YES WE HACK

yousign

YOUSIGN

Privates Bug-Bounty-Programm

ANWENDERBERICHT

WARUM HABEN SIE SICH FÜR BUG BOUNTY ENTSCHIEDEN?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

Es gibt ja viele Plattformen, hauptsächlich in den USA. Wir wollten aber gewisse Garantien von den ethischen Hackern, die wir zu unseren Programmen einladen. Und YesWeHack konnte uns diese Garantien geben. Das sorgte für das nötige Vertrauen, um ein Bug-Bounty-Programm zu starten.

WELCHEN WERT BRINGT BUG BOUNTY GEGENÜBER HERKÖMMLICHEN CYBER-SICHERHEITSLÖSUNGEN WIE PENTESTS?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

Mit Bug Bounty profitieren wir von einem breiten Qualifikationsspektrum und unterschiedlichsten Sichtweisen. Jeder Hunter hat seine eigene Vorgehensweise – einen einzigartigen Ansatz, der einen bestimmten Angriff ausmacht. Das unterscheidet Bug Bounty von Penetrationstests und stellt eine viel größere Herausforderung dar. Mit Bug Bounty haben wir die Pentest-Welt hinter uns gelassen, um von 10, 20 oder 30 verschiedenen Perspektiven zu profitieren und unsere Teams wirklich zu fordern.

Interessant ist auch, dass nicht alle ethischen Hacker unbedingt Cybersecurity-Experten sind. Das gesamte Ökosystem ist vertreten und wir können einzelne Hunter nach Nationalität, Fähigkeiten und ihrem Ranking auf der Plattform auswählen.

Der größte Nutzen von Bug Bounty ist jedoch die Kontinuität, die Wiederholung und die Testkosten: Sobald wir eine neue Version veröffentlichen, integrieren wir das bestehende Programm und erhalten sofort Feedback zur Sicherheit der neuen Version. Wir müssen nicht erst ein Jahr auf den nächsten Pentest warten, um die Sicherheit unseres Updates zu überprüfen. Dieser Ansatz ist stattdessen in unseren Projektlebenszyklus eingebettet.

Unser Testumfang entwickelt sich ständig weiter – und die Bugs auch. Sicherheitslücken kommen jeden Tag dazu, nicht nur einmal im Jahr. Und dank Bug Bounty können wir sie rechtzeitig erkennen und schließen. So können wir unsere Dienste fast ständig überwachen, was sehr beruhigend ist. Es wäre auch finanziell nicht tragbar, bei jeder Bereitstellung einen Pentest durchzuführen, obwohl wir es eigentlich müssten.

Man bekommt einfach unglaublich viel fürs Geld. Yousign führt jedes Jahr einen Penetrationstest durch. Und das ist ziemlich teuer verglichen mit einem Bug-Bounty-Programm. Genau betrachtet ist das schon ein bisschen irre: Beides kostet ungefähr das gleiche, aber beim Bug Bounty wird das ganze Jahr hindurch getestet, beim Audit nur eine Woche.

yousign

BEDEUTEN BUG-BOUNTY-PROGRAMME DAS ENDE VON PENTESTS? ODER WERDEN SIE SICH WEITERHIN ERGÄNZEN?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

Bei Yousign setzen wir weiterhin beides ergänzend ein. In manchen Branchen könnte es das Ende von Penetrationstests bedeuten, in unserer jedoch nicht: Als Trusted Third-Party Provider sind wir zu regelmäßigen Audits verpflichtet. In einem weniger strengen regulatorischen Umfeld würde ich wahrscheinlich nur noch auf Bug Bounty setzen.

Das Bug-Bounty-Programm ist zudem sehr wichtig für unseren Vertrieb und unser Marketing: Es ist eindeutig ein Alleinstellungsmerkmal bei großen potenziellen Kunden. Wir weisen bei jedem Angebot und in jeder Ausschreibung explizit darauf hin, weil es im Markt als eine Art Gütesiegel für hohe Qualität gilt.

WIE LASSEN SICH DIE ERGEBNISSE VON PENTESTS UND BUG BOUNTY VERGLEICHEN?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

Zwar erhalte ich ähnliche Berichte, aber Bug Bounty sind es viel mehr als nach einem Penetrationstest. Dazu kommt, dass – wenn wir nach einem Pentest für den identischen Testumfang ein Bug Bounty machen – immer weitere Sicherheitslücken entdeckt werden.

Ein Problem von Penetrationstest ist, dass die Ergebnisse stark vom Fachwissen des Pentesters abhängen. Unser letzter Pentest hat einige relevante Dinge aufgezeigt. Vergleicht man aber die Ergebnisse mit dem anschließenden Bug-Bounty-Programm, war das nur die Spitze des Eisbergs.

“ Wenn wir nach einem Pentest für den identischen Testumfang ein Bug Bounty machen – immer weitere Sicherheitslücken entdeckt werden.

HAT SICH ETWAS BEI IHREN TEAMS VERÄNDERT, SEIT SIE BUG-BOUNTY-PROGRAMME NUTZEN?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

Auf jeden Fall. Anfangs habe ich allein die Programme betreut, dann aber schon bald die Entwicklerteams einbezogen, damit sie die Prozesse selbst erledigen können, wie z. B. Huntern direkt antworten oder Bugs beheben. Die meisten Berichte betrafen das Anwendungsteam, also mussten sie sich den Tatsachen stellen und besser werden.

Auch bemerkten wir bald, dass ihre Interaktionen mit den Huntern sich auf ihre Ergebnisse und Arbeitsweisen auswirkten: Die Sicherheit ist jetzt nicht nur effektiver in die Entwicklung integriert, auch die Denkweisen haben sich geändert – man behält jetzt die Security stets im Hinterkopf. Man könnte sagen, dass sie es nicht nur den Kunden, sondern auch den Huntern recht machen wollen.

WAS KOMMT ALS NÄCHSTES?

KEVIN DUBOURG, BUG BOUNTY PROGRAM MANAGER, YOUSIGN:

Der nächste Schritt besteht darin, Bug Bountys noch stärker einzusetzen. Neben den aktuellen Programmen in unseren Produktions- und Staging-Umgebungen wollen wir Bug Bountys auch in unseren CI/CD-Workflow einbetten, um unsere zahlreichen Funktions- und Unit-Tests zu erweitern. Das dürfte uns noch agiler machen. Bug Bounty ist zweifellos ein wichtiger Bestandteil unseres CI/CD-Ansatzes.

Vielleicht werden wir mit der Zeit auch zu einem öffentlichen Programm wechseln.

ÜBER

YES WE HACK

YesWeHack wurde 2015 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 25.000 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

yousign