jemanden auch einen «Nerd» nennen. Leider wurde das Wort «Hacker» durch die Medien vorbelastet. Viele Leute assoziieren damit etwas Negatives, Gefährliches oder Kriminelles. Aber ein Hacker an sich ist einfach ein Ausnahmetalent, ein hochspezialisierter Experte. Jetzt kommt es einfach darauf an, wie er seine Talente nutzt und nutzen darf.

Was waren deine Ziele? Welche sind es heute?

Ich habe mir schon immer ein selbstbestimmtes Leben gewünscht. Viel Freiheit und Flexibilität, dass ich nach meinen eigenen Idealen und Visionen leben kann. Deshalb wollte ich auch Informatiker werden. Unabhängig und von einem beliebigen Ort aus über das Internet arbeiten, diese Idee hat mir gefallen. Auch der schnelle Wandel, immer am Ball bleiben und jeden Tag Action – das fasziniert mich noch heute. Diese grundlegenden Ziele haben sich eigentlich bis heute nicht wesentlich verändert. Mittlerweile sind bei mir aber auch andere Bedürfnisse entstanden; zum Beispiel Nachhaltigkeit, also etwas für die Zukunft aufzubauen. Oder auch wirklich etwas zurückzugeben an mein Umfeld und die Schweiz.

Worin unterscheidet sich ein ethischer Hacker von anderen Hackern?

Stark vereinfacht kann man Hacker in zwei Gruppen unterteilen: nämlich die Guten, das sind die ethischen Hacker, und die Bösen, also Cyberkriminelle.

Mit den Cyberkriminellen ist es ähnlich wie im echten Leben. Da gibt es welche, die mal bei Rot über die Ampel fahren – vielleicht sogar unabsichtlich. Es gibt Taschen- und Gelegenheitsdiebe bis hin zu richtig üblen und gefährlichen Schurken. Oft organisieren sich diese auch in Gruppen. Das können Räuberbanden oder mafiaartige Clans sein. Die Bedrohung im Internet ist also sehr vielfältig und komplex. Letztes Jahr wurden Cyberrisiken zum ersten Mal als das allergrösste Unternehmensrisiko definiert, weltweit und auch in der Schweiz. Man ist sich also einig: Cyberkriminelle sind eine grosse Bedrohung für die Sicherheit unserer Welt.

Zum Glück gibt es da nun aber auch gute Hacker, also ethische Hacker oder oft auch White-Hat-Hacker genannt. Diese haben keine kriminellen Absichten, im Gegenteil. Sie wollen die Welt verbessern und Organisationen aktiv dabei unterstützen, sich vor bösen Hackern zu schützen. Jedoch ist das für sie nicht so einfach.

«Hacker können in zwei Gruppen unterteilt werden: die Guten, das sind die ethischen Hacker, und die Bösen, also Cyberkriminelle.»

Warum? Wie funktionieren ethische Hacker?

In der Schweiz ist die Zusammenarbeit mit ethischen Hackern noch viel zu wenig etabliert. Ein ethischer Hacker geht mit anderen Augen durch die Welt. Er sieht das Ganze auf seine Weise, er will wirklich verstehen, wie etwas abläuft, ob die Dinge korrekt funktionieren und sicher sind. Wenn er sich zum Beispiel in einem Onlineshop eine neue Computertastatur bestellt, klickt er sich nicht einfach unbewusst durch, gibt seine Kreditkarteninformationen ein und wendet sich einer anderen Tätigkeit zu. Nein, er verbringt damit oft Stunden. Er schaut sich den Quellcode des Onlineshops an, will verstehen, wie das Ganze aufgebaut ist, welche Technologien verwendet wurden, welche Systeme dahinterstehen, wo seine Kreditkarteninformationen hingesendet werden, was damit geschieht und ob damit alles in Ordnung ist. Also die Liebe zur Technik, seine Neugier und sein Wissensdurst sind es, was ihn antreibt.

Nun ist es aber so, dass es keine perfekten IT-Systeme gibt. Dafür ist das Ganze einfach zu komplex und verändert sich dauernd. So gibt es laufend kleinere oder grössere Fehler in einem Computersystem. Wenn der ethische Hacker gut ist und sich lange genug damit auseinandersetzt, findet er diese – eigentlich immer. Genau das ist Teil dieser Faszination. Man weiss, dass es irgendwo einen Fehler geben muss, jetzt muss man ihn nur noch finden. Das ist wie ein Videospiel, also eine Challenge.

«Das ist wie ein Videospiel, also eine Challenge.»

Wenn ein ethischer Hacker eine Schwachstelle gefunden hat, was macht er damit? An wen wendet er sich?

