YES WE HACK

INTERNATIONALE LUXUSMARKE

Privates Bug-Bounty-Programm

ANWENDERBERICHT

KONTEXT

- Schnelles Umsatzwachstum durch digitale Kanäle
- Zunehmende Cyber-Angriffe in den letzten neun Monaten

AGILES UNTERNEHMEN

- Skalierbares agiles Framework
- DevSecOps-Plattform (für kontinuierliche Integration)
- Weltweites SOC-Team, 24/7 im Einsatz

HERAUSFORDERUNGEN

- Abstimmen der Security mit der agilen Entwicklung sowie dem zweiwöchentlichen Release-Zyklus
- Audits können bis zu einem Monat dauern, sind aber immer noch nicht gründlich genug
- Unsystematische Meldung von Sicherheitslücken über verschiedene Kanäle

SOLUTION

- Privates Bug-Bounty-Programm von YesWeHack
- Gemeinsame Entwicklung einer Richtlinie zur Offenlegung von Sicherheitslücken (VDP) mit YesWeHack

Unser Kunde, ein internationales Unternehmen aus der Luxusbranche, stand vor einer Herausforderung, die viele CISOs kennen.

Der Kunde erlebte einen massiven Anstieg von Cyberangriffen (über eine Million in den letzten neun Monaten), der hauptsächlich auf die zunehmende Digitalisierung des Unternehmens zurückging. Diese digitale Strategie umfasst mehr als eine Milliarde Webseiten, Cloud-Erweiterungen, die Öffnung von Informationssystemen sowie die verstärkte Verwendung von APIs – unterstützt durch eine agile Entwicklung mit kontinuierlicher Integration.

Dem Unternehmen war klar: Der allgegenwärtige digitale Wandel erforderte eine höhere Sicherheit. Benötigt wurde eine moderne, effiziente Sicherheitslösung, mit der sich die Cyber-Security besser in den Griff bekommen ließ. Zugleich sollte das neue Modell agil, innovativ und effektiv sein, da alle 15 Tage neue Releases herauskommen.

Es war Zeit für Veränderung und Fortschritt. Nach Beratungen mit verschiedenen Anbietern entschied sich die weltbekannte Luxusmarke für YesWeHack, um eine Crowdsourcing-Sicherheitsstrategie umzusetzen und eigene Bug-Bounty-Programme zu starten.

Lesen Sie im Folgenden, wie das Unternehmen die Crowdsourcing-Sicherheitsstrategie anging, sie weiterentwickelte und was für die Zukunft geplant ist.

VORGEHENSWEISE UND RAMP-UP

1 DEFINITION DER PROGRAMME

Unser Kunde startete zunächst zwei private Bug-Bounty-Programme: eines für die speziellen Infrastrukturen in China und im APAC-Raum, das andere für den „Rest der Welt". Die Programme umfassten ein Dutzend URLs, mehrere Anwendungen und einige Backend-APIs.

Beim Budget und der Höhe der Belohnungen richtete sich der Kunde nach der Empfehlung von YesWeHack, mit einem Budget von 15.000 € „klein anzufangen". Auch stimmte man unserem Vorschlag zu, pro Bericht eine Belohnung von 100 € bis 1000 € auszusetzen.

„Im Gegensatz dazu, was US-Anbieter erzählen, kann man ein Bug-Bounty-Programm auch mit einem kleinen Budget starten." Stellvertretender CISO einer internationalen Luxusmarke

⟶ TIPP VOM KUNDEN

Nutzen Sie die Kompetenz und Beratung von YesWeHack, um den Umfang und die Staffelung der Belohnungen festzulegen.

2 AUSWAHL DER HUNTER

Für China benötigte unser Kunde lokale Hunter, die Mandarin beherrschen. Zudem verlangte die spezielle Art der Anwendungen, der einzigartige Handels- und Kaufansatz sowie die grundlegend anderen Tools als in Europa und den USA, dass diese ethischen Hacker mit den lokalen Gepflogenheiten des Landes vertraut waren.

