INTIGRITI

Einführung in Bug Bounty Programme für Unternehmen

Agile Sicherheitstests mit der Power der Gemeinschaft

E-BOOK

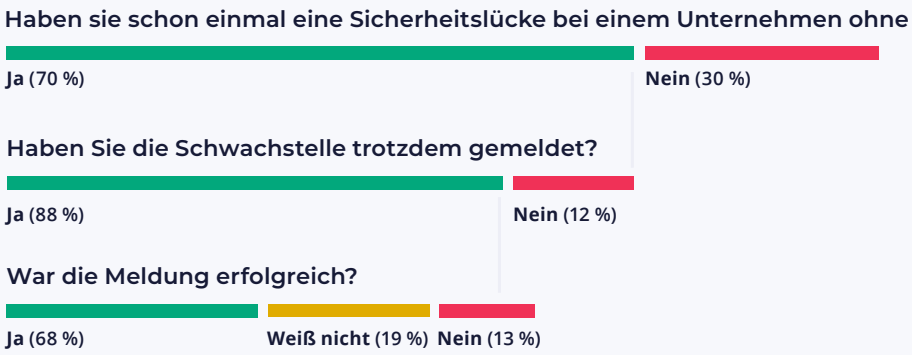
Inhalt

Unternehmen ohne Strukturen für die Meldung von Sicherheitslücken können nicht auf Warnhinweise von Sicherheitsexperten reagieren

Die zunehmende Digitalisierung von Unternehmensprozessen führt dazu, dass Hacker/-innen immer größere Angriffsflächen für böswillige Angriffe vorfinden. Die Personaldecke vieler IT-Abteilungen wiederum ist schon jetzt sehr dünn. Die Sicherheitsansätze, mit denen versucht wird, den neuen Anforderungen gerecht zu werden, gleichen eher dem Löschen von Brandherden als dem proaktiven Bekämpfen von Schwachstellen, bevor Cyberkriminelle sie ausnutzen können.

Die Notwendigkeit, sich proaktiv zu schützen, ist so hoch wie nie zuvor. Eine einfache, aber bewährte Möglichkeit, sich vor Cyber-Bedrohungen zu schützen, besteht darin, ethische Hacker/-innen an Bord zu nehmen. Doch wer sind diese ethischen Hacker/-innen? Und wo können Sie sie finden? Sollen wir Ihnen etwas verraten? Es kann durchaus sein, dass sie bereits versucht haben, Kontakt mit Ihnen aufzunehmen.

Dem Ethical Hacker Insights Report 2021 zufolge zeigen die Ergebnisse einer Umfrage unter ethischen Hacker/-innen, dass 70 % der Befragten schon mindestens einmal Sicherheitslücken in Webseiten von Unternehmen entdeckt haben, für deren Meldung es nur leider kein erkennbares System gab (beispielsweise in Form von Informationen zur Meldung von Sicherheitslücken). Dankenswerterweise bemühen sich 88 % von ihnen weiterhin, die Unternehmen zu kontaktieren, bei denen sie Sicherheitsrisiken finden – doch nur zwei Drittel (68 %) der Meldungen verlaufen erfolgreich.



Quelle: The Ethical Hacker Insights Report 2021 | Intigriti

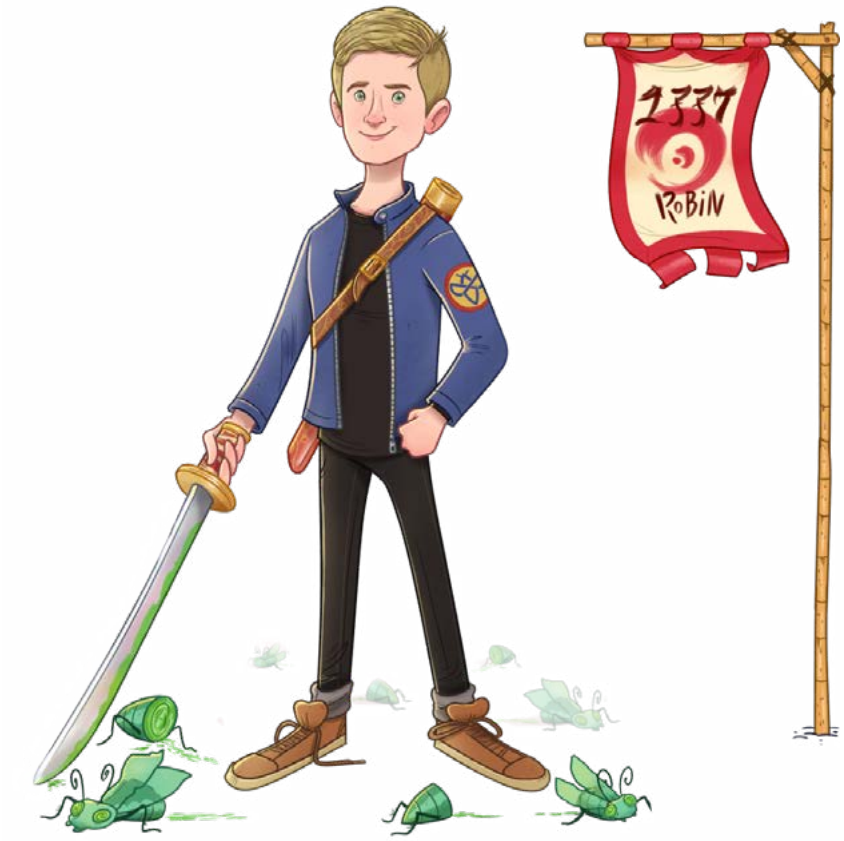
Was tun Unternehmen zur Lösung des Problems?

Bug Bounty Programme bieten Unternehmen die Möglichkeit, zum Aufdecken von Schwachstellen mit unabhängigen Sicherheitsforschern (sogenannten ethischen bzw. „guten“ „White-Hat“-Hacker/-innen) zusammenzuarbeiten. Die meisten Sicherheitsforscher/-innen nutzen für die Meldung von Schwachstellen gemeinschaftliche („crowdsourced“) Sicherheits- bzw. Bug Bounty Plattformen wie Intigriti. Der Grund hierfür ist, dass diese gemeinschaftlich betriebenen Plattformen den Sicherheitsforscher/-innen die beste Infrastruktur für ihre Tätigkeit und eine strukturierte, sichere und zuverlässige Kommunikation mit Unternehmen bieten.

Die kontinuierliche Zusammenarbeit mit ethischen Hacker/-innen ermöglicht es Unternehmen, ihre Schwachpunkte zu erkennen und zu beheben. Dies stärkt nicht nur ihre Cybersicherheit, sondern ermöglicht es ihnen auch, Cyberkriminelle auszumanövrieren.