Er kann herausfinden, welche Firma den Onlineshop betreibt, und diese kontaktieren. Aber da prallen oft zwei Welten aufeinander. Der Hacker ist stolz auf seinen Fund und möchte, dass die Schwachstelle so schnell wie möglich behoben wird, damit niemand zu Schaden kommt durch das latente Sicherheitsrisiko. Die Firma auf der anderen Seite weiss oft nicht, wer für so eine Anfrage intern verantwortlich ist, und versteht auch nicht, von was der Hacker überhaupt spricht – das Ganze ist viel zu technisch. Vielleicht bekommt die Firma Angst, fühlt sich bedroht und weiss nichts Besseres, als mit den Anwälten zu drohen. Solche Diskussionen können oft sehr schnell destruktiv und frustrierend werden. Der ethische Hacker meint es eigentlich gut, er will helfen, aber die Firma kann damit einfach nicht umgehen – ist mit seiner Anfrage oder Meldung überfordert. Hinzu kommt, dass unser Rechtssystem sehr streng und nicht auf ethische Hacker ausgelegt ist. Das Leben von einem ethischen Hacker ist also nicht einfach. Entweder schweigt er und macht sich mitschuldig oder er versucht sich mitzuteilen und riskiert damit Probleme, die er nicht will.

Wo liegt hierbei die Schwierigkeit im Schweizer Rechtssystem?

Im Grunde befindet sich ein ethischer Hacker immer schon fast mit einem Bein im Gefängnis – das, obwohl er nichts Kriminelles vorhat. Denn schon nur dadurch, dass er die Funktionsweise eines IT-Systems analysiert, macht er sich strafbar. Das Schweizer Strafrecht sieht dies nicht vor – im Gegenteil: Artikel 143bis StGB richtet sich explizit gegen unbefugtes Eindringen in ein fremdes Datenverarbeitungssystem.

Symbolbild eines Cyberkriminellen. (Foto: Shutterstock)

Im Gegensatz zu einem herkömmlichen IT-Spezialisten steht der ethische Hacker in keinem Auftragsverhältnis mit der betroffenen Firma. Daher muss er im schlimmsten Fall mit einer Verfolgung durch den Eigentümer des untersuchten Systems rechnen. Um mit dieser Grauzone besser umzugehen und die ethischen Hacker zu schützen, gibt es den sogenannten Legal Safe Harbor.

Was ist ein Legal Safe Harbor?

Um mit ethischen Hackern zusammenzuarbeiten, braucht es Spielregeln. Oft werden diese durch eine Vulnerability Disclosure Policy (VDP) oder einen Verhaltenskodex (Code of Conduct) definiert. Zunächst werden darin die ethischen Hacker und Sicherheitsforscher zu einem regelkonformen Verhalten verpflichtet. Also dass sie nur in guten Absichten handeln und nichts kaputt machen dürfen. Man gibt ihnen also die Erlaubnis, von aussen über das Internet nach Schwachstellen zu suchen, wenn dies dazu dienen soll, das System zu verbessern. So kann man auch definieren, welche Systeme getestet werden dürfen und welche nicht. Wichtig ist für den ethischen Hacker auch, zu wissen, wie er seine Befunde melden kann. Wie der Prozess funktioniert und wie schnell die Schwachstellen dann behoben werden. Ist dieses regelkonforme Verhalten vom ethischen Hacker gegeben, verpflichtet sich die jeweilige Organisation, im Gegenzug auf jede Strafverfolgung zu verzichten und darüber hinaus auch dazu, den Sicherheitsforschern rechtlich zur Seite zu stehen, sollte eine entsprechende Verfolgung von dritter Seite angestrengt werden. Dieser Schutz für die ethischen Hacker nennt man einen Legal Safe Harbor, also einen sicheren Hafen, in dem sie sich ohne Risiko bewegen können.

Wie etabliert ist der Legal Safe Harbor in der Schweiz?

In der Schweiz sind solche Vulnerability Disclosure Policies und auch der Legal Safe Harbor noch sehr wenig verbreitet. Die Schweizerische Post hat sich im Vorfeld des öffentlichen Hackertests für das E-Voting-System bereits 2018 intensiv Gedanken dazu gemacht und hat zusammen mit Bund und Kantonen eine entsprechende Formulierung erarbeitet. Diese wurde kürzlich sogar öffentlich zur Verfügung gestellt unter www.bugbounty.ch/legal-safe-harbor und kann so auch von anderen Organisationen weiterverwendet werden.

Was braucht es, damit eine Organisation konstruktiv mit ethischen Hackern zusammenarbeiten kann?

Das mindeste, was jede Organisation in der Schweiz haben müsste, wäre eine Vulnerability Disclosure Policy auf der Webseite. Also ein Bekenntnis, dass man für das Melden von Sicherheitslücken dankbar ist und dass es einen klaren Prozess gibt, wie diese Meldungen eingereicht werden können und von der Organisation bearbeitet werden. Obschon VDP sehr wichtig ist, ist es nur ein passiver Ansatz. Wenn jemand von einer Schwachstelle weiss, kann er sie melden, fertig. Viel Spannender ist es aber, proaktiv mit ethischen Hackern zusammenzuarbeiten. Diese also aufzurufen und zu motivieren, ganz gezielt nach Schwachstellen zu suchen. Dazu braucht es ein Bug-Bounty-Programm.

