YES WE H/CK

BlaBlaCar

BLABLACAR

Öffentliches Bug Bounty programm

FALLSTUDIE

YES WE HACK

WAS HAT SIE DAZU BEWOGEN, EIN BUG BOUNTY-PROGRAMM ZU STARTEN?

ALAIN TIEMBLO, WEB SECURITY LEAD ENGINEER UND LEITENDER INGENIEUR FÜR WEB-SICHERHEIT BEI BLABLACAR:

In der Vergangenheit haben wir klassische Audits eingesetzt: Schwachstellen-Scans, Penetrationstests, Code-Analysen und so weiter. Damit konnten wir bereits Vieles aufdecken. Im Laufe der Zeit erhielten wir immer häufiger Nachrichten von Trollen in sozialen Netzwerken, die uns über potenzielle Schwachstellen berichteten – aber ohne Vorankündigung und ohne jegliche Details.

Wir bekamen auch einige E-Mails über den Kundensupport zu Schwachstellen, aber auch hier ohne verwertbare Informationen. Diese Leute wollten bezahlt werden, bevor sie Details weitergeben. Da es aber da keinen „bewiesenen" Fehler gab, war das für uns unmöglich.

Als diese Nachrichten immer zahlreicher wurden, entschieden wir uns, ein Bug Bounty-Programm zu starten, um diese Art von Meldungen zu kanalisieren und zu institutionalisieren.

Wir haben verschiedene Bug Bounty-Plattformen in Europa verglichen und uns für YesWeHack entschieden, vor allem aus regulatorischen und datenhoheitlichen Gründen. Ein weiteres Entscheidungskriterium war die Anzahl der aktiven Hacker auf der Plattform: es lohnt sich nicht, Geld und Energie in ein Bug Bounty-Programm zu stecken, wenn es nicht genügend Hacker gibt, die effektiv nach Schwachstellen zu suchen.

Gleichzeitig haben wir die security.txt auf unserer Webseite integriert, um Hacker auf die YesWeHack-Plattform zu leiten, da ein Bug Bounty -Programm eine gute Möglichkeit ist, CVD (Coordinated Vulnerabilities Disclosure) zu fördern.

"Wir haben verschiedene Bug Bounty-Plattformen in Europa verglichen und uns für YesWeHack entschieden, vor allem aus regulatorischen und datenhoheitlichen Gründen.

KÖNNEN SIE DEN VERLAUF IHRES PROGRAMMS VON ANFANG AN BESCHREIBEN?

ALAIN TIEMBLO:

Wir haben unser privates Programm Ende 2017 gestartet. Wichtig war dabei die Anlaufphase, denn gleich bei Programmstart erhielten wir sehr viele Berichte, mit deren Hilfe wir unser Programm präzisieren konnten; so konnten wir etwa unsere Arbeitsbereiche und die Art der Schwachstellen, die gemeldet werden sollten, besser definieren.

Von Anfang an erhielten wir „echte" und potenziell kritische Schwachstellen, die uns von der Relevanz des Modells und der Wirksamkeit der Plattform überzeugten.

Nach einer Woche begann die Gesamtzahl der Berichte abzunehmen. Dafür wurden die Berichte, die eintrafen, immer interessanter, weil die Hacker in unser Produkt „eindrangen" und Berichte produzierten, die wirklich spezifisch für unser Business waren.

Nach dem ersten Monat wurde es ruhiger, so dass wir neue Hacker in das Programm einluden, um einen frischen Blick und neue Fähigkeiten zu bestimmten Aspekten zu bekommen.

Mit dem privaten Bug Bounty-Programm hat unser Team auch gelernt, wie man Berichte verwaltet, klassifiziert und qualifiziert und wie man die Programmregeln anpasst.

Sieben Monate nach Start des privaten Programms beschlossen wir, auf ein öffentliches Programm umzusteigen. Wir wollten einfach mehr Forscher in unserem Programm haben. Da wir mit der Kommunikation und dem Austausch mit den Hackern während der privaten Phase sehr zufrieden waren, waren wir zuversichtlich, dass der Übergang klappt.

