Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Segreteria generale
Centro nazionale per la cibersicurezza (NCSC)

1° luglio 2021

Progetto pilota «Programma bug bounty dell'Amministrazione federale»

Rapporto finale

Indice

1 Sintesi

Dal 10 al 21 maggio 2021, il Centro nazionale per la cibersicurezza (NCSC) ha eseguito il primo programma bug bounty per l'Amministrazione federale in collaborazione con la società Bug Bounty Switzerland Sagl (BBS), il Dipartimento federale degli affari esteri (DFAE) e i Servizi del Parlamento (SP). In questo contesto 15 hacker etici hanno testato complessivamente sei sistemi informatici del DFAE e dei SP per individuare eventuali falle di sicurezza.

In totale sono state rilevate e segnalate dieci vulnerabilità, di cui una classificata come «critica». Tra le vulnerabilità segnalate, quattro sono state rimosse già nella fase di test pilota. Alla fine sono stati versati 9240 franchi per ricompensare gli hacker che hanno partecipato al progetto. Il numero complessivo delle vulnerabilità segnalate è relativamente basso per un primo test con un gruppo di hacker etici e mostra che tutti i sistemi verificati dispongono di un alto livello di sicurezza.

Sui 49 900 franchi massimi autorizzati a copertura dei costi, sono stati impiegati circa 27 300 franchi. I fondi non utilizzati saranno accantonati per i prossimi programmi bug bounty nell'Amministrazione federale.

Il progetto pilota ha dimostrato che con i programmi bug bounty è possibile individuare ed eliminare efficientemente le vulnerabilità dei sistemi informatici e, così, contribuire in modo significativo alla cibersicurezza della Confederazione.

Sulla base delle esperienze e delle conoscenze acquisite, l'NCSC prevede di eseguire programmi bug bounty in maniera continuativa e possibilmente sul maggior numero possibile di sistemi e applicazioni dell'Amministrazione federale.

2 Situazione iniziale

Un metodo efficace ed economicamente vantaggioso per scoprire eventuali vulnerabilità dei sistemi informatici è rappresentato dai programmi bug bounty. Mentre nel contesto internazionale questo metodo è già noto da alcuni anni e impiegato anche da organizzazioni statali, in Svizzera non è ancora molto diffuso.

Nei programmi bug bounty, i cosiddetti «hacker etici» – che operano in un quadro definito e nel rispetto della legge – sono incaricati di individuare eventuali vulnerabilità nei sistemi informatici e nelle applicazioni di un'organizzazione. Per ciascuna vulnerabilità trovata, documentata e convalidata («bug») gli hacker vengono ricompensati («bounty») in base alla gravità della falla.

[1] Per dare seguito alla richiesta del Parlamento di eseguire questo genere di programmi e raccogliere prime esperienze in tale ambito, l'NCSC ha pianificato e realizzato un progetto pilota bug bounty, in collaborazione con la società BBS, il DFAE e i SP.

L'Amministrazione federale, come altri settori regolamentati, deve soddisfare requisiti severi in termini di protezione dei dati ed esige pertanto che i dati siano conservati su server in Svizzera. BBS è l'unico fornitore noto in Svizzera che soddisfa tali condizioni, ragione per cui il progetto pilota è stato svolto con questa società. La piattaforma sviluppata da BBS è completamente gestita sul territorio svizzero, si basa su tecnologie cloud avanzate e soddisfa i requisiti della Confederazione e di altri settori regolamentati, come quello delle infrastrutture critiche.

Lo scopo del progetto pilota era mostrare l'utilità dei programmi bug bounty per l'Amministrazione federale, individuare ed eliminare eventuali falle di sicurezza e ridurre così i ciber-rischi in modo efficace ed economicamente vantaggioso. Inoltre il progetto è servito ad acquisire esperienze su come integrare un programma bug bounty nei processi di sicurezza esistenti.

3 Esecuzione

Nel quadro del progetto pilota è stato sviluppato, eseguito e valutato un programma bug bounty ad hoc in base alle esigenze dell'Amministrazione federale.

Per il programma erano stati stabiliti una durata limitata, chiari sistemi informatici target, un preventivo dei costi fisso e un numero limitato di hacker etici. Gli hacker etici ammessi al programma sono stati invitati specificatamente per questo progetto pilota.

Sono stati selezionati in totale sei sistemi informatici del DFAE e dei SP. Inoltre, per questo primo test il gruppo di hacker etici è stato circoscritto a professionisti noti all'NCSC o a BBS che si sono già distinti in altri progetti.

L'attuazione del programma bug bounty era affidata a BBS ed è stata seguita costantemente dall'NCSC come pure da rappresentanti del DFAE e dei SP. Il test doveva servire a gettare le basi per una discussione su come procedere nell'utilizzo dei programmi bug bounty.

[1] 20.4594 Po. Bellaïche «Istituzionalizzare l'hackeraggio etico e aumentare la cibersicurezza» (https://www.parlament.ch/it/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20204594)

Particolarmente interessante si è rivelata la collaborazione tra gli hacker e i fornitori di prestazioni responsabili dei sistemi e delle applicazioni. Grazie a un'ottima documentazione delle vulnerabilità individuate dagli hacker etici, i fornitori di prestazioni responsabili hanno compreso il processo di rilevamento delle falle e hanno avviato immediatamente le procedure per eliminarle.

Una volta rimosse le vulnerabilità, sono stati avvisati gli hacker, che hanno eseguito un ulteriore controllo per stabilire se erano necessari altri miglioramenti.

Questa preziosa collaborazione, caratterizzata da grande fiducia reciproca, costituisce la base per la realizzazione di programmi bug bounty di successo.

Panoramica sullo svolgimento del progetto pilota:

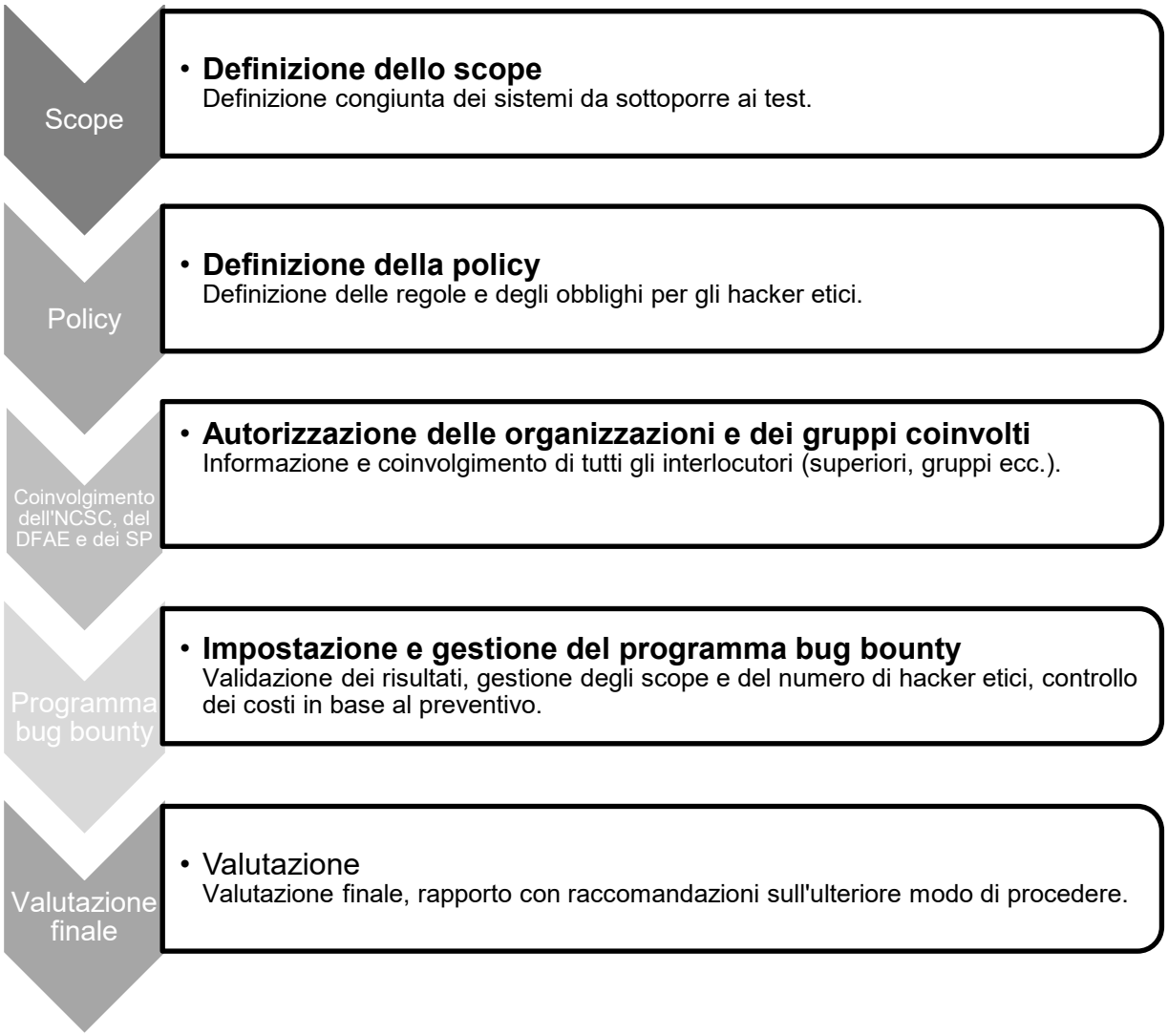

Figura 1: Svolgimento del progetto pilota

4 Risultati

Durante la fase di test, che ha avuto luogo dal 10 maggio alle ore 00.01 al 21 maggio alle ore 12.00, sono state segnalate in totale dieci vulnerabilità, di cui nove confermate come valide. In un caso si trattava infatti di un doppione, secondo le regole del programma bug bounty.

Il numero maggiore di segnalazioni di vulnerabilità all'inizio del programma corrisponde alla situazione tipica che viene a crearsi nel caso dei primi test effettuati su nuove condizioni quadro («scope») da parte di hacker etici a causa delle regole competitive che vigono tra loro.

Dato che i programmi bug bounty promuovono un approccio agile e il numero di segnalazioni è rimasto basso, dal secondo giorno del programma sono stati aggiunti sistemi supplementari nello scope autorizzato per i test (da 3 a 6 sistemi). Gli hacker etici hanno confermato le buone condizioni di sicurezza dei sistemi del DFAE e dei SP («the scope is hard»).

In seguito è stato introdotto un ulteriore adeguamento del programma: altri hacker etici sono stati invitati a prendere parte al progetto per incrementare la capacità dei test (da 9 a 15 hacker).

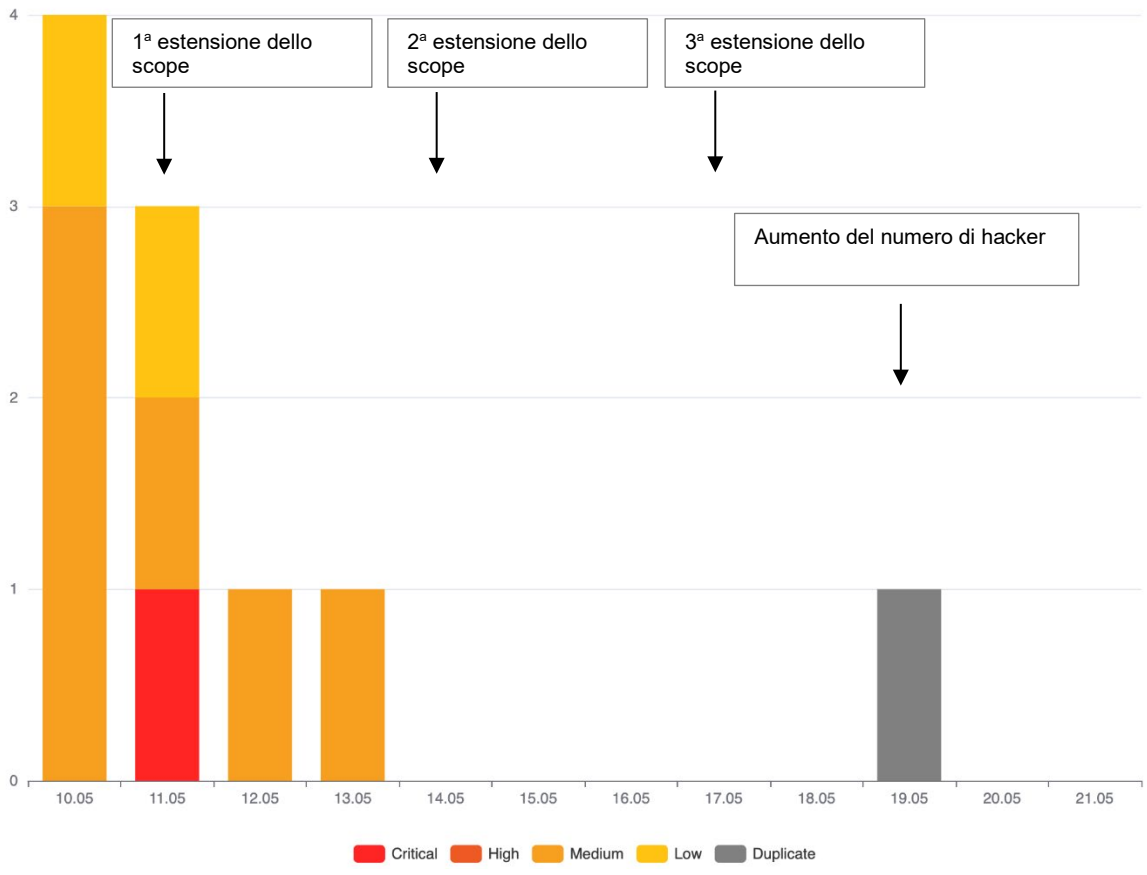

Figura 2: Segnalazioni pervenute secondo il livello di criticità

Le falle di sicurezza segnalate sono state suddivise secondo le seguenti categorie:

	Critico	Elevato	Medio	Basso	Nessuno	Totale
Sistema di test A	0	0	0	1	0	1
Sistema di test B	0	0	0	0	0	0
Sistema di test C	0	0	2	0	0	2
Sistema di test D	1	0	5	1	0	7
Totale	**1**	**0**	**7**	**2**	**0**	**10**

I sistemi informatici specifici oggetto del progetto pilota bug bounty sono stati denominati con le lettere A–D, poiché non saranno resi noti.

5 Finanziamento

Per la realizzazione di questo progetto pilota la Confederazione ha fissato un importo massimo di 49 900 franchi da impiegare per prestazioni esterne. Di seguito il riepilogo dei costi:

Importo massimo dei costi	CHF	49 900.00
Spese per avvio, attuazione tecnica ecc.	CHF	13 375.00
Ricompense versate	CHF	9 240.00
Saldo	**CHF**	**27 285.00**

I fondi inutilizzati saranno impiegati per altri programmi bug bounty nell'Amministrazione federale. L'obiettivo è di eseguire ulteriori programmi bug bounty possibilmente in modo continuativo.

6 Conclusione

Il progetto pilota ha dimostrato che i programmi bug bounty permettono di individuare ed eliminare efficientemente le vulnerabilità dei sistemi informatici. Secondo le valutazioni effettuate, il ritorno sull’investimento («return on invest») è da considerarsi elevato. L’esecuzione di un programma bug bounty per l’Amministrazione federale da parte dell’NCSC contribuisce in modo significativo alla riduzione dei ciber-rischi della Confederazione.

I riscontri sia dei SP sia del DFAE sono del tutto positivi. Molte unità amministrative evidenziano un fabbisogno di prestazioni nel quadro di un programma bug bounty. È stato dimostrato che l’amministrazione centrale e il supporto garantiti dal settore Gestione delle vulnerabilità dell’NCSC e l’eliminazione decentralizzata delle vulnerabilità tra i fornitori di prestazioni responsabili sono efficienti e sostenibili.

Sulla base delle esperienze e delle conoscenze acquisite con il progetto pilota, l’NCSC prevede di eseguire programmi bug bounty in maniera continuativa e sul maggior numero possibile di sistemi e applicazioni dell’Amministrazione federale.

Pertanto occorre avviare al più presto il processo di appalto. Fino ad allora, i fondi destinati al progetto pilota non utilizzati saranno impiegati per portare avanti il programma bug bounty nell’Amministrazione federale.