YES WE HACK

OUTSCALE

OUTSCALE

Öffentliches Bug-Bounty-Programm

ANWENDERBERICHT

YES WE HACK

3DS OUTSCALE

WARUM HABEN SIE EIN BUG-BOUNTY-PROGRAMM EINGEFÜHRT?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Wir sind seit 2014 nach ISO 27001 zertifiziert und müssen deshalb mit Penetrationstests nach Schwachstellen suchen. Anfangs erwiesen sich Pentests als nützlich. Doch mit der Zeit waren die Ergebnisse eher dürftig. Wie uns schnell klar wurde, fehlte dem Pentester wegen der kurzen Audits von 2 bis 3 Wochen die Zeit, kritischere Schwachstellen zu finden. Bestenfalls wurde etwas angedeutet. Worum es aber konkret ging, mussten wir dann selbst herausfinden.

Auch hatten wir gehört, dass Bug Bounty bei bekannten US-Unternehmen gut funktioniert.

Wir haben dann mit einem Red Team und Bug Bounty – mit ethischen Hackern mit unterschiedlichstem Background – unsere Anwendungsbereiche getestet und neue Schwachstellen gefunden.

Hätten wir nur auf ein Red Team gesetzt, hätten wir das gleiche Zeitproblem wie mit klassischen Pentests gehabt. Also haben wir ein Bug-Bounty-Programm gestartet in der Überzeugung, dass nur weil die Pentester nichts mehr finden, das nicht heißen muss, dass es keine Probleme gibt.

Wir begannen mit einem privaten Programm mit 15 Huntern, weil wir bei unseren Anwendungen ein paar Sicherheitsprobleme vermuteten. Und die Hunter fanden einige erhebliche Schwachstellen. Darauf haben wir sukzessive mehr Hunter eingeladen, bevor wir für zwei Bereiche ein öffentliches Programm starteten: unseren Infrastrukturdienst und unser Kundenportal.

BESCHREIBEN SIE KURZ DIE ENTWICKLUNG IHRES PROGRAMMS.

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Die Implementierung des Programms war relativ schnell in einem Jahr erledigt. Als wir dann das öffentliche Programm starteten, gab es keinen starken Anstieg bei den Sicherheitslücken. Wir begannen mit einer Staffelung mit geringen Belohnungen. Die erhöhten wir schrittweise, damit sich mehr Hunter beteiligten, bis das Programm schließlich gut für uns funktionierte.

HABEN SIE SICH AUCH DESHALB FÜR YESWEHACK ENTSCHIEDEN, WEIL ES EINE EUROPÄISCHE PLATTFORM IST?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Absolut. Als wir die Idee für ein Bug-Bounty-Programm hatten, wollten wir damit sowohl die SecNumCloud-Qualifizierung der französischen IT-Sicherheitsbehörde ANSSI als auch die HDS-Zertifizierung erreichen. Daher hielten wir es für sinnvoll, mit einem Partner im Land zusammenzuarbeiten, der die Vertraulichkeit unserer Daten gewährleisten kann.

IST EINE INLÄNDISCHE PLATTFORM FÜR IHR MARKTKONZEPT VON VORTEIL?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Ja. Für unsere französischen und europäischen Kunden ist das ein wichtiger Aspekt. Zu unseren Kunden zählen öffentliche und staatsnahe Institutionen sowie kritische Infrastrukturbetreiber, die weder wollen, dass ihre Daten das Land verlassen, noch dass sie keine Kontrolle über die eigenen Daten mehr haben. Als Anbieter von Cloud-Diensten gibt die Zusammenarbeit mit einer inländischen Plattform wie YesWeHack unseren Kunden die Gewissheit, dass die gesamte Handhabung der Schwachstellen von Ende zu Ende effektiv kontrolliert wird.

Im weiteren Sinne ist das Bug-Bounty-Programm für Outscale ein Wettbewerbsvorteil, weil es eine aktive Security garantiert: Während wir früher halbjährliche Pentests und regelmäßige Scans durchführten, suchen wir jetzt ständig nach Sicherheitslücken. Sobald ein Hunter eine Schwachstelle meldet, nehmen wir diese automatisch in unsere Korrekturrunde auf. Unsere Kunden können sich darauf verlassen, dass wir nicht erst auf Updates von Dritten warten, um Schwachstellen zu schließen. Auch können wir Sicherheitslücken so in intern entwickelten Produkten erkennen und beheben.

WAS IST DER WAHRE WERT VON BUG BOUNTY?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Erstens haben die ethischen Hacker keinen Zeitdruck. Sie können sich alle Zeit der Welt nehmen, um komplexe Schwachstellen zu finden, einen Exploit weiterzuentwickeln, Korrekturen vorzuschlagen und einen ausführlichen Bericht zu schreiben. Im Gegensatz dazu gibt es bei Pentests oft nur wenige Scans und zwei oder drei CVEs, ohne dass konkret nachgewiesen wird, wie und ob sich potenzielle Schwachstellen ausnutzen lassen.

Die vielfältige Community ist ein weiterer Vorteil: Ich kann mich sowohl mit Huntern austauschen, die auf Benutzeroberflächen spezialisiert sind, als auch mit Experten für Anwendungsdienste. Jeder von ihnen achtet auf verschiedene, komplizierte Dinge, die einem Prüfer ohne Spezialwissen entgehen würden. Manchmal denke ich, man muss schon ein bisschen verrückt sein, um so etwas zu bemerken! Ich habe Zugang zu umfassendem Fachwissen. Da werden Dinge gefunden, die uns sonst entgehen würden.

> **“ Ich habe Zugang zu umfassendem Fachwissen. Da werden Dinge gefunden, die uns sonst entgehen würden.**

Mein Team ist mit den verschiedenen Ansätzen vertraut, da wir mit Menschen sprechen, die ganz unterschiedlich an das Schwachstellen-Management herangehen. Manchmal müssen wir erklären, dass ein Ergebnis keine Schwachstelle ist, sondern dass sie da etwas falsch angegangen sind.

Und mit der Zeit entwickelt man eine persönliche Beziehung zu einzelnen Huntern. Wenn ein ethischer Hacker erhebliche Sicherheitslücken gefunden hat und komplexere Dinge testen möchte, geben wir ihm dafür die Ressourcen oder den Zugang. Eine derart intensive Zusammenarbeit ist mit Pentestern, die ständig überfordert sind und knappe Termine erfüllen müssen, unmöglich zu realisieren.

YES WE HACK

3DS OUTSCALE

BEDEUTEN BUG-BOUNTY-PROGRAMME DAS ENDE VON PENTESTS? ODER WERDEN SIE SICH WEITERHIN ERGÄNZEN?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Meiner Meinung nach haben beide Ansätze ihre Berechtigung: Ich verwende Penetrationstests, weil sie für die Zertifizierung wichtig sind und um bestimmte Standards einzuhalten. So kann ich die Kunden zufriedenstellen, die diese Zertifizierungen benötigen. Bug Bounty dagegen erfüllt die Notwendigkeit einer höheren operativen Security und konzentriert sich auf all die Dinge, die sich mit Pentests und klassischen Scans nicht erkennen lassen.

HAT SICH ETWAS IN IHREN TEAMS VERÄNDERT, SEIT ES BEI OUTSCALE BUG-BOUNTY-PROGRAMME GIBT?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Im SOC (Security Operations Center) organisieren wir die bestehenden Programme, die Belohnungen, halten Kontakt zu Huntern, entwickeln neue Programme und kümmern uns um die Anpassung des Testumfangs. Die Bug-Bounty-Berichte gehen an mein SOC-Team, das dann jede Schwachstelle einstuft.

In 90 Prozent der Fälle handelt es sich um keine kritischen Schwachstellen, die sich dann schnell klassifizieren lassen. Bestehen Zweifel, diskutieren wir das intern. Besonders interessante Schwachstellen bespricht der zuständige Manager mit seinem Team. Wir erörtern dann mögliche Auswirkungen, denkbare Lösungen, die Empfehlungen des Hunters und wie wir dafür sorgen können, dass so etwas nicht mehr vorkommt. Durch diesen Austausch lernt das ganze Team dazu.

> **“ Bug Bounty dagegen erfüllt die Notwendigkeit einer höheren operativen Security und konzentriert sich auf all die Dinge, die sich mit Pentests und klassischen Scans nicht erkennen lassen.**

BEDEUTET DAS AUCH, DASS IHR TEAM ENGER ZUSAMMENARBEITET?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Ja, weil die Neugier geweckt wird. Etwas ist interessant und das will man verstehen. Sich mit einer echten Schwachstelle auf der Plattform zu beschäftigen, hat immer etwas Konkreteres.

SIND IHRE TEAMS UND DAS UNTERNEHMEN JETZT AGILER?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Wir arbeiten an einer kontinuierlichen Integration und Bug Bounty bietet sich für unsere agilen Methoden an.

Erhalten wir einen Bericht über Schwachstellen, ermitteln wir zuerst die CVSS-Punktzahl. Anhand dieser Punktzahl legen wir dann den Termin fest, bis wann die Sicherheitslücke geschlossen sein muss. Der Bericht wird direkt an die betroffenen Teams gesendet, damit sie das korrigieren. Gleiches gilt für die Dependencies im Code: Sie gehen zur F&E-Abteilung, die das analysiert und Versions-Upgrades entwickelt. Bug Bounty liefert hier einen Input wie jedes andere Verfahren und so gemeldete Schwachstellen werden über Tickets verwaltet.

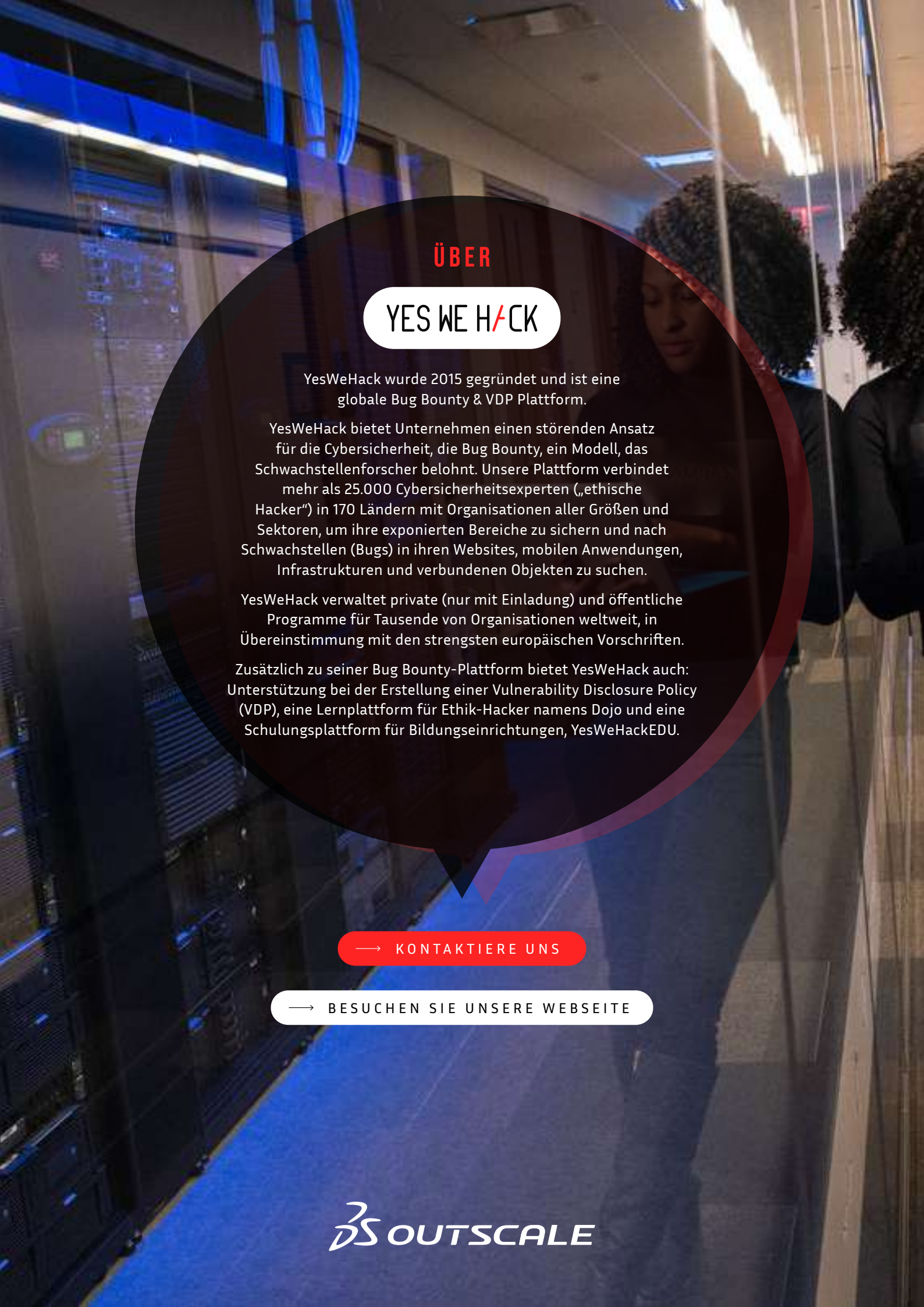
Wie schnell wir etwas bearbeiten, hängt von der Dringlichkeit ab: Ist eine schnelle Korrektur nötig, liefern wir umgehend einen Patch, der dann auch Teil der nächsten Version wird. In diesem Fall erstellen (oder modifizieren) wir eine User Story mit diesen neuen Elementen, die dann als Entwicklungsgrundlage dienen.

WAS KOMMT ALS NÄCHSTES?

EDOUARD CAMOIN, CISO, 3DS OUTSCALE:

Wir werden den Testumfang unserer Programme erweitern. Auch werden wir ethische Hacker ermutigen, sich stärker in unsere Produkte einzuarbeiten (über das webbasierte Frontend hinaus). Und wir werden die Belohnungsstaffelung erhöhen.

Ich würde den Huntern auch gern Zugang zu unseren privaten Plattformen geben, damit sie noch intensiver testen können. Wir haben das bereits einmal mit fest programmierten Datenextraktions-Szenarien auf unseren Testplattformen ausprobiert. Die Ergebnisse waren recht aufschlussreich. Dafür müssen die Hunter jedoch einen speziellen Testumfang erhalten, was wiederum zeitaufwendig ist.



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

3DS OUTSCALE