8 ottobre 2009 13:28

Furto dell'indentità digitale col phishing: limiti e caratteristiche del 'certificato del sito web'

di Deborah Bianchi*

È di pochi giorni fa la notizia che la posta di Google (Gmail) è stata attaccata da pirati informatici. Alla Bbc risultano rubati e messi in rete circa 30 mila indirizzi. Sono state coinvolte, infatti, anche altre net companies come Hotmail (ora Windows Live Hotmail), America Online e Yahoo.
La tecnica di cui si sono serviti gli hacker si chiama phishing (il pescare) . Viene realizzato un sito web con la stessa interfaccia telematica di un sito istituzionale come Poste italiane o come quello di un istituto di credito, si invia una mail massiva (spamming) alla collettività e si chiede di introdurre nome e password adducendo motivazioni giustificate da una verifica di sicurezza delle credenziali di accesso al servizio o cose simili.

Il malcapitato inserisce i suoi dati e… il gioco è fatto. L'hacker ha ottenuto le informazioni che gli permetteranno di succhiare soldi dal conto on line dell'utente gabbato. Una volta perpetrato il phishing si passa al furto di identità. Utilizzando le credenziali estorte il criminale si sostituisce alla persona e procede a effettuare nell'internet operazioni finanziarie o acquisti al suo posto.

Quando il soggetto offeso si rende conto dell'illecito è ormai troppo tardi. L'istituto di credito presso cui è allocato il conto on line si scarica dalle responsabilità in quanto il crimine si è consumato fuori dalle porte digitali del proprio palazzo e il cliente sconta sulla propria pelle il rischio sicurezza dell'ambiente informatico salvo ipotesi in cui per policy aziendale o per clausola apposita nel contratto venga previsto il rimborso.

Attualmente nel panorama normativo nazionale non esiste una fattispecie dedicata a questo tipo di crimine. Spesso si invoca la truffa e i reati contro la fede pubblica per il furto di identità come vedremo più avanti.

Come difendersi? È affidabile il certificato del sito web?

Uno dei consigli più opportuni che potrebbero prospettarsi, premesso che non si tratta di un rimedio risolutivo, è di affidarsi a strutture munite di certificato del sito web**. Il certificato del sito web è una carta elettronica con validità di 1 o 2 anni in cui un'autorità accreditata certifica l'identità del titolare dell'architettura telematica.** Occorre prestare molta attenzione al**certificatore**. Deve trattarsi di ente conosciuto e di stimata fama altrimenti è meglio non fidarsi. Si riportano di seguito le utilissime indicazioni diffuse dal Ministero della Difesa sul proprio sito (http://www.difesa.it/SMD/Staff/Reparti/II-reparto/CERT/Tips_Tricks/Certificati+Digitali+dei+siti+Web.htm), con l'avvertenza che **anche il certificato potrebbe a sua volta essere taroccato**. Come difendersi anche da questa insidia? Aggiornando continuamente il nostro browser di navigazione mediante appositi servizi di allerta sui certificati fasulli.

Dal sito del ministero della difesa

CERTIFICATI DIGITALI DEI SITI WEB

Visitando un sito WEB che per motivi di sicurezza richiede che la connessione sia cifrata, tipicamente i siti bancari, avrete certamente notato comparire in basso a destra un lucchetto. Cliccando su di esso, potrebbe presentarsi una finestra di dialogo che vi annuncia che vi è una malfunzione nel nome o data del certificato del sito WEB che state visitando. Capire cosa è un certificato di un sito WEB può aiutare a proteggere la vostra privacy.

Cosa sono i certificati dei siti WEB?

La cifratura dei dati scambiati via internet tra società ed utenti è una pratica comune, specie per le transazioni finanziarie e comunque ogni volta che si vuole evitare che le informazioni vengano intercettate e lette da dei malintenzionati. La comparsa di un lucchetto in basso a destra del browser e la modifica nella URL, in alto a sinistra, del protocollo di navigazione da “http” a “l’https”, sono le evidenze che la trasmissione dati viene cifrata. Occorre però assicurasi che il sito WEB con cui siete in comunicazione sia effettivamente chi dice di essere. La verifica che il certificato sia valido, contribuisce a proteggervi dai malintenzionati che creano siti malevoli per carpire le vostre informazioni.

Se un sito WEB ha un certificato valido, significa che un’autorità ha verificato che l’indirizzo del sito appartiene realmente a quell’organizzazione o società. Quando digitate un URL o seguite un link su un sito WEB sicuro, il vostro browser controllerà automaticamente il certificato secondo la seguente procedura di verifica:

1. l'indirizzo del sito WEB è abbinato all'indirizzo sul certificato

2. il certificato è firmato da un’autorità riconosciuta dal browser come “trusted authority”

Potete fidarvi di un certificato?

Il livello di fiducia che potete ripore in un certificato è legato alla autorevolezza dell'organizzazione e dell’autorità che lo emesso. Se l'indirizzo del sito WEB concorda con l'indirizzo sul certificato, il certificato è firmato da un autorità certificata di fiducia e la data è valida, potete essere raggionevolmente sicuri che il sito è realmente quello che dichiara di essere. Tuttavia, a meno che non verifichiate personalmente l'impronta digitale unica di quel certificato chiamando direttamente l'ente emettitore, non vi è modo per essere assolutamente sicuri.

Dando fiducia a un certificato, si da implicitamente fiducia all’autorità che lo ha emesso e che ha effettuato questa verifica per voi. Tuttavia, è importante sapere che le autorità di certificazione non sono tutte uguali, ma assumono diversi livelli di fiducia a seconda di quanto più rigorosi sono nella convalida delle informazioni richieste. Per default, il vostro browser contiene una lista di più di 100 autorità di fiducia certificate. Questo significa che vi state fidando di tutte quelle autorità certificate per verificare e convalidare adeguatamente le informazioni.

Come controllate un certificato?

Dopo aver cliccato sul lucchetto in basso a destra della finestra del browser, verificate le proprietà del certificato come segue:

* Chi emette il certificato – E’ importante assicurarvi che il certificato sia stato legittimato da un’autorità certificata. Alcune organizzazioni inoltre hanno proprie autorità di certificazione che emettono certificati validi all’interno della propria intranet.

* A chi è intestato il certificato - Il certificato dovrebbe essere intestato all'organizzazione che possiede il sito WEB. Non fidarsi se il nome sul certificato non si abbina al nome dell'organizzazione o alla società prevista.

* Data di scadenza - La maggior parte dei certificati sono emessi con validità di uno o due anni. Fa eccezione il certificato dell’autorità di certificazione che per motivi organizzativi può avere validità decennale. Fate attenzione alle organizzazioni che hanno certificati validi per più di due anni o con i certificati scaduti.

Nel visitare un sito WEB, vi potrebbe capitare una finestra di dialogo con un errore relativo al certificato del sito. Ciò può accadere se il nome con cui è registrato il certificato non si abbina al nome del sito, se avete scelto di non fidarvi dell'azienda che lo ha emesso, o se il certificato è scaduto. Generalmente vi verrà richiesto di se intendete comunque accettarlo solo per quella volta, o in mo definitivo. La confusione è a volte facile da risolvere. Se siete incerti che il certificato sia valido o mettete in discussione la sicurezza del sito, non trasmettete informazioni personali o sensibili.

**** Deborah Bianchi,*** *avvocato specializzato in diritto applicato alle nuove tecnologie, esercita nel Foro di Pistoia e Firenze in materia civile e amministrativa.*