Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundeskanzlei BK

Bereich Digitale Transformation und IKT-Lenkung (DTI)

18. Oktober 2022

Bug-Bounty-Programm eIAM

Bericht

Inhaltsverzeichnis

1 Management Summary

eIAM ist das Zugriffs- und Berechtigungssystem der Bundesverwaltung für Web-Applikationen und native Mobile Apps. Der für den eIAM-Service verantwortliche Bereich Digitale Transformation und IKT-Lenkung (DTI) der Bundeskanzlei, das Bundesamt für Informatik und Telekommunikation (BIT) als Systembetreiberin und das für das Bug-Bounty-Programm zuständige Nationale Zentrum für Cybersicherheit (NCSC) haben ein Private-Bug-Bounty-Programm gemeinsam mit der Firma Bug Bounty Switzerland AG vom 30. August bis 11. Oktober 2022 durchgeführt.

Insgesamt wurden 28 Schwachstellen identifiziert und gemeldet. 14 davon wurden als gültig bestätigt. Es wurden CHF 5’700 an Belohnungen an die ethischen Hacker ausbezahlt.

Die Gesamtzahl an gemeldeten Schwachstellen ist für einen erstmaligen Test mit ethischen Hackern im Vergleich durchschnittlich. Es wurden keine kritischen Sicherheitslücken gefunden.

Das Bug-Bounty-Programm von eIAM wird nun pausiert, um die gesammelten Erfahrungen auszuwerten und die allfälligen organisatorischen Anpassungen für einen möglichen weiteren Lauf umzusetzen.

2 Ausgangslage

eIAM ist das Zugriffs- und Berechtigungssystem der Bundesverwaltung für Web-Applikationen und native Mobile Apps. eIAM ist damit die zentrale Login-Infrastruktur des Bundes. Der Service wird von über 1’000 Fachapplikationen verwendet. Über die eIAM-Infrastruktur erfolgen durchschnittlich 550'000 Anmeldungen pro Tag. Der Bereich Digitale Transformation und IKT-Lenkung (DTI) ist für die Steuerung und Führung der Infrastruktur zuständig. Das Bundesamt für Informatik und Telekommunikation (BIT) stellt die Entwicklung und den Betrieb sicher.

Bug-Bounty-Programme sind eine effektive und wirtschaftlich attraktive Methode, um Schwachstellen aufzudecken, sind. Standardisierte Sicherheitstests reichen heute häufig nicht mehr aus, um die versteckten Lücken zu finden. Das im Frühjahr 2021 durchgeführte Pilotprojekt in der Bundesverwaltung hat gezeigt, dass mittels Bug-Bounty-Programmen Schwachstellen in IT-Systemen und Anwendungen effizient identifiziert und angegangen werden können. Aufgrund dieser Erkenntnisse hat der Bund im August 2022 eine Plattform für Bug-Bounty-Programme beschafft[1].

Im Rahmen von Bug-Bounty-Programmen werden ethische Hacker – Hacker, die 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 auf Basis eines internationalen, anerkannten Standards.

[1] Bundesverwaltung beschafft Plattform für Bug Bounty-Programme (admin.ch)

3 Durchführung

Der für den eIAM-Service verantwortliche Bereich DTI der Bundeskanzlei, das BIT als Systembetreiberin und das für das Bug-Bounty-Programm zuständige NCSC haben diese Systemüberprüfung gemeinsam mit der Firma Bug Bounty Switzerland AG durchgeführt.

Das Bug-Bounty-Programm von eIAM hat vom 30. August bis 11. Oktober 2022 stattgefunden. Die zugelassenen ethischen Hacker wurden spezifisch für dieses Private-Bug-Bounty-Programm eingeladen. Die Durchführung fand auf der Abnahme-Umgebung von eIAM statt, die gleich aufgebaut ist wie die Produktionsumgebung. In der Abnahme-Umgebung stehen nur Test-Daten zur Verfügung.

Am Anfang wurden das System für Account Management sowie diverse Login-Funktionalitäten (CH-Login, Harrods-Login, eIAM-Login und FED-Login) als Scope definiert und ausgewählt. Nach vier Wochen wurde der Scope auf weitere Funktionalitäten ausgeweitet (delegiertes Management und KeyCloak OIDC).

Der Kreis wurde auf ethische Hacker eingeschränkt, die dem NCSC oder Bug Bounty Switzerland AG bekannt sind und sich bereits in anderen Projekten bewährt haben. Die Anzahl der ethischen Hacker wurde im Verlauf des Programms von 9 auf 32 erhöht.