Was ist ein Bug-Bounty-Programm?

Bug Bounty ist eine Kopfgeldjagd im Internet. Im Rahmen eines Wettbewerbs werden Belohnungen (Bounties) ausgezahlt für gefundene Sicherheitslücken (Bugs). Auch hier gibt es klare Spielregeln und es darf nur in besten Absichten gehandelt werden. Aber zusätzlich gibt es einen finanziellen Anreiz für die ethischen Hacker. Denn diese investieren oft Tage, wenn nicht Wochen oder Monate in das Aufspüren von Schwachstellen und Zusammenbauen von neuen Angriffsszenarien. Es ist also nur fair, dass sie für ihre Leistung auch entschädigt werden.

Die Höhe einer Belohnung hängt vom Schweregrad der gefundenen Schwachstelle ab. Wenn man aufzeigt, wie Daten gestohlen werden oder gleich das ganze System lahmgelegt werden könnte, gibt es natürlich mehr Geld als für mittelschwere oder leichte Sicherheitsprobleme. Das Spannende an einem Bug-Bounty-Programm ist, dass man jeweils nur den ersten ethischen Hacker bezahlt, der eine Schwachstelle findet. So entsteht unter den ethischen Hackern eine riesige Motivation, der Beste und Schnellste zu sein. Man bekommt somit nicht nur Zugriff auf absolute Ausnahmetalente, sondern kann es sich auch leisten, davon Hunderte zu beschäftigen, weil eben nicht ihre Arbeitszeit bezahlt wird, sondern nur derjenige, der als Erstes eine kritische Schwachstelle findet. Der Return on Investment (ROI) eines Bug-Bounty-Programms ist riesig.

«Bug Bounty – Kopfgeldjagd im Internet»

Die Geschäftsleitung von Bug Bounty Switzerland von links nach rechts: Florian Badertscher (CTO), Matthias Jauslin (COO), Lukas Heppler (CSO), Sandro Nafzger (CEO).

Gibt es noch andere Vorteile von Bug Bounty?

Ja, da gibt es zahlreiche Vorteile. Das Allerwichtigste ist, dass man eine realistische Risikoeinschätzung erhält. Diese ist leider bei beinahe allen Schweizer Unternehmen nicht korrekt. In der Schweiz wird viel in die IT-Sicherheit investiert, deshalb fühlt man sich sicher. Dass die heute etablierten Testmethoden aber nicht mehr ausreichen, um die wirklich kritischen und komplexen Schwachstellen in IT-Systemen zu finden, weiss man in der Schweiz schlicht und einfach nicht. Ein guter Hacker kann beinahe jedes IT-System innerhalb weniger Stunden oder Tage hacken.

Kann man rechtzeitig herausfinden, ob man gehackt wurde?

In der Regel erst dann, wenn es schon zu spät ist und man bereits gehackt wurde. So ist es nicht verwunderlich, dass 50 % aller Organisationen in der Schweiz bereits Opfer einer Cyberattacke wurden. Im Schnitt kostet so ein Vorfall rund 4,7 Millionen Schweizer Franken. Bei grossen Firmen deutlich mehr. Ganz zu schweigen vom enormen Reputationsverlust.

Wie kann man sich am besten vor Cyberangriffen schützen?

Anstatt einfach weiterzumachen wie bisher und abzuwarten, bis man Opfer einer Cyberattacke wird, kann man sich proaktiv dagegen schützen, indem man ethische Hacker dazu einlädt, genauso nach Sicherheitslücken zu suchen, wie es ein Cyberkrimineller tun würde. Einfach mit dem Vorteil, dass diese Sicherheitslücken nur aufgezeigt und nicht ausgenutzt werden. Damit ein sogenannter Bug-Bounty-Hunter eine Belohnung erhält, muss er Schritt für Schritt dokumentieren, wie er vorgegangen ist. Dadurch kann der Fehler dann sehr schnell reproduziert, verstanden und nachhaltig behoben werden. Ein Bug-Bounty-Programm findet meist direkt auf den produktiven Systemen statt. Also unter realen Bedingungen, denn nur so erhält man eine realistische Risikoeinschätzung und kann die gefundenen Probleme schnell und nachhaltig beheben.

Ist es nicht gefährlich, seine eigenen Systeme unter Eigenbeschuss zu setzen?

Nein, nicht wenn man weiss, wie es geht. Mit unserer Firma Bug Bounty Switzerland wollen wir die Zusammenarbeit mit ethischen Hackern nun in der Schweiz etablieren. Wir haben keinen Zweifel daran, dass Bug-Bounty-Programme auch in der Schweiz schnell zum neuen Standard für IT-Sicherheitstests werden (wie es im Ausland übrigens schon lange der Fall ist). Denn es gibt keine effektivere und effizientere Methode, um die Sicherheit von IT-Systemen nachhaltig zu verbessern. ■

BUG BOUNTY
SWITZERLAND