

SOPHOS

Sophos Endpoint Security and Control Windows XPe/Windows Embedded Standard guida al test

Versione prodotto: 9.0

Data documento: settembre 2009



Sommario

- 1 Informazioni sulla guida.....3
- 2 Preparazione dei test.....3
- 3 Installazione del software di sicurezza.....3
- 4 Test di rilevamento delle minacce.....4
- 5 Test del controllo applicazioni.....5
- 6 Test del controllo dati.....6
- 7 Test del controllo dispositivi.....6
- 8 Copyright.....7

1 Informazioni sulla guida

Questa guida è rivolta agli amministratori di rete che vogliono proteggere i computer con sistema operativo Windows XP Embedded (Windows XPe) o Windows Embedded Standard.

Le versioni embedded di Windows possono essere compilate con varie possibilità di personalizzazione, pertanto questa guida non mira a discutere se ciascuna di esse possa essere protetta con successo. Essa cerca invece di spiegare come eseguire dei controlli dopo l'installazione, per verificare il corretto funzionamento del software di sicurezza Sophos.

Questa guida presuppone che sia già stata utilizzata Enterprise Console per installare e gestire il software di sicurezza Sophos sulla vostra rete.

Essa descrive come fare per:

- Installare il software di sicurezza Sophos sui computer che utilizzano Windows XPe/Windows Embedded Standard.
- Verificare che il software riceva i regolari aggiornamenti.
- Testare il rilevamento delle minacce
- Testare il controllo di applicazioni, dati e dispositivi.

Importante: Se verranno completati con successo tutti i test di questa guida, ci impegneremo a fare dei ragionevoli sforzi, sulla base delle pratiche commerciali standard di Sophos, per fornire il supporto tecnico. Per informazioni, consultare l'articolo 63797 della knowledge base del supporto Sophos (<http://www.sophos.it/support/knowledgebase/article/63797.html>)

2 Preparazione dei test

Prima di cominciare

- Selezionare i computer con sistema operativo Windows XPe/Windows Standard Embedded come computer di prova.
- Assicurarsi che il file di rilevamento del virus EICAR sia già installato o pronto da installare sui computer di prova.
- Assicurarsi che MSN Messenger Live sia pronto da installare sui computer di prova durante il test del controllo applicazioni.

3 Installazione del software di sicurezza

Prima di eseguire il test è necessario:

- Installare il software di sicurezza sui computer di prova.
- Verificare che il software stia ricevendo gli aggiornamenti.

3.1 Installazione del software

L'installazione di Sophos Endpoint Security and Control 9.0 per Windows richiede la medesima procedura che si utilizza su qualsiasi altro computer con sistema operativo Windows.

È possibile svolgere una delle seguenti operazioni:

- **Installazione automatica.** In Enterprise Console, trovare i computer di prova e assicurarsi che dispongano di un criterio di aggiornamento valido. Selezionare i computer, cliccarvi col tasto destro del mouse e selezionare **Proteggi computer**.
- **installazione manuale** Ai computer di prova, cercare la cartella da cui i computer ricevono l'aggiornamento ed eseguire il programma di installazione di Sophos.

Nota: La cartella da cui i computer ricevono l'aggiornamento si può trovare cercando nei **Percorsi bootstrap** in Enterprise Console.

3.2 Verifica dell'aggiornamento

E' opportuno verificare che i computer di prova stiano ricevendo gli aggiornamenti di Sophos.

Ai computer di prova:

1. Sulla barra delle applicazioni, cliccare col tasto destro del mouse sull'icona di Sophos e selezionare **Aggiorna ora**. Attendere che l'aggiornamento venga completato.
2. Aprire Sophos Endpoint Security and Control.
3. Sulla home page, nel pannello **Status**, controllare che l'orario di **Ultimo aggiornamento** sia cambiato.

4 Test di rilevamento delle minacce

4.1 Controllare che il rilevamento funzioni

Per verificare che Sophos Endpoint Security and Control riesca a rilevare le minacce, eseguire un test EICAR come descritto sotto.

1. Sui computer di prova, tentare di copiare un file di test EICAR sul computer (o di eseguire EICAR se è già presente nel computer).
I computer di prova dovrebbero visualizzare un allarme virus.
2. Controllare che i computer di prova mostrino il file EICAR nel Gestore quarantena e che i dati siano corretti.

4.2 Controllo allarmi

Andare su Enterprise Console e fare quanto segue:

1. Controllare che le schede nella vista elenco computer mostrino il nome del virus, la posizione e l'orario in cui è stato rilevato.
2. Controllare che i dati computer per i computer di prova mostrino i dati corretti

Cancellare quindi gli allarmi.

4.3 Cancellare gli allarmi

1. Sui computer di prova, cancellare l'allarme dal Gestore quarantena.
2. In Enterprise Console, cancellare l'allarme nel dialogo **Risolvi allarmi ed errori**.

5 Test del controllo applicazioni

5.1 Configurazione del controllo applicazioni

1. In Enterprise console, aprire un criterio di controllo applicazioni.
2. Configurare il criterio in modo da bloccare MSN Live Messenger.
3. Applicare il criterio ai computer di prova.
4. In Enterprise Console, verificare che la modifica al criterio sia stata applicata, e che i computer di prova siano conformi al criterio.

5.2 Controllare che il controllo applicazioni funzioni

1. Sui computer di prova, cliccare con il tasto destro del mouse sull'icona SESC e selezionare **Aggiorna ora**.
2. Provare ad installare e ad aprire MSN Live Messenger.
3. Controllare che venga visualizzato un allarme. L'applicazione dovrebbe essere visualizzata nel Gestore quarantena e tutti i dati dovrebbero essere corretti, compreso il tipo.
4. In Enterprise Console, controllare la vista elenco computer e la pagina dati computer.

5.3 Cancellare gli allarmi e ripristinare il criterio

1. Sui computer di prova, cancellare gli allarmi dal Gestore quarantena.
2. In Enterprise Console, ripristinare il criterio del controllo applicazioni alle sue impostazioni originarie.
3. Controllare che il computer e la console siano conformi al criterio modificato.

6 Test del controllo dati

6.1 Configurazione del controllo dati

1. In Enterprise Console, creare un criterio del controllo dati ed aprirlo.
2. Nella scheda **Regole criteri**, cliccare su **Gestisci regole**.
3. Nella finestra di dialogo **Gestione regole del controllo dati**, cliccare su **Aggiungi regola contenuti**.
4. Inserire un nome per la Regola. Sotto **Regola contenuti** cliccare sul link "Dove il file contiene".
5. Nella finestra di dialogo **Gestione Content Control List**, selezionare un CCL e fare clic su **OK**.
6. Sotto **Contenuto regola**, cliccare sul collegamento "Seleziona destinazione" e controllare **Memorie rimovibili**. Cliccare su **OK**.
7. Nella finestra di dialogo **Gestione regole del controllo dati**, selezionare la regola creata e cliccare su **OK**.
8. Chiudere tutti i dialoghi e applicare il criterio ai computer di prova.

6.2 Verificare che il controllo dati funzioni

1. Sui computer di prova, aprire Sophos Endpoint Security and Control.
2. Sulla home page, nel pannello **Status**, verificare che il controllo dati venga visualizzato come abilitato.
3. Fare clic sull'icona del **log del controllo dati**. Controllare che la scansione del controllo dati sia stata avviata.

7 Test del controllo dispositivi

7.1 Configurazione del controllo dispositivi

1. In Enterprise console, aprire un criterio di controllo applicazioni.
2. Configurare il criterio per bloccare **Modem** e **Wireless**.

Nei dati computer, la colonna Conformità al criterio di controllo del dispositivo dovrebbe mostrare "In attesa di policy transfer " e poi "Come nel criterio".

3. Applicare il criterio ai computer di prova.
4. Controllare che il computer sia ora conforme al criterio.

7.2 Verificare che il controllo dispositivi funzioni

1. Connettere modem e dispositivi wireless ai computer.
Dovrebbe apparire un allarme a fumetto per ogni dispositivo bloccato
2. Aprire Sophos Endpoint Security and Control. Sulla home page, cliccare su **Log del controllo dispositivi** e controllare che il dispositivo sia bloccato.
3. Controllare che il Device Manager di Windows mostri che il dispositivo è stato disabilitato.
4. Usare il dispositivo wireless per tentare di contattare una rete wireless
Windows dovrebbe mostrare che il dispositivo è bloccato e non può rilevare reti.
5. Usare il Device Manager di Windows per testare il modem. Verificare che il modem non possa essere testato.

7.3 Ripristino del criterio del controllo dispositivi

1. In Enterprise console, impostare il criterio del controllo dispositivi come segue.
 - Modem Accesso completo.
 - Wireless Accesso completo.
2. Applicare il criterio ai computer di prova.
3. Controllare che i computer siano conformi al criterio.
4. Sui computer di prova, cliccare sull'icona del **Log del controllo dispositivi** e controllare che il dispositivo sia abilitato.
5. Sