SANS SECURING THE HUMAN | ADVANCTION

OUCH! | Marzo 2014

Newsletter mensile di suggerimenti sulla sicurezza informatica

OUCH!

IN QUESTO NUMERO...

Windows XP: siamo giunti al termine

Introduzione

Windows XP ha dimostrato nel corso degli anni di essere uno dei sistemi operativi più popolari nella storia dell'informatica tanto che è stato utilizzato sulla maggior parte dei computer nel mondo. Si tratta però di un sistema operativo datato e presto Microsoft ne terminerà il supporto. Rilasciato più di dodici anni fa, XP non verrà più supportato dalla casa produttrice dall'8 aprile 2014. Ciò significa che Microsoft, da quella data, non rilascerà più nuove versioni né aggiornamenti né patch di sicurezza. Con approssimativamente il 25% di computer desktop nel mondo che ancora si basano su questo sistema operativo, milioni di persone saranno a rischio quando tutto questo accadrà. Non saranno solo gli utenti casalinghi a essere toccati da questo evento, ma anche tutte quelle aziende che utilizzano XP negli uffici, nei sistemi di controllo industriale, nei Bancomat, nei sistemi medicali, nei terminali POS e in altri dispositivi. Nei prossimi paragrafi descriveremo quali sono i rischi a cui si può andare incontro da quando Windows XP non verrà più supportato e come fare per proteggersi.

L'autore di questo numero

Jason Fossen lavora alla Enclave Consulting come specialista di sicurezza negli ambienti Windows. Autore del corso SANS "Securing Windows with the Critical Security Controls (SEC505)", Jason figura anche tra gli autori del blog **http://cyber-defense.sans.org/blog/**.

Il ciclo di vita di un sistema operativo

Ogni sistema operativo per computer ha un tempo di vita limitato. Il produttore che lo ha creato fornirà aggiornamenti e patch che aggiungeranno nuove caratteristiche, miglioreranno la stabilità e le performance e manterranno il sistema sicuro. Da un certo momento in poi il produttore non lo supporterà più perché dovrà focalizzare le sue risorse sulle nuove tecnologie. Ciò significa che quando un sistema operativo non è più supportato, il produttore non rilascerà più aggiornamenti e patch, sebbene sia cosciente che i computer installati nel mondo siano vulnerabili ad attacchi da parte dei criminali informatici. Questo è ciò che succederà con Windows XP da aprile in poi: Microsoft smetterà di risolvere i problemi di Windows XP.

Come proteggersi

Il modo migliore per proteggersi è utilizzare un sistema operativo attivamente supportato. Se potete permettervelo, vi raccomandiamo di acquistare un nuovo computer: molti computer che ospitano Windows XP non sono in grado di supportare i moderni sistemi operativi. Se non potete permettervi un nuovo computer, aggiornate

Windows XP: siamo giunti al termine

quello già in vostro possesso. Per le aziende, la transizione potrebbe essere meno impegnativa migrando a Windows 7 anziché Windows 8, poiché l'interfaccia grafica del primo è più simile a quella di Windows XP. Windows 8 è comunque più sicuro delle versioni precedenti grazie a significativi miglioramenti nel software. Potete considerare inoltre altri sistemi operativi, come il Mac OS X di Apple.

Da quando Windows XP non sarà più supportato, il modo migliore per proteggervi è migrare a un nuovo sistema operativo, attivamente supportato dal suo produttore, e mantenerlo costantemente aggiornato.

Questo è il momento giusto per cambiare, non dovete perdere altro tempo. Nel caso non possiate cambiare il vostro Windows XP prima di aprile, tenete in considerazione questi suggerimenti.

- Utilizzate il computer con Windows XP solo per quelle funzioni o applicazioni assolutamente necessarie. Per esempio, la vostra azienda utilizza un vecchio programma che funziona solo su Windows XP e per questa ragione non potete aggiornarlo. In questo caso, non utilizzate quel computer per nessun altro scopo, in special modo per leggere le email o navigare.

- Se dovete utilizzare Windows XP per navigare, non usate Internet Explorer, bensì un altro browser come Firefox, Chrome o Opera. Assicuratevi che il browser sia sempre aggiornato e che il suo produttore continui a supportarlo anche su Windows XP.

- Non utilizzate più le applicazioni di Windows XP che aprono file da Internet, come Windows Media Player. Usate invece applicazioni separate di altri produttori di cui è garantito l'aggiornamento.

- Utilizzate un servizio di sicurezza di rete, come OpenDNS, gratuito e affidabile. Servizi come questo impediscono al vostro sistema di visitare siti maligni. Inoltre, alcuni servizi possono individuare i tentativi del vostro computer di collegarsi a server di Botnet, indizio che il vostro sistema è infetto.

- Assicuratevi che il software di sicurezza che avete installato, come ad esempio l'antivirus, sia ancora supportato e mantenuto per Windows XP.

Windows XP: siamo giunti al termine

- Se il vostro computer non deve collegarsi a Internet (ad esempio perché lo utilizzate solo per comporre del testo), scollegatelo dalla rete. Se deve essere collegato, assicuratevi che sia dietro a un firewall e che il firewall locale blocchi tutto il traffico verso di esso. Le aziende potrebbero voler isolare tutti i sistemi Windows XP su una rete separata, in modo che quando vengono infettati, non infettino il resto dell'azienda.
- Effettuate salvataggi regolari dei computer Windows XP in preparazione di quando potranno essere infettati. Mantenete almeno uno di questi backup offline, su un drive USB disconnesso. Se siete costretti a ripristinare il vostro sistema, considerate il ripristino su un computer nuovo poiché se doveste ripristinare su Windows XP, il sistema verrà probabilmente infettato un'altra volta.

Se state utilizzando Windows XP in azienda, il vostro datore di lavoro potrebbe aver ulteriori passi da seguire. Ricordate che queste sono contromisure da adottare per un breve lasso di tempo poiché non sono in grado di sostituirsi a un sistema operativo aggiornato e sicuro. Presto o tardi dovrete migrare a un nuovo sistema.

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

Microsoft: Fine del supporto per Windows XP:
http://windows.microsoft.com/it-it/windows/end-support-help
OpenDNS:
www.opendns.org
Migrare a Windows 7:
http://windows.microsoft.com/it-it/windows7/help/upgrading-from-windows-xp-to-windows-7#T1=tab01
OUCH: Il salvataggio dei dati:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_it.pdf

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