

German
Data
Security



G Data Whitepaper 2009

Sicurezza del sistema in Windows 7

Marc-Aurél Ester & Ralf Benz Müller
G Data Security Labs



Go safe. Go safer. G Data.



Sommario

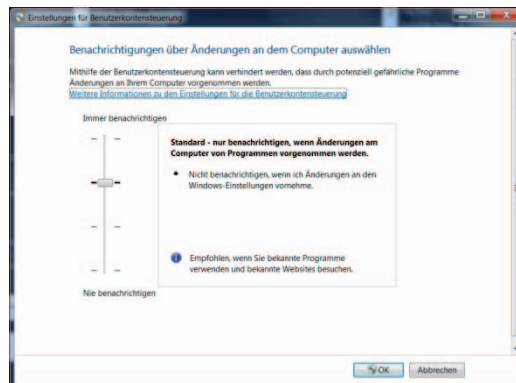
1. Windows 7 ai blocchi di partenza.....	2
2. Controllo degli account utente	2
3. Windows Firewall	3
4. Estensioni dei nomi di file.....	3
5. AppLocker	4
6. Windows Defender	4
7. Bitlocker	5
8. Bitlocker to go	5
9. Conclusione.....	6

1. Windows 7 ai blocchi di partenza

Windows 7 è il diretto successore di Windows Vista, che era stato accolto con molta perplessità, soprattutto dalle aziende. La quota sul mercato di Windows Vista corrisponde a circa il 30%, mentre Windows XP detiene ancora il 58%. Con Windows 7 Microsoft cerca di risolvere i punti critici presenti in Windows Vista, che avevano provocato malumore e discussioni sia presso gli utenti privati sia presso le aziende. Quindi Windows 7, rispetto a Vista, utilizza meno risorse e presto sarà disponibile anche in una versione speciale per netbook e dispositivi simili. Con Windows 7 viene inoltre resa pubblica la nuova interfaccia grafica DirectX-11. Il sistema è stato ottimizzato anche per l'uso con dischi SSD, riducendo il tempo di avvio. Anche i comandi sono stati modernizzati. Non da ultimo, Windows 7 pare essere più sicuro del suo predecessore. Di seguito verranno illustrate le principali novità e modifiche inerenti la sicurezza apportate in Windows 7. Verrà mostrata l'efficacia dei meccanismi di protezione, dove sussistono margini di miglioramento, e cosa invece è peggiorato rispetto a Windows Vista. Si potrà inoltre constatare che anche la più recente versione di Windows necessita di una potente soluzione antivirus.

2. Controllo degli account utente

Purtroppo la sicurezza non è sempre sinonimo di comodità. La dimostrazione lampante di questa affermazione è la gestione degli account utente in Vista. Molti utenti si sono lamentati del fatto che le finestre di conferma del controllo account utente compaiono troppo spesso e rallentano il flusso di lavoro. Per questo motivo, molti utenti hanno preso in mano la situazione e disattivato immediatamente i fastidiosi messaggi di avviso. In questo modo, però, si rende inutilizzabile un efficace strumento contro i software nocivi, i quali riescono a procurarsi automaticamente i diritti necessari per l'installazione.



Per contrastare questa tendenza, ora in Windows 7 è possibile impostare quattro diversi livelli per la visualizzazione dei messaggi di avviso del controllo account utente (UAC).

1. Segnalare sempre quando un programma o un utente desidera modificare il sistema.
2. Segnalare solo quando un programma vuole apportare modifiche al sistema.
3. Segnalare solo quando un programma tenta di apportare modifiche al sistema. In questa modalità lo sfondo dello schermo non viene oscurato.
4. Nessun messaggio.

Si può prevedere quindi che molti utenti preferiranno non adottare le prime due modalità. In questo modo, però, si riduce anche l'efficacia della protezione.

Tuttavia, anche quando la visualizzazione UAC è attivata, il malware può insinuarsi nel sistema. Durante la fase Beta di Windows 7 sono già stati sferrati con successo diversi attacchi che hanno compromesso il sistema e disattivato completamente la visualizzazione UAC.

