YES WE H/CK

deezer

DEEZER

Öffentliches Bug-Bounty-Programm

ANWENDERBERICHT

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

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

Vor rund zwei Jahren, bevor wir unser Bug-Bounty-Programm starteten, haben wir mit internen Security-Audits unseren Code überprüft – so etwas hatten wir nie zuvor bei deezer gemacht. Dank dieser Tests konnten wir erstmals einige offensichtliche Sicherheitslücken schließen.

Dann wurden wir auf Bug Bounty und YesWeHack aufmerksam. Die Benutzerfreundlichkeit der Plattform hat uns überzeugt, selbst ein Programm zu starten. Uns wurden sehr schnell interessante Schwachstellen gemeldet. Und weil alles so reibungslos ablief, haben wir den Testumfang sukzessive erweitert.

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

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

Bei einigen unserer Services machen wir jährliche Audits, die ein bis drei Wochen dauern. Aber dieser Ansatz ist teuer, konzentriert sich nur auf wenige Services und liefert auf Dauer keine wirklich interessanten Ergebnisse.

Mit Bug Bounty erhalten wir dagegen das ganze Jahr über ständig Feedback zu verschiedenen Testbereichen und können Bugs sehr schnell erkennen.

> **"Mit Bug Bounty erhalten wir das ganze Jahr über ständig Feedback zu verschiedenen Testbereichen und können Bugs sehr schnell erkennen.**

Bug Bounty rechnet sich auch: Wir legen die Höhe der Belohnung für jede gefundene Schwachstelle selbst fest.

Zudem garantiert uns Bug Bounty, dass die Tester unterschiedlichste Qualifikationen haben. Bei Penetrationstests ist jeder Berater hochspezialisiert. Wir neigen dann eher dazu, Beratern vorzugeben, was wir von dem Pentest erwarten. Bei Bug Bounty waren dagegen einige Berichte der Hunter eine echte Überraschung: Sie lieferten uns völlig neue Ergebnisse für Szenarien, die wir bislang gar nicht bedacht hatten.

Auch schätze ich die Qualität der Berichte, also wie Fehler über YesWeHack gemeldet werden. Man merkt, dass die Hunter wirklich versuchen, einen funktionellen, reproduzierbaren POC [Proof of Concept] anzubieten, den wir leicht erneut testen können.

Die Berichte unserer normalen Audits sind im Allgemeinen recht ausführlich. Mit Bug Bounty erhalten wir eine gleichwertige Qualität, wenn die Hunter gut sind und sich richtig reinhängen.

Es ist extrem hilfreich, wenn wir Berichte mit Screenshots oder Videos erhalten. Das ist dann so viel leichter nachzuvollziehen und zu überprüfen. Auch die Kommunikation mit den betroffenen Teams klappt dadurch besser.

deezer

HELFEN IHNEN DIE HUNTER DABEI, GEMELDETE BUGS ZU ANALYSIEREN UND ZU BEHEBEN?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

Ja, die Hunter helfen uns bei der Reproduktion der Bugs. In einigen Fällen bitten wir sie dann zu prüfen, ob die Schwachstelle behoben wurde. Wir haben auch ein großes internes Entwicklerteam, das sich um das Patch-Management kümmert.

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

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

Für mich sind beide weiterhin eine gute Ergänzung. Bug Bounty bietet eine umfassendere, tiefergehende Prüfung als ein Audit. Wir verwenden Penetrationstests für neue Services oder für Bereiche, bei denen wir bereits wissen, dass es Probleme gibt.

deezer

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

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

Das Sicherheitsbewusstsein ist zweifellos gestiegen. Die Bug-Bounty-Berichte haben uns geholfen, einige wichtige Security-Projekte einzuführen. Unsere Ziele und Einstellung hinsichtlich der Cybersicherheit haben sich weiterentwickelt – und Bug Bounty ist einer der Gründe dafür.

Auch haben wir unseren Prozess zum Erfassen, Sortieren und Valideren von Berichten angepasst. Je nach den Schwachstellen in einem validierten Bericht wird ein internes Ticket erstellt und dem zuständigen Team zugewiesen, dass sich dann darum kümmert, wobei die Prioritäten für die Ticket-Bearbeitung variieren.

FINDEN SIE BUG BOUNTY HILFREICH, UM DAS VERTRAUEN VON KUNDEN ZU STÄRKEN?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

Ja. Mit einem öffentlichen Bug-Bounty-Programm zeigen und betonen wir, wie ernst wir die Sicherheit und Transparenz nehmen. Wir setzen uns damit ja „kontrollierten“ Angriffen aus und berücksichtigen das wertvolle Feedback der Hunter-Community.

Bei deezer gibt es außerdem ein Team, das sich um Betrugsfälle kümmert. Schließlich werden die Künstler und Labels danach bezahlt, wie viele Leute sich ihre Titel angehört haben. Um ihre Einnahmen zu garantieren, müssen wir sie vor Betrug über die Plattform schützen. Das ist ein wesentlicher Bestandteil unserer Cybersecurity-Strategie – und gehört auch zum Testumfang unseres Bug-Bounty-Programms.

