

I rimanenti miti, anch'essi popolari, che riguardano la sicurezza di Windows rispetto a Linux sono inficiati dal fatto di essere basati solo su un singolo metro di giudizio -- un singolo aspetto per misurare la sicurezza. Questo è vero sia che i dati provengano da ricerche esistenti, aneddoti o persino leggende metropolitane.

Uno dei più popolari è che, "ci sono molti più avvisi di sicurezza per Linux piuttosto che per Windows, e quindi Linux è meno sicuro di Windows". Un altro è, "Il lasso di tempo che in media trascorre tra la scoperta di una vulnerabilità a quando una patch per quella vulnerabilità viene rilasciata è maggiore per Linux rispetto a Windows, e quindi Linux è meno sicuro di Windows."

L'ultima è la più misteriosa di tutte. E' un mistero imponderabile che qualcuno possa giungere alla conclusione che il lasso di tempo che impiega Microsoft tra la scoperta di una vulnerabilità e il rilascio del fix per quella vulnerabilità è migliore rispetto a quello di qualunque altro sistema operativo, oltre ad essere migliore di quello di Linux. Microsoft impiegò sette mesi per risolvere una delle più serie falle di sicurezza (Microsoft Security Bulletin MS04-007 ASN.1 Vulnerability, eEye Digital Security publishes the delay in advisory AD20040210), e ci sono vulnerabilità che Microsoft ha apertamente dichiarato che non saranno mai riparate. Il bollettino di sicurezza MS03-010 su una vulnerabilità di Denial Of Service in Windows NT cita che la falla non verrà mai risolta. Più recentemente, Microsoft ha dichiarato che non risolverà le vulnerabilità di Internet Explorer per i sistemi operativi più vecchi di Windows XP. Statisticamente parlando, sette mesi tra la scoperta ed il rilascio di una patch potrebbe non avere un riscontro drammatico sulla media riguardante la velocità di risoluzione dei problemi solo se esistono sufficienti esempi di eccellente velocità di risposta per affossare anomalie come queste, assumendo che siano anomalie. Ma è sufficiente un caso di "non la risolverò mai" per portare la media statistica oltre qualsiasi possibilità di recupero.

Mistero ancora più inspiegabile, se si considera che significato abbia suggerire che Linux rappresenta un rischio di sicurezza superiore rispetto a Windows perchè il tempo che passa in media tra la scoperta di una vulnerabilità e il rilascio di una patch è superiore per Linux rispetto a Windows. Fatevi questa domanda: se doveste avere un attacco di cuore in questo preciso istante (facciamo corna! ndt), in quale reparto di emergenza vorreste essere ricoverati? Vorresti andare in quello con una velocità di risposta maggiore dal check-in al trattamento medico o vorreste piuttosto essere portati in un reparto con un record minore in termini di velocità checkin-trattamento, ma dove i pazienti con le patologie più gravi ricevono sempre immediata attenzione?

Chiunque sceglierebbe quest'ultimo, ma non necessariamente perchè l'informazione precedente prova che è un reparto migliore. L'ultima scelta è preferibile perchè include due metri di giudizio, uno dei quali è più importante per te in quel preciso momento. E' possibile affermare con certezza che la maggior parte delle persone eviterebbe un certo ospedale se sapesse di avere più possibilità di morire di attacco di cuore aspettando che un dottore finisca di sistemare la frattura di qualcuno, non importa quanto impressionante possa essere il tempo medio di reazione per ogni emergenza. Il problema è che il precedente esempio non ci da abbastanza informazioni per prendere la decisione migliore. Non ci dice come l'ospedale con il migliore tempo di reazione considera la priorità dei casi. Sarebbe ideale conoscere cose come il tasso di mortalità dei casi di emergenza, e così via.

Ovviamente, l'unico modo per produrre delle raccomandazioni utili è di raccogliere quanti più parametri possibili sui pronto soccorso locali, e poi bilanciare questi parametri intelligentemente. Sarebbe oltremodo irresponsabile raccomandare un pronto soccorso per un attacco di cuore basandosi solamente su un singolo parametro come quello del tasso di velocità tra tutte le emergenze, specialmente quando le informazioni che porterebbero ad una scelta ideale sono già disponibili.

E' in ugual modo irrazionale ed irresponsabile effettuare raccomandazioni o importanti scelte di business basandosi su un solo metro di giudizio come il tempo medio che intercorre tra la scoperta di una debolezza e il fix per quel dato sistema operativo, o il numero di avvisi di sicurezza per un dato prodotto.

Qualsiasi parametro preso singolarmente porta a confusione in termini di importanza. Consideriamo l'assunto che ci sono più avvisi di sicurezza per software Linux rispetto a Windows. Questa statistica non ha significato, perché lascia la domanda più importante senza risposta. Di tutti gli avvisi di sicurezza, quante delle vulnerabilità riportate rappresentano un rischio tangibile? Quanto sono severi questi rischi? In che modo espongono i tuoi sistemi ad un danno serio? Queste sono le domande importanti. Cos'è preferibile, un sistema operativo con 100 falle che espongono i tuoi sistemi a danni insignificanti o addirittura a nessuno danno, e possono essere sfruttati solamente da utenti con un valido account e accesso fisico alla macchina oppure preferisci un sistema operativo con una falla critica che permette a qualsiasi hacker dalle cattive intenzioni da Internet di cancellare tutte le informazioni sul tuo server? Chiaramente, il numero di avvisi da solo non è un parametro significativo per considerare la sicurezza di un sistema operativo rispetto ad un altro.