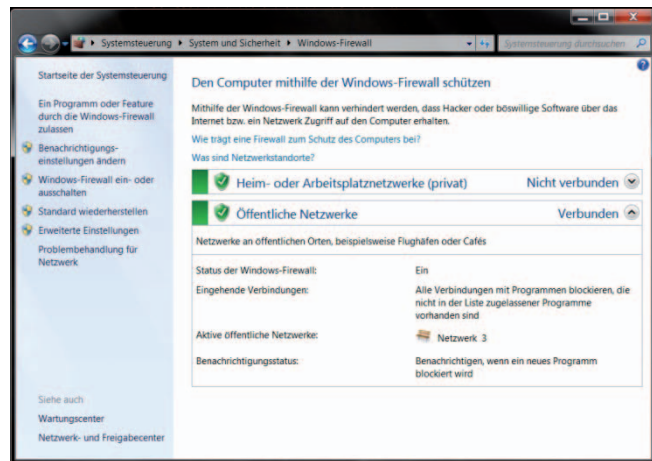
Task non verificati

Nonostante il monitoraggio costante, in Windows vi sono automatismi che vengono esclusi dal controllo degli account utente. Utilizzando la pianificazione dei task è possibile, ad esempio, avviare i programmi all'avvio del sistema con i diritti di amministratore, senza che venga visualizzata alcuna richiesta di conferma per l'utente. In questo modo i virus possono insinuarsi nel sistema.

Con il nuovo controllo degli account utente, Microsoft ha privilegiato la comodità a spese della sicurezza. Le impostazioni più deboli possono consentire l'ingresso di programmi dannosi senza alcuna richiesta, i quali si potranno in seguito propagare nel sistema. Queste semplificazioni del controllo, adottate con superficialità, penalizzano la sicurezza. Nell'ambito della gestione dei diritti, Microsoft dovrebbe trarre ispirazione dai concetti degli ambienti Unix e Mac OS X, decisamente più efficaci e più semplici da utilizzare.

3. Firewall

Microsoft ha preso seriamente le critiche rivolte a Windows Firewall e ha lavorato molto per migliorare la comodità d'uso del firewall in Windows 7. Per determinate applicazioni le regole vengono create automaticamente. È stata semplificata anche la gestione delle serie di regole tramite la procedura guidata ed ora è possibile creare senza problema nuove serie di regole. Inoltre, è possibile configurare il funzionamento del firewall a seconda dell'ambiente, ad esempio definire regole più severe per le WLAN pubbliche rispetto alle reti aziendali. Si possono inoltre assegnare vari profili ad ogni scheda di rete.

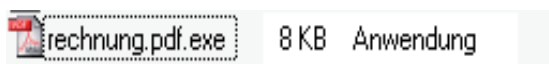


L'utilizzo di un firewall è sicuramente significativo, ma non lo è altrettanto delegare agli utenti la creazione e la gestione delle serie di regole. Molti utenti privati vengono sovraccaricati di responsabilità e possono solo indovinare. Un clic sbagliato può bloccare l'accesso a Internet o impedire l'uso delle stampanti collegate in rete. La decisione di chiedere all'utente in caso di dubbio non era, e non è neppure ora, una soluzione valida. Sarebbe realmente utile disporre di un firewall che decide autonomamente quali dati autorizzare. Questa funzionalità viene offerta soltanto da prodotti specializzati nella protezione Internet.

Esattamente come in precedenza, il firewall può essere disattivato, anche da programmi dannosi. Windows Firewall non offre quindi una funzione di autoprotezione, come invece i firewall dei prodotti specifici per la sicurezza. In questo frangente i prodotti in commercio sono decisamente più completi ed efficaci.

4. Estensioni dei nomi di file

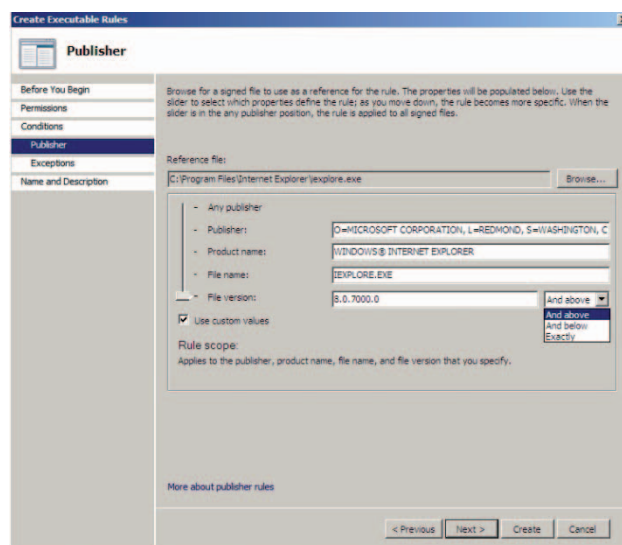
Fin da Windows 9x la gestione delle estensioni dei nomi di file presentava delle lacune. Microsoft ritiene tuttora che l'utente non debba vedere il suffisso dopo il nome del file nei tipi di file conosciuti. Questa „funzione“ viene sfruttata da decenni dai truffatori online. Funziona in questo modo: nell'impostazione predefinita, le estensioni dei nomi di file noti, come „.exe“, „.scr“ o perfino „.doc“ vengono nascoste. Viene visualizzato soltanto il nome del file con la relativa icona. Tuttavia, un aggressore è in grado di camuffare un file eseguibile con un'icona qualsiasi a sua scelta. Se un programma nocivo viene diffuso con il logo standard dei PDF, è difficile per un utente stabilire se si tratti realmente del tipo di file indicato dall'icona. Un utente che riceve questo tipo di file per e-mail può essere tratto in inganno e pensare di poter aprire il file senza alcun pericolo.



