Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Nationales Zentrum für Cybersicherheit NCSC

NCSC

Q&A

Bug-Bounty-Programm der Bundesverwaltung

Version: 23.12.2022

Inhalt

1 Was ist ein Bug-Bounty-Programm?

Bug-Bounty-Programme dienen dazu, in Zusammenarbeit mit ethischen Hackern allfällige Verwundbarkeiten in IT-Systemen und in Anwendungen zu identifizieren, zu dokumentieren und zu beheben. Die ethischen Hacker nutzen eigene Methoden, die erlauben, Schwachstellen zu identifizieren, die mit klassischen Penetrationstests oder Security Reviews nicht immer gefunden werden können.

2 Warum setzt die Bundesverwaltung auf Bug-Bounty-Programme?

Bug-Bounty-Programme bieten eine wichtige Unterstützung, damit Unternehmen und auch die Bundesverwaltung ihre IT-Systeme proaktiv auf Schwachstellen prüfen lassen können. Es ist eine effiziente Methode mit einem hohen Return on Investment (ROI) und verbessert das Vertrauen der Öffentlichkeit in die geprüften Systeme («Public Trust»). Bug-Bounty basiert auf dem Crowd-Source Ansatz, d. h. das Know-how der Security Community wird eingesetzt.

Die Bundesverwaltung hat eine wichtige Vorbildrolle gegenüber der Wirtschaft und Gesellschaft. Mit der Institutionalisierung von Bug-Bounty, ethischem Hacking und Crowd-Source-Ansätzen sendet die Bundesverwaltung wichtige Signale in Bezug auf die Erhöhung der Cyberresilienz der Schweizer Infrastruktur.

3 Welches ist die Rolle des NCSC beim Bug-Bounty-Programm?

Das NCSC ist verantwortlich für das Bug-Bounty-Programm der Bundesverwaltung, insbesondere die Beschaffung und die Verwaltung der zentralen Plattform zur Durchführung von Bug-Bounty-Programmen. Bei den Bug-Bounty-Programmen hat das NCSC eine koordinative und unterstützende Aufgabe gegenüber den Verwaltungseinheiten. Ebenfalls informiert das NCSC regelmässig über die Ergebnisse der Bug-Bounty-Programme der Bundesverwaltung.

Konkret sind dies folgende Aufgaben:

- Planung, Priorisierung und Durchführung von Programmen;
- Unterstützung der Verwaltungseinheiten bei der Programmgestaltung und Plattform Schulung;
- Koordination und Kommunikation zwischen den Verwaltungseinheiten und dem Plattform-Betreiber Bug Bounty Switzerland AG;
- Verwaltung und Administration der zentralen Bug-Bounty-Plattform;
- Technische Beurteilung und Triagierung der Schwachstellen in Zusammenarbeit mit Bug Bounty Switzerland;
- Kommunikation in Zusammenarbeit mit den Verwaltungseinheiten;
- Gewährleistung der konformen Rechnungs- und Zahlungsabläufe der Programme.

4 Warum arbeitet die Bundesverwaltung mit Bug Bounty Switzerland AG zusammen?

Das NCSC hat im August 2022 eine zentrale Plattform für Bug-Bounty-Programme beschafft und wird in Zukunft gemeinsam mit der Firma Bug Bounty Switzerland AG in der

Bundesverwaltung Bug Bounty-Programme durchführen. Dank der etablierten Bug Bounty-Plattform und der grossen Community der ethischen Hacker von Bug Bounty Switzerland AG stehen die nötigen Werkzeuge bereit, um weitere Programme der Bundesverwaltung erfolgreich zu starten. Bug Bounty Switzerland AG zählt zu den Pionieren der Schweizer Bug Bounty Szene. Sie bringt eine grosse Expertise bei der Durchführung von Bug Bounty-Programmen und bei der Zusammenarbeit mit ethischen Hackern mit.

5 Was ist ein «Ethical Hacker» im Bug-Bounty-Programm?

Ein ethischer Hacker, oder Hacker mit guten Absichten, ist ein Sicherheitsexperte, der IT-Systeme und Produkte im Auftrag prüft. Dabei sucht er nach Schwachstellen, die auch ein Hacker mit bösartigen Absichten ausnutzen könnte. Bei dieser Schwachstellen-Suche halten sich die ethischen Hacker an einen vordefinierten Rahmen, welcher im Bug-Bounty-Programm festgelegt wird. Finden ethische Hacker eine Schwachstelle, melden sie diese und nutzen sie nicht zu ihrem eigenen Vorteil aus. Für gefundene Schwachstellen wird eine Belohnung (Bounty) ausbezahlt. Die Höhe der Belohnung richtet sich nach der Kritikalität der gefundenen Lücke.

6 Welche IT-Systeme werden geprüft?

Welche Systeme geprüft werden (Scope), bestimmen die jeweiligen Verwaltungseinheiten der Bundesverwaltung in Absprache mit dem NCSC.

7 Wie hoch sind die Belohnungen («Bounties»)? Sind diese generell festgelegt?

Der Bounty-Betrag ist variabel und abhängig von der Kritikalität sowie Relevanz der gefundenen Schwachstelle. Die jeweiligen Bounties werden von den Verwaltungseinheiten, welche ein Bug-Bounty-Programm durchführen, in Zusammenarbeit mit dem NCSC jeweils selbst festgelegt. Sie können daher von Programm zu Programm unterschiedliche ausfallen. Damit Transparenz geschaffen wird, werden die möglichen Bounty-Auszahlungen anhand eines sogenannten «Bounty Grid» zu Beginn eins Programms festgelegt und den ethischen Hackern kommuniziert.

8 Wenn Sicherheitslücken gefunden werden, heisst dies, dass der Bund nicht gut gearbeitet hat und ein unsicheres System im Einsatz hatte? Warum wurden die gemeldeten Sicherheitslücken nicht schon vorgängig gefunden?

Die Technologie entwickelt sich rasch und es entstehen dadurch auch stetig neue Angriffsmöglichkeiten. Damit ist die IT-Sicherheit ein laufender Prozess. Bug-Bounty-Programme dienen dazu, in Zusammenarbeit mit ethischen Hackern, allfällige Verwundbarkeiten in IT-Systemen und in Anwendungen zu identifizieren, zu dokumentieren und zu beheben. Die ethischen Hacker nutzen eigene Methoden, die erlauben, weitere Schwachstellen zu identifizieren, die mit klassischen Penetrationstests nicht immer gefunden werden können.

9 Ist es nicht unverantwortlich, Hacker auf so wichtige Systeme loszulassen?

Bei den eingesetzten Hackern handelt es sich um ethische Hacker, die hochspezialisiert sind und sich sehr verantwortungsvoll Verhalten auf der Suche nach Schwachstellen. Mit ihrer Tätigkeit wollen sie etwas Positives bewirken und dazu beitragen, dass die getesteten Systeme immer wie sicherer werden. Bei der Teilnahme an einem Bug-Bounty-Programm müssen alle ethischen Hacker die Programmrichtlinien akzeptieren und verpflichten sich, sich an die aufgeführten Regeln zu halten.

10 Warum veröffentlichen Sie nicht die kompletten Schwachstellen-Meldungen?

Aus Sicherheitsgründen werden keine Details der Schwachstellen veröffentlicht. Die Ergebnisse werden aber summarisch und zusammenfassend publiziert.

11 Werden alle gefunden Sicherheitslücken jeweils sofort behoben? Was passiert, wenn ein Bug gefunden wird?

Jede Schwachstelle wird jeweils sofort analysiert und die Risiken eingeschätzt. Das Vorgehen für die Behebung der Schwachstellen ist daher abhängig vom Risiko der Ausnutzung der Schwachstelle und die damit verbundenen möglichen Schäden. Je nach Einschätzung dieses Risikos wird die Behebung der Schwachstelle priorisiert.

