«Ein Bug-Bounty-Programm ist ein richtiger Game-Changer»

Im Ausland sind Bug-Bounty-Programme schon etabliert – in der Schweiz noch nicht. Um dies zu ändern, gründeten Sandro Nafzger und sein Team im April 2020 Bug Bounty Switzerland. Im Interview sagt Nafzger, warum die Digitalisierung ohne ethische Hacker langfristig gar nicht möglich ist. Interview: Coen Kaat

Bug Bounty Switzerland ist nun seit rund einem Jahr operativ tätig. Wie war das erste Geschäftsjahr?
Sandro Nafzger: Das hätte nicht besser verlaufen können. Unser Timing war perfekt. Wir kamen weder zu früh noch zu spät auf den Markt. Früh genug, um die ersten zu sein. Aber auch nicht so früh, dass der Markt noch nicht bereit war für unser Angebot.

Sie sind die Ersten. Sind Sie noch immer die Einzigen?
Ja, wir sind die einzigen Anbieter von ganzheitlichen Bug-Bounty-Lösungen in der Schweiz. Wir sind also Marktführer (lacht). Ich gehe davon aus, dass jedes Unternehmen, das heute Penetration Tests nutzt, auch ein Bug-Bounty-Programm braucht und künftig betreiben wird. In diesem jungen Markt wird es also schon bald etwas mehr Bewegung geben.

Wie reagieren potenzielle Kunden auf Ihr Angebot?
Die Reaktionen sind sehr unterschiedlich. Grundsätzlich wartet natürlich niemand darauf, dass wir ihnen sagen, dass sie vermutlich mir nichts, dir nichts gehackt werden könnten. Die Unternehmen brauchen ein wenig Zeit, um diese Botschaft zu verarbeiten. Wir suchen unsere Ansprechpartner daher auch sehr gezielt aus und reden nur mit CISOs und CIOs, von denen wir ausgehen, dass sie empfänglich sind dafür.

Fokussieren Sie sich nur auf den Schweizer Markt?
Ja, und zwar sehr bewusst. Wir sehen hierzulande einen grossen Bedarf und auch eine Dringlichkeit. Im Ausland existieren solche Programme teilweise schon seit Jahren. In der Schweiz ist man sich dem latenten Risiko vor Cyberattacken noch zu wenig bewusst. Auch dass Bug-Bounty-Programme die effektivste und auch effizienteste Art sind, IT-Systeme zu testen, ist noch zu wenig bekannt.

Wer braucht alles ein Bug-Bounty-Programm?
Jedes Unternehmen, das ein IT-System betreibt, das für den Unternehmenserfolg relevant ist.

Wie beurteilen Sie die Sicherheitslage in der Schweiz?
Schweizer Firmen investieren viel in Cybersecurity. Darum geht man davon aus, dass wir hierzulande sicher sind. Aber das ist ein Trugschluss. Herkömmliche Testmethoden wie etwa Penetration Tests können viele kritische Schwachstellen nicht finden. So kommt es denn auch, dass wir in sämtlichen Systemen, die wir testen, binnen weniger Stunden zahlreiche kritische Sicherheitslücken finden. Ernstzunehmende Sicherheitslücken, die etwa das Ausführen von beliebigem Code oder das Abfliessen von Daten ermöglichen. Das heisst, die Risikoeinschätzung der meisten Schweizer Firmen ist heutzutage oft komplett unrealistisch.

Wie etabliert sind Bug Bountys in der Schweiz?
Schweizer Unternehmen kommen langsam auf den Geschmack. Mittlerweile gibt es hierzulande ein paar Vorzeigefirmen und -projekte, die Stolz sind auf ihre Bug-Bounty-Programme und den Sicherheitsvorsprung, den sie dadurch erzielen. Auch der dafür notwendige partizipative Ansatz – also die Zusammenarbeit mit ethischen Hackern – etabliert sich langsam in der Schweiz.

