Bug Hunting: tra responsabilità, etica e collaborazione

Quando scoprite una vulnerabilità non documentata – un cosiddetto **zeroday** – oppure siete un'azienda che produce software e vi viene segnalato un bug, cosa fate?

Siete responsabili?
Siete etici?

Il mercato dei bug sta diventando sempre più complesso, connesso a fortissimi interessi economici e caratterizzato da diverse scale di grigio. Seppur esistono delle prassi internazionali (anche in ambito ENISA) che regolano la ***Coordinated Vulnerability Disclosure***, chiamata anche **CVD,** non sempre la collaborazione tra fornitore e ricercatore di sicurezza porta a un corretto riconoscimento dei bug e, quindi, a un miglioramento generale.

In una situazione di non sempre corretta adozione della CVD, il **buonsenso** e **l'etica** diventano allora la strada da seguire, cercando di essere **responsabili** nelle cose che si fanno, adottando sempre **trasparenza** e **collaborazione.**

In questo senso, i termini **Responsabilità ed Etica** si riferiscono non solo ai **ricercatori di bug**, ma anche ai **fornitori di prodotti** hardware e software in quanto una "stretta collaborazione" consente e rinforza la volontà di entrambi di ridurre il rischio per tutte le parti interessate, oltre che per tutti gli utilizzatori di quel prodotto specifico.

Premesso che ancora oggi si discute se sia corretto **divulgare**

le vulnerabilità pubblicamente, oppure **tenerle segrete fino alla realizzazione della *fix***, c'è da dire che spesso si è davanti a mancate risposte dei *vendor* di prodotto ai ricercatori di bug, cosa che in regime di buon senso è paradossale oltre che controproducente per tutti.

Ecco quindi che il *vendor* (anche se non ha un programma di Responsible Disclosure o di *bug bounty*), dovrebbe essere **riconoscente** al singolo ricercatore che lo informa di una vulnerabilità che lui stesso non ha rilevato sul suo prodotto, cosa che alle volte non accade e che in alcuni casi finisce sui giornali o in cause legali, cosa che abbiamo visto accadere anche a *big player* quali Google, Apple e Microsoft.

Ma comprendo che il contesto è complicato.

Avere sul *National Vulnerability Database* (CVN) dei CVE del proprio prodotto può dare fastidio a tutti i produttori, in quanto sta a significare che le cose non siano state fatte "a regola d'arte".

Ma è anche vero che **se quelle vulnerabilità non fossero pubbliche** – e se, magari, la ***weaponization*** abbia avuto luogo in maniera efficace per poi armare Virus, Rat e Malware di altra natura – la cosa potrebbe finire molto, ma molto peggio.

Occorre quindi sviluppare software sicuro, attivando tutti i corretti programmi di sicurezza; ma **siamo grati ai ricercatori che scoprono i bug**, perché rendono le nostre applicazioni più sicure **e ci aiutano a vedere oltre, arrivando anche dove noi non eravamo riusciti a farlo.**

Articolo a cura di **Massimiliano Brolli**

https://www.ictsecuritymagazine.com/articoli/bug-hunting-tra-responsabilita-etica-e-collaborazione/