A nostro avviso, è assolutamente incomprensibile il fatto che Microsoft da un lato tormenti gli utenti con innumerevoli finestre di dialogo, a cui essi sono in grado di rispondere correttamente solo in rari casi, dall'altro continui a non supportare gli utenti nelle situazioni in cui occorre rilevare manovre di inganno reali da parte di programmi di malware. Esempio: 2-3 frasi

5. AppLocker

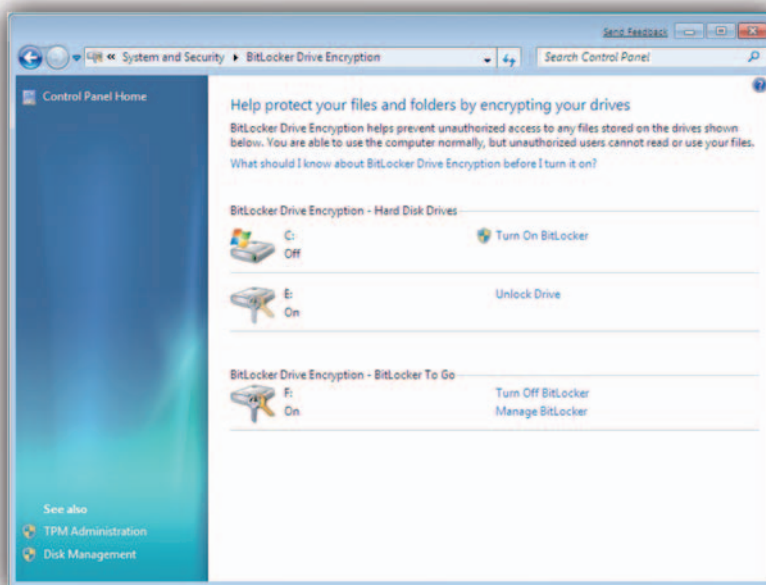
Con AppLocker gli amministratori possono controllare quali applicazioni sono autorizzate ad essere eseguite in una rete aziendale. Questa opzione era già disponibile nei Criteri restrizione software in Windows XP e in Windows Vista. Tuttavia, questa funzione non ha riscosso molto consenso presso gli amministratori poiché la gestione e la manutenzione di queste regole può richiedere un enorme dispendio di tempo. Ad esempio, ad ogni aggiornamento è necessario creare e gestire un nuovo valore hash. Ora, grazie alle regole di pubblicazione, è possibile integrare un software in modo permanente dato che l'identificazione avviene tramite la firma digitale, ormai utilizzata dalla maggior parte delle applicazioni. È possibile impostare: produttore, nome del prodotto, nome del file e numero di versione. Naturalmente, in base a questi criteri, è possibile impostare anche blocchi che impediscano l'esecuzione di determinate applicazioni.



AppLocker può essere un'arma realmente efficace nella lotta contro il malware e le regole di pubblicazione semplificano l'utilizzo di questo strumento. Tuttavia, anche i certificati possono essere scardinati e si teme che l'efficacia di questa protezione sia solamente temporanea.

6. Windows Defender

Windows Defender è diventato un componente integrante del sistema a partire da Windows Vista. Si tratta di un programma di scansione antispyware. Nei test comparativi, però, Windows Defender non convince. In un test comparativo eseguito solo pochi mesi addietro con altri prodotti antivirus, infatti, è stato rilevato solo il 20% dei virus installati. Con i siti Web che hanno tentato di installare programmi spyware, si è raggiunta una percentuale di poco superiore, pari al 37,5%. Uno dei problemi è che Defender utilizza solo un riconoscimento basato su valori hash e non un proprio filtro URL.



Windows Defender non è considerato da Microsoft come una soluzione antivirus completa, il suo scopo è proteggere dai principali virus e spyware appositamente creati per Windows. Gli utenti Windows sprovveduti potrebbero credere che Windows Defender svolga le funzioni di un programma antivirus e a torto avventurarsi senza protezione. Windows Defender non può e non deve sostituire una soluzione antivirus completa.