> **“ Mit einem öffentlichen Bug-Bounty-Programm zeigen und betonen wir, wie ernst wir die Sicherheit und Transparenz nehmen.**

YES WE HACK

WAS KOMMT ALS NÄCHSTES?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

Vorerst werden wir unsere bisherige Strategie weiterfolgen: Wir beleben das Programm immer wieder neu, wenn die Hunter-Aktivität nachlässt. Wie viel Feedback wir erhalten, hängt oft davon ab, wie stark die Medien über deezer berichten. Kommunizieren wir intensiver oder starten Kampagnen, werden auch die Hunter auf unser Programm aufmerksam.

Als Nächstes erwägen wir höhere Prämien, um ethische Hacker zu ermutigen, komplexere Schwachstellen zu finden.

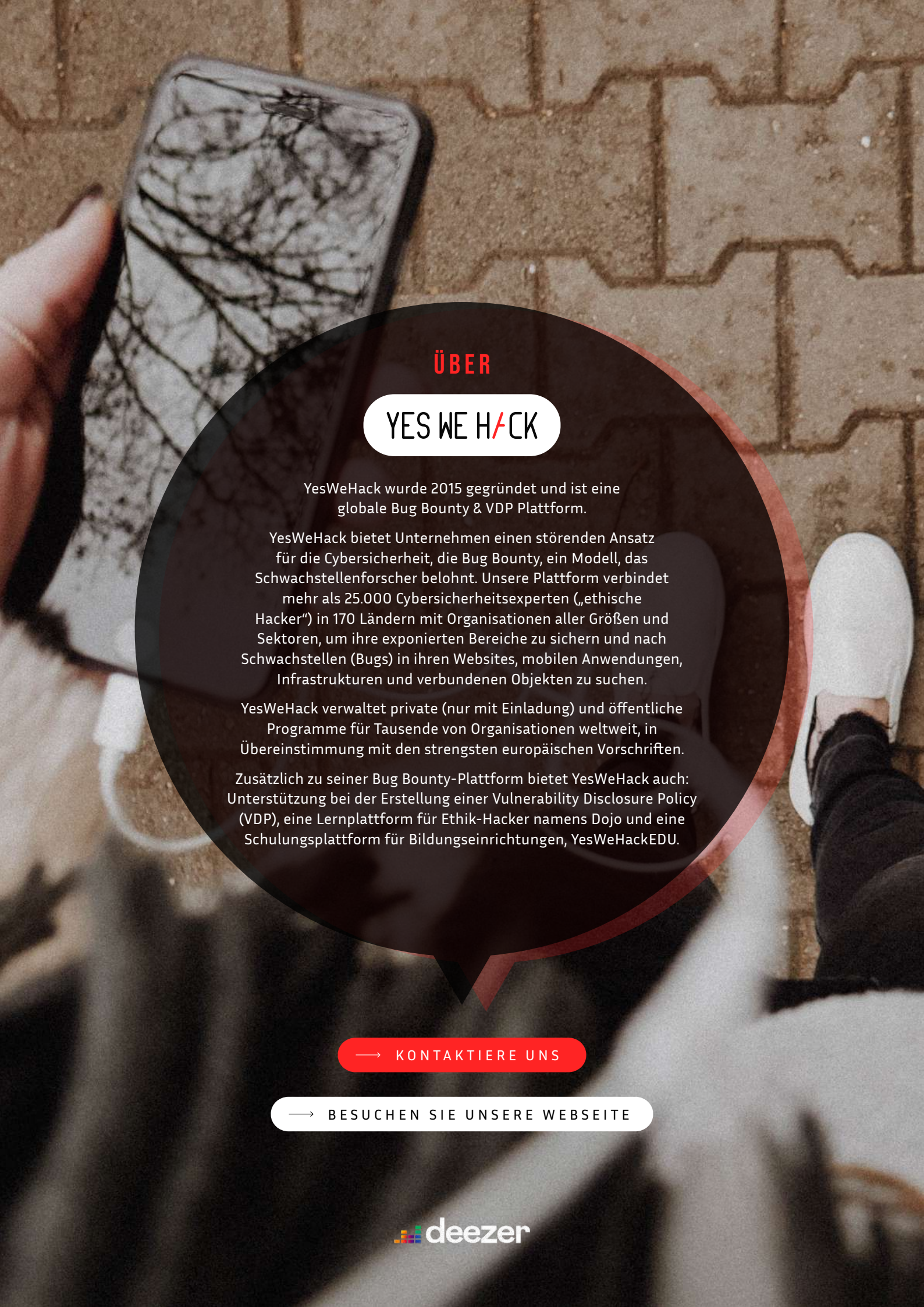
HABEN SIE TIPPS FÜR CISOS ODER START-UPS, DIE AUCH EIN BUG-BOUNTY-PROGRAMM STARTEN WOLLEN?

ROMAIN LODS, HEAD OF ENGINEERING, DEEZER:

Es ist immer besser, dass seine Sicherheitslücken vor dem Beginn eines Projekts zu kennen – statt zu warten, bis es zu viele Schwachstellen gibt, die sich nicht mehr in den Griff bekommen lassen, weil man sich bei der Architektur falsch entschieden hat.

Wenn ich sehe, was uns unser Bug-Bounty-Programm gebracht hat, wäre es besser gewesen, wenn wir diese Erkenntnisse so früh wie möglich berücksichtigt hätten.

Daher würde ich empfehlen, nicht zu lange mit der Implementierung von Tools wie Bug Bounty zu warten. Denn so minimieren Sie Ihre Abhängigkeit von Altsystemen, die sich nachträglich nur schwer absichern lassen.



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

deezer