12 Nach welchen Kriterien werden die Hacker ausgewählt?

Die Auswahl der ethischen Hacker erfolgt durch das NCSC, welches das Bug-Bounty-Programm des Bundes verantwortet, zusammen mit Bug Bounty Switzerland AG. Die Auswahl erfolgt anhand des Programm-Scopes und den betroffenen Technologien. Dabei steht die Fachkenntnis der Hacker, die momentane Verfügbarkeit sowie die positive Erfahrung aus anderen Bug-Bounty-Programmen im Vordergrund.

Bei jedem ethischen Hacker erfolgt vorgängig eine Hintergrundprüfung (engl. KYC – know your customer process) durch Bug Bounty Switzerland AG.
Um sicherzustellen, dass nur identifizierte und überprüfte ethische Hacker an Programmen teilnehmen können - und z. B. keine Transaktionen an ethische Hacker getätigt werden, die beispielsweise auf einer Sanktionsliste geführt werden - überprüft Bug Bounty Switzerland AG die Identität und Integrität der Hacker.
Bei der Teilnahme an einem Bug-Bounty-Programm müssen alle ethischen Hacker die Programmrichtlinien akzeptieren und verpflichten sich, sich an die aufgeführten Regeln zu halten.
Meist werden öffentlich aus dem Internet zugängliche Systeme geprüft, ohne zusätzliche Berechtigungen. Diese Systeme sind in der Regel bereits heute durch die Öffentlichkeit erreichbar. Die Zusammenarbeit mit ethischen Hackern hilft die dabei vorhandenen Risiken realistisch einzuschätzen und möglichst schnell zu minimieren.

13 Nehmen nur Hacker aus der Schweiz teil?

Die ethischen Hacker stammen sowohl aus der Schweiz wie auch aus dem Ausland. Ziel ist eine gute und breite Mischung des Fachwissens und die Nutzung der kollektiven Intelligenz.

14 Welche weiteren Bug-Bounty-Programme sind geplant? Wo finde ich weitere Informationen dazu?

Im Rahmen des Bug-Bounty-Programms der Bundesverwaltung werden fortlaufend weitere Systeme getestet und ins Programm aufgenommen. Das NCSC berichtet in regelmässigen Abständen über den Fortschritt der Programme. Weitere Informationen finden sich auf der NCSC Internetseite.

15 Wird das Bug-Bounty-Programm auch der öffentlichen Verwaltung (Gemeinden und Kantone) angeboten?

Das Bug-Bounty-Programm des NCSC steht aktuell den Verwaltungseinheiten der Bundesverwaltung zur Verfügung. Es wird geprüft, ob und in welchem Umfang die Dienstleistung den Kantonen und Gemeinden angeboten werden kann.

16 Wie werden die Bug-Bounty-Projekte finanziert?

Die zentrale Bug-Bounty-Plattform sowie Grundleistung für die Durchführung von Bug-Bounty-Programmen in der Bundesverwaltung werden durch das NCSC zentral finanziert. Die Belohnungen (Bounties) für ein Bug-Bounty-Programm werden jeweils vom durchführenden Departement oder dessen Verwaltungseinheit bezahlt.

17 Wie lange dauert ein Bug-Bounty-Programm?

Die Dauer wird durch das NCSC in Absprache mit der durchführenden Verwaltungseinheit festgelegt und kann von unterschiedlicher Dauer sein. Die Dauer kann von wenigen Wochen bis zu einem stetigen und kontinuierlichen Programm sein, bei welchem kein Programm-Ende definiert wird.

18 Was ist der Unterschied zwischen einem privaten und öffentlichen Bug-Bounty-Programm?

Bei einem privaten Bug-Bounty-Programm erfolgt die Teilnahme aufgrund einer Einladung (unter Berücksichtigung der oben erwähnten Aufnahmekriterien). Das bedeutet, dass die Steuerung und Skalierung der Anzahl Teilnehmenden, vom Programmmanagement übernommen wird.

Ein halbprivates Bug-Bounty-Programm ist gegen aussen für die Öffentlichkeit ersichtlich, Programmdetails werden aber keine preisgegeben und die Teilnahme ist nur nach einem

erfolgreich durchlaufenen Bewerbungsverfahren (inkl. oben erwähnten Aufnahmekriterien) möglich. Die Steuerung der Anzahl Teilnehmenden hängt nach wie vor vom Programmmanagement ab
Öffentliche Bug-Bounty-Programme stehen, allen interessierten Fachpersonen und der Öffentlichkeit zur Verfügung, es gibt keine spezifischen Aufnahmekriterien.

19 Wie läuft ein Bug-Bounty-Programm ab?

In einem ersten Schritt werden die Ziele des Bug-Bounty-Programms definiert sowie die Rollen und Prozesse geklärt. Danach wird auf der Bug-Bounty-Plattform von Bug Bounty Switzerland AG ein Bug-Bounty-Programm erstellt und dafür sämtliche relevanten Rahmenbedingungen definiert (Scope, Bounty Grid, Legal Safe Harbor, usw.).

Falls das Bug-Bounty-Programm privat ist (siehe vorgängige Frage), werden die gewünschten ethischen Hacker eingeladen und die Anzahl bei Bedarf sukzessive erhöht. Die erhaltenen Meldungen werden von Bug Bounty Switzerland AG und dem NCSC validiert und anschliessend an die entsprechende Verwaltungseinheit zur Behebung weitergeleitet.

Je nach Bedarf werden regelmässige Statusmeetings durchgeführt oder es erfolgt lediglich ein Debriefing zur Auswertung vom Programm am Ende der Laufzeit.

20 Dürfen ethische Hacker nach Ablauf des Bug-Bounty-Programms weiter nach Verwundbarkeiten suchen?

Anhand der Programmrichtlinien wird festgelegt, in welchem Zeitraum die ethischen Hacker nach Verwundbarkeiten suchen dürfen und somit Bounties ausbezahlt werden. Ausserhalb der Bug-Bounty-Programmrichtlinien dürfen gefundene Schwachstellen jederzeit über den Coordinated Vulnerability Disclosure-Prozess gemeldet werden, es werden aber keine Bounties ausbezahlt.

21 Werden nur Testumgebungen getestet oder auch produktive Systeme?

Grundsätzlich erfolgen Bug-Bounty-Programme auf produktiven Systemen und unter realistischen Bedingungen, um einen bestmöglichen Erkenntnisgewinn sicherzustellen. In Ausnahmefällen können aber auch Prüfungen auf Test- oder produktionsnahen Systemen durchgeführt werden. Dies wird zusammen mit der jeweiligen Verwaltungseinheit festgelegt.

22 Inwiefern können Bug-Bounty-Programme einen strategischen Beitrag zur Sicherheit von Infrastrukturen bei Verwaltungen und Unternehmen leisten?

Jedes IT-System verfügt höchstwahrscheinlich über noch unbekannte Schwachstellen. Mit einem Bug-Bounty-Programm lassen sich diese meist schnell und zuverlässig finden. Die Zusammenarbeit mit ethischen Hackern ist eine sehr effektive Art, die Sicherheit der eigenen IT-Systeme zu verbessern. Ebenfalls wird die Transparenz und die öffentliche Wahrnehmung

erhöht (Public Trust).

23 Wo werden die Resultate der Bug-Bounty-Programme veröffentlicht?

Die Kommunikation der Ergebnisse erfolgt durch die Verwaltungseinheiten und in Absprache mit dem NCSC. Das NCSC publiziert die Ergebnisse regelmässig auf der NCSC Internetseite. Es werden keine technischen Details zu den Schwachstellen veröffentlicht.