YES WE HACK

GROUPE ADP

GROUPE ADP

Öffentliches Bug-Bounty-Programm

ANWENDERBERICHT

WARUM HABEN SIE EIN BUG-BOUNTY-PROGRAMM GESTARTET?

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

Dieses Projekt wurde vom Group-Security-Team eingeführt. Ich hatte bislang keine Erfahrung mit Bug Bounty, aber wir haben sehr schnell die Vorteile und die Leistungsfähigkeit des Modells erkannt. Obwohl ich keine konkreten Sicherheitsbedenken hatte, sind mir die Vorteile jetzt bewusst. Die Bug-Berichte der ethischen Hacker zeigen Schwachstellen auf, die wir und unsere Auditoren sonst nicht erkannt hätten – und die Angreifer hätten ausnutzen können.

ERIC VAUTIER, GROUP CISO, GROUPE ADP:

Bei der Cybersecurity ist Antizipation alles. Man muss den Hackern immer einen Schritt voraus sein und neue Trends genau im Auge behalten. In der digitalen Welt bedeutet ein herkömmlicher Schutz, dass man nur reagieren kann. Das lässt sich vermeiden, indem man direkt mit Huntern zusammenarbeitet, die die gleichen Methoden wie Hacker verwenden und wie Hacker denken.

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

Heute ist Bug Bounty ein Eckpfeiler unserer Web-Security-Strategie. Natürlich müssen die Regeln für das Programm sorgfältig festgelegt werden: Man muss die Tests richtig strukturieren, damit sich die Hunter nicht verzetteln. Klare Grenzen schon bei der Einrichtung des Programms sind wichtig. Wir begannen mit einem eng abgestecktem Testumfang und haben ihn dann schrittweise erweitert.

“Das lässt sich vermeiden, indem man direkt mit Huntern zusammenarbeitet, die die gleichen Methoden wie Hacker verwenden und wie Hacker denken.

WELCHEN WERT BRINGT BUG BOUNTY VERGLICHEN MIT DEN ÜBLICHEN CYBER-SICHERHEITSLÖSUNGEN WIE PENTESTS?

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

Die große Stärke von Bug Bounty ist, dass ständig getestet wird. Pentests erfolgen immer zu einem bestimmten Zeitpunkt, nicht nach jeder Code-Änderung. Beim Bug Bounty sind die Hunter dagegen permanent aktiv. Sie achten auf alles, was neu ist, d. h. sie können erkennen, ob eine Änderung womöglich zu Sicherheitslücken führt.

ERIC VAUTIER, GROUP CISO, GROUPE ADP:

Ideal wären systematische Tests von jedem Update unserer Website. Das würde bedeuten: ein Pentest pro Woche oder noch öfter... Jeder weiß, dass das nicht machbar ist. Aber mit Bug Bounty ist diese kontinuierliche Überprüfung möglich.

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

Ich erhalte Berichte, die ich von unseren Pentests nicht kenne. Sie sind auch viel ausführlicher, insbesondere zur Website-Navigation. Auditoren haben diesen Ansatz nicht unbedingt. Auch ist ein Pentest zeitlich begrenzt, während sich Hunter einfach die Zeit nehmen können, um so weit wie möglich zu gehen. Nach und nach lernen sie unseren Anwendungsbereich immer besser kennen und können sich noch stärker in Details vertiefen.

ERIC VAUTIER, GROUP CISO, GROUPE ADP:

Ein Bug-Bounty-Programm kann auch mehr funktionale und nicht nur technische Schwachstellen in Anwendungen aufdecken. Das ist für mich der größte Unterschied zu Penetrationstests. Es ist eine vollkommen andere Sichtweise. Ein Pentest basiert oft auf automatisierten Tools, während Bug Bounty einen menschlicheren Ansatz hat, der auf diesen Tools aufbaut.

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

Der Austausch mit ethischen Hackern ist auch interessant. Sie helfen uns, gefundene Schwachstellen zu verstehen und sie richtig zu beheben. So können wir ihre Expertise nutzen.

Natürlich ist mit einem Bug-Bounty-Programm ein gewisser Aufwand verbunden: Man muss offen sein, um nachzuvollziehen, was die Hunter versucht haben, man muss mit ihnen reden... Wir müssen uns vollkommen neue Fragen stellen, z. B.: Wie könnte ein Angreifer unsere Security aushebeln?

YES WE H/CK

GROUPE ADP

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

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

Für mich funktioniert das eine nicht ohne das andere. Einerseits testen wir mit beiden nicht unbedingt das Gleiche. Andererseits können wir nicht einfach Neuland betreten, ohne vorher ein gewisses Maß an Sicherheit zu haben. Bug Bounty beginnt bei einer ausgereifteren Stufe im logischen Ablauf der Ereignisse. Man braucht eine minimale, grundlegende Security, bevor man ein Bug-Bounty-Programm startet. Allerdings müssen wir für den heutigen Umfang keine Pentests mehr durchführen. Bug Bounty allein ist ausreichend. Man muss die Messlatte von Anfang an auf das richtige Niveau setzen. Dann kann man den Prozess regelmäßig wiederholen.

> **“ Allerdings müssen wir für den heutigen Umfang keine Pentests mehr durchführen. Bug Bounty allein ist ausreichend.**

WIE PASST BUG BOUNTY ZU IHREM AGILEN ANSATZ?

DANIEL DIEZ, HEAD OF THE DIGITAL FACTORY DIVISION, GROUPE ADP:

Wie alle anderen haben auch wir Management-Tools für Quellen, Builds, Projekte und Leistungsanalysen. Wir nutzen zudem Tools, mit denen wir jeden neuen Schwachstellen-Bericht vom Bug-Bounty-Programm erfassen und abarbeiten. Bei jedem Sprint überprüfen wir, welche relevanten Daten wir berücksichtigen sollten, damit wir Probleme sofort angehen können.

WARUM HABEN SIE EIN ÖFFENTLICHES PROGRAMM GESTARTET? INWIEFERN HAT DAS IHREN BUG-BOUNTY-ANSATZ VERÄNDERT?

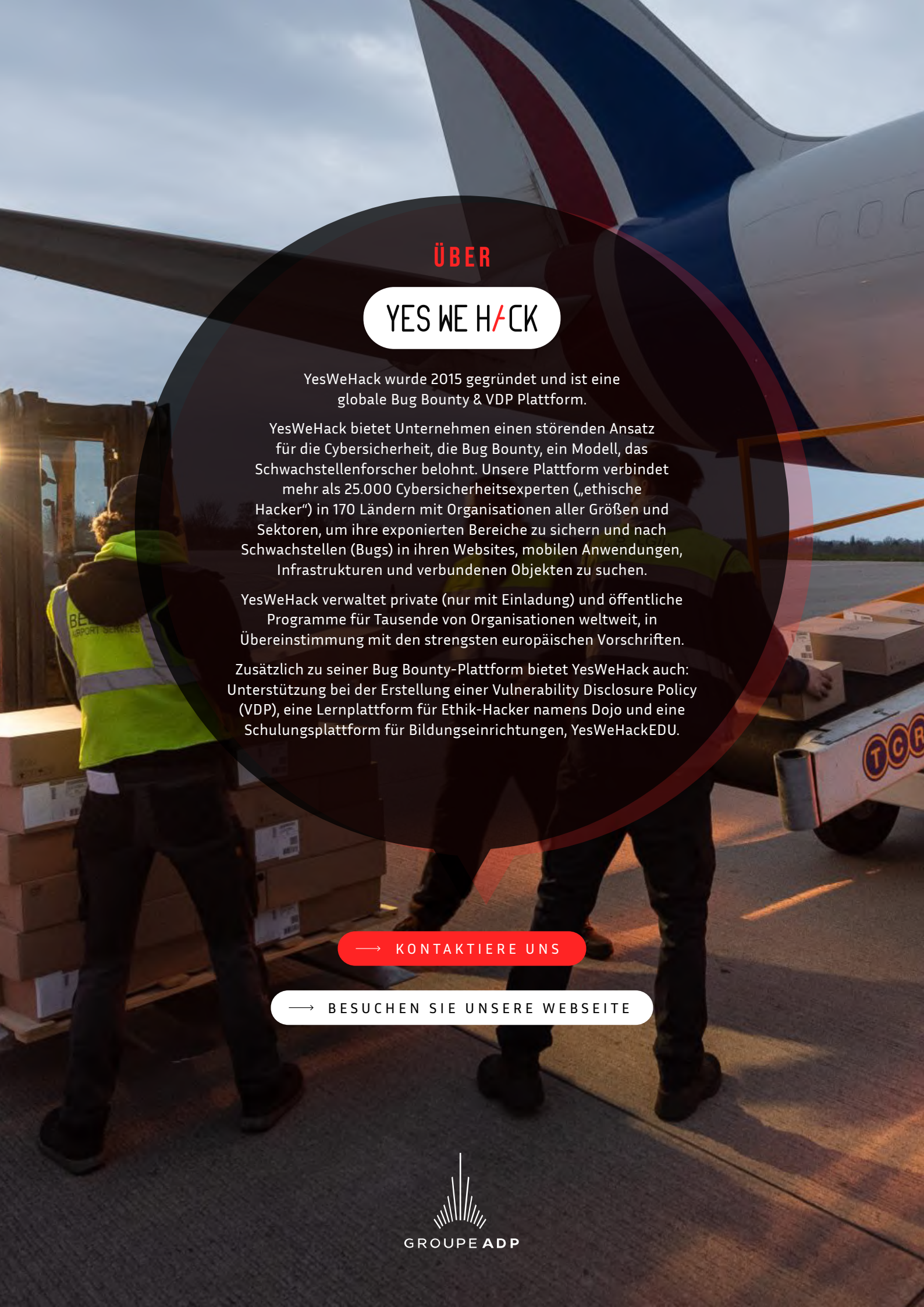
ERIC VAUTIER, GROUP CISO, GROUPE ADP:

Der Hauptvorteil ist, dass sehr viel mehr getestet wird und wir so unser Sicherheitsprofil maximal stärken können. Auch erhalten wir einen einzigen Kanal, über den Schwachstellen auf unserer Website gemeldet werden.

WAS KOMMT ALS NÄCHSTES?

ERIC VAUTIER, GROUP CISO, GROUPE ADP:

Wir werden den Testumfang auf andere Anwendungen erweitern und auch in anderen Geschäftsbereichen das gleiche Modell einführen: zuerst ein privates, dann später ein öffentliches Bug-Bounty-Programm.



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

GROUPE ADP