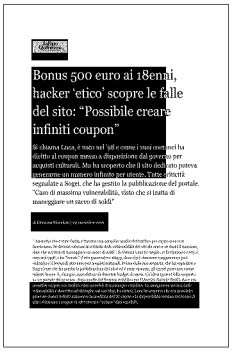
il Fatto Quotidiano.it

Bonus 500 euro ai 18enni, hacker 'etico' scopre le falle del sito: "Possibile creare infiniti coupon"

Si chiama Luca, è nato nel '98 e come i suoi coetanei ha diritto al coupon messo a disposizione dal governo per acquisti culturali. Ma ha scoperto che il sito dedicato poteva generarne un numero infinito per utente. Tutte criticità segnalate a Sogei, che ha gestito la pubblicazione del portale. "Caso di massima vulnerabilità, visto che si tratta di maneggiare un sacco di soldi"

di Eleonora Bianchini | 29 novembre 2016

"Ammetto che è stato facile, è bastata una semplice analisi del traffico per capire cosa non funzionava. Se dovessi valutare la criticità delle vulnerabilità del sito da zero a 10 darei il massimo, dato che si tratta di maneggiare un sacco di soldi". Si chiama Luca (o meglio, si fa chiamare così), è nato nel 1998, e ha "bucato" il sito governativo 18app, dove chi è diventato maggiorenne può richiedere il bonus di 500 euro per acquisti culturali. Prima della sua scoperta, che ha segnalato a Sogei (ente che ha gestito la pubblicazione del sito) ed è stata riparata, gli utenti potevano creare infiniti bonus. E, dunque, approfittare di illimitati budget di spesa. Un'altra (grave) falla scoperta su un portale del governo, dopo quelle del Sistema pubblico per l'identità digitale (Spid), dove era


Bonus 500 euro ai 18enni, hacker 'etico' scopre le falle del sito: "Possibile creare infiniti coupon"

possibile carpire con facilità i dati sensibili di qualunque cittadino. La spiegazione tecnica delle vulnerabilità è descritta nel dettaglio sul suo blog. In sintesi, Luca ha scoperto che era possibile: generare buoni infiniti attraverso la modifica dell'Id utente e la disponibilità residua dei bonus di altri; eliminare i coupon di altri utenti e "rubare" dati sensibili.

"Una vulnerabilità non è altro che un'eccezione non gestita un errore non previsto che, se sfruttata bene, ti permette di ottenere un qualche vantaggio", spiega Luca, hacker etico che si limita a definirsi "appassionato autodidatta di informatica e sicurezza". "La prima falla documentata, quella più interessante – prosegue – è relativa ad una problematica nella gestione dell'autenticazione che consentirebbe ad un malintenzionato di creare coupon utilizzando la disponibilità del bonus altrui; in poche parole, creare buoni infiniti. Sempre correlata a questa prima vulnerabilità, ci sarebbe anche la possibilità di eliminare i coupon generati da altri utenti: in questo caso si potrebbero creare grossi danni all'integrità del portale. L'ultima vulnerabilità documentata infine riguarda le informazioni sensibili e la privacy degli utenti: sembra infatti che con un breve richiesta chiunque potrebbe ricavare i dati anagrafici di altri utenti".

Specifica che per "'bucare' servono buone competenze in ambito informatico, anche per quanto riguarda la conoscenza delle varie tipologie di sistemi e applicativi web in particolare", ma che in questo caso trovare le falle sia stato molto semplice. Possibile che tanti ne abbiano approfittato "incassando" più bonus? "Da quanto ho capito dalla corrispondenza che ho avuto con Sogei non si sono verificate violazioni di questo tipo. Comunque ora le vulnerabilità sono state risolte e non è più possibile aggirare il sistema di sicurezza come era possibile in precedenza".

Un hacker 'etico' Luca: buca i sistemi per segnalarne i difetti ai programmatori che le devono riparare. Gli operatori di Sogei come hanno reagito alle segnalazioni? "Sono intervenuti molto rapidamente con la procedura di messa in sicurezza e mi hanno ringraziato". Ma per lui questa non era la prima volta: "In passato ho già segnalato vulnerabilità a enti governativi o istituzionali che gestiscono le infrastrutture critiche". Quali, però, non si può dire perché "a differenza di questa volta, non hanno autorizzato la pubblicazione della 'ricerca' nel mio blog e per questo non si è parlato e non posso parlarne". Quel che è certo è che 'testerà' altri siti. Sempre istituzionali.