FALLSTUDIE

OVHcloud

ÖFFENTLICHES BUG BOUNTY PROGRAMM

Mai 2020

YES WE HACK

Können Sie uns sagen, was Sie dazu bewogen hat, ein Bug-Bounty Programm einzuführen?

Julien Levrard, Verantwortlicher für Konformität und Sicherheit:

Historisch gesehen ist Sicherheit ein Teil der DNA von OVHcloud. Es ist inhärent in unserem Geschäft als Infrastrukturanbieter und in allen Dienstleistungen, die wir anbieten.

Das hohe Sicherheitsniveau unserer Infrastruktur muss eine ständige Forderung und für unsere Kunden ein Motor des Vertrauens sein. Es basiert auf physischen und logischen Schutzmaßnahmen und Kontrollaktivitäten, Scans, internen und externen Eindringungstests, Codeüberprüfungen, Konfigurationsüberprüfungen und mehr. Einige dieser Maßnahmen werden fortlaufend von unseren Teams durchgeführt, andere beruhen auf der Zusammenarbeit mit vertrauenswürdigen Dritten.

Wir haben vor einigen Jahren ein Bug-Bounty-Programm mit YesWeHack gestartet, um eine weitere Sicherheitsebene zu unseren bestehenden Systemen hinzuzufügen.

Wir sehen gemeinsame Werte unserer Unternehmen, entwickeln im gleichen Ökosystem, teilen die gleiche Leidenschaft und die gleichen europäischen Wurzeln. Teilweise haben wir aus diesen Gründen mit dieser Plattform begonnen – wir waren einer der ersten Kunden von YesWeHacks öffentlichem Programm und haben unser Programm bei einer live Bug Bounty in der "Nacht des Hacks" gestartet.

Erhöht Bug Bounty das Vertrauen Ihrer Kunden?

Ja, das tut es. OVHcloud arbeitet mit verschiedenen Arten von Kunden zusammen. Einige von ihnen betreiben ihre Infrastruktur selbst und sind sehr empfindlich gegenüber technischer Kommunikation. Unsere Kommunikation basiert daher auf Transparenz und Informationstiefe.

Andere Kunden sind wachsamer in Bezug auf unsere Fähigkeit, vertrauenswürdige Dritte wie Zertifizierungsprüfer oder externe Dienstleister einzubeziehen. **Die Bug Bounty ist daher ein zusätzliches Vertrauenselement für einige unserer Kunden, die mehr als herkömmliche Sicherheitsmittel verlangen.**

YesWeHack arbeitet mit großen, sensiblen und «souveränen» französischen Unternehmen wie Betreibern wichtiger Infrastruktur zusammen, und wir positionieren uns in diesem Markt. **Bug Bounty mit YesWeHack ist eines der Elemente dieses vertrauenswürdigen Ökosystems und wird zu einem « Must-Have » für Organisationen wie die unsere.**

Und es ist auch eine Frage des Images gegenüber der Forschungsgemeinschaft, die Teil dieses Ökosystems ist: Durch YesWeHack können wir mit Menschen interagieren, die über andere Kanäle nicht unbedingt zugänglich sind.

Was bietet Ihnen ein Bug-Bounty-Programm im Vergleich zu den oben erwähnten Mitteln (Audits, Scans, Eindringtests usw.)?

Ein Bug-Bounty Programm bringt uns mit Experten in Kontakt, die unsere Teams in Bezug auf die ganze Vielfalt der von uns verwendeten Technologien ergänzen: OpenStack, Kubernetes, Machine Learning Tools, KI und so weiter. **Es ist unmöglich, ein Team von Pentestern mit fortgeschrittenen Fähigkeiten in all diesen Technologien zu finden.** Mit YesWeHack haben wir leichten Zugang zu Experten in diesen verschiedenen Technologien, die sagen: *«Ich bin ein Kubernetes-Experte, also werde ich mir alle Bounty-Bug-Programme anschauen, zu denen es Kubernetes-Angebote gibt, um das Thema zu vertiefen.»* **Dies vervollständigt unseren Sicherheitsansatz wirksam, indem es eine komplementäre Sichtweise zu der unserer Teams bringt.**

Ein weiterer sehr wichtiger Punkt ist, dass Bug Bounty einen formalen Rahmen für die Schwachstellenberichte bietet und es uns ermöglicht, ethischen Hackern einen rechtlich sicheren Einstiegspunkt zu bieten. Dies ist zwar nicht der einzige Kanal für die Schwachstellenberichte bei OVHcloud, aber wir empfehlen, dass Personen, die Schwachstellen identifizieren, unser Programm durchlaufen.

Dies ermöglicht uns einen einzigen eingehenden Fluss und einen damit verbundenen Prozess für das Management von Schwachstellenberichten. Sie ist daher ein strukturierendes Element unserer Coordinated Vulnerability Disclosure.

