
YES WE HACK
OVHcloud
OVHCLOUD
Öffentliches Bug-Bounty-Programm
ANWENDERBERICHT

WARUM HABEN SIE EIN BUG-BOUNTY-PROGRAMM GESTARTET?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

Die Sicherheit steht bei OVHcloud seit jeher im Mittelpunkt. Für uns als Infrastrukturanbieter ist sie ein integraler Bestandteil unseres Geschäfts und sämtlicher Dienstleistungen. Eine sichere Infrastruktur ist für uns ein Muss und bildet zugleich die Grundlage für das Vertrauen unserer Kunden. Diese Sicherheit basiert auf physischen und logischen Schutz- und Kontrollmaßnahmen, internen und externen Pentests sowie Überprüfungen von Code und Konfigurationen. Um einen Teil der Security kümmern sich unsere Teams ständig, den Rest übernehmen vertrauenswürdige Partner.

Wir haben vor Jahren ein Bug-Bounty-Programm für OVH bei YesWeHack begonnen, um unsere Systeme um eine zusätzliche Sicherheitsstufe zu erweitern. Unsere Unternehmen teilen die gleichen Werte, die gleiche Passion und das gleiche Ökosystem – und wir haben beide europäische Wurzeln. Nicht zuletzt aus diesen Gründen haben wir uns für YesWeHack entschieden. Und so hatten wir als eines der ersten Unternehmen ein öffentliches Programm bei YesWeHack, das wir bei einer Live Bug Bounty in der „Nuit du Hack“ (Hacking-Nacht) starteten.

STÄRKT BUG BOUNTY DAS VERTRAUEN IHRER KUNDEN?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

Definitiv. OVHcloud arbeitet mit verschiedenen Arten von Kunden zusammen: Einige betreiben ihre Infrastruktur selbst, andere haben hohe Standards für technische Informationen. Transparenz und Verlässlichkeit sind daher die Grundlage unserer Kommunikation. Andere Kunden legen Wert darauf, dass wir vertrauenswürdige Dritte wie Zertifizierungs-Auditoren oder externe Dienstleister einbeziehen. Bug Bounty bietet Kunden, die mehr als die üblichen Sicherheitsmaßnahmen verlangen, ein zusätzliches Vertrauenselement.

YesWeHack arbeitet mit großen strategischen Marktakteuren wie kritischen Infrastrukturbetreibern zusammen – genau wie wir. Bug Bounty mit YesWeHack ist ein Element dieses vertrauenswürdigen Ökosystems und wird zu einem „Must-Have“ für Unternehmen wie uns. Es ist aber auch eine Image-Frage gegenüber der Hunter-Community, die Teil dieses Ökosystems ist: Über YesWeHack können wir uns mit Menschen austauschen, zu denen wir sonst kaum Kontakt hätten.

> **Ein Bug-Bounty-Programm bringt uns mit Experten zusammen, die unsere Teams bei unserem gesamten Technologie-Spektrum ergänzen.**

WELCHE VORTEILE BIETET IHNEN BUG BOUNTY GEGENÜBER ANDEREN SICHERHEITSPRÜFUNGEN WIE AUDITS, SCANS ODER PENTESTS?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

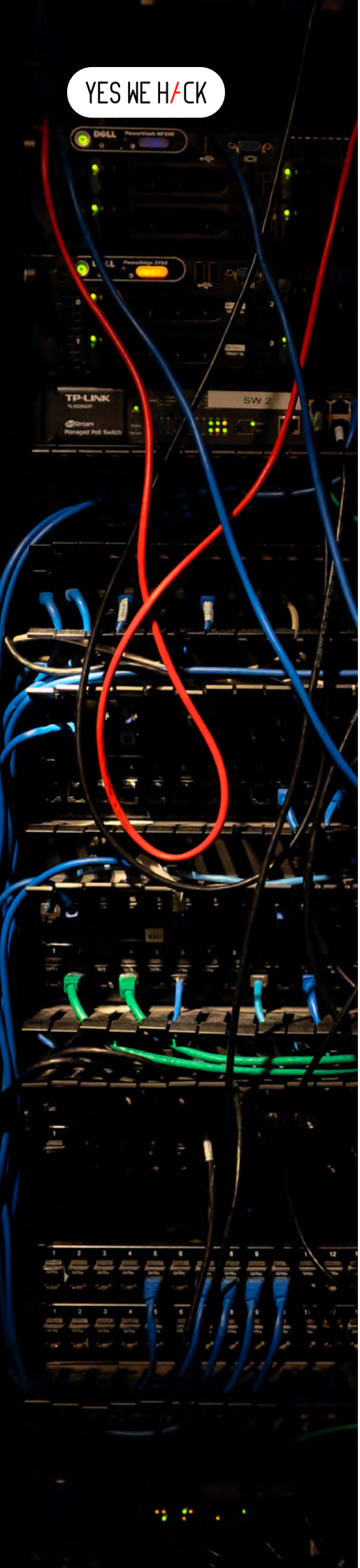
Ein Bug-Bounty-Programm bringt uns mit Experten zusammen, die unsere Teams bei unserem gesamten Technologie-Spektrum ergänzen – wie OpenStack, Kubernetes, maschinelles Lernen oder KI. Ein Pentester-Team mit einer solchen Fachkompetenz für all diese Technologien gibt es einfach nicht.

