Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Direttori: Sergio Pellegrino e Giovanni Valcarenghi

Edizione di mercoledì 7 maggio 2014

SOLUZIONI TECNOLOGICHE

HeartBleed il baco che fa tremare il mondo

di **Teamsystem.com**

www.teamsystem.com

HeartBleed, nelle ultime settimane ne abbiamo sentito parlare tutti. Sotto un nome che in italiano significa "cuore sanguinante" [illegible] **OpenSSL più** [illegible] ate contro **hacker e criminali** che avrebbero potuto mettere a rischio i nostri dati. Non era così.

Due anni di letargo

Appena scoperto, il bug HeartBleed è stato **immediatamente corretto** e questa è la buona notizia. Però ce n'è anche un'altra meno buona ed è quella che ha spinto **Bruce Schneier**, noto esperto di **sicurezza** e **crittografia** di **Co3 Systems**, a dichiarare senza mezzi termini: "***È un problema catastrofico***". Ma di cosa si tratta? Diciamo subito che non è stato un hacker o una banda di mascalzoni digitali a bucare il sistema che protegge il trasferimento di dati sensibili fra il nostro computer e i siti che utilizzano il sistema Https. Si è trattato più che altro di un **errore umano** che ha lasciato aperta questa falla in un aggiornamento risalente a circa due anni fa. Da allora, **il sistema** che tutti ritenevano sicuro ha continuato a lavorare come niente fosse, ma al suo interno **conteneva una porticina aperta**. "*Il baco HeartBleed – dichiara Schneier sul suo blog - permette a chiunque su internet di leggere la memoria dei sistemi che dovevano invece essere stati protetti dal* ***protocollo OpenSSL. Ciò compromette i codici segreti usati per identificare i provider e criptare il traffico dei dati, i nomi e le password degli utenti. Questa falla permette ai cyber criminali di ascoltare le comunicazioni, rubare dati e sostituirsi addirittura a servizi o a utenti*****".**

Cosa è successo

Appena la falla è stata scoperta (stiamo parlando di circa il **66% dei siti mondiali** interessati e del **40% dei primi mille siti italiani** più visitati)**, è partito l'allarme generale e tanti gestori di siti e utenti comuni hanno ricevuto una mail che li invitava immediatamente a cambiare i propri dati di accesso ai servizi online. Il problema vero però, è che HeartBleed esiste da due anni e nessuno può sapere se sia stato utilizzato o meno e con quali danni reali. Con un aggiornamento tempestivo (se tempestivo può essere riferito a un lasso di due anni), il problema è stato risolto, ma non c'è modo di calcolare con precisione se e quante password o**

informazioni siano state intercettate durante tutto questo tempo.

Chi è stato colpito

Secondo le ultime stime, i siti interessati da questo bug sono circa mezzo milione e fra di essi ci sono grossi nomi. Google, **Instagram**, **Facebook**, **YouTube**, **Yahoo!**, **Microsoft**, **Bing** e **Wikipedia** hanno subito installato l'aggiornamento. **LinkedIn**, **eBay** e **PayPal**, invece, non sono mai stati in pericolo.

Per controllare se uno dei siti in cui abbiamo conservato i nostri dati sensibili è ancora affetto da HeartBleed o ha applicato subito l'aggiornamento che chiude la falla, si trovano in rete dei servizi gratuiti come questo (https://filippo.io/Heartbleed/). È possibile fare una verifica al volo, scrivendo semplicemente l'indirizzo della pagina web da controllare.

Una rivelazione di questa portata ha fatto tremare il web e mostrato al mondo che nulla su internet può considerarsi veramente sicuro. Cambiare immediatamente tutte le nostre password e farlo spesso, magari dandoci delle scadenze programmate per il futuro, rimane tuttavia l'unica, saggia, importantissima cosa da fare.