Abgesehen von den Vorteilen des Bug Bounty als Modell, möchte ich die **YesWeHack-Plattform hervorheben, die sehr bequem ist und über eine einfach zu bedienende Benutzeroberfläche verfügt. Das OVHcloud-Team, das Bug Bounty verwaltet, gibt uns ausgezeichnetes Feedback zum Workflow-Management, zur Handhabung von Berichten und zur Interaktion mit Forschern.**

Die APIs ermöglichen es uns, alle nützlichen Informationen automatisiert in unsere eigenen Tools und Dashboards zu integrieren und auch unser Vergabebudget oder die Aktivität jedes Programms zu verfolgen.

Auf einen Blick können wir den Status unserer Programme erkennen und unserem Management Indikatoren präsentieren: **Bug Bounty ist vollständig in unsere Strategie und das Management unserer globalen Sicherheit integriert.**

Wie passt Bounty Bug in Ihre agilen Vorgangsweise?

Unser Bug-Bounty Programm wird von unserem Pentester-Team betrieben: Zwei Manager sind für das Programm sowie für die Animation der Hacker community verantwortlich. Dann nehmen sie Kontakt zu den verschiedenen Teams auf, die von den Schwachstellen betroffen sind, damit wir sie in unsere Managementsysteme integrieren und sicherstellen können, dass sie behoben werden.

Sobald die Schwachstellen über die Plattform gefunden wurden, werden sie in unsere Prozesse integriert: Wir verfügen im Rahmen der ISO 27001-Zertifizierung über einen organisatorischen Mechanismus, der Sicherheitsmanagementsystem genannt wird – einschließlich der Prozesse, Rollen und Verantwortlichkeiten, die dokumentiert sind und sicherstellen, dass jede Schwachstelle, jeder Vorfall und jede potenzielle Bedrohung von unseren Teams behandelt und im Laufe der Zeit überwacht wird und Gegenstand eines präzisen Aktionsplans ist, dessen Anwendung – je nach Empfindlichkeit des betreffenden Produkts und des damit verbundenen Anforderungsniveaus – überprüft wird.

Dank der YesWeHack-API haben wir die Schwachstellenberichte leicht in diesen Prozess integriert: alles wird über Tickets verwaltet, die in unseren Dashboards eingesehen und bei Bedarf von unseren externen Auditoren abgerufen werden können.

Sie sind in einem öffentlichen Programm. Wie läuft der Informationsaustausch mit der Hacker-Community?

Die Verwaltung eines Bug Bounty-Programms ist eine echte Verpflichtung gegenüber allen Interessengruppen, die sich dafür einsetzen, das Internet sicherer zu machen. Wir haben die Verantwortung, bei der Behandlung und Behebung der uns zur Kenntnis gebrachten Schwachstellen rigoros und transparent vorzugehen

Was die Dinge einfacher macht, ist, dass die Plattform die Beziehung zwischen Kunden und Forschern sowohl rahmt als auch erleichtert – mit einem sehr reichen und direkten Informationsaustausch.

Wir befinden uns in einem Verhältnis, in der wir offen über die Ergebnisse diskutieren. Auch darüber, wie eine Schwachstelle zu analysieren ist. Wir haben einen sehr produktiven Informationsaustausch, den wir mit keinem anderen Mittel erreichen können.

Nächste Schritte?

Wir arbeiten an den Tickets, die von den Schwachstellenberichten generiert werden, um sie auf standardisierte Weise in unser globales Risikomanagementmodell zu integrieren. Ziel ist es, in der Lage zu sein, unser Risikomanagement unabhängig von der Informationsquelle – nachgewiesener Vorfall oder Schwachstellenbericht – zu standardisieren. Ziel ist es daher, alle Möglichkeiten der API auszuschöpfen, um die Verarbeitung von Berichten weiter zu automatisieren.

Wir haben auch bestimmte Forscher identifiziert, die in unserem öffentlichen Programm besonders erfolgreich sind, mit denen wir ausgezeichnete Beziehungen pflegen oder die über sehr spezifische Fähigkeiten verfügen, um sie zu Programmen einzuladen, die bestimmten Produkten gewidmet sind. Das soll noch in diesem Jahr geschehen.

Über YesWeHack : YesWeHack ist Europas führende Bug-Bounty-Plattform. Die Plattform bringt Unternehmen, die Sicherheitslücken in ihrer digitalen Infrastruktur schließen wollen, mit über 15.000 ethischen Hackern, bezeichnet als "Hunter", zusammen. Die Hunter gehen nach den Regeln und Vorgaben des Kunden vor und werden ergebnisbasiert bezahlt. Neben der Bug Bounty Plattform bietet YesWeHack eine Stellenbörse für IT-Sicherheitsexperten. Ein gemeinnütziges Forum zur koordinierten Aufdeckung von IT-Sicherheitslücken (zerodisclo.com) sowie der Bug-Bounty-Aggregator FireBounty.com gehören außerdem zum Angebot. Unternehmen und Organisationen wie Deezer, BlaBlaCar, der Flughafen Paris und das französische Verteidigungsministerium vertrauen auf YesWeHack. Gegründet wurde YesWeHack 2013 in Frankreich. Hauptfirmensitz ist Paris. Mehr Informationen unter www.yeswehack.com