INTERNATIONALE VERSICHERUNGSGRUPPE

Privates Bug-Bounty-Programm

ANWENDERBERICHT

KÖNNTEN SIE SICH KURZ VORSTELLEN?

Ich bin Group CISO eines multinationalen Versicherungsunternehmens. Mein Team ist mit der Aufgabe betreut, einen „Cyber-Schutzschild" für den Konzern und all seine Tochtergesellschaften einzurichten, der neue Sicherheitsleistungen für unsere Tochtergesellschaften umfasst – einschließlich Bug Bounty.

WARUM HABEN SIE BESCHLOSSEN, EIN BUG-BOUNTY-PROGRAMM ZU STARTEN?

Das Thema Bug Bounty kam erstmals bei Gesprächen mit den CISOs großer Finanzinstitute auf. Eine Empfehlung von Unternehmen mit derart hohen Sicherheitsanforderungen gab für meine Entscheidung den Ausschlag. Wir haben klein angefangen – und die Ergebnisse waren überzeugend. Also haben wir nach und nach mehrere Bug-Bounty-Programme gestartet. Das ist ein neuer Ansatz, der mit einer gewissen Lernkurve verbunden ist.

YES WE H/CK

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

Bug Bounty bietet vor allem die Garantie einer kontinuierlichen Überprüfung – nicht nur punktuelle Tests wie bei „klassischen" Penetrationstests. Wenn ich jedes Jahr einen zweiwöchigen Pentest durchführe, sind wir praktisch die restlichen 50 Wochen „ungeschützt", was nicht mehr hinnehmbar ist. Ergänzend können auch automatisierte Tests sinnvoll sein, aber die sind nicht ausgereift genug. Bei Bug Bounty habe ich ethische Hacker, die ständig an den von mir festgelegten Bereichen arbeiten.

Diese Kontinuität ist besonders bei häufigen Bereitstellungen in einem zunehmend agilen Entwicklungskontext wichtig.

Mit Bug Bounty sind wir auch flexibler. Beispielsweise muss ich Umgebungen noch in der Entwicklung oder in der Validierungsphase testen, bevor sie in die Produktion gehen. Dafür immer wieder klassische Pentests zu machen, ist ebenfalls problematisch. Bei der YesWeHack-Plattform können wir die Regeln für jedes Programm, einschließlich der Staffelung der Belohnungen, genau an die Phase jedes Projekts anpassen.

Erwähnenswert ist auch die Reaktionsfähigkeit und Verfügbarkeit: Es wird immer schwieriger – wenn nicht unmöglich – kurzfristig kompetente Pentester zu finden, wenn man sie am dringendsten braucht, also bei einer neuen Release. Bei Bug Bounty ist das mit einem Klick erledigt und das Programm beginnt sofort: Man kann jederzeit Tests durchführen und erhält während des Prozesses sehr schnell die Bestätigung, dass ein Problem behoben ist.

> **“ Bei Bug Bounty ist das mit einem Klick erledigt und das Programm beginnt sofort: Man kann jederzeit Tests durchführen und erhält während des Prozesses sehr schnell die Bestätigung, dass ein Problem behoben ist.**

Überrascht hat uns auch die Vielfalt der gemeldeten Schwachstellen. Wir entdecken immer mehr „Praxisprobleme". Beispielsweise haben Hunter mehrere kleine Schwachstellen gefunden, die in ihrer Gesamtheit unabsehbare Angriffe ermöglicht hätten. Solche Schwachstellen wurde bis dahin nicht angegangen, weil wir darauf nicht hingewiesen wurden. Wir sind jetzt in der Lage, so etwas gründlich zu korrigieren.

Beim Bug Bounty versetzt man sich wirklich in einen Hacker hinein.

BEDEUTET BUG BOUNTY DAS ENDE VON PENTESTS ODER ERGÄNZEN SICH BEIDE?

Für mich ergänzt sich das. Die Realität ist jedoch, dass es zu wenige Prüfungsunternehmen für die Anzahl der notwendigen Audits gibt. Darin liegt der entscheidende Wert von Bug Bounty. Zudem haben Penetrationstests gewisse Grenzen und Einschränkungen: Sie müssen vorab mit einem Start- und Enddatum geplant werden und erfordern ein Projektmanagement. Hier den Zeitplan einzuhalten ist – besonders bei der agilen Entwicklung – wirklich schwierig. Gibt es bei einer Bereitstellung in einem Bereich zwei Tage Verspätung, sind die Pentester nicht mehr verfügbar, was ein echtes organisatorisches Problem darstellt.

Was mir auch an Bug Bounty gefällt, ist die Überprüfung, ob Sicherheitslücken geschlossen wurden. Bei einem normalen Pentest erhält man fast nie eine solche Überprüfung. Wenn mir ein Entwickler nach einem Audit sagt „Ich habe den Fehler behoben", habe ich nur sein Wort. Beim Bug Bounty kann ich diese Kontrolle an den Hunter delegieren, der völlig objektiv ist.

So kann ich eine Schwachstelle beheben und die Korrektur dabei validieren – im Gegensatz zum üblichen Quervergleich, nachdem alle Schwachstellen behoben sind. Wird jetzt eine ernste oder kritische Schwachstelle entdeckt, weiß ich, dass sie schnell behoben ist – und ich kann ruhig schlafen! (Lacht)

YES WE HACK

GAB ES SEIT DEM START DES BUG-BOUNTY-PROGRAMMS NOCH WEITERE VERÄNDERUNGEN?

Das Bewusstsein [für Sicherheitsprobleme] wurde sicherlich geschärft. Aber was mir hauptsächlich auffällt, ist die schnellere Korrekturrate bzw. die Patching-Häufigkeit. Unsere Entwickler beheben Fehler jetzt viel schneller. Um den Huntern zu antworten, sie zu belohnen, Berichte abzuschließen usw. müssen die Entwickler schneller reagieren. Dies wiederum führt zu einer viel kürzeren Zeit bis zur Fehlerbehebung.

UND HINSICHTLICH DER AGILITÄT?

Wie gesagt, wir haben vor einer Release spezielle Programme für Testumgebungen implementiert. Dadurch können wir Schwachstellen frühzeitiger in einem Projekt erkennen und beheben. Erstens lernen unsere Entwickler so während der Arbeit etwas dazu. Zweitens beschleunigt das unsere Bereitstellungen, da wir uns in der Validierungs- und Release-Phase um weniger Patches kümmern müssen.

Wir sind reaktionsschneller geworden, wovon Entwickler und Unternehmen gleichermaßen profitieren.

WAS KOMMT ALS NÄCHSTES?

Unser erster Schritt besteht darin, weitere Assets der Gruppe sukzessive einem Bug Bounty zu unterziehen, und dann in diesen Bereichen schrittweise vom Black-Box- zum Grey-Box-Testing zu kommen.

Im zweiten Schritt – den wir jetzt erreicht haben – wollen wir den Service weltweit bei unseren Tochtergesellschaften einführen. Wir möchten ihnen etwas anderes, etwas Zukunftsorientiertes bieten, damit sie einen neuen Ansatz für die Cybersicherheit und Audits entwickeln können.

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