L'algoritmo di sicurezza dell'e-commerce SHA1 è a rischio

L'algoritmo utilizzato per l'e-commerce e le transazioni bancarie ha problemi di sicurezza. A gennaio 2017 i browser non accetteranno più certificati SHA1

SHA1, uno di algoritmi crittografici più importanti di Internet, **sta mostrando alcuni problemi di sicurezza**. La conferma che il protocollo presenta dei rischi è arrivata da un team di ricercatori internazionali composta da **Centrum Wiskunde & Informatica** in Olanda, **Inria** in Francia, e la **Nanyang Technological University** di Singapore. E' da tempo che si è a conoscenza dei rischi e per questo i principali browser hanno programmato di **smettere di accettare le firme basate su SHA1 a partire da gennaio del 2017**.

I problemi sembrano però essere più gravi del previsto. Il team di ricercatori ha infatti accertato un'ipotesi di attacco informatico prima dell'ultima data di accettazione del protocollo di sicurezza. Se ciò avvenisse i dati degli utenti e le transazioni compiute su numerosi siti di e-commerce sarebbero a repentaglio.

Il problema di SHA1 è che anche una piccolissima modifica come l'aggiunta o cancellazione di una singola virgola può provocare danni irreparabili come è tipico delle funzioni crittografiche di tipo hash. Nel momento in cui due differenti messaggi dovessero produrre lo stesso identico hash, si creerebbero dei valichi alle firme. Tutto ciò si traduce in problemi seri per le transazioni bancarie, download di software e comunicazioni tra siti.

Gli attacchi del passato hanno minato la sicurezza

Se si guarda al passato, attacchi simili sono stati messi in piedi ad esempio per **spiare reti sensibili iraniane**. Ciò che è stato costruito sfruttava Microsoft Windows Update per poter infettare i pc e renderli quindi "visibili". O ancora nel 2008 un team di esperti informatici e ricercatori sulla sicurezza hanno sfruttato le debolezze di SHA1 per creare un **certificato sockets layer in grado di autenticare praticamente qualsiasi sito web** di loro scelta.

Si stima che un attacco di portata elevata (che contempli una serie di attacchi in contemporanea) sarebbe costato nel 2012 circa 700.000 dollari, contro un costo di appena 173.000 dollari nel 2018. L'abbassamento dei costi accompagnato da maggiori potenze di calcolo ha reso l'SHA-1 veramente pericoloso per la sicurezza dei sistemi. I ricercatori raccomandano per questo che ci sia quanto prima una **migrazione verso SHA-2 o SHA-3**.

La recente ricerca ha dimostrato che SHA-1 è più debole rispetto a quanto si pensasse. E' per questo che gli sviluppatori di browser e le autorità di certificazione stanno prendendo in considerazione una proposta che dovrebbe anticipare la migrazione dei certificati HTTPS basato SHA1 già ad inizio del 2016. Un ritardo nella migrazione rappresenterebbe un eccessivo rischio per la sicurezza degli utenti.

TI CONSIGLIAMO DI LEGGERE ANCHE...

Container e sicurezza, un dibattito sempre aperto

Analisi del comportamento umano per la sicurezza dei dati online

Sicurezza online: gli strumenti di protezione destinati a scomparire – 2

Sicurezza online: gli strumenti di protezione destinati a scomparire – 1

Attacchi informatici: quali trend nella prima metà del 2015

ARTICOLO PUBBLICATO IL 12 OTTOBRE 2015

FACCI SAPERE COSA NE PENSI!

Il tuo indirizzo email non sarà pubblicato. I campi obbligatori sono contrassegnati *

Commento

Nome *

Email *

Sito web

COMMENTO ALL'ARTICOLO