Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Generalsekretariat EFD
Nationales Zentrum für Cybersicherheit NCSC

1. Juli 2021

Pilotprojekt «Bug Bounty-Programm der Bundesverwaltung»

Abschlussbericht

Inhaltsverzeichnis

1 Management Summary

Das Nationale Zentrum für Cybersicherheit (NCSC) hat vom 10. bis 21. Mai 2021 zusammen mit Bug Bounty Switzerland GmbH, dem Eidgenössischen Departement für auswärtige Angelegenheiten (EDA) und den Parlamentsdiensten (PD) das erste Bug Bounty-Programm für die Bundesverwaltung durchgeführt. Dabei wurden insgesamt sechs IT-Systeme von EDA und PD von total 15 ethischen Hackern auf Sicherheitslücken getestet.

Insgesamt wurden zehn Schwachstellen identifiziert und gemeldet, darunter eine, die als kritisch einzustufen ist. Vier der gemeldeten Schwachstellen konnten bereits während der Pilotdurchführung behoben werden. Schlussendlich wurden CHF 9'240.- an Belohnungen an die Hacker ausbezahlt. Die Gesamtanzahl an Schwachstellenreports ist für einen erstmaligen Test mit ethischen Hackern im Vergleich tief und zeigt auf, dass sämtliche der getesteten IT-Systeme über eine hohe Sicherheitsmaturität verfügen.

Vom verfügbaren Kostendach (CHF 49'900.-) wurden rund CHF 27'300.- aufgebraucht. Der Restbetrag wird für weitere Bug Bounty-Programme in der Bundesverwaltung zurückgestellt.

Das Pilotprojekt hat gezeigt, dass mit Bug Bounty-Programmen Schwachstellen in IT-Systemen effizient identifiziert und behoben werden können und damit ein wichtiger Beitrag zur Cybersicherheit des Bundes geleistet werden kann.

Durch die gewonnenen Erfahrungen und Erkenntnisse sieht das NCSC vor, das Bug Bounty-Programm kontinuierlich auf möglichst viele Systeme und Anwendungen der Bundesverwaltung auszuweiten.

2 Ausgangslage

Eine effektive und wirtschaftlich attraktive Methode, um Schwachstellen aufzudecken, sind Bug Bounty-Programme. Während diese international schon seit einigen Jahren bekannt sind und auch von staatlichen Organisationen genutzt werden, ist deren Verbreitung in der Schweiz noch nicht stark vorgeschritten.

Im Rahmen von Bug Bounty-Programmen werden «ethische Hacker» – Hacker, welche in einem definierten Rahmen legal nach Schwachstellen suchen – dazu aufgerufen, Schwachstellen in den IT-Systemen und Anwendungen einer Organisation aufzuspüren. Für jede gefundene, dokumentierte und bestätigte Schwachstelle (Bug) erhält der erfolgreiche Hacker eine Belohnung (Bounty), abgestuft nach Schweregrad der gefundenen Schwachstelle.

Aufgrund des Willens des Parlaments, solche Programme durchzuführen[1] und um erste Erfahrungen damit zu sammeln, hat das NCSC in Zusammenarbeit mit Bug Bounty Switzerland GmbH (BBS), dem EDA und den PD ein «Bug Bounty-Pilotprojekt» geplant und durchgeführt.

Die Bundesverwaltung – wie auch andere regulierte Branchen – stellt strenge Anforderungen an den Datenschutz und fordert daher einen Datenstandort in der Schweiz. Bug Bounty Switzerland hat als einziger bekannter Anbieter in der Schweiz diese Bedingungen erfüllt. Daher wurde der Pilot mit dieser Firma durchgeführt. Die von BBS entwickelte Plattform wird vollständig in der Schweiz betrieben. Die Plattform basiert auf modernen Cloud-Technologien und erfüllt die Bedürfnisse von Bund und anderen regulierten Branchen wie beispielsweise von kritischen Infrastrukturen.

Ziel des Pilotprojekts war, den Nutzen von Bug Bounty-Programmen für die Bundesverwaltung aufzuzeigen, Sicherheitslücken zu finden und diese zu schliessen und damit die Cyberrisiken effektiv und kosteneffizient zu senken. Ausserdem sollten Erfahrungen gesammelt werden, wie ein Bug Bounty-Programm in den bestehenden Sicherheitsprozess integriert werden kann.

3 Durchführung

Im Rahmen des Pilotprojekts wurde ein massgeschneidertes Bug Bounty-Programm für die Bundesverwaltung aufgebaut, betrieben und ausgewertet.

Das Bug Bounty-Programm zeichnete sich durch eine limitierte Zeitdauer, klar definierte Zielsysteme, ein fixes Projektbudget und eine limitierte Anzahl ethischer Hacker aus. Die zugelassenen ethischen Hacker wurden spezifisch für diesen Piloten eingeladen.

Als Ziele wurden insgesamt sechs IT-Systeme von EDA und PD ausgewählt. Zudem war der Kreis der Bug Bounty-Jäger in diesem ersten Test auf ethische Hacker eingeschränkt, welche BBS oder dem NSCS bekannt sind und sich bereits in anderen Projekten bewährt haben.

Die Durchführung des Bug Bounty-Programms oblag BBS, wurde aber durch das NCSC sowie Vertreter des EDA und der PD eng begleitet. Mit dem Test sollte die Grundlage für eine Diskussion zum weiteren Vorgehen in Bezug auf die Nutzung von Bug Bounty-Programmen

[1] 20.4594 Po Bellaïche «Ethisches Hacking institutionalisieren und Cybersicherheit erhöhen» (https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20204594)

geschaffen werden.

Interessant war vor allem das Zusammenspiel zwischen den Hackern und den jeweiligen Leistungserbringern, die für die Systeme und Anwendungen verantwortlich sind. Dank der sehr guten Dokumentation der gefundenen Schwachstellen durch die ethischen Hacker konnten die verantwortlichen Leistungserbringer das Auffinden der Schwachstellen nachvollziehen und sofort mit der Behebung starten.

War eine Lücke behoben, wurde dies dem Hacker zurückgemeldet, der wiederum kontrollieren konnte, ob allenfalls Nachbesserungen notwendig sind.

Diese wertvolle und von gegenseitigem hohen Vertrauen geprägte Zusammenarbeit ist die Basis für die erfolgreiche Durchführung des Bug Bounty-Programms.

Übersicht über den groben Ablauf des Pilotprojekts:

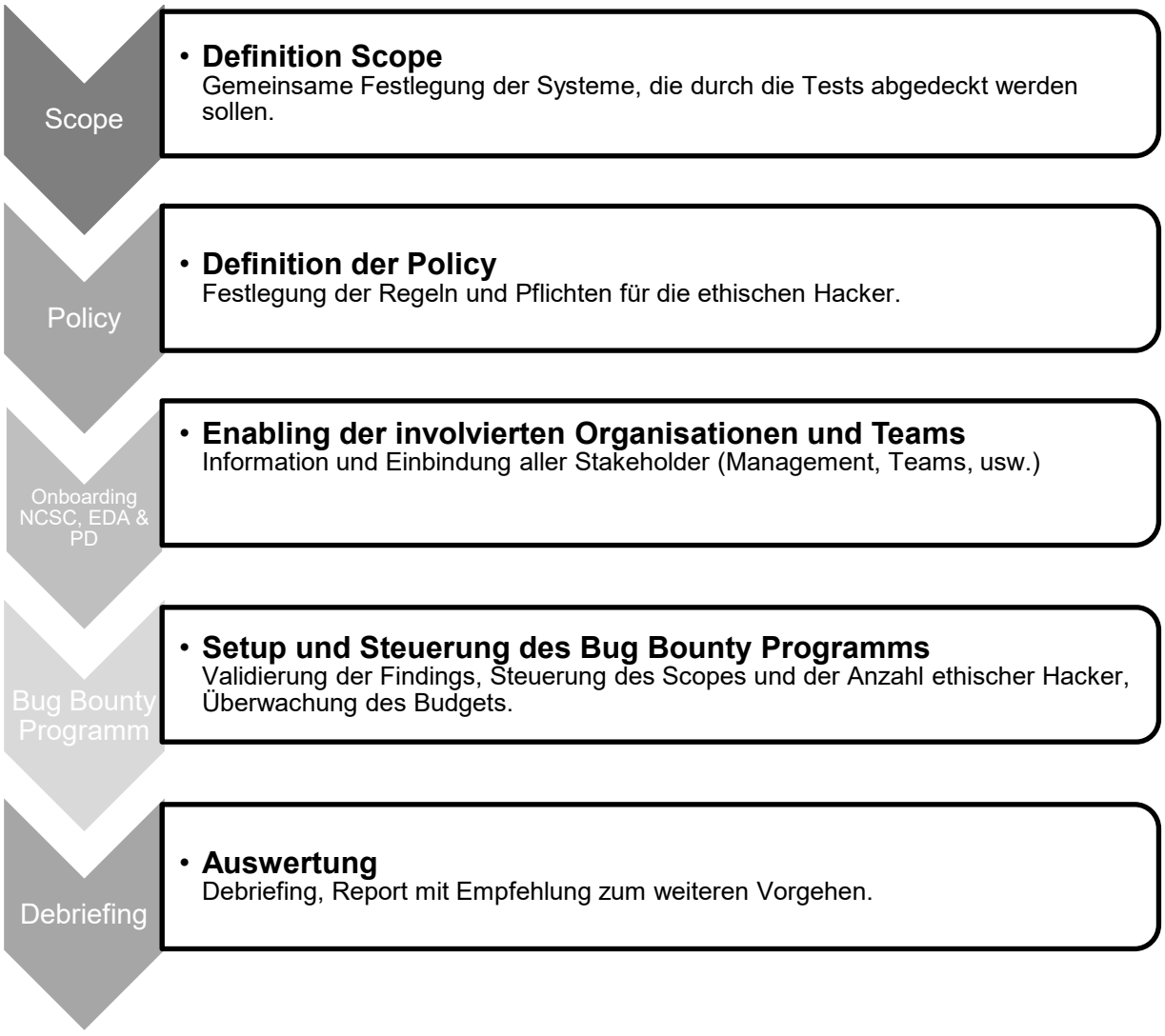

Abbildung 1: Ablauf Pilotprojekt

4 Resultate

Vom Start am 10. Mai, 00.01 Uhr, bis zum Ende der Tests am 21 Mai 2021, 12.00 Uhr, wurden insgesamt zehn Schwachstellen gemeldet. Neun Schwachstellen wurden als gültig bestätigt. Ein Report, gemäss den Regeln des Bug Bounty-Programms, war ein Duplikat.

Die Häufung an Schwachstellenreports zu Beginn des Programms entspricht dabei dem typischen Bild, das bei erstmaligen Tests auf neuen Scopes durch ethische Hacker aufgrund der kompetitiven Regeln entsteht.

Da Bug Bounty-Programme ein agiles Vorgehen fördern und die Anzahl an Reports tief blieb, konnten ab dem 2. Tag des Programms zusätzliche Systeme mit in den erlaubten Scope für die Tests aufgenommen werden (Erhöhung von ursprünglich 3 auf 6 Systeme). Der gute Security-Zustand der Systeme des EDA und der PD wurde durch die eingeladenen ethischen Hacker bestätigt («the scope is hard»).

Als weitere Anpassung wurden zusätzliche ethische Hacker in das Pilotprojekt eingeladen, um die Tests breiter abzustützen (Erhöhung von ursprünglich 9 auf 15 Hacker).