Zudem wollten wir eine Botschaft an die Community senden: Jeder, der eine Schwachstelle findet, kann sie uns öffentlich melden! Natürlich erhielten wir nach der Umstellung auf ein öffentliches Programm mehr Berichte, aber es war sehr überschaubar.

ANTONIN LE FAUCHEUX, CISO BEI BLABLACAR:

Heute streben wir nach Qualitätsberichten über immer komplexere Schwachstellen, die mehr Einsatzzeit für Hacker erfordern und vor allem sehr erfahrene Hacker ansprechen. Deshalb haben wir unsere Belohnungen für kritische und hohe Schwachstellen deutlich erhöht. Heute besteht unsere Herausforderung darin, mit Unterstützung von YesWeHack wertvolle Schwachstellen aufzudecken, ohne dass unser Belohnungsbudget „explodiert".

IM VERGLEICH ZU TRADITIONELLEN LÖSUNGEN WIE PENTESTS?

ANTONIN LE FAUCHEUX:

Für mich hat jedes Tool seinen Nutzen. Der Vorteil von Bug Bounty ist in erster Linie das Crowdsourcing: bei einem Audit stehen ein paar Berater zur Verfügung, während mit Bug Bounty potenziell hunderte oder tausende von Sicherheitsexperten an unserem Programm arbeiten.

Dann gibt es eine beständige Suche an 365 Tagen im Jahr, rund um die Uhr. Ein Pentest hingegen findet normalerweise über einen begrenzten Zeitraum statt und ist eine „Momentaufnahme“. Die Kontinuität von Bug Bounty ist entscheidend, um Fehler so früh wie möglich zu erkennen, da wir unsere Anwendungen sehr häufig aktualisieren.

Ein weiteres wichtiges Unterscheidungsmerkmal ist, dass Bug Bounty ergebnisorientiert ist: Man zahlt nur für das, was man bekommt.

Demgegenüber sind bei Pentests die Geldmittel vergeben, egal ob etwas Nützliches gefunden wird oder nicht. Dies hilft uns auch dabei, uns intern ein Budget für IT-Sicherheit sichern: Wir können erklären, dass wir nur Leute bezahlen, die für uns wichtige Schwachstellen finden, anstatt Auditoren dafür zu bezahlen, um „mal zu sehen“, ob sie etwas finden, ohne Verpflichtung auf Ergebnisse.

Das Bug Bounty-Konzept ist auch eine Message an die Hacker. Immer noch drohen viele Unternehmen damit, Hacker, die Schwachstellen gemeldet haben, strafrechtlich zu verfolgen. Als Folge davon gibt es eine Art Trauma unter ethischen Hackern, die Schwachstellen finden. Sie zögern, die betroffenen Organisationen zu kontaktieren, aus Angst, schlecht behandelt oder gar bestraft zu werden.

Mit unserem öffentlichen Programm senden wir diese sehr starke Message an die Community: Wir möchten, dass ihr uns Fehler meldet und dafür geben wir euch einen legalen und sicheren Rahmen, mit einer vertrauenswürdigen dritten Partei zwischen uns, um sicherzustellen, dass alles glatt läuft.

Wir wollen, dass die Hacker denken: „Ich habe eine Schwachstelle auf BlaBlaCar gefunden und werde für diese Arbeit legal und ohne Risiko belohnt“. Das ist besser, als wenn einige Leute diese Schwachstellen auf dem Schwarzmarkt verkaufen...

BlaBlaCar

WIE GEHEN SIE INTERN MIT DEN FEHLERBERICHTEN UM?

ANTONIN LE FAUCHEUX:

Für die Behandlung von Fehlerberichten ist unser Sicherheitsteam zuständig. Das Team nimmt eine erste Qualifikation vor, um den Schweregrad des Fehlers festzulegen, und entscheidet, ob er sofortige Aufmerksamkeit erfordert oder nicht. Wenn der Fehler komplex ist, besprechen wir ihn mit dem gesamten Team.

