SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Giugno 2016

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

La crittografia

Cos'è la crittografia?

Il termine "crittografia" è sempre più utilizzato e ne avrete probabilmente sentito parlare nell'ambito della protezione delle informazioni. La crittografia, altrimenti detta cifratura, può spesso non essere compresa perfettamente, così come difficile è comprenderne i limiti. In questa newsletter illustreremo in modo accessibile cos'è la crittografia, come vi protegge e cosa dovete fare per implementarla nel modo corretto.

L'autore di questo numero

Francesca Bosco (**@francibosco**) è ricercatrice e project officer, gestisce progetti correlati al cybercrime, alla sicurezza informatica e all'abuso delle tecnologie. Lavora presso l'organizzazione delle Nazioni Unite "Interregional Crime and Justice Research Institute" ed è cofondatrice del Tech and Law Center.

I vostri device conservano un'enorme quantità di informazioni sensibili: documenti personali, immagini e email. Se dovessero andar persi o vi venissero sottratti, chiunque ne entrasse in possesso potrebbe accedere a tutto ciò che vi è conservato. Oltre alle informazioni, se utilizzate un device mobile per transazioni online, ad esempio per l'ebanking o lo shopping, qualcuno potrebbe monitorare queste attività e venire in possesso delle vostre informazioni, come il numero di conto corrente o della carta di credito. La crittografia vi protegge in queste situazioni contribuendo ad assicurare che persone non autorizzate non siano in grado di avere accesso alle vostre informazioni.

La crittografia esiste da qualche migliaio di anni. Con il progredire della tecnologia, si è fatta molto sofisticata, ma viene utilizzata per i medesimi scopi: inviare un messaggio segreto da un luogo a un altro assicurando che solo le persone autorizzate a leggerne il contenuto possano avervi accesso. Quando le informazioni non sono crittografate, vengono dette "in chiaro", poiché chiunque potrebbe leggerle o accedervi. La crittografia converte queste informazioni in un formato non intelleggibile chiamato testo cifrato. La crittografia moderna usa complesse operazioni matematiche e una chiave unica per convertire le nostre informazioni in testo cifrato. La chiave è ciò che blocca o sblocca le informazioni. Nella maggior parte dei casi la chiave è una password o un passcode.

Cosa può essere crittografato?

Ci sono in genere due tipi di informazioni da cifrare: i dati a riposo (come ad esempio i dati memorizzati sullo smartphone) e i dati trasmessi (le email che state recuperando o i messaggi agli amici).

La crittografia

È fondamentale cifrare i dati a riposo per proteggere le informazioni nel caso che computer, tablet o smartphone vengano perduti o vi siano stati sottratti. Al giorno d'oggi, tutti questi dispositivi sono estremamente potenti e contengono un'incredibile mole di informazioni, ma, purtroppo, è anche facile perderli. Ci sono anche altri tipi di dispositivi mobili che possono contenere informazioni sensibili, come le chiavette USB o i dischi esterni. La cifratura dell'intero disco (Full Disk Encryption - FDE) è una tecnica di crittografia molto usata che permette di cifrare l'intero disco del vostro sistema. Qualsiasi file sul sistema viene automaticamente cifrato, senza che dobbiate decidere cosa proteggere e cosa no. Attualmente, molti computer sono dotati dell'FDE, ma probabilmente è necessario attivarla manualmente. Sui sistemi Mac viene chiamata FileVault, e sui computer Windows, a seconda della versione, potrete usare Bitlocker o Device Encryption. Anche molti dispositivi mobili supportano l'FDE. iOS su iPhone e iPad attiva automaticamente FDE, una volta che è stato configurato il passcode. A partire da Android 6.0 (Marshmallow), viene richiesto di abilitare FDE per default, nel caso che l'hardware soddisfi dei requisiti minimi.

La cifratura è un modo estremamente efficace che vi consente di proteggere le informazioni, ma è tanto forte quanto sarà forte la chiave che userete.

L'informazione è vulnerabile anche quando viene trasmessa: se non è cifrata può essere monitorata, modificata e catturata online. Per questo motivo è necessario assicurarsi che le comunicazioni e le transazioni online siano protette. Verificate che l'URL cominci con https:// e che sia presente l'icona del lucchetto nel browser o che la barra dell'URL diventi verde. Un altro esempio riguarda l'invio e la ricezione delle email. La maggior parte dei programmi offrono la possibilità di cifrare la comunicazione: verificate con il vostro fornitore di servizio come configurarla. Un terzo esempio di cifratura dei dati trasmessi è tra due utenti in chat che usano app come iMessage, WhatsApp, Telegram, Signal, Wickr. Questo tipo di app usa una cifratura chiamata end-to-end, ovvero tra i due punti che partecipano alla conversazione, che impedisce a una terza entità di accedere ai dati durante il loro trasferimento da un sistema all'altro. Ciò significa che solo voi e il vostro interlocutore potete leggere ciò che è stato inviato.

Usare la crittografia nel modo giusto

Per assicurarvi di essere protetti quando usate la crittografia, è fondamentale usarla nel modo corretto.

La crittografia

- La crittografia che usate è tanto forte quanto lo è la vostra chiave. Se qualcuno la indovina o vi ha accesso in qualche modo, accederà anche ai vostri dati, per cui è necessario proteggerla. Se usate un passcode o una password per renderla sicura, fate in modo che sia forte e unica. Più una password è lunga, più è difficile da trovare. Non dimenticatevela, perché senza di essa non potrete decodificare la chiave e decifrare le informazioni. Se non riuscite a ricordare tutte le password, vi suggeriamo di utilizzare un password manager.
- La crittografia che usate è tanto forte quanto lo è la sicurezza dei vostri dispositivi: se vengono compromessi o infettati da malware, la cifratura potrà essere scavalcata dai cybercriminali. Ecco perché è molto importante rendere sicuro il device con altri accorgimenti, ad esempio usando anti-virus, password forti e mantenendolo costantemente aggiornato.
- Molte app e programmi per computer offrono ora la crittografia forte per proteggere i dati e le comunicazioni. Se state valutando un app o un programma che non la supporta, considerate un'alternativa.

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
securingthehuman.sans.org/ouch/archives

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

Le Passphrases:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_it.pdf
I Password Manager:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_it.pdf
Il Malware:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_it.pdf
Tablet e sicurezza:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_it.pdf

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