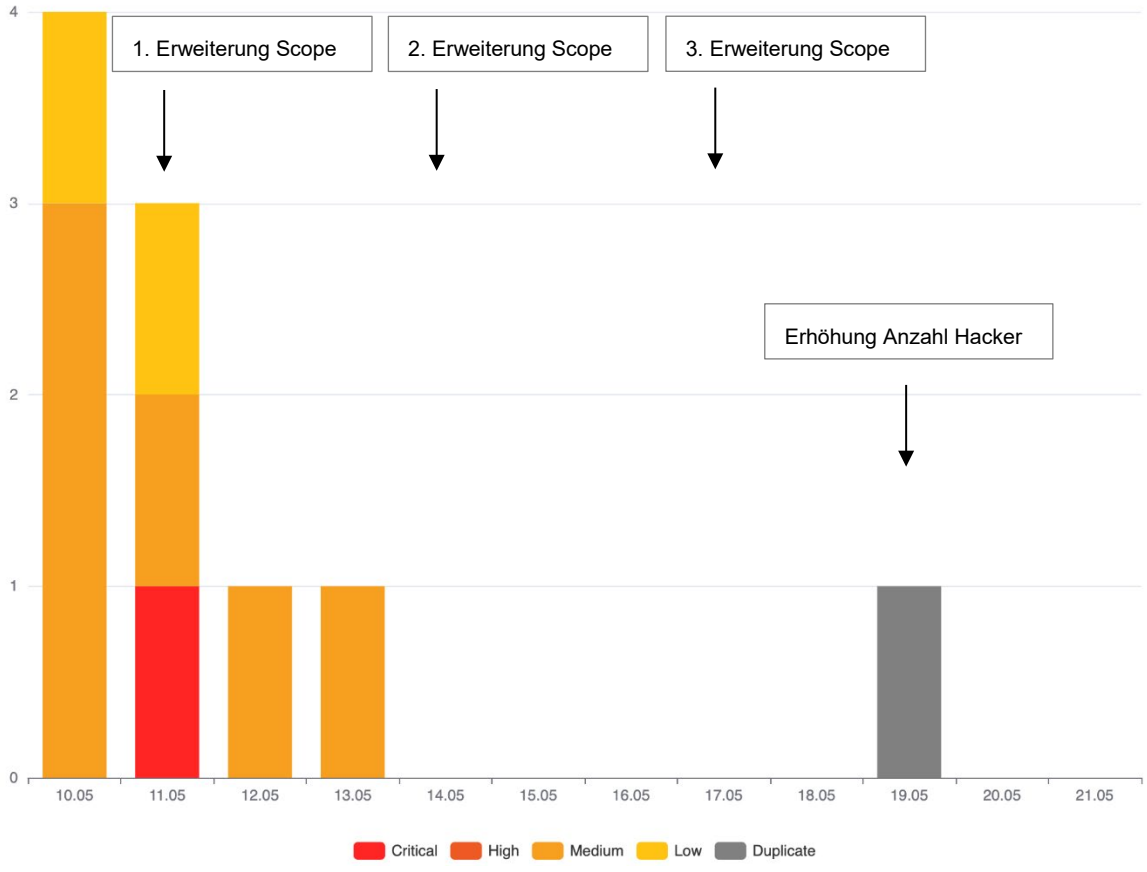

Abbildung 2: Eingegangene Reports nach Kritikalität

Die gemeldeten Sicherheitslücken liessen sich folgendermassen aufteilen:

	Critical	High	Medium	Low	None	Total
Testsystem A	0	0	0	1	0	1
Testsystem B	0	0	0	0	0	0
Testsystem C	0	0	2	0	0	2
Testsystem D	1	0	5	1	0	7
Total	**1**	**0**	**7**	**2**	**0**	**10**

Welche IT-Systeme konkret Teil des Bug Bounty-Pilotprojekts waren, wird nicht kommuniziert. Deshalb werden diese Systeme mit «Testsystem A – D» beschrieben.

5 Finanzierung

Für die Durchführung dieses Pilotprojektes stellte der Bund ein Kostendach von CHF 49'900.- für externe Leistungen zur Verfügung. Die Kostenzusammenstellung präsentiert sich folgendermassen:

Kostendach	CHF	49'900.00
Aufwand für Onboarding, technische Umsetzung usw.	CHF	13'375.00
Ausbezahlte Bounties	CHF	9'240.00
Restbetrag	**CHF**	**27'285.00**

Der genannte Restbetrag wird zurückgestellt und für weitere Bug Bounty-Programme der Bundesverwaltung eingesetzt. Dabei ist es Ziel, möglichst nahtlos weitere Bug Bounty-Programme durchzuführen.

6 Fazit

Das Pilotprojekt hat gezeigt, dass mit Bug Bounty-Programmen Schwachstellen in IT-Systemen und Anwendungen effizient identifiziert und behoben werden können. Der «Return on Invest» wurde als hoch identifiziert. Durch den Betrieb eines Bug Bounty-Programmes für die Bundesverwaltung durch das NCSC kann ein wichtiger Beitrag zur Reduktion der Cyberrisiken des Bundes geleistet werden.

Das Echo sowohl der PD als auch der IT EDA war durchwegs positiv. Von diversen Verwaltungseinheiten besteht der Bedarf nach Leistungen im Rahmen eines Bug Bounty-Programmes. Es hat sich gezeigt, dass die zentrale Verwaltung und Unterstützung durch das Schwachstellenmanagement des NCSC und die dezentrale Behebung der Schwachstellen bei den verantwortlichen Leistungserbringern effizient und nachhaltig ist.

Durch die gewonnenen Erfahrungen mit dem Piloten und den Erkenntnissen aller Beteiligten sieht das NCSC vor, das Bug Bounty-Programm kontinuierlich auf möglichst viele Systeme der Bundesverwaltung auszuweiten.

Der Beschaffungsprozess soll deshalb möglichst rasch gestartet werden. In der Übergangsphase soll mit den verbleibenden Mitteln aus dem Pilotprojekt das gestartete Bug Bounty-Programm in der Bundesverwaltung weitergeführt werden.