Ethisches Hacking einfach erklärt

„Hacking“ bedeutet, Computerprogrammierungs- oder technische Kenntnisse dazu zu nutzen, Cybersicherheitssperren zu durchbrechen. In der Berichterstattung der Mainstream-Medien wird das Thema Hacking leider vorwiegend mit kriminellen Aktivitäten assoziiert – dem Gegenteil von dem, was ethisches Hacking auszeichnet.



Wofür steht die Bezeichnung Hacker/-in?

Ethische Hacker/-innen sind Menschen, die sich – genau wie bösartige Hacker – besonders gut mit Systemen, Codes und Programmierung auskennen. Und auch ihre Motivation ist das Ziel, das Abwehrsystem ihres Zielobjekts zu durchbrechen. Der große Unterschied: Ethische Hacker/-innen bewegen sich, wie ihr Name impliziert, auf dem Boden des Gesetzes, und sie klären die Unternehmen, mit denen sie zusammenarbeiten, über Schwachstellen auf.

Viele Unternehmen (einschließlich Google, Facebook und Microsoft) engagieren längst ethische Hacker/-innen, die ihnen helfen Cyber-Sicherheitslücken in ihren digitalen Assets ausfindig zu machen.

Wir von Intigriti bezeichnen ethische Hacker/-innen bevorzugt als **Sicherheitsforscher/-innen**. Wir sind der Ansicht, dass diese Bezeichnung den zahllosen Stunden des Forschens, Studierens und der Hartnäckigkeit besser gerecht wird, die es kostet, Sicherheitslücken zu finden, ohne sich etwas von dem zuschulden kommen zu lassen, was gemeinhin mit dem Begriff Hacker/-in verbunden wird.

Warum engagieren Unternehmen ethische Hacker/-innen?

Es gibt verschiedene Gründe, warum Unternehmen ethische Hacker/-innen beschäftigen. Allem voran ermöglicht die Unterstützung durch ethische Hacker/-innen es Ihnen, eine defensive Strategie mit einem offensiven Ansatz zu verfolgen.

Ethische Hacker/-innen sind hochqualifiziert und können das Verhalten böswilliger Hacker/-innen auf sichere Weise nachahmen, um Schwachstellen und blinde Flecken in der Angriffsoberfläche eines Unternehmens herauszuarbeiten. Die Zusammenarbeit mit ethischen Hacker/-innen ermöglicht es den Unternehmen, ihre Schwachpunkte zu erkennen und zu beheben. Dies stärkt nicht nur ihre Cybersicherheit, sondern ermöglicht es ihnen auch, Cyberkriminellen immer einen Schritt voraus zu sein.

Ein weiterer Grund, warum Unternehmen ethische Hacker/-innen engagieren, ist die Tatsache, dass sie hierdurch ihre Haftung begrenzen können. Falls es zu einem tatsächlichen Cyberangriff kommt, können sie vorweisen, was sie unternommen haben, um einen solchen Angriff zu verhindern.

Ethische Hacker/-innen zu engagieren ermöglicht es Unternehmen außerdem:

- zu zeigen, wie wichtig ihnen kontinuierliche Sicherheitstests sind
- das Risiko von Verlusten durch einen Cyberangriff zu reduzieren
- ihre Reputation und Glaubwürdigkeit in Sachen Datenschutz zu verbessern
- sich besser gegen die sich stetig weiterentwickelnden Cyber-Bedrohungen zu wappnen
- die Entwicklung des eigenen Teams auf der Grundlage wichtiger Erkenntnisse und Einblicke voranzutreiben

Die genaue Bezeichnung der Hacker/-innen kann je nach Art ihrer Tätigkeit für das jeweilige Unternehmen variieren (Bug Bounty Jäger/-in, Penetrationstester/-in, ...).

> Dass wir mit ethischen Hackern zusammenarbeiten, zeigt, dass wir wirklich alles versuchen und nicht einfach herumsitzen und darauf warten, dass etwas passiert.

JEAN-FRANÇOIS SIMONS
CISO UND DATENSCHUTZBEAUFTRAGTER, BRUSSELS AIRLINES

Bug Bounty Konzepte einfach erklärt

Bug Bounty Programm

Sicherheit suchende Unternehmen können ein Bug Bounty Programm ausschreiben, mit dem sie unabhängigen Sicherheitsforscher/-innen Anreize bieten, für sie nach Bugs zu suchen und ihnen ihre Funde zu melden. Diese Programme können öffentlich ausgeschrieben werden (das heißt, jede/-r kann sich beteiligen) oder als geschlossene Programme, für die einzelne Forscher/-innen persönlich angesprochen werden. Außerdem können sie zeitlich befristet oder unbefristet sein. Die meisten Unternehmen entscheiden sich allerdings für Letzteres, um kontinuierliche Sicherheitstests sicherzustellen.

Bugs

Als Bugs werden Schwachstellen und Lücken in Sicherheitssystemen bezeichnet. Wann Bugs als neuartig und wichtig gelten, hängt vom Umfang des Programms ab; Aufgabe der Sicherheitsforscher/-innen ist es, Bugs schnell, zuverlässig und nachvollziehbar einschließlich Erklärung der Schwachstelle zu melden.

Bounty (Prämie)

Wird die Meldung von dem Unternehmen, an das sie gesendet wird, als relevant erachtet, erhält der Forscher/die Forscherin eine Prämie, dem englischen Ursprung entsprechend als „Bounty“ (Kopfgeld) bezeichnet. Die Höhe der Prämie hängt ab vom Reifegrad der Sicherheitsstrategie des Unternehmens und von den potenziellen Auswirkungen des Sicherheitsfehlers. Die Höhe des Betrags, den der/die Forscher/-in bekommt, kann zwischen 50 und mehreren Tausend Euro für eine einzige Fehlermeldung liegen.

Bug Bounty Plattform

Die meisten Sicherheitsforscher/-innen nutzen für die Meldung von Schwachstellen gemeinschaftliche („crowdsourced“) Sicherheits- bzw. Bug Bounty Plattformen wie Intigriti. Der Grund hierfür ist, dass diese gemeinschaftlich betriebenen („crowdsourced) Plattformen den Sicherheitsforscher/-innen die beste Infrastruktur für ihre Tätigkeit bieten und eine strukturierte, sichere und zuverlässige Kommunikation mit Unternehmen gewährleisten.

Sicherheitsforscher/-innen

In Fachkreisen auch als Bug Bounty Jäger/-innen, White-Hat-Hacker/-innen und ethische Hacker/-innen bezeichnet. Sicherheitsforschende sind Cybersicherheitsexpert/-innen, die ihre Hacking-Fähigkeiten und -Erfahrung für positive Zwecke nutzen. Manche der Intigriti-Forscher/-innen sind in Vollzeit als Bug Bounty Jäger/-innen im Einsatz, andere wiederum als Vollzeitbeschäftigte für Unternehmen. 50 % der Intigriti-Community sind als Penetrationstester/-innen tätig.

Schwachstellenmanagement im Unternehmen mit Intigriti - so geht‘s

Triage und Kundensupport

Unsere Kunden werden unterstützt von einer der marktführenden Triage-Abteilungen, einem für sie zuständigen Kundenbetreuer (Customer-Success-Manager) und einem Programm-Manager.

Forscher/-in **sucht** nach **Schwachstelle**

Forscher/-in **reicht** über Intigriti einen **Bericht ein**

Das **Triage-Team** von Intigriti nimmt **Kontakt** mit dem/der Forscher/-in auf

Das **Triage**-Team von Intigriti leitet Schritte zur **Qualitätssicherung** ein

Kunde erhält einen auftragsgemäßen, maßgeschneiderten und detaillierten **Bericht**

Kunde akzeptiert den Bericht; daran anschließend **automatische** Veranlassung der **Bezahlung**

Penetrationstests versus Bug Bounty Programm

Sowohl Bug Bounty Programme als auch Penetrationstests (auch „Pentests“) dienen dazu, Sicherheitslücken zu identifizieren, die von Hacker/-innen ausgenutzt werden könnten. Dennoch unterscheiden sie sich in einigen wesentlichen Punkten. Pentests erfassen den Ist-Zustand an einem bestimmten Zeitpunkt, während Bug Bounty Programme kontinuierlich laufen.

Beim Pentest erhalten Sie zwar einen Testnachweis und eine Übersicht über einzelne Schwachstellen, die innerhalb des Testzeitfensters festgestellt wurden, doch sobald Sie neue Funktionen einführen oder Updates vornehmen, ändert sich Ihr Sicherheitsstatus. Dies ist der Punkt, an dem Bug Bounty Programme eine gute Weiterverfolgungsoption darstellen.

Ein weiterer großer Unterschied zwischen Pentests und Bug Bounty Programmen besteht in den Kosten. Bei der Bug Bounty Plattform erhalten die Sicherheitsforscher/-innen eine Prämie, wenn sie einen zuvor unentdeckten Schwachpunkt melden. Was Sie zahlen, hängt davon ab, wie kritisch die Sicherheitslücke ist – Sie zahlen je nach Schweregrad des Fehlers. Bei Pentests hingegen wird die Leistung bezahlt, die der/die ethische Hacker/-in erbringt.

Bug Bounty Programme unterliegen, anders als Pentests, keiner bestimmten Methode. Unternehmen, die sich für Intigritis ethische Hacking-Plattform entscheiden, zahlen beispielsweise eine Grundgebühr für die Veröffentlichung ihres Programms in einer kontrollierten Umgebung. Dies bietet der Community der ethischen Hacker/-innen die Möglichkeit, die Sicherheit der digitalen Strukturen des Unternehmens zu beurteilen und einen kreativeren Ansatz zu wählen.

Die Programme können als offen für die gesamte Gemeinschaft oder als #geschlossene Programme definiert werden. Ein geschlossenes Programm bedeutet, dass sich nur Forscher beteiligen können, die persönlich hierzu eingeladen werden.

	PENTEST	BUG BOUNTY
Geltungsdauer		
Teamgröße	KLEINE TEAMS ODER EINZELPERSONEN	TAUSENDE SICHERHEITSFORSCHER/-INNEN IN GESCHÜTZTEM RAHMEN
Ansatz	TECHNIKORIENTIERT	KREATIVER ANSATZ
Zeitliche Begrenzung	ZEITLICH BEFRISTET	KONTINUIERLICH
Abrechnung	BEZAHLUNG NACH ZEIT	ERGEBNISBASIERTE ZAHLUNG
Geltungsdauer	BEGRENZTER AUSSCHNITT	KONTINUIERLICHE TESTS
Fachwissen	FACHWISSEN UND KOMPETENZEN EINZELNER ZUSTÄNDIGER	FACHWISSEN UND KOMPETENZEN DER GEMEINSCHAFT

Wie Kinepolis sein Bug Bounty Programm nutz, um die Sicherheit seiner Systeme zu wahren

Die Herausforderung
Größtmögliche IT-Sicherheit für alle Webseiten und Systeme

Für ein führendes, international agierendes Kinounternehmen wie Kinepolis ist die unternehmenseigene Internet-Plattform die wichtigste Schnittstelle für die Interaktion mit den Kunden. Die Sicherheit des Systems zu wahren ist daher von allergrößter Bedeutung, weshalb Kinepolis bereits einen Penetrationstest-Partner hinzugezogen hatte, um sich bei der Bewältigung der Anforderungen in Sachen IT-Sicherheit unterstützen zu lassen.

Die Lösung
Kontinuierliche Sicherheitstests

Kinepolis hat sich entschieden, seine Penetrationstests durch ein Bug Bounty Programm über die Intigriti-Plattform zu ergänzen. Das Unternehmen lud die der Community angehörenden Sicherheitsforscher/-innen ein, auf sichere und kontrollierte Weise Schwachstellen in seinen Systemen aufzuspüren. Die Entscheidung, mit ethischen Hacker/-innen zu arbeiten, fiel zunächst nicht leicht.

- „Die größte Herausforderung im Vorfeld der Zusammenarbeit mit Intigriti war die Angst vor dem Unbekannten.“ Andererseits ist es natürlich so, dass eine Webseite, sobald sie freigegeben ist, sowieso allen offensteht. Alle haben Zugriff – Leute mit guten Absichten genauso wie bösartige Hacker/-innen.“

Schaffung einer zusätzlichen Qualitätssicherungs-ebene

Die Intigriti-Plattform ist die zentrale Drehscheibe für die Kommunikation zwischen den externen Forscher/-innen und Kinepolis. Sobald ein/-e Forscherin eine Schwachstelle findet, wird diese der Plattform gemeldet, damit die Triage-Experten von Intigriti die Lücke überprüfen können.

Das Ergebnis
Größtmögliche Systemsicherheit durch gemeinsamen Einsatz

Die Sicherheitsforscher/-innen von Intigriti und Kinepolis hatten ein gemeinsames Ziel: die Systeme für die Endnutzer sicher zu halten. Die Intigriti Bug Bounty Plattform gab den internen IT-Sicherheits-Teams das gute Gefühl, auf umfassende Unterstützung vertrauen und hochwertige Sicherheitstests gewährleisten zu können.

> Das Triage-Verfahren von Intigriti stellt sicher, dass nur wirkliche Probleme bei unserem IT-Team eingehen, das sich dann umgehend an die Lösung begeben kann.

BJORN VAN REET
CIO – KINEPOLIS GROUP

KINEPOLIS

BRANCHE
Unterhaltungskino

ANZAHL DER KINOS
111 weltweit

BESCHÄFTIGTE
4.600

Wie Bug Bounty Programme Unternehmen helfen, Probleme in puncto Cybersicherheit zu bewältigen

Die Herausforderung

Fachräftemangel im Bereich Cyber-Sicherheit

95 % der Sicherheitsexperten geben an, dass der Fachkräftemangel im Bereich Cybersicherheit eine **immer größere Herausforderung** darstellt (SearchSecurity).

Cyber-Bedrohungen den entscheidenden Schritt voraus sein

Umfragen unter Sicherheitsfachkräften zeigen, dass 59 % angeben, dass die Anforderungen auf der Arbeit **kaum Möglichkeiten für eigene Weiterentwicklung lassen** (SearchCompliance) – und zugleich immer neue Cybersicherheitsbedrohungen hinzukommen.

Wachsende Angriffsfläche

Digitale Transformation, Einstieg in Cloud-Systeme, schnelle Skalierbarkeit und immer neue Entwicklungszyklen führen dazu, dass auch die Angriffsfläche immer größer wird. Das Ergebnis ist ein massiver **Anstieg der Cyber-Bedrohungen** – weltweit und Jahr für Jahr mehr (Help Net Security).

Die Bug Bounty Lösung

Sicherheitsexperten-Netz erschließen

Einbeziehung der Kompetenz, Erfahrung, Kreativität und des Fachwissens **Tausender von Sicherheitsexpertinnen und -experten**

Investition in die Weiterentwicklung Ihres Teams

Wie bösartige Hacker/-innen sind auch Bug Bounty Jäger/-innen auf genau das aus, was Ihr Team übersieht. Unternehmen, die es Ihren internen Fachkräften ermöglichen, durch Meldungen externer Forscher/-innen und im Austausch mit ihnen zu lernen, **investieren in den eigenen Kompetenz-Pool**.

Sicherheit kontinuierlich testen

Ein fortlaufendes Bug Bounty Programm ermöglicht es Unternehmen, ihre **Sicherheitstests auszubauen und zu skalieren**. Ihre Sicherheits-Teams erhalten schneller Kenntnis von Schwachstellen, sodass sie schneller Patches herausbringen können.

Die Herausforderung

Kosten und Grenzen von Pentests

Die Kosten eines hochwertigen Pentests liegen im Durchschnitt bei 8.500–25.500 € (10.000–30.000 US-Dollar) (RSI Security). Regelmäßige Pentests wären äußerst **kostspielig ohne nachhaltig zu sein,** da die Bezahlung nach Zeit und nicht ergebnisbasiert erfolgt.

Sicherheitsbewusstsein

Immer alle Sicherheitsgefahren im Blick zu behalten, ist eine große Herausforderung für interne Cybersicherheitsteams. Konfigurationsfehler und Unsicherheiten beim Codieren können schnell **erhebliche Kosten und Datenschutzverletzungen** verursachen.

Ressourcenmangel

Angemessene Ressourcen für ausreichende Cybersicherheit vorzuhalten, kann angesichts steigender Kosten und immer neuer Verfahren zur Gewährleistung **anhaltenden Wachstums** eine große Herausforderung sein.

Die Bug Bounty Lösung

Ergebnisbasierte Zahlung

Bug Bounty Jäger/-innen erhalten eine Belohnung, wenn sie eine neue, realistische und nachvollziehbare Sicherheitslücke innerhalb des vorgegebenen Settings aufdecken. Bezahlt wird ergebnisbasiert, das heißt, das **Kosten-Nutzen-Verhältnis** ermöglicht einen deutlich höheren Wirkungsgrad bei unverändertem Test-Budget.

Win-Win: Unterstützung und zusätzliches Wissen durch ethische Hacker/-innen

Der kontinuierliche Zufluss an hochwertigen und **wirkungsorientierten Meldungen** bewirkt zugleich ganzjährig ein enormes Plus an Inspiration, Hacking-spezifischem Denken und Bewusstseinsschärfung seitens der beteiligten IT- und Entwicklungs-Teams.

Zentralisieren von Sicherheitstests

Bug Bounty Programme ermöglichen es Unternehmen, die Systeme zum Schutz ihrer Cybersicherheit kontinuierlich **über eine Plattform** und mit der Power der Gemeinschaft prüfen zu lassen.

Wie Brussels Airlines mittels Bug Bounty Programm seine IT-Sicherheit erhöht

Die Herausforderung Intern grünes Licht für Bug Bounty Programme zu erhalten

Das Thema ethisches Hacking und Bug Bounty Konzepte zog schon vor vielen Jahren die Aufmerksamkeit von Jean-François Simons, CISO bei Brussels Airlines, auf sich. Trotzdem war die Vorstellung, externe Sicherheitsaktivisten unentdeckte Fehler suchen zu lassen, keine leichte Entscheidung für das Management-Team.

Doch Simons gelang es klar zu machen, warum die Fluglinie besser mit ethischen Hacker/-innen zusammen- als gegen sie arbeiten sollte.

- „Wir brauchen die Unterstützung ethischer Hacker/-innen, um unsere IT-Sicherheit zu stärken, bevor böswillige Hacker/-innen eine mögliche Schwachstelle finden, die sie uns mit Sicherheit nicht melden werden.“

Die Lösung

Bereinigende Penetrationstests als Vorstufe vor Bug Bounty Programm

Das Team von Jean-François Simons entschied sich für Penetrationstests als ersten Schritt vor dem Start eines Bug Bounty Programms:

- „Pentests eignen sich meines Erachtens für regelmäßige Prüfläufe zur Verbesserung der allgemeinen Sicherheit unserer Systeme. Die nächsten Schritte überlässt man dann den Experten einer Bug Bounty Plattform."

Simons erklärt weiter: „Ethische Hacker/-innen sind genau auf einzelne Fachgebiete spezialisiert – die einen auf webseitenübergreifendes Skripting, andere auf SQL-Einschleusung, und so weiter. Pentests beinhalten auch SQL-Einschleusung, aber auf einer übergeordneten Ebene." Die im Rahmen unseres Programms entdeckten Schwachstellen waren nur für sehr spezialisierte und hochqualifizierte Leute auffindbar."

Das Ergebnis

PR-Vorteile, Fachliche Kooperation und stärkeres Sicherheitsbewusstsein

Der Wert von Intigriti für Brussels Airlines liegt nicht allein im Aufspüren von Bugs und Schwachstellen. Simons verweist auch auf die PR-Vorteile:

- „Dass wir ein Bug Bounty Programm einsetzen, zeigt, dass wir wirklich einen Schritt weiter gehen. Sollte tatsächlich einmal ein größeres Problem auftreten, wird uns das sehr von Nutzen sein. Dass wir mit ethischen Hackern zusammenarbeiten, zeigt, dass wir wirklich alles versuchen und nicht einfach herumsitzen und darauf warten, dass etwas passiert."

