



Cyber-Sicherheitsrat
Deutschland e.V.

Werkzeugkasten Cybersicherheit



Bug Bounty-Programme

Definition, Einsatzgebiete & Diskussion

Wir sind wehrhaft

Cybersicherheit erscheint uns oft als unbezwingbare Aufgabe: ein **asymmetrisches Setting**, das Angreifern einen taktischen Vorteil gegenüber Sicherheitsexperten verschafft, wachsende Möglichkeiten und die **Professionalisierung von Cyberkriminellen, unklare Zuständigkeiten** und regulatorische Anforderungen bei IT-Sicherheitsinstitutionen und vieles mehr.

Das kann deprimieren.

Was wir dabei oft vergessen sind die vielen Menschen, Ressourcen und Werkzeuge auf der anderen Seite, die tagtäglich daran arbeiten, Wirtschaft und Gesellschaft sicherer zu machen. In der Vergangenheit wurden **wirkungsvolle und starke Methoden** entwickelt, die nur an den richtigen Stellen genutzt werden müssen, um Angreifern einen Schritt voraus zu sein.

Es gibt für alles eine Lösung, man muss sie nur finden – vor allem im Bereich Cybersicherheit. Diese Publikationsreihe stellt übersichtsartig die wichtigsten **Methoden im Kampf gegen Cyberattacken** mit ihren Einsatzgebieten sowie Vor- und Nachteilen vor, damit zukünftig die richtigen Werkzeuge an den passenden Stellen parat stehen.

Ich wünsche Ihnen eine anregende Lektüre und interessante Einblicke in den Werkzeugkasten Cybersicherheit.



Hans-Wilhelm Dünn

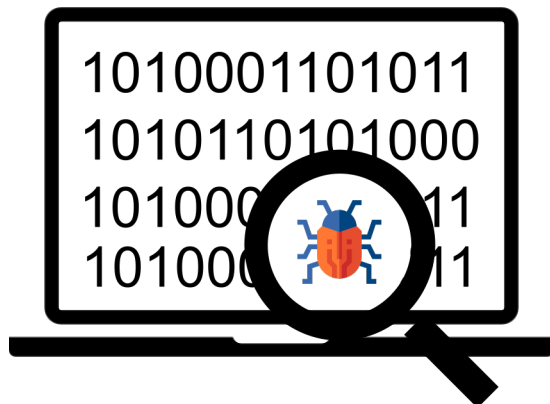
Präsident

Cyber-Sicherheitsrat Deutschland e.V.

Bug Bounty – Was ist das?

Bug Bounty-Programme sind ein **prämiensbasierter Ansatz** zur Auffindung von Schwachstellen in Softwareprodukten. Nach der Art von **Kopfgeldjägern** betätigen sich IT-Spezialisten in ausgeschriebenen **Wettbewerben**, um Fehler („bugs“) zu finden, um anschließend mit einer Prämie („bounty“) honoriert zu werden.

Hersteller von Softwareprodukten nutzen diese Methode, um Schwachstellen von „freundlichen“ Hackern entdecken zu lassen, bevor feindliche Hackerangriffe diese ausnutzen.



Wie sind die Programme gestaltet?


Die Höhe der Prämien ist abhängig vom jeweiligen Bug Bounty-Programm sowie von der Komplexität der gefundenen Fehler. Von einigen hundert bis zu mehreren tausend US-Dollar Belohnung reichen die **Prämienhöhen**, in Einzelfällen können auch bis zu 1 Mio. US-Dollar ausgezahlt werden.

Die gemeldeten Schwachstellen müssen in der Regel **reproduzierbar** sein, um den Herstellern eine Anpassung der Software zu ermöglichen. Man unterscheidet bei den Wettbewerben zwischen **offenen Programmen**, an denen prinzipiell jede und jeder teilnehmen kann sowie **geschlossenen Programmen**, bei denen die Teilnahme auf einen bestimmten Adressatenkreis beschränkt ist, der per Einladung angesprochen wird.