Warum nur langsam?
Die dafür nötige Fehler- und Lernkultur fehlt irgendwie in der DNA der perfekten Schweiz. Bei einem Bug-Bounty-Programm geht es darum, proaktiv Sicherheitslücken zu finden und eine konstruktive und schnelle Lernkultur zu etablieren. Dabei geht es gar nicht darum, dass irgendwer irgendetwas falsch gemacht hat. Es geht darum, dass man eine neue Erkenntnis gewinnen konnte. Das erfordert aber dennoch Mut. Glücklicherweise haben wir aktuell durchaus ein paar Schweizer CISOs, die öffentlich über diesen Kulturwechsel reden. Und ich bin davon überzeugt, dass auch wir einen wichtigen Beitrag dazu leisten. Darum ist Bug Bounty Switzerland mehr als nur eine Firma.

PERSÖNLICH

Sandro Nafzger ist der führende Experte für Bug-Bounty-Programme und Crowdsourced Cybersecurity in der Schweiz. Er hilft Schweizer Organisationen, ihre IT-Sicherheit auf das nächste Level zu bringen – damit ihre digitale Transformation gelingt. Er hat als Gesamtprojektleiter den Public Intrusion Test (PIT) für E-Voting geleitet und hat als externer Mitarbeiter das konzernweite Bug-Bounty-Programm der Schweizerischen Post aufgebaut. Quelle: Bug Bounty Switzerland

Als was sehen Sie Bug Bounty Switzerland denn dann?

Wir sind eine Bewegung. Ein Bug-Bounty-Programm ist nicht einfach ein weiterer inkrementeller Schritt, sondern ein richtiger Game-Changer. Binnen kürzester Zeit bringt man die Informationssicherheit auf ein komplett neues Level. Und etabliert eine sehr agile und effektive Unternehmenskultur. Wir sehen uns selbst als Aufklärer, die versuchen, eine völlig neue Art der Zusammenarbeit in der Schweiz zu etablieren. Das geht aber nicht alleine. Darum spannen wir ein Netzwerk zwischen den Firmen, die bereits so arbeiten, und denen, die umstellen wollen. Mit dieser wachsenden Community können wir bewirken, dass es zu einem Dominoefffekt kommt und Bug-Bounty-Programme schnell zum neuen Standard für Sicherheitstest werden.

« Langfristig ist die digitale Transformation ohne Bug-Bounty-Programme gar nicht möglich. »

Sandro Nafzger, CEO, Bug Bounty Switzerland

Wo muss bei Schweizer Firmen noch ein Umdenken stattfinden?

Sicherheit ist ein kontinuierlicher Lern- und Verbesserungsprozess, an dem man täglich arbeiten muss. Früher baute man ein System, prüfte dieses ein- bis zweimal pro Jahr mit einem Penetration Test und beurteilte es aufgrund dessen als sicher. Dieses Vorgehen funktioniert aber nicht mehr in unserer heutigen, vernetzten und dynamischen Welt. Hier muss die Sicherheit eines IT-Systems beinahe täglich überprüft und verbessert werden. Dieses Verständnis ist in der Schweiz aber nur selten vorhanden. Somit verfügt eigentlich jedes IT-System – das noch kein Bug-Bounty-Programm hat – über kritische Sicherheitslücken, die von Cyberkriminellen sofort ausgenutzt werden könnten. Hinzu kommt, dass die interne Innovationsfähigkeit einer Organisation sehr begrenzt ist. Aus anderen Unternehmensbereichen weiss man das schon lange. Bug Bounty ist eigentlich nichts anderes als Open-Innovation. Es geht darum, mit einer globalen Community von herausragenden Experten zusammenzuarbeiten und deren kollektive Intelligenz zu nutzen. Also durch einen konstruktiven Dialog mit ethischen Hackern täglich von ihnen etwas Neues zu lernen. Ohne ein Bug-Bounty-Programm könnte man sich das gar nicht leisten.

Warum?

Selbst die erfolgreichste Firma kann nur eine gewisse Anzahl hochbezahlter IT-Sicherheitsexperten einstellen. Mit einem Bug-Bounty-Programm hingegen

Das Team von Bug Bounty Switzerland: (v.l.) CTO Florian Badertscher, COO Matthias Jauslin, CSO Lukas Heppler und CEO Sandro Nafzger.

profitiert man von der Expertise zahlreicher Spezialisten weltweit. Und bezahlen muss man nur diejenigen, die als Erstes einen kritischen Fehler finden. Verglichen mit dem möglichen Schadensausmass der gefundenen Schwachstellen sind die ausbezahlten Bountys zudem meistens lächerlich gering. Wer etwa eine Lücke bei einer Bank findet, mit der man beliebigen Code ausführen und das ganze System herunterfahren könnte, bekommt vielleicht 5000 Franken. Der Return on Investment für die Firmen ist also riesig.