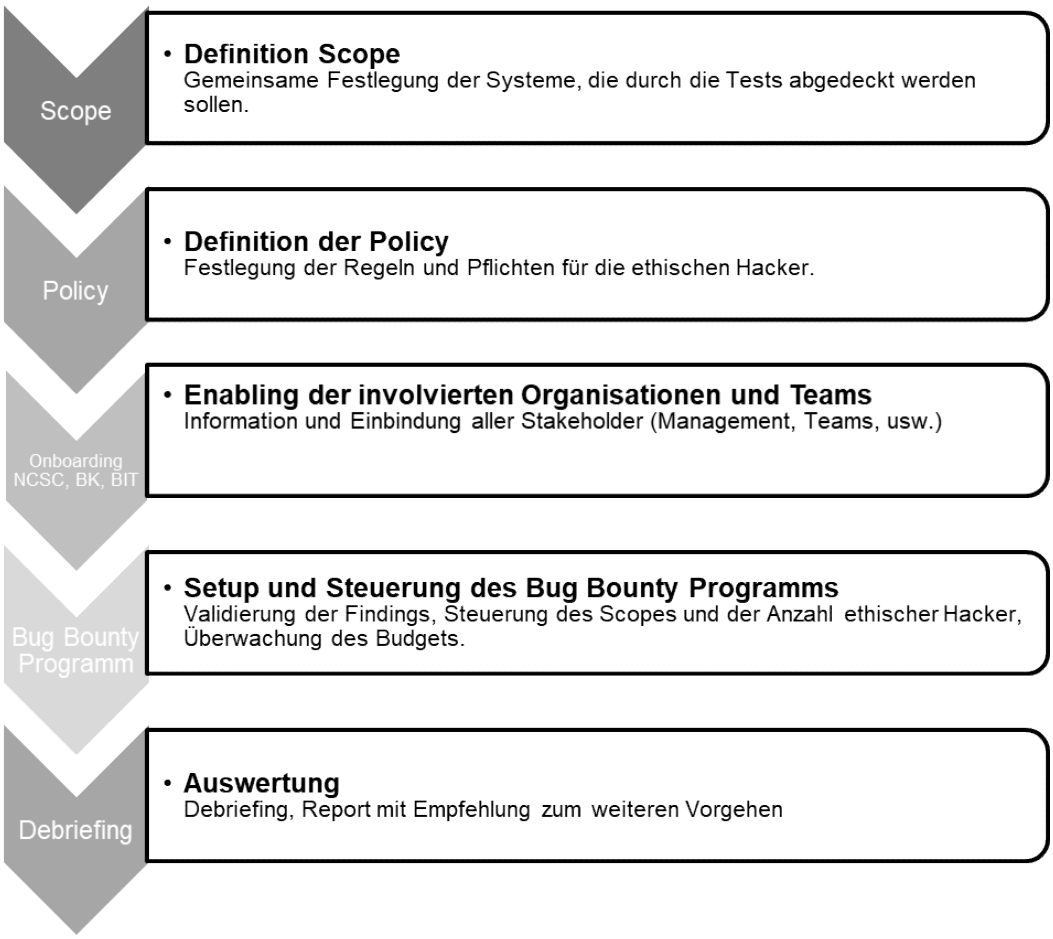
Die Schwachstellen wurden anhand der weltweit anerkannten Skala CVSS[2] auf Grund ihrer Kritikalität in «tief», «mittel», «hoch» oder «kritisch» eingestuft. Die Skala erlaubt eine sachliche Diskussion zwischen den verantwortlichen Stellen und den ethischen Hackern über die Kritikalität und die Auswirkung der Schwachstelle. Eine Abweichung zwischen der gemeldeten Kritikalität und der bestätigten Kritikalität ist nicht ungewöhnlich und kann mit den von der Skala vorgegebenen Parametern begründet werden.

Das Entwicklungsteam von eIAM hat die Behebung der bestätigten Findings mit den folgenden Regeln priorisiert:

- Kritisch: sofortige Behebung
- Hoch: rasche Behebung
- Mittel: Behebung Anhand der Release-Planung
- Tief: optionale Behebung, ja nach Auswirkung

[2] Siehe z.B. https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Für das Bug-Bounty-Programm des Bundes wurde ein Standardvorgehen definiert, das erfolgreich durchlaufen wurde:

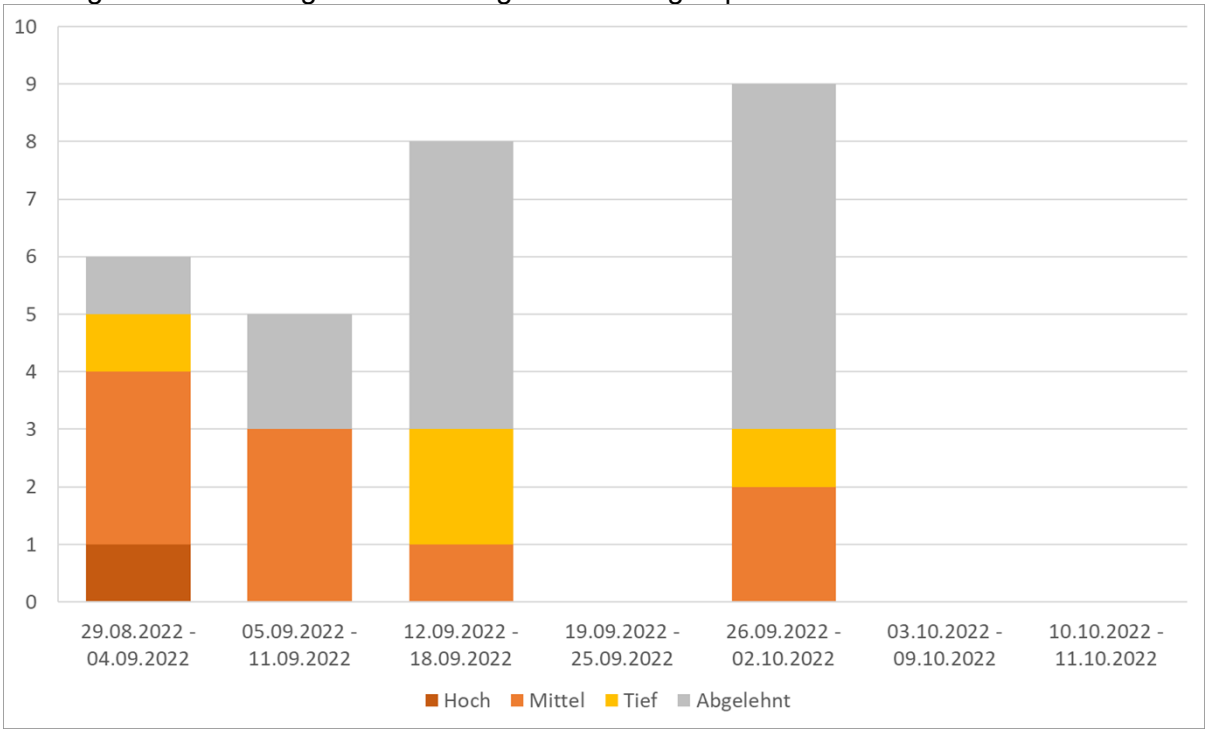


Das Bug-Bounty-Programm von eIAM wird pausiert, damit die gesammelten Erfahrungen ausgewertet und die allfälligen organisatorischen Anpassungen für einen möglichen weiteren Lauf umgesetzt werden können.

4 Resultate

Vom Start am 30. August 2022 um 09:00 Uhr bis zum zwischenzeitlichen Ende des Programms am 11. Oktober 2022 um 23:59 Uhr, wurden insgesamt 28 Schwachstellen gemeldet. 14 Schwachstellen wurden als gültig bestätigt. Die Gründe, um eine gemeldete Schwachstelle abzulehnen, waren insbesondere duplizierte Meldungen oder Meldungen ausserhalb des vordefinierten Scope.

Die folgende Grafik zeigt die Verteilung der Meldungen pro Woche:



Die bestätigten Sicherheitslücken liessen sich folgendermassen aufteilen:

	Kritisch	Hoch	Mittel	Tief	Total
Anzahl Schwachstellen	**0**	**1**	**9**	**4**	**14**

Die Schwachstelle mit Kritikalität «hoch» konnte während des Programms geschlossen werden. Die anderen Schwachstellen fliessen in die Planung der nächsten Releases ein.

Die Häufung an Schwachstellen-Reports zu Beginn des Programms entspricht dem typischen Bild, das bei erstmaligen Bug-Bounty-Programmen auf neuen Scopes durch ethische Hacker aufgrund der kompetitiven Regeln entsteht.

Interessant war das Zusammenspiel zwischen den Hackern und den operativen IT-Stellen, die für die Systeme und Anwendungen verantwortlich sind. Dank der sehr guten Dokumentation der gefundenen Schwachstellen durch die ethischen Hacker konnten die verantwortlichen Stellen das Auffinden der Schwachstellen nachvollziehen und sofort mit der Analyse starten. Diese wertvolle und von gegenseitigem Vertrauen geprägte Zusammenarbeit ist die Basis für die erfolgreiche Durchführung von Bug-Bounty-Programmen.

5 Finanzierung

Die Durchführung wurde in Rahmen des Betriebsbudgets von eIAM organisiert. Die Höhe der bezahlten Bountys (Belohnung) liegt bei CHF 5’700.

6 Fazit

Während der ersten Wochen des eIAM Bug-Bounty-Programms hat sich gezeigt, dass Schwachstellen effizient identifiziert und angegangen werden konnten. Die Qualität und der Inhalt der Meldungen haben gezeigt, dass diese Methode komplementär zu anderen Methoden funktioniert. Dies, weil die ethischen Hacker Schwachstellen melden, die bei üblichen Sicherheitstests nicht immer gefunden werden können.