Große Unternehmen wie Apple, Meta, Google oder Microsoft unterhalten eigene Bug-Bounty-Programme. Es gibt jedoch auch **Plattformen**, die im Auftrag anderer Unternehmen Bug Bounty-Programme ausschreiben. Zu den größten Plattformen dieser Art zählen YesWeHack, Open Bug Bounty, Hackerone, Bugcrowd, Intigriti und Synack.



Welche Chancen gibt es?



Die Methode kann unter bestimmten Umständen **kostengünstiger** und **effektiver** zu einer Verbesserung der Sicherheitssituation führen als andere Tools. So entstehen durch den prämierten Ansatz für Hersteller nur relevante Kosten, sofern tatsächliche Fehler gefunden werden, anders als beispielsweise bei einem Penetrationstest, bei dem auch die Beauftragung und Durchführung honoriert werden muss. Insgesamt wird auf diese Weise vermutlich mehr **Zeitaufwand** in die Prüfung investiert, als bei einem durchschnittlichen Penetrationstest avisiert wird.

Zudem profitieren Bug Bounty-Programme von der Schwarmintelligenz zahlreicher IT-Fachkräfte, die mit **unterschiedlichen Herangehensweisen** und Hintergründen die Systeme prüfen. So kann eine Vielzahl von **externen Fachleuten** eingebunden werden. Teilnehmer in den Wettbewerben erhalten die Möglichkeit an herausfordernden Aufgaben zu arbeiten, in einem ethisch korrekten Rahmen zu hacken und dabei ihr fachliches Profil zu schärfen. Neben dem persönlichen Zugewinn an Erfahrung und Reputation winken zudem **attraktive Finanz- oder Sachprämien**.

Welche Risiken gibt es?

Der mögliche **Kostenvorteil** von Bug Bounty-Programmen kann sich ins Gegenteil verkehren, sofern innerhalb des Wettbewerbs besonders viele Sicherheitslücken aufgedeckt werden. In einem solchen Fall besteht auch die Gefahr, dass die firmeninternen IT-Abteilungen mit der **Masse an Schwachstellenmeldungen** überfordert werden und eine effektive Behebung der Sicherheitslücken ausbleibt.

Durch die Arbeit mit externen Fachleuten liegt bei den Teilnehmenden keine **Kenntnis über die firmeninternen Bedürfnisse** vor, wie es beispielsweise bei beauftragten Pentestern der Fall ist. Gibt es beispielsweise bekannte und als akzeptabel eingestufte weniger kritische Sicherheitslücken werden diese in den Wettbewerben trotzdem als Schwachstellen gemeldet.

Das Prüfen von Systemen durch externe Hacker sorgt generell für ein **gesteigertes Risiko bezüglich der Daten- und Informationssicherheit**. Teilnehmende Hacker sind zwar angehalten die Schwachstellen zuerst an die Organisatoren des Wettbewerbs zu melden, dafür sollte jedoch die Prämiengestaltung attraktiv genug sein, damit besonders riskante Schwachstellen nicht im Darknet oder auf anderen Wegen gewinnbringend weitergegeben werden.



Wem nutzen Bug Bounty-Programme?



Prinzipiell können alle Betreiber und Hersteller von Software, von der in Bug Bounty-Programmen generierten **Schwarmintelligenz** profitieren. Insbesondere **Netzbetreiber, Fintech-Unternehmen** aber auch **öffentliche Institutionen** sind Adressaten für diese Art von Sicherheitsüberprüfung.

In der Vergangenheit haben nicht nur die großen Techfirmen und Web-Anwendungen auf Bug Bounty-Programme zurückgegriffen, sondern auch öffentliche Institutionen wie das amerikanische Verteidigungsministerium oder die Europäische Union mit dem Projekt Free and Open Source Software Auditing (EU-FOSSA).

Fazit

Bug Bounty-Programme können eine **sinnvolle Ergänzung** in einem Mosaik von Sicherheitsmaßnahmen sein, die externe Expertise sinnvoll einbinden kann. **Zusätzlich** zu regelmäßigen Pentests können Bug Bounty-Programme eine kontinuierliche Prüfung der Systeme sicherstellen. Die **Methodenvielfalt** geht mit gesteigerten Kosten einher, erhöht jedoch die Sicherheit beträchtlich und kann ein frühzeitiges Entdecken von Schwachstellen gewährleisten.