Sobald die Schwachstelle intern qualifiziert wurde, wird das betroffene Entwicklerteam über ein von der YesWeHack-Plattform bereitgestelltes Ticketing-System benachrichtigt. Dieses Ticketing-System ermöglicht es uns, den Fortschritt einzelner Teams beim Patching-Prozess zu überwachen und sie bei Bedarf direkt anzusprechen.

Als nächstes kommt die Überprüfung der Korrektur zusammen mit dem Hacker. Oft ist das nur eine Formalität, weil wir uns meistens selbst im Vorfeld überprüft haben. Dennoch ist es immer interessant, den Blick von außen zu haben. Manchmal gibt es Überraschungen und der Hacker sagt uns, dass etwas nicht korrekt repariert wurde.

YES WE HACK

BlaBlaCar

KONNTEN SIE INTERNE VERÄNDERUNGEN IN IHREN TEAMS BEOBACHTEN, SEIT SIE EIN BUG BOUNTY-PROGRAMM GESTARTET HABEN?

ANTONIN LE FAUCHEUX:

Wir berücksichtigen Sicherheitsaspekte heute viel stärker und sprechen in internen Schulungen nicht mehr über potentielle Fehler. Vielmehr zeigen wir konkrete Fälle, die uns im Rahmen unseres Programms aufgezeigt wurden, was viel mehr Wirkung hat.

> **“ Bug Bounty ist über ein Ticketing-System in den Workflow jedes Teams integriert. Die Idee ist, dass Sicherheitslücken Aufgaben wie alle anderen sind, die wir jedem betroffenen Team mit der richtigen Priorität zuweisen.**

WIE PASST BUG BOUNTY IN IHREN AGILEN ANSATZ?

ANTONIN LE FAUCHEUX:

Bug Bounty ist über ein Ticketing-System in den Workflow jedes Teams integriert. Die Idee ist, dass Sicherheitslücken Aufgaben wie alle anderen sind, die wir jedem betroffenen Team mit der richtigen Priorität zuweisen.

Da wir kontinuierlich liefern, macht uns die Fähigkeit, unseren Programmumfang mit einem Klick zu erweitern und Dinge in diesen neuen Bereichen schnell zu erkennen, auch agiler: Sobald eine Anwendung aktualisiert wird, können wir sie testen lassen, die Ergebnisse berücksichtigen und einfach eine Feedback-Schleife einrichten.

WAS IST DER NÄCHSTE SCHRITT IN IHRER BUG BOUNTY-STRATEGIE?

ANTONIN LE FAUCHEUX:

Der nächste Schritt ist die weitere Feinabstimmung unseres Programms, um die Qualität unserer Berichte kontinuierlich zu verbessern und immer bessere Hacker für uns zu gewinnen.

ÜBER

YES WE HACK

YesWeHack wurde 2013 gegründet und ist eine globale Bug Bounty & VDP Plattform.

YesWeHack bietet Unternehmen einen störenden Ansatz für die Cybersicherheit, die Bug Bounty, ein Modell, das Schwachstellenforscher belohnt. Unsere Plattform verbindet mehr als 23.000 Cybersicherheitsexperten („ethische Hacker") in 170 Ländern mit Organisationen aller Größen und Sektoren, um ihre exponierten Bereiche zu sichern und nach Schwachstellen (Bugs) in ihren Websites, mobilen Anwendungen, Infrastrukturen und verbundenen Objekten zu suchen.

YesWeHack verwaltet private (nur mit Einladung) und öffentliche Programme für Tausende von Organisationen weltweit, in Übereinstimmung mit den strengsten europäischen Vorschriften.

Zusätzlich zu seiner Bug Bounty-Plattform bietet YesWeHack auch: Unterstützung bei der Erstellung einer Vulnerability Disclosure Policy (VDP), eine Lernplattform für Ethik-Hacker namens Dojo und eine Schulungsplattform für Bildungseinrichtungen, YesWeHackEDU.

⟶ KONTAKTIERE UNS

⟶ BESUCHEN SIE UNSERE WEBSEITE

BlaBlaCar