Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Centro nazionale per la cibersicurezza NCSC

Q&A - Programma «bug bounty» dell'Amministrazione federale

Versione: 23.12.2022

Contenuto

1 Che cos'è un programma «bug bounty»?

I programmi «bug bounty» servono a identificare, documentare e risolvere eventuali vulnerabilità nei sistemi informatici e nelle applicazioni grazie alla collaborazione con hacker etici. Questi ultimi utilizzano metodi specifici che permettono loro di individuare i punti deboli che non sempre possono essere scoperti tramite i classici test e controlli di sicurezza («penetration test» e «security review»).

2 Perché l'Amministrazione federale utilizza programmi «bug bounty»?

I programmi «bug bounty» sono uno strumento utile con cui le imprese e l'Amministrazione federale possono far verificare in modo proattivo i propri sistemi informatici per individuare eventuali vulnerabilità. Si tratta di un metodo efficiente con un elevato ritorno sull'investimento («return on invest», ROI) che migliora la fiducia del pubblico nei confronti dei sistemi verificati («public trust»). Un programma «bug bounty» si basa sull'approccio «crowdsourcing», che sfrutta cioè le competenze della cosiddetta «security community».

L'Amministrazione federale ricopre un ruolo modello per l'economia e la società. Attraverso l'istituzionalizzazione dei programmi «bug bounty», la collaborazione con hacker etici e il «crowdsourcing» lancia un chiaro segnale sull'importanza di rafforzare la ciber-resilienza dell'infrastruttura svizzera.

3 Qual è il ruolo dell'NCSC nei programmi «bug bounty»?

L'NCSC è responsabile del programma «bug bounty» dell'Amministrazione federale, più precisamente dell'acquisizione e della gestione della piattaforma centrale per l'esecuzione di programmi «bug bounty». In questi programmi l'NCSC riveste un ruolo di coordinamento e supporto per le varie unità amministrative. Allo stesso tempo, l'NCSC informa regolarmente sui risultati dei programmi «bug bounty» dell'Amministrazione federale.

Nel concreto svolge i seguenti compiti:

- pianificazione, definizione delle priorità ed esecuzione dei programmi;
- supporto alle unità amministrative nella definizione del programma e nell'utilizzo della piattaforma didattica;
- coordinamento e comunicazione tra le unità amministrative e il gestore della piattaforma Bug Bounty Switzerland SA;
- gestione e amministrazione della piattaforma centrale per i programmi «bug bounty»;
- valutazione tecnica e triage delle vulnerabilità in collaborazione con Bug Bounty Switzerland;
- comunicazione in collaborazione con le unità amministrative;
- garanzia della conformità dei processi di fatturazione e pagamento dei programmi.

4 Perché l'Amministrazione federale collabora con Bug Bounty Switzerland SA?

Nell'agosto del 2022 l'NCSC ha acquisito una piattaforma centrale per i programmi «bug bounty» e, in futuro, assieme alla ditta Bug Bounty Switzerland SA, attuerà programmi «bug bounty» presso l'Amministrazione federale. Grazie a questa piattaforma affermata e alla grande comunità di hacker etici di Bug Bounty Switzerland SA, l'Amministrazione dispone di tutti gli strumenti necessari per avviare con successo i prossimi programmi. Bug Bounty Switzerland SA è una delle società pioniere nel panorama «bug bounty» svizzero. Vanta un grande know-how nella realizzazione di questi programmi e nella cooperazione con hacker etici.

5 Che cosa si intende per «hacker etico» nel programma «bug bounty»?

Un hacker etico, detto anche hacker con buone intenzioni, è un esperto di sicurezza incaricato di verificare i sistemi e i prodotti informatici. Cerca le vulnerabilità che un hacker malintenzionato potrebbe invece sfruttare a suo vantaggio. In questa ricerca gli hacker etici si attengono a linee guida predefinite, contenute nel programma «bug bounty». Nel caso i cui dovessero scovare una vulnerabilità, sono tenuti a segnalarla e non possono sfruttarla per trarne un vantaggio personale. Per ogni vulnerabilità individuata è previsto un compenso («bounty»), il cui importo è stabilito in base alla criticità della falla trovata.

6 Quali sistemi informatici vengono verificati?

Le singole unità amministrative federali stabiliscono assieme all'NCSC quali sistemi devono essere sottoposti a verifica («scope»).

7 A quanto ammontano i compensi («bounty»)? È prevista una tariffa fissa?

I compensi sono variabili e dipendono dalla criticità e dalla rilevanza della vulnerabilità individuata. Sono stabiliti dalle unità amministrative che eseguono i programmi «bug bounty», d'intesa con l'NCSC. Per questo motivo possono variare di programma in programma. Ai fini di trasparenza, l'erogazione dei compensi viene fissata sulla base di una tabella («bounty grid») all'inizio del programma e comunicata all'hacker etico.

8 Se si riscontrano falle di sicurezza, significa che la Confederazione non ha svolto un buon lavoro e che sta usando un sistema non sicuro? Perché le falle di sicurezza segnalate non sono state individuate prima?

La tecnologia si sviluppa rapidamente e, di conseguenza, si presentano in continuazione nuove possibilità di attacco. La sicurezza informatica è dunque in continua trasformazione. I programmi «bug bounty» servono a identificare, documentare e risolvere eventuali vulnerabilità nei sistemi informatici e nelle applicazioni grazie alla collaborazione con hacker etici. Questi ultimi utilizzano metodi specifici che permettono loro di individuare i punti deboli che non sempre possono essere scoperti tramite i classici test e controlli di sicurezza.

9 Non è irresponsabile lasciare agli hacker libero accesso a sistemi così importanti?

Gli esperti incaricati sono hacker etici, profili altamente specializzati che ricercando le vulnerabilità agiscono in modo responsabile. Con la loro attività intendono fornire un contributo positivo affinché i sistemi verificati diventino sempre più sicuri. Tutti gli hacker etici che partecipano a un programma «bug bounty» sono tenuti ad accettare le linee guida del programma e a rispettare le regole indicate.

10 Perché non vengono pubblicate nella loro interezza le segnalazioni relative alle vulnerabilità?

Per motivi di sicurezza non vengono pubblicati i dettagli riguardanti le vulnerabilità. I risultati vengono resi noti in modo sommario e riassuntivo.

11 Le falle di sicurezza riscontrate vengono risolte immediatamente? Che cosa succede se viene scoperto un bug?

Per ogni vulnerabilità si eseguono subito un'analisi e una valutazione dei rischi. La procedura volta a eliminare una vulnerabilità dipende quindi dal rischio di sfruttamento di quest'ultima e dagli eventuali danni connessi. In base alla stima di questo rischio si stabilisce l'ordine di priorità per l'eliminazione delle falle.

12 In base a quali criteri vengono selezionati gli hacker?

In collaborazione con Bug Bounty Switzerland SA, l'NCSC seleziona gli hacker etici responsabili del programma «bug bounty» della Confederazione. La selezione si basa sul contesto di esecuzione del programma e sulle tecnologie coinvolte. Sono quindi centrali le conoscenze specifiche dell'hacker, la sua disponibilità e l'esperienza maturata nell'ambito di altri programmi «bug bounty».

Per ogni hacker etico la società Bug Bounty Switzerland SA svolge in via preliminare un controllo approfondito (processo «KYC»: «know your customer»).
Questo permette di garantire che possano partecipare ai programmi solamente hacker etici identificati e sottoposti a controllo e che, ad esempio, non vengano effettuate transazioni con chi figura in una lista di soggetti sanzionati. Bug Bounty Switzerland SA si occupa della verifica dell'identità e dell'integrità degli hacker.
Tutti gli hacker etici che intendono partecipare a un programma «bug bounty» sono tenuti ad accettare le linee guida del programma e a rispettare le regole indicate.
Nella maggior parte dei casi i sistemi controllati sono pubblicamente accessibili da Internet e non richiedono ulteriori autorizzazioni. Di solito questi sistemi sono già disponibili per il pubblico. La collaborazione con gli hacker etici aiuta a valutare realisticamente i rischi connessi e a ridurli al minimo il più rapidamente possibile.

13 Partecipano solamente hacker provenienti dalla Svizzera?

Gli hacker etici provengono sia dalla Svizzera sia dall'estero. L'obiettivo è approfittare di un ampio ventaglio di conoscenze specialistiche e utilizzare l'intelligenza collettiva.

14 Quali sono gli altri programmi «bug bounty» previsti? Dove si trovano ulteriori informazioni al riguardo?

Nell'ambito del programma «bug bounty» dell'Amministrazione federale vengono costantemente testati altri sistemi, che sono in seguito integrati nel programma. A cadenza regolare l'NCSC riferisce in merito ai progressi dei programmi. Sono disponibili ulteriori informazioni sul sito Internet dell'NCSC.

15 Il programma «bug bounty» viene offerto anche all'amministrazione pubblica (Comuni e Cantoni)?

Al momento, il programma «bug bounty» dell'NCSC è a disposizione delle unità dell'Amministrazione federale. Si sta valutando se e in quale misura il servizio possa essere offerto ai Cantoni e ai Comuni.

16 Come vengono finanziati i progetti «bug bounty»?

La piattaforma centrale «bug bounty» e il servizio di base per l'esecuzione del programma «bug bounty» presso l'Amministrazione federale vengono finanziati dall'NCSC in modo centralizzato. I compensi («bounty») vengono pagati dal dipartimento o dall'unità amministrativa che organizza il programma.

17 Quanto dura un programma «bug bounty»?

La durata viene stabilita dall'NCSC in accordo con l'unità amministrativa incaricata dell'esecuzione. Un programma può durare alcune settimane ma può anche essere concepito come un processo costante e continuo, senza una data di scadenza.

18 Qual è la differenza tra un programma «bug bounty» privato e uno pubblico?

Nel caso di un programma «bug bounty» privato, gli hacker etici possono partecipare soltanto su invito (se rispettano i criteri di ammissione sopra menzionati). Ciò significa che il controllo e l'adeguamento del numero di partecipanti sono affidati alla gestione del programma.
Un programma «bug bounty» semiprivato è reso pubblico ma i dettagli non vengono divulgati; gli hacker etici possono parteciparvi solamente se superano la procedura di candidatura (e se rispettano i criteri di ammissione sopra menzionati). Anche in questo caso, il controllo del numero di partecipanti dipende dalla gestione del programma.

Un programma «bug bounty» pubblico è aperto a tutti gli esperti interessati e al pubblico. La partecipazione non è subordinata ad alcun criterio di ammissione specifico.

19 Come si svolge un programma «bug bounty»?

In una prima fase si definiscono gli obiettivi del programma «bug bounty» nonché i ruoli e i processi. In seguito, sulla piattaforma «bug bounty» di Bug Bounty Switzerland SA viene elaborato un apposito programma. In questa fase vengono definite tutte le condizioni quadro rilevanti («scope», «bounty grid», «legal safe harbor» ecc.).

Se il programma «bug bounty» è privato (v. domanda precedente), gli hacker etici selezionati ricevono un invito. Il loro numero può essere aumentato progressivamente, in base alle necessità. Le segnalazioni ricevute vengono validate da Bug Bounty Switzerland SA e dall'NCSC e inoltrate all'unità amministrativa toccata affinché proceda all'eliminazione delle vulnerabilità.

A seconda del caso si convocano riunioni di aggiornamento a cadenza regolare o si valuta il programma alla sua conclusione.

20 Una volta concluso il programma «bug bounty», gli hacker etici sono autorizzati a continuare a cercare le vulnerabilità?

Le linee guida del programma stabiliscono il periodo di tempo durante il quale gli hacker etici sono autorizzati a cercare le vulnerabilità e quindi a percepire i compensi. Al di fuori di questo periodo, le vulnerabilità individuate possono essere segnalate in qualsiasi momento tramite il processo «coordinated vulnerability disclosure». Tuttavia non sarà corrisposto alcun compenso.

21 Vengono verificati soltanto gli ambienti di test o anche i sistemi produttivi?

In linea di principio si eseguono i programmi «bug bounty» su sistemi produttivi e in condizioni realistiche per massimizzare le conoscenze. In casi eccezionali, tuttavia, i controlli possono essere eseguiti anche su sistemi di test o su sistemi simili a quelli di produzione. La decisione è presa in accordo con la rispettiva unità amministrativa.

22 In che misura i programmi «bug bounty» possono fornire un contributo strategico alla sicurezza delle infrastrutture di amministrazioni e imprese?

Ogni sistema informatico contiene molto probabilmente delle vulnerabilità ancora sconosciute che, grazie a un programma «bug bounty», è possibile individuare in modo rapido e affidabile. La collaborazione con hacker etici è un metodo molto efficace per migliorare la sicurezza dei sistemi informatici. Al contempo, contribuisce ad aumentare la trasparenza e la fiducia dell'opinione pubblica («public trust»).

23 Dove vengono pubblicati i risultati dei programmi «bug bounty»?

I risultati sono comunicati dalle unità amministrative, d’intesa con l’NCSC. Quest’ultimo li pubblica regolarmente sulla propria pagina Internet. Non viene divulgato alcun dettaglio tecnico relativo alle vulnerabilità.