YesWeHack fand für den Kunden ein Hunter-Team, das diese Erwartungen perfekt erfüllte.

⟶ TIPP VOM KUNDEN

Lassen Sie sich von YesWeHack bei der Auswahl der Hunter für die erste Runde unterstützen.

3 PROGRAMMSTART

Der erste Bericht traf innerhalb von 30 Minuten nach dem Start des Programms ein. Nach nur vier Stunden lagen mehr als acht Berichte vor, die auf eine kritische Sicherheitslücke und zwei allgemeine Schwachstellen hinwiesen.

⟶ TIPP VOM KUNDEN

1. *Starten Sie Ihr Bug-Bounty-Programm nicht kurz vor Feierabend, wenn Sie nachts schlafen wollen.*

2. *Schnell reagieren ist wichtig: Hunter sind motivierter, engagierter und beteiligen sich länger aktiv an Ihrem Programm, wenn Sie baldmöglichst antworten. Unser Ziel ist eine Rückmeldung zu den erhaltenen Berichten innerhalb von drei Tagen.*

4 NAHTLOSE INTEGRATION

Um Berichte über Schwachstellen schnell und zuverlässig zwischen den ethischen Hackern und Entwicklungsteams auszutauschen, verwendet unser Kunde den JIRA-Connector von YesWeHack. Tickets werden so direkt an die Teams gesendet, was das Schließen von Sicherheitslücken erleichtert.

Erfahren Sie mehr darüber, wie die Bug-Tracking-Integration von YesWeHack die DevSecOps-Kommunikation und -Zusammenarbeit verbessert.

5 ZWEI MONATE NACH DEM PROGRAMMSTART

Zwei Monate nach dem Start des Bug-Bounty-Programms lagen rund 30 Berichte vor und 60 % der Sicherheitslücken waren behoben. Dank diesem ersten Einsatz des Bug-Bounty-Modells konnte unser Kunde das Ausmaß der Mängel in seiner Infrastruktur erkennen – insbesondere in China. ***„Wir hatten umfangreiche Penetrationstests unserer chinesischen Infrastruktur durchgeführt. Aber dabei konnten nicht die kritischen Sicherheitslücken gefunden werden, die unser Bug-Bounty-Programm aufgedeckt hat."*** Stellvertretender CISO einer internationalen Luxusmarke

AUSBAU DER BUG-BOUNTY-PROGRAMME

Nachdem der Kunde sich mit der Funktionsweise eines Bug-Bounty-Programms vertraut gemacht hatte, beschloss man, den Umfang zu erweitern, die Belohnungen zu erhöhen und neue Hunter einzuladen.

Bei YesWeHack raten wir unseren Kunden immer, klein anzufangen und den Umfang Schritt für Schritt zu erweitern. Diese erste Phase ist nicht nur wichtig, um zu verstehen, wie ethische Hacker arbeiten und wie sie denken, sondern auch, um nicht gleich zu Anfang von einer Flut von Berichten überwältigt zu werden.

NÄCHSTE SCHRITTE

Als weltbekannte Luxusmarke erhält unser Kunde regelmäßig Meldungen zu Sicherheitslücken über unterschiedlichste Kommunikationskanäle, u. a. vom Servicecenter, per E-Mail oder aus sozialen Netzwerken. Dies macht es schwierig, alles zu zentralisieren, an die richtigen Personen weiterzuleiten und Sicherheitslücken nach Schweregrad zu priorisieren.

Um die Meldung Schwachstellen besser zu organisieren, hat unser Kunde mithilfe von YesWeHack eine Richtlinie zur Offenlegung von Sicherheitslücken – kurz „VDP“ für „Vulnerability Disclosure Policy“ – verfasst. So lassen sich

- Anfragen zentralisieren, damit sie intern die richtigen Zuständigen erreichen,
- Fehlalarme reduzieren, da nur Hunter Schwachstellen über ein spezielles, detailliertes Online-Formular melden, und
- Berichtsformate der VDP und des Bug-Bounty-Programms standardisieren, um interne Prozesse zu optimieren und eine umfassende Automatisierung zu ermöglichen.

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