

Uno studio affascinante e preoccupante sulla sicurezza delle password

Che le parole chiave scelte dagli operatori informatici rappresentino una vistosa debolezza dell'intera architettura di sicurezza informatica di un'azienda, è fatto noto. Meno noto è quanto questa debolezza sia vistosa.

L'ufficio dell'ispettore generale del Dipartimento dell'interno degli Stati Uniti ha appena pubblicato un documento, che può essere oltremodo istruttivo anche per i nostri esperti di sicurezza informatica.

L'ispettore generale ha cercato di violare le parole chiave degli 85.000 e passa dipendenti del Dipartimento dell'interno, ottenendo risultati oltremodo preoccupanti: il 21% delle parole chiave scelte dai dipendenti sono state violate con semplici algoritmi.

Pubblicità

<#? QUI-PUBBLICITA-MIM-[ALDIG02] ?#>

Gli esperti di sicurezza informatica, ingaggiati dall'ispettore generale, hanno messo a punto una lista di più di 1, 5 miliardi di parole, estraendole da questi archivi:

- dizionari in più lingue,
- terminologia usata dal governo degli Stati Uniti,
- riferimenti a cultura pop,
- sequenze banali di tastiera, e simili.

Il problema non riguarda solo il fatto che 18.174 parole chiave sono state decodificate, ma il fatto che 288 di esse facevano riferimento a profili di elevata sicurezza. Nei primi 90 minuti di sviluppo dell'attacco informatico, era ben il 16% la percentuale di parole violate.

L'audit ha messo inoltre un'altra debolezza della sicurezza: molti dipendenti non utilizzavano sistematicamente un'autentica a due fattori.

Il rapporto mette anche in evidenza come questa debolezza non sia solo da imputare ai dipendenti, ma anche ai responsabili della sicurezza informatica, che non sempre adottano delle politiche di sicurezza, nella scelta della parola chiave, che potrebbero

rendere più difficoltoso il tentativo di violazione.

Ad edificazione dei lettori, ecco una tabella con le parole chiave usate più frequentemente, seguite dal numero di utenti che le usavano:

- Password-1234 | 478
- Br0nc0\$2012 | 389
- Password123\$ | 318
- Password1234 | 274
- Summ3rSun2020! | 191
- Orlando_0000 | 160
- Password1234! | 150
- ChangeIt123 | 140
- 1234password\$ | 138
- ChangeItN0w! | 130

il costo complessivo di questo studio, compreso il costo degli esperti esterni utilizzati, è stato inferiore a 15.000 \$ e credo che un investimento del genere difficilmente possa essere più remunerativo, nei confronti della sensibilizzazione sul tema della scelta custodia sicura delle parole chiave.

Se qualche lettore ha effettuato interventi di audit, simile a questi, sono certo che tutti gli addetti alla sicurezza informatica saranno lieti di conoscere i risultati.

[Vedi allegato documento \(pdf\)](#)

Adalberto Biasiotti



Licenza [Creative Commons](#)

www.puntosicuro.it