Das eröffnet den DevOps- und Digitalisierungs-Teams von Brussels Airlines völlig neue Kooperationsmöglichkeiten. Die Leute können durch das, was aufgedeckt wird, lernen. Außerdem hat die Zusammenarbeit mit ethischen Hacker/-innen bewirkt, dass mehr IT-Fachkräfte von Brussels Airlines sich der vorhandenen Cybersicherheitsbedrohungen bewusst sind und aktiv daran beteiligen, die Informationssicherheit zu verbessern.

- „Wir wollten ein so unangreifbares IT-Sicherheits-System wie möglich. Deshalb haben wir uns an die ethischen Hacker/-innen von Intigriti gewendet, die tatsächlich eine kritische Sicherheitslücke fanden, die wir dann entschärfen konnten."

brussels airlines

BRANCHE

Luftfahrt

UMSATZ

1,6 Mrd. EUR

PASSAGIERE

10,2 Millionen

Selbstgehostete Bug Bounty Programme oder Ausschreibung über eine Plattform. Was eignet sich am besten?

Ethische Hacker/-innen verwenden sehr viel Zeit darauf, Sicherheitslücken aufzudecken und diese den betroffenen Unternehmen zu melden. An diesem Punkt von zentraler Bedeutung ist ein unkompliziertes, durchdachtes System, über das sie Ihnen diese Schwachstellen melden können. Es ist nicht nur ein Anreiz, verantwortungsvoll mit ihren Erkenntnissen umzugehen, sondern maximiert auch ihre Chancen, ihre Bemühungen erfolgreich abzuschließen.

Auf der nächsten Seite finden Sie eine Übersicht über die Hauptunterschiede zwischen selbst gehosteten Programmen und Bug Bounty Plattformen.

	SELBSTGEHOSTETE PROGRAMME	BUG BOUNTY PLATTFORMEN
Programm-Beteiligung	**Reaktiver und passiver Einsatz** Wohlgesinnte Kunden, Bürger/-innen und ethische Hacker/-innen informieren Firmen über potenzielle Sicherheitslücken.	**Aktiver Einsatz** Dauerhaftes Engagement von Sicherheitsforscher/-innen, basierend auf Prämien, Punkt- und Belohnungs- beziehungsweise Bewertungssystemen, Hacking-Events, Weiterbildung usw.
Anforderungen an System für die Meldung von Sicherheitslücken	**Bedarf** Vorhalten eines Sicherheitslücken-Meldesystems, das sicherstellt, dass Außenstehende erkennen, wie sie Ihrem Unternehmen Sicherheitslücken melden können, die sie gefunden haben.	**Empfehlung** Unternehmen sollten auf Ihrer Webseite einen Punkt mit Hinweisen zur Meldung von Sicherheitsproblemen (engl. VDP/ „Vulnerability disclosure policy“) anbieten, die Personen, die eine Schwachstelle melden wollen, direkt zum Programm des Unternehmens führt.
Validieren von Meldungen	**Intern** Im Falle nicht ausreichender Ressourcen kann durch das Handling nicht relevanter Meldungen sehr viel Zeit verloren gehen.	**Triagieren von Meldungen** Triage-Teams bilden eine Art Schutzschild, das die Qualität eingehender Meldungen über Sicherheitslücken prüft, bevor diese an Ihr Unternehmen weitergeleitet werden.
Handling von Mitteilungen	**Intern** Zuständigkeit liegt bei dem für die Abwicklung eingehender Meldungen zuständigen Team.	**Triagieren von Mitteilungen** Abwicklung von Kommunikationsaufgaben über die Plattform. Vermittlung zwischen Kunden und Forscher/-innen über eine gesonderte Triage-Abteilung.
Budgetzuweisung und Zahlungsabwicklung	**Manuell** Abwicklung über zuständige Finanzabteilung. Internationale Zahlungen können sich durchaus kompliziert gestalten und schon bei kleinen Fehlern hohe Gebühren verursachen. Für eine gute Pflege der Beziehung mit Forscher/-innen ist es wichtig, umgehende Zahlungen zu gewährleisten.	**Über die Plattform** Die Zahlung erfolgt automatisch, sobald eine Meldung vom Unternehmen als relevant akzeptiert wurde. Zahlung und Verwaltung werden von der Plattform übernommen.
Verantwortungsvolle Offenlegung	**Einladung** Forscher/-innen werden gebeten, Fehler auf verantwortungsvolle Art und Weise offenzulegen.	**Plattform-spezifische Vereinbarung** Forscher/-innen müssen einwilligen, Fehler auf verantwortungsvolle Art und Weise offenzulegen.

Wie die Europäische Kommission die Absicherung von Open-Source-Software unterstützt

Die Herausforderung Unterstützung von Open-Source-Communities bei der Absicherung ihrer Software

Die Europäische Kommission erkannte die zentrale Bedeutung von Open-Source-Software im Jahr 2014, als der sogenannte Heartbleed-Bug erhebliche Verluste hervorrief und weltweit Auswirkungen hatte. Damals verpflichtete die Europäische Kommission sich, Open-Source-Communities darin zu unterstützen, ihre Software abzusichern.

Im Januar 2016 startete die Europäische Kommission das ISA²-Programm, mit dem digitale Lösungen gefördert werden, die es öffentlichen Verwaltungen, Unternehmen sowie Bürgerinnen und Bürgern in Europa ermöglichen, interoperable grenz- und sektorenübergreifende öffentliche Dienstleistungen zu nutzen. Das Programm unterstützt eine Reihe unterschiedlicher Maßnahmen zur Entwicklung von Interoperabilitätslösungen.

Eine dieser Maßnahmen mit dem Titel Sharing and Re-Use (gemeinsame Nutzung und Weiterverwendung von Informationen) (2016.13) wurde dem Open Source Program Office (OSPO) zugewiesen. Im Rahmen dieser Maßnahme beschloss das OSPO, Bug Bounty Programme einzusetzen, um Open-Source-Software, die in öffentlichen Verwaltungen weit verbreitet ist, abzusichern. Diese Bemühungen werden 2021 mit der laufenden Maßnahme fortgesetzt.

Die Lösung

Absicherung von drei Open-Source-Software-Angeboten durch Einsatz von Bug Bounty Services

Im Rahmen der Aktion *Sharing and Re-use* (Gemeinsame Nutzung und Wiederverwendung, 2016.31) beschloss die Kommission, Bug Bounty Programme einzusetzen, eine Form von Sicherheitstests, die auf einem partizipativen Ansatz basieren (Crowdsourced Security Tests). Am 11. Januar 2021 wurden unter Einsatz der Bug Bounty Plattform von Intigriti drei Bug Bounty Programme gestartet.