7. Bitlocker

La cifratura dei dati critici è un elemento sempre più importante. Per questo motivo Microsoft ha introdotto con Vista la tecnologia Bitlocker. Rispetto a Windows Vista, Microsoft ha risolto un grave problema di BitLocker. Infatti fino ad oggi l'utilizzo di BitLocker in un secondo momento richiedeva grandi sforzi, tra cui anche la riduzione della partizione del sistema. In seguito Microsoft ha fornito „BitLocker Drive Preparation Tool“ che semplificava l'intera procedura. Come in precedenza, le funzioni di cifratura di BitLocker per il disco fisso sono disponibili soltanto nelle versioni Ultimate ed Enterprise. Attualmente Windows 7 crea per BitLocker direttamente durante l'installazione un'enorme partizione di 200 MB o di 400 MB se è stato installato „Windows Recovery Environment“. BitLocker opera in combinazione con i chip TPM, presenti in molti notebook. Nei computer desktop si trova principalmente nei dispositivi aziendali. Se il dispositivo non è dotato di un chip TPM, si può salvare la chiave di cifratura su una chiavetta USB, che però si dovrà inserire ogni volta che si avvia il dispositivo, procedura alquanto complicata se confrontata con l'alternativa open source „True Crypt“. Tuttavia, BitLocker offre un'opzione interessante, soprattutto per le aziende, che permette di salvare la chiave generale nella „Active Directory“. Se accade che un utente dimentichi la password o perda la chiavetta USB, l'amministratore è in grado di recuperare i dati di accesso. Quanto sia alto il rischio di un potenziale abuso di questa funzione dipende dal livello di protezione dell'Active Directory.

8. Bitlocker to go

Bitlocker „da asporto“ è una novità di Windows 7 che permette di cifrare supporti dati mobili, come chiavette USB e schede SD. L'autenticazione avviene tramite immissione di una password o tramite Smartcard. Anche questa opzione permette di creare una chiave generale nella „Active Directory“. Oltre a ciò, gli amministratori possono forzare l'uso di „Bitlocker to go“ non appena vengono salvati i dati su un supporto dati mobile. Anche in Windows XP e Vista è possibile utilizzare „Bitlocker to go“ per leggere i dati codificati, tuttavia è un'operazione alquanto complicata. Occorre infatti copiare i dati sul disco fisso dopo l'immissione della password. Anche a questo punto, però, i supporti non sono scrivibili. Per motivi di sicurezza, non è consigliabile forzare la copia dei dati su un disco fisso non cifrato.

9. Conclusione

Per concludere, occorre chiedersi quanta protezione sia stata aggiunta in Windows 7. Windows è così sicuro da rendere superfluo l'utilizzo di un software di protezione? Con Vista Microsoft ha integrato in Windows molte funzioni di protezione. Tuttavia, le novità sono soprattutto a livello estetico e indirizzate prevalentemente ai clienti aziendali. „BitLocker“, „BitLocker to go“ e „AppLocker“ sono inclusi soltanto nelle versioni Ultimate ed Enterprise e quindi sono previsti principalmente per l'utilizzo nelle imprese. Per i clienti privati Microsoft ha cercato di rendere accessibili le tecnologie di protezione consolidate con Vista.

- A causa dei vari livelli di impostazione, la funzione di controllo degli account utente è diventata più vulnerabile ad eventuali abusi. Non è stata inclusa la funzione di pianificazione dei task.
- Come in precedenza, non vengono visualizzate le estensioni dei nomi dei file, quindi i truffatori possono continuare a mimetizzare i loro programmi dannosi con le icone di file innocui.
- Con Windows Defender viene presentata agli utenti una soluzione di protezione che in realtà è inefficace.

In effetti Windows 7 può vantare qualche funzione di protezione in più, tuttavia non rappresenta una reale evoluzione rispetto a Vista. Purtroppo molte funzioni di protezione si possono eludere. È solo una questione di tempo e gli specialisti del malware saranno in grado di fornire tecniche di aggressione adeguate ai delinquenti del mercato criminale online. Anche in futuro, quindi, per proteggere i computer Windows da attacchi ed abusi, saranno necessari software di protezione in grado di offrire una protezione efficiente ed efficace e semplici da usare.

Appendice:

Disponibilità dei meccanismi di protezione nelle diverse versioni di Windows 7

Funzione	Versione Windows 7					
	Starter	Home Basic	Home Premium	Professional	Enterprise	Ultimate
EFS				●	●	●
Bitlocker					●	●
Bitlocker to go					●	●
UAC	●	●	●	●	●	●
Windows Defender	●	●	●	●	●	●
Windows Firewall	●	●	●	●	●	●
DEP	●	●	●	●	●	●