Was verstehen Unternehmen häufig falsch, wenn es um Bug Bountys geht?

Im Gespräch mit möglichen Kunden merken wir oft, dass diese Bug-Bounty-Programme mit Cyberkriminellen assoziieren. Das eine hat mit dem anderen aber überhaupt nichts zu tun. Ein Cyberkrimineller würde sich nämlich nie bei einem Bug-Bounty-Programm anmelden. Dort muss er sich ausweisen und an Spielregeln halten. Warum auch? Die IT-Systeme stehen ja im Internet und werden von Cyberkriminellen direkt angegriffen. Der Umweg über ein Bug-Bounty-Programm ergibt also keinen Sinn. Mit einem Bug-Bounty-Programm geht man also kein zusätzliches Risiko ein – wie viele Unternehmen anfänglich befürchten. Ganz im Gegenteil, man erhält endlich eine realistische Risikoeinschätzung und kann diese Risiken dann sehr schnell und nachhaltig beseitigen. Denn jeder Bug Bounty Hunter meldet nicht nur eine gefundene Schwachstelle, sondern auch eine ganz genaue und ausführliche Schritt-für-Schritt-Anleitung, wie er vorgegangen ist. So kann eine Schwachstelle sofort reproduziert und behoben werden. Vom Topmanagement bis zum Entwickler weiss also jeder sofort, was Sache ist und was getan werden muss, um das Problem zu lösen.

Wie misst man den Erfolg eines Bug-Bounty-Programms? Entweder man investiert viel Geld und findet nichts, oder man investiert viel Geld, um herauszufinden, dass das eigene IT-System nicht sicher ist und auch wieder Investitionen benötigt.

Also es wäre natürlich sehr schön, wenn wir nichts finden würden (lacht). Aber das habe ich bis heute noch nicht erlebt. Falls nichts gefunden wird, lädt man einfach mehr ethische Hacker ein. Bei einem Bug-Bounty-Programm bezahlt man ja nur für valide und relevante Schwachstellen. Man kann also theoretisch unendlich viele ethische Hacker engagieren. Sollte dann immer noch nichts gefunden werden, kostet das Ganze praktisch nichts und man hat wirklich einen handfesten Beweis für das Sicherheitslevel des getesteten Systems. Der offensichtlichste Nutzen eines Bug-Bounty-Programms ist also, dass man endlich eine realistische Risikoeinschätzung hat und die gefundenen Schwachstellen schnell beheben kann. So kann man das Risiko von Cyberattacken signifikant senken.

Und mittel- bis langfristig?

Bug-Bounty-Programme fördern die digitale Transformation enorm; langfristig ist sie ohne gar nicht möglich. Jedes IT-System verfügt über kritische Schwachstellen und lässt sich daher meist sofort hacken. Es ist völlig egal, wie digital ein Unternehmen ist. Wenn die Firmendaten gestohlen oder verschlüsselt werden, verliert man nicht nur das Vertrauen der Kunden. Dann ist auch die digitale Transformation gescheitert. Somit ändert sich auch die Rolle der Informationssicherheit. Der CISO nimmt eine Schlüsselrolle ein und wird zum Treiber von Innovation und Geschäftserfolg.

Was sind die nächsten Schritte für Bug Bounty Switzerland?

Wir haben im ersten Jahr gezeigt, dass unser weltweit einzigartiges Bug-Bounty-Modell funktioniert und die Schweiz bereit ist dafür. Bei uns stehen nun einige spannende Themen an, zum Beispiel werden wir in diesem Jahr die Umwandlung in eine AG vornehmen. Auch sind wir daran, unser Team zu vergrössern, um der steigenden Nachfrage gerecht zu werden. Wir sind daran, uns gut aufzustellen für die Zukunft.

Das vollständige Interview finden Sie online
www.swisscybersecurity.net