Die für die Bug Bounty Programme ausgewählte Software:

1. **MOODLE**
   Eine E-Learning-Plattform, die von öffentlichen Verwaltungen und Universitäten weltweit verwendet wird.

2. **ZIMBRA**
   Eine bekannte E-Mail- und Groupwarelösung mit Kalender- und File-Sharing-Funktionen.

3. **ELEMENT (MATRIX)**
   Eine Instant-Messenger-Plattform, die von öffentlichen Verwaltungen in Frankreich und Deutschland verwendet wird.

Die Bug Bounty Programme wurden über das Programm ISA² der Kommission finanziert, aber der Schwerpunkt lag komplett auf Open-Source-Software, die von den öffentlichen Diensten der EU verwendet wird.

European Commission

BRANCHE

Öffentliche Verwaltung

GRÜNDUNG

1958

ANZAHL MITARBEITENDE

> 10.000

Das Ergebnis: Modernere Sicherheitstests mit sofortigem Effekt

Innerhalb weniger Wochen lagen Berichte über Sicherheitslücken vor. In einer Software wurden drei als „kritisch“ eingestufte Sicherheitslücken gefunden. Darüber hinaus wurde mindestens eine für alle drei Softwareprojekte relevante Sicherheitslücke entdeckt und offengelegt, deren Bedeutung als „hoch“ eingestuft wurde.

Die Sicherheitslücken zu kennen ermöglichte es den Open-Source-Communities, diese schnell mit einem Patch beheben und damit die Software sicherer machen zu können.

> Bug Bounty Plattformen passen perfekt zu Open-Source-Software, denn hier hilft eine Community (die der ethischen Hacker) der anderen. Das ist Zusammenarbeit auf höchstem Niveau.

MIGUEL DÍEZ BLANCO
PROJEKTLEITER OPEN SOURCE PROGRAMME OFFICE BEI DIGIT – EUROPÄISCHE KOMMISSION.

Auf die Frage zu ihren Erfahrungen hieß es bei **Zimbra**:

- „Das machen wir wieder! Für Zimbra war die Teilnahme am Bug Bounty Programm der Europäischen Kommission ein wertvolles und lohnendes Projekt. Es war eine großartige Übung für uns, die uns aufgerüttelt hat, rund um die Uhr wachsam zu bleiben; die gefundenen Sicherheitsprobleme waren größtenteils von niedrigem bis mittlerem Schweregrad und hingen mit Scripts und Anfragebetrug zusammen, würden aber von unserem Verwundbarkeitsscanner nicht erfasst.“

Zur Motivation in Bezug auf die Lernplattform **Moodle LMS** erklärt Produktmanager Sander Bangma:

- „Moodle ist das weltweit anpassungsfähigste und vertrauenswürdigste Open-Source-Lernmanagementsystem, und da ist Sicherheit natürlich von allergrößter Wichtigkeit. Bei der Entwicklung von Moodle ist das Thema Sicherheit fester Bestandteil des Konzepts, und die Teilnahme am ISA-Bug Bounty Programm war für uns eine willkommene Ergänzung zur weiteren Verbesserung der Sicherheit von Moodle.“

Was ihre Erfahrungen mit Intigritis Bug Bounty Plattform betrifft, erklärt **Matrix**:

- „Intigriti hat erstklassigen Service geliefert, da die Berichte im Vorfeld triagiert wurden und dafür gesorgt wurde, dass wir uns nur um bereits validierte Meldungen kümmern mussten. Der Schweregrad der meisten gemeldeten Sicherheitslücken war zwar gering, aber wir haben auch einige Berichte über schwerwiegendere Fehler erhalten.“

Über Bug Bounty Communities

Ethische Hacker/-innen sind hochgradig wissbegierige, neugierige und den Dingen auf den Grund gehende Menschen. Sie lieben es, ihr Wissen über die schnelllebige und sich unablässig verändernde Sicherheitslandschaft zu erweitern. Der Ethical Hacker Insights Report 2021 zeigte, dass 70 % der Intigriti-Hacker/-innen bei der Plattform mitmachen, um Neues zu lernen und ihre Fähigkeiten auszubauen, und 40 % insbesondere die Herausforderung lieben.

Um als Sicherheitsforscher/-in erfolgreich zu sein, ist es wichtig, beim Hacking immer wieder eine neue Perspektive einnehmen zu können, ungebremst kreativ zu sein und sich nicht zu scheuen, Dinge gegen den Strich zu bürsten.

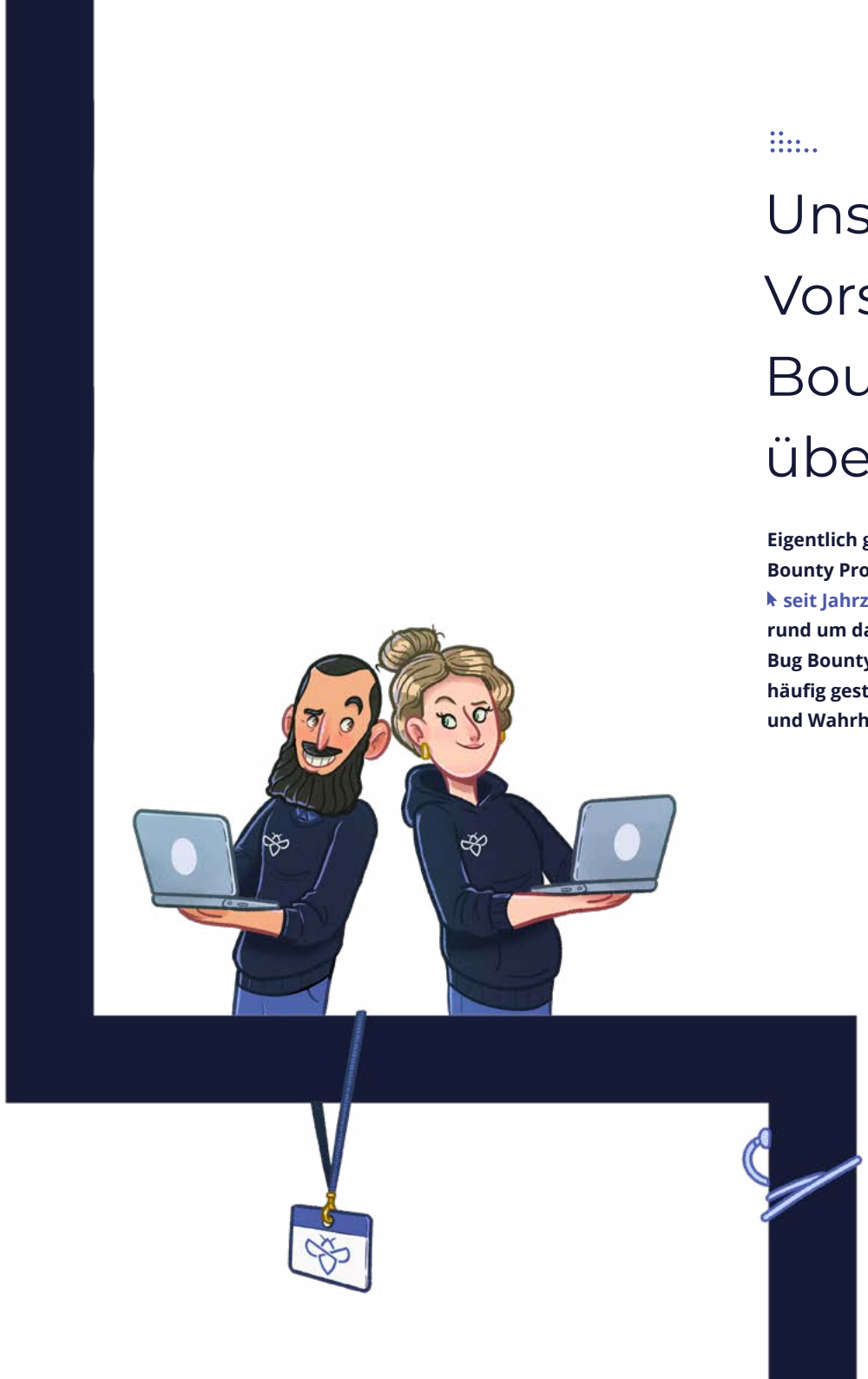
Die Vorteile, beim Aufspüren von Sicherheitslücken den legalen Weg zu wählen, liegen auf der Hand: das Geld, die Anerkennung und dass es mit Coolsein verbunden ist. Vor allem aber heißt ethisches Hacking, Teil einer Gemeinschaft von Leuten zu sein, denen es ein großes Bedürfnis ist, anderen zu helfen.

21 % der Befragten geben an, dass ihr Hauptanliegen ist, etwas Sinnvolles zu tun, und ebenfalls 21 %, den Kampf gegen Cyberkriminalität zu unterstützen.

Warum arbeiten ethische Hacker mit Intigriti?

* Multiple-Choice-Fragen. Die Befragten konnten mehr als eine Antwort wählen.

Quelle: The Ethical Hacker Insights Report 2021 | Intigriti



Unsicherheit und falsche Vorstellungen von Bug Bounty Programmen überwinden

Eigentlich gibt es überhaupt nichts daran zu deuten, worum es bei Bug Bounty Programmen geht. Doch obwohl es Bug Bounty Programme bereits seit Jahrzehnten gibt, halten sich noch immer manche Fehlvorstellungen rund um das Thema. Dies führt dazu, dass manch eine/-r zögerlich ist, in Bug Bounty Programme zu investieren. Hier die Antworten auf sechs häufig gestellte Fragen, die Ihrem Unternehmen helfen, zwischen Mythos und Wahrheit zu unterscheiden.

#Q1

Setze ich mein Unternehmen nicht einem zusätzlichen Risiko aus, wenn ich eine ethische Hacker/-innen-Gemeinschaft einschalte?

Fakt ist, dass Sie, sobald Sie im Internet aktiv sind oder digitale Systeme betreiben, von Hacker/-innen ausgespäht werden können – und böswillige Akteure werden Sie nicht fragen, ob Sie das System Ihres Unternehmens hacken dürfen. Eine ebenso einfache wie bewährte Methode, sich gegen Cyber-Bedrohungen zu schützen ist es, ethische Hacker/-innen hinzuzuziehen. Bug Bounty Programme ermöglichen es, diese Strategie in größerem Stil zu verfolgen, indem sie einen partizipatives („Crowdwourcing-")Konzept für Sicherheitstests bieten.

#Q2

Besteht die Möglichkeit, dass böswillige Hacker/-innen bei der Plattform mitmachen, um als vermeintlich ethische Hacker/-innen aufzutreten?

Das ist aus vielen Gründen äußerst unwahrscheinlich: Ethische Hacker/-innen, die sich bei Intigriti anmelden, müssen eine Reihe rechtlicher Schritte durchlaufen, bevor sie Zugang zur Plattform erhalten. Hierzu zählt unter anderem eine amtliche Überprüfung ihrer Identität.

Darüber hinaus sind Bug Bounty Plattformen nicht wirklich interessant für Cyberkriminelle, was das Aufspüren von Angriffszielen angeht. Bösartige Hacker/-innen suchen in der Regel Möglichkeiten, andere mit minimalem Aufwand schädigen zu können. In dem Moment, in dem Ihr Unternehmen ein Bug Bounty Programm ausschreibt, erklärt es öffentlich, dass es das Thema Sicherheit ernst nimmt, sodass Ihr Profil augenblicklich nicht mehr dem Profil des idealen Hacking-Opfers entspricht.

#Q3

Wir machen bereits jedes Jahr einen Penetrationstest. Brauchen wir zusätzlich noch ein Bug Bounty Programm?

Bei einem Penetrationstest setzen Sie auf eine Person oder eine kleine Gruppe von Menschen – das schränkt die Möglichkeit unterschiedlicher Herangehensweisen ein und bedeutet, dass Sie immer wieder auf die Angriffsmethoden und den Ansatz derselben Person/-en setzen. Die Bezahlung erfolgt nach Stunden oder erbrachter Leistung. Aufgrund ihrer Kosten sind Pentests in der Regel zeitlich befristet und die Pentester/-innen erhalten die Anweisung, sich auf einen begrenzten Ausschnitt zu beschränkten. Ein klassisches Beispiel ist, dass nur bestimmte Cyberangriffsmethoden ausprobiert oder für den Kunden besonders wichtige Bereiche überprüft werden.

Penetrationstester/-innen können durchaus Schwachstellen von hohem Gefährdungspotenzial aufdecken, haben aber wenig Zeit, in die Tiefe zu gehen. Außerdem können sie nichts zum Sicherheitsstatus eines Unternehmens nach Abschluss des Tests sagen. Sobald Ihr Unternehmen beispielsweise ein Update macht oder ein neues Feature herausbringt, verändert sich seine digitale Landkarte und somit auch sein Sicherheitsstatus.

Die Zielsetzung von Penetrationstests ist eine gänzlich andere als die von Bug Bounty Plattformen. Ziel von Penetrationstests ist es, anhand einzelner Sicherheitsprüfungen den Sicherheitsstatus Ihrer Informationen zu einem bestimmten Zeitpunkt zu ermitteln. Bei Bug Bounty Programmen hingegen geht darum, Ihre digitalen Systeme durch kontinuierliche Prüfungen im Blick zu halten.

#Q4

Wir setzen automatische Scanprogramme ein. Bringt das nicht fast genauso viel?

Automatische Scanprogramme kratzen an der Oberfläche des Angriffspotenzials Ihres Unternehmens und identifizieren schwerwiegende Sicherheitslücken. Damit eignet sie sich durchaus dazu, leicht auffindbare Fehler an der Oberfläche zu erkennen, nicht aber, Schwachstellen aufzuspüren, die bei komplexeren Angriffen zum Tragen kommen können.

Die Scanner sind so programmiert, dass sie bekannte Muster von Schwachstellen und Sicherheitslücken erkennen. Böswillige Hacker/-innen tun genau das Gegenteil – genauso wie ethische Hacker/-innen. Sie setzen auf Kreativität und unkonventionelle Denkansätze. Außerdem ist es ein zusätzlicher Anreiz für sie, unentdeckte und schwer fassbare Sicherheitslücken aufzuspüren und hierfür eine geldwerte Belohnung (das „Kopfgeld“) zu erhalten. Die Wahrscheinlichkeit ist also sehr viel größer, dass sie komplexe, aber potenziell schädliche Schwächen in Ihrem System herausarbeiten als ein automatischer Scanner.

#Q5

Was ist der Unterschied zwischen einem öffentlichen und einem geschlossenen Bug Bounty Programm? Und was ist das Richtige für mein Unternehmen?

Öffentlich ausgeschriebene Programme sind allen Interessierten zugänglich. Sie machen sich das Fachwissen Tausender von Forscher/-innen zunutze und sind für Programme mit bereits sehr hohem Sicherheits-Reifegrad gedacht.

Geschlossene Programme bieten Ihrem Unternehmen die Möglichkeit, passend zu den Anforderungen und der Zielsetzung des Programms ausgewählte Communities und Forscher/-innen hinzuzuziehen. Auf diese Weise können Sie Forscher/-innen zu einem Programm einladen, die ihnen bereits vertraut sind, oder bestimmen, welche Art von Forscher/-innen Zugang zu dem Programm bekommen soll. Das Programm ist nur denjenigen bekannt, die zur Teilnahme eingeladen werden, und es können zu jedem Zeitpunkt weitere Forscher/-innen hinzugeladen werden.

Die meisten Unternehmen wählen für den Anfang ein geschlossenes Bug Bounty Programm, bevor sie es später zu einem öffentlichen Programm erweitern. Diese Option eignet sich auch für Unternehmen mit sensibler Testumgebung. Unabhängig von der gewählten Variante kann für jedes Programm ein eigenes Regelwerk aufgestellt werden, das vorgibt, was zum Aufgabenbereich zählt und was nicht, wie hoch das Budget angesetzt wird, welches Prämienschema gilt usw.

#Q6

Wann ist der richtige Zeitpunkt, ein Bug Bounty Programm aufzulegen? Sind wir schon so weit?

Grundsätzlich können Sie jederzeit eine Zusammenarbeit mit ethischen Hacker/-innen starten. Unserer Erfahrung ist es sinnvoll, vor dem Auflegen eines Programms übergeordnete Sicherheitstests durchzuführen (beispielsweise automatische Scans oder Pentests). Das ermöglicht es Ihren Fachleuten, vorab schwerwiegende Sicherheitslücken zu schließen, die sich im Rahmen eines Programms zweifellos zeigen würden, und Ihnen, Ihr Bug Bounty Budget sinnvoller zu nutzen.

Die meisten Unternehmen machen sich gerne zunächst ein erstes Bild von einer Bug Bounty Plattform, bevor sie sich für ein öffentliches Programm entscheiden. In diesem Fall lohnt es sich, mit einem geschlossenen Programm zu beginnen. Das bedeutet, zunächst mit einigen wenigen ausgewählten Sicherheitsforscher/-innen zu arbeiten und nicht gleich mit dem gesamten Netzwerk. Es steht Ihnen auch frei, die Testbereiche einzuschränken oder die Forscher/-innen auf bestimmte Arten von Mängeln anzusetzen, zum Beispiel Schwachstellen mit potenziell finanziellen Auswirkungen. All diese Aspekte können Sie im Projektumfang definieren.

Wenn Sie dann das Gefühl haben, auch mehr Meldungen bewältigen zu können, können Sie den Umfang nach und nach so lange erweitern, bis Sie so weit sind, das Programm öffentlich zu machen (sofern das Ihr Wunsch ist). Und ganz gleich, für welches Programm Sie sich entscheiden: Unser Kundenbetreuungs-Team steht Ihnen gerne bei jedem Schritt Ihrer Reise mit ausgezeichnetem Support zur Seite.

Über Intigriti

Agile Sicherheitstests mit der Power der Gemeinschaft

Die Bug Bounty Plattform von Intigriti bietet kontinuierliche, realitätsnahe Sicherheitstests, die Unternehmen helfen, ihre Assets und ihren Namen zu schützen. Unsere Gemeinschaft ethischer Hacker/-innen unterziehen die Sicherheitssysteme unserer Kunden harten Belastungsproben – denn unsere Tests sind die gleichen, die auch bösartige Hacker/-innen durchführen würden.

> 40.000 Forscher/-innen

Über 40.000 Sicherheitsforscher/-innen nutzen Intigriti für die Suche nach Bugs – und wir werden immer mehr!

Mehr als 300 aktive Bug Bounty Programme

Unternehmen aller Größen und verschiedenster Branchen vertrauen bei der Ausschreibung ihrer Bug Bounty Programme auf Intigriti.

DSGVO-konform

Wir garantieren die Einhaltung höchster Sicherheitsstandards.

Starke europäische Präsenz

Nimmt man die an Hacker/-innen ausgezahlten Prämien als Grundlage, liegen 8 der 10 erfolgreichsten Länder in Europa. Ungeachtet dessen ist Intigriti jedoch ein weltweit agierendes Unternehmen. Im Jahr 2020 gingen aus 140 Ländern Meldungen über Sicherheitslücken ein.

Triage und Kundensupport

Unseren Kunden zur Seite steht ein branchenweit anerkanntes Triage-Team, ein eigens für sie zuständiger Kundenbetreuer (Customer-Success-Manager) und ein Programm-Manager.

www.intigriti.com

Intigriti hackwithintigriti @intigriti intigriti

Kontakt

Sie wünschen Hilfe beim Einstieg in die Kooperation mit ethischen Hackern? Unsere Spezialisten helfen Ihnen gerne, den größtmöglichen Erfolg Ihres Bug Bounty Programm zu gewährleisten. Melden Sie sich noch heute bei den brillantesten und erfahrensten Sicherheitsforscher/-innen der Welt.

WWW.INTIGRITI.COM

HELLO@INTIGRITI.COM

Illustration: Zwoltopia