Mit YesWeHack haben wir einen unkomplizierten Zugang zu Experten für verschiedenste Technologien – z. B. zu Kubernetes-Spezialisten, die sich die Bug-Bounty-Programme für Kubernetes herauspicken und sich da richtig gut auskennen. Das ist eine sinnvolle Ergänzung unseres Security-Ansatzes, die unseren Teams neue Sichtweisen eröffnet.

Bug Bounty bietet uns zudem einen offiziellen Rahmen für Schwachstellen-Berichte. So können wir ethischen Hackern rechtlich einen sicheren Einstiegspunkt bieten. Das ist zwar nicht die einzige Möglichkeit, wie man OVHcloud über Schwachstellen informieren kann. Aber wir empfehlen allen, die eine Sicherheitslücke entdecken, sie über unser Programm zu melden. So erhalten wir alles über eine zentrale Stelle und können die Schwachstellen-Berichte dann weiterleiten. Bug Bounty ist damit ein zentrales Element unserer koordinierten Offenlegung von Schwachstellen (Coordinated Vulnerability Disclosure, CVD).

Neben den grundlegenden Vorteilen des Bug-Bounty-Modells bietet YesWeHack eine äußerst intuitive Benutzeroberfläche. Das OVHcloud-Team, das unser Bug-Bounty-Programm betreut, ist vom Workflow-Management, der Handhabung von Berichten und dem Austausch mit Huntern begeistert.

Über die APIs können wir alle nützlichen Informationen automatisch in unsere Tools und Dashboards integrieren und auch unser Budget für Belohnungen und die Aktivität bei unseren Programmen verfolgen. Wir sehen den Status unserer Programme auf einen Blick und können dem Management schnell Kennzahlen vorlegen. Bug Bounty ist vollständig in unsere globale Security-Strategie integriert.



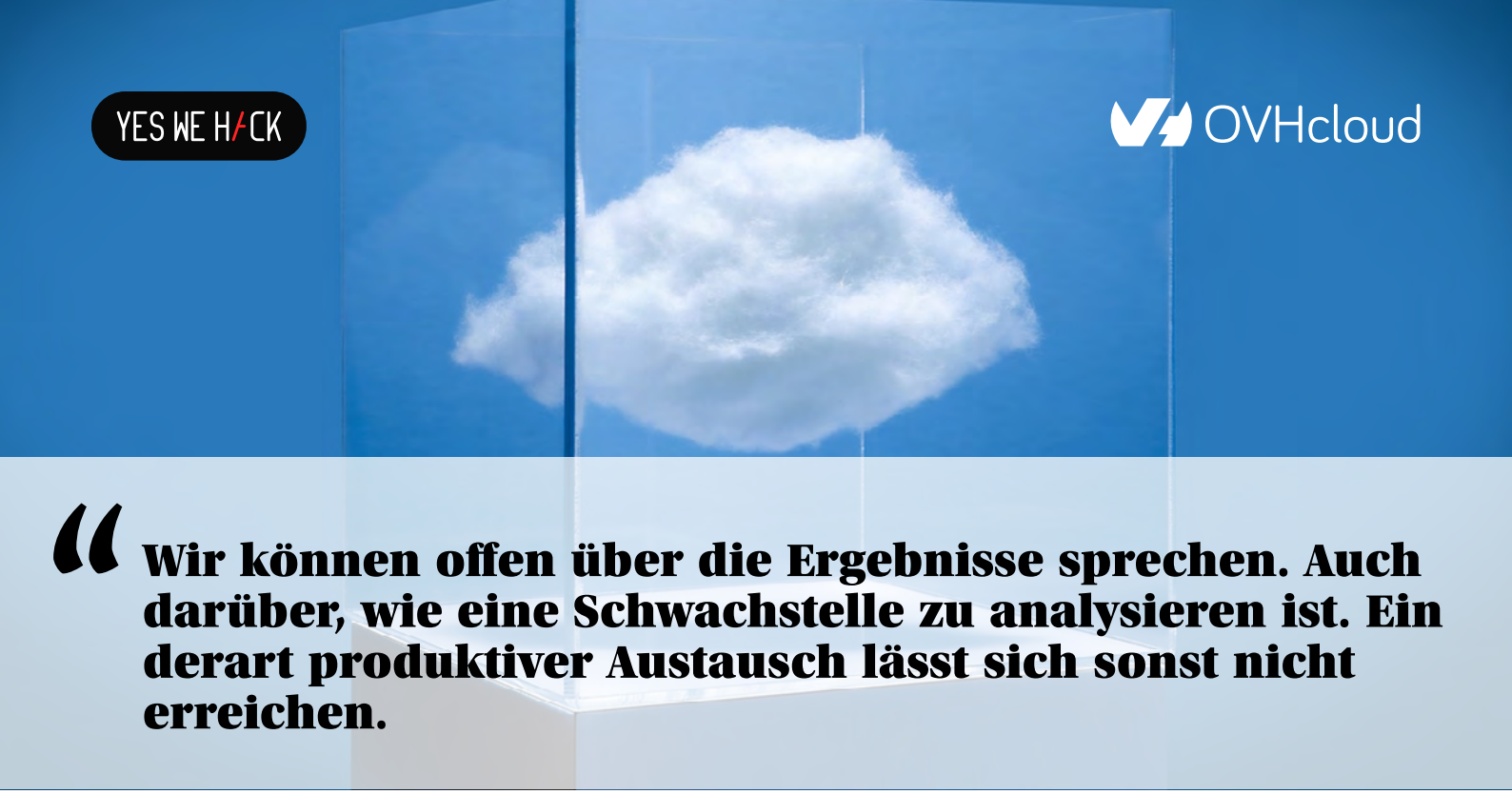
OVHcloud

WELCHE ROLLE SPIELT BUG BOUNTY FÜR IHRE AGILE ENTWICKLUNG?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

Unser Pentester-Team leitet auch das Bug-Bounty-Programm: Zwei Manager sind für das Programm sowie für die Zusammenarbeit mit der Hunter-Community zuständig. Bei Schwachstellen arbeiten sie mit den betroffenen Teams zusammen, damit wir alles in unseren Management-Systemen erfassen und sicher wissen, dass Sicherheitslücken geschlossen wurden.

Werden Schwachstellen über die Plattform gefunden, integrieren wir sie in unsere Prozesse: Wir haben dafür extra ein Security-Management-System als Teil unserer ISO 27001-Zertifizierung. Alles wird dokumentiert – Prozesse, Rollen und Zuständigkeiten. So wird sichergestellt, dass unsere Teams jede Schwachstelle, jeden Vorfall und jede potenzielle Bedrohung bearbeiten und langfristig im Auge behalten. Das alles fließt auch in unseren konkreten Aktionsplan ein, der wiederum von den Sicherheitsanforderungen des jeweiligen Produkts abhängt. Dank der YesWeHack-API haben wir die Bug-Bounty-Berichte einfach in diesen Prozess integriert: Alles wird über Tickets verwaltet, die in unseren Dashboards eingesehen und auch von externen Auditoren abgerufen werden können.



> **Wir können offen über die Ergebnisse sprechen. Auch darüber, wie eine Schwachstelle zu analysieren ist. Ein derart produktiver Austausch lässt sich sonst nicht erreichen.**

WIE FUNKTIONIERT DER AUSTAUSCH MIT DEN HUNTERN BEI IHREM ÖFFENTLICHEN PROGRAMM?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

Das Management eines Bug-Bounty-Programms ist zugleich eine Verpflichtung gegenüber allen Beteiligten, die sich für eine bessere Online-Sicherheit einsetzen. Wir sehen es als unsere Pflicht, bei der Handhabung und Behebung von gemeldeten Schwachstellen rigoros und transparent vorzugehen. Das wird durch den Rahmen erleichtert, den die Plattform für die Beziehungen zwischen Kunde und Huntern bietet – sie ermöglicht einem intensiven, direkten Austausch. Wir können offen über die Ergebnisse sprechen. Auch darüber, wie eine Schwachstelle zu analysieren ist. Ein derart produktiver Austausch lässt sich sonst nicht erreichen.

WAS KOMMT ALS NÄCHSTES?

JULIEN LEVRARD, SECURITY OPERATIONS MANAGER, OVHCLOUD:

Wir arbeiten derzeit an der standardisierten Integration der Tickets, die nach Schwachstellen-Berichten erstellt werden, in unser globales Risiko-Management-Modell. Wir wollen so unser Risikomanagement unabhängig von der Informationsquelle vereinheitlichen – also unabhängig davon, ob es sich um einen tatsächlichen Vorfall oder einen Schwachstellen-Bericht handelt. Das Ziel ist es, das volle Potenzial von APIs auszuschöpfen, um das Reporting noch stärker zu automatisieren.

Auch wissen wir aus unserem öffentlichen Programm, welche Hunter spezielle Fähigkeiten besitzen oder besonders erfolgreich sind. Zu diesen Experten haben sehr gute Beziehungen und wollen sie wahrscheinlich noch dieses Jahr zu Programmen für bestimmte Produkte einladen.

ÜBER

YES WE HACK

YesWeHack wurde 2015 gegründet und ist eine globale Bug Bounty & VDP Plattform.

YesWeHack bietet Unternehmen einen innovativen Ansatz für die Cybersicherheit, die Bug Bounty, ein Modell, das Schwachstellenforscher belohnt. Unsere Plattform verbindet Zehntausende 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

OVHcloud