La newsletter mensile sulla sicurezza informatica per gli utenti di

OUCH!

IN QUESTO NUMERO...

- Cos'è la crittografia?
- Crittografare i dati memorizzati
- Crittografare le comunicazioni

La crittografia

Cos'è la crittografia?

Avrete sicuramente sentito parlare dei termini crittografia e cifratura (che considereremo qui equivalenti) e di come sia possibile fare uso di questo strumento per proteggere le informazioni. Il concetto di crittografia può a volte apparire confuso e ha tra i suoi limiti quello di non essere la soluzione definitiva per la propria protezione. In questa newsletter spiegheremo in termini semplici cos'è la crittografia, perché dovete utilizzarla e come implementarla adeguatamente.

L'autore di questo numero

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) è un consulente di Washington, DC. Per il SANS Institute è lead instructor del corso Mobile Device Security and Ethical Hacking (SEC575) e autore di Incident Response Team Management (MGT535).

Chiunque di noi conserva una quantità impressionante di informazioni sensibili sui propri dispositivi: documenti finanziari, immagini, email o dati sanitari. Se vi dovesse capitare di perdere uno dei vostri dispositivi, tutte le informazioni in esso contenute potrebbero diventare preda di chiunque ne venga in possesso. Nel caso, inoltre, in cui utilizziate il vostro dispositivo per condurre transazioni sensibili di banking o shopping online, un criminale informatico potrebbe monitorarne le attività e impossessarsi delle vostre informazioni, come il conto in banca o i numeri delle carte di credito. La crittografia vi viene in aiuto in queste situazioni facendo in modo che persone non autorizzate non siano in grado di accedere o modificare le vostre informazioni.

Quando l'informazione non è crittografata è detta "in chiaro": ciò significa che chiunque può facilmente leggerla o averne accesso. La crittografia converte questa informazione in un formato non leggibile chiamato "testo cifrato". La crittografia funziona applicando complesse operazioni matematiche e una chiave unica per convertire i dati in testo cifrato.
La chiave è ciò che blocca o apre le vostre informazioni: solo le persone in possesso di quella sequenza di numeri e lettere potranno decifrare e accedere alle informazioni. Per proteggere le vostre informazioni cifrate dovete prima di tutto proteggere la vostra chiave.
Normalmente la crittografia funziona in due modalità: potete cifrare i dati memorizzati ("data at rest"),come ad esempio i dati conservati nel laptop, o proteggerli durante la loro trasmissione (le informazioni trasmesse online).

Crittografare i dati memorizzati

La crittografia dei dati memorizzati ha come obiettivo primario la protezione delle informazioni nei casi in cui il vostro computer, il tablet o lo smartphone vadano persi o vengano sottratti. Venti anni fa questo problema non esisteva, poiché la maggior parte dei computer era costituita da dispositivi pesanti e difficilmente trasportabili. Al

La crittografia

giorno d'oggi, molti laptop pesano poco più di un chilo mentre gli smartphone solo pochi etti, ma nonostante questo sono estremamente potenti, possono conservare una quantità di informazioni decisamente importante e possono altresì essere perduti molto facilmente. Anche altri dispositivi mobili, come le chiavette USB e i CD ROM, possono memorizzare informazioni sensibili. Una tecnica molto utilizzata per crittografare le informazioni sui vari dispositivi viene chiamata Full Disk Encryption (FDE), ovvero crittografia completa del disco. Con questo termine si identifica la tecnologia che permette di cifrare automaticamente tutto il contenuto di un sistema, senza dover decidere cosa cifrare e cosa lasciare in chiaro. Molti sistemi operativi moderni sono già dotati di questa funzionalità: basta solo attivarla. Il Mac OS X, ad esempio, mette a disposizione FileVault, mentre alcune versioni di Windows includono BitLocker. Se il vostro computer supporta la Full Disk Encryption vi raccomandiamo di attivarla. Anche molti smartphone supportano la FDE per la memoria interna: l'iOS, ad esempio, attiva la FDE automaticamente non appena viene inserita una password. Per verificare che il vostro computer o smartphone supporti la Full Disk Encryption, chiedete al vostro helpdesk di riferimento o al vostro superiore in azienda. Per i personal computer vi suggeriamo di contattare il produttore del computer o di leggere la documentazione online.

La crittografia è un modo efficace per proteggere le vostre informazioni, ma la sua sicurezza di basa sulla segretezza della chiave

Crittografare le comunicazioni

Le informazioni sono anche vulnerabili durante la loro trasmissione: se i dati non sono cifrati, possono essere catturati online. Per questo motivo è necessario fare in modo che tutte le comunicazioni online di tipo confidenziale, come ad esempio l'online banking, le email o l'accesso ai social network, siano cifrati. Il tipo più comune di cifratura online è il protocollo HTTPS, utilizzato per crittografare il traffico tra il vostro browser e il sito web. Se l'URL del browser inizia con https:// , se appare un lucchetto chiuso o se la barra dell'URL diventa verde, state comunicando con una sessione cifrata.

Fate attenzione quando vi collegate a una rete WiFi pubblica: usate sempre collegamenti crittografati quando possibile. Quando, infine, inviate o ricevete email, assicuratevi che il vostro programma di gestione della posta elettronica spedisca i messaggi attraverso un canale criptato. La maggior parte di questi programmi consente di farlo: riferitevi al vostro Internet Provider per sapere come attivare la crittografia della posta elettronica.

Implementare la crittografia nel modo corretto

Indipendentemente da quale tipo di cifratura state utilizzando e da come lo utilizzate, tenete sempre in considerazione i seguenti suggerimenti.

© The SANS Institute 2014

La crittografia

- La crittografia è forte quanto la chiave che usate: se qualcuno ne viene a conoscenza, potrà avere accesso ai vostri dati, anche se saranno cifrati. Proteggete la chiave in modo adeguato.
- Se utilizzate un codice o una password per proteggere la vostra chiave, assicuratevi che sia lunga e sicura, non perdetela e non dimenticatevela. Se non ne siete più in possesso, non potrete più recuperare i vostri dati.
- La crittografia è robusta quanto la sicurezza del vostro computer: se il vostro PC è stato compromesso o infettato da un attacco informatico, potrebbe essere possibile bypassare la crittografia. Per tale motivo, proteggete il vostro computer e i vostri dispositivi mobili in modo adeguato.
- Quando vi vengono proposte diverse possibilità di implementazione della crittografia, scegliete sempre la più forte.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
http://www.securingthehuman.org

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

Mac OS X Filevault:	http://support.apple.com/kb/HT4790?viewlocale=it_IT
Crittografia in iOS:	http://support.apple.com/kb/ht4175?viewlocale=it_IT
Crittografia in Android:	http://www.fastweb.it/smartphone-e-gadget/come-fare-per-criptare-il-dispositivo-android/
Crittografia in Windows:	http://windows.microsoft.com/it-it/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Rendere sicuro il computer:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201212_it.pdf
Programmi di gestione password:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_it.pdf

OUCH! è pubblicata dal progetto Securing The Human del SANS Institute e viene distribuita con licenza Creative Commons BY-NC-ND 3.0.
Sei libero di distribuire questa newsletter o utilizzarla nei tuoi programmi di awareness senza però modificarne i contenuti.
Per traduzioni o ulteriori informazioni, contatta ouch@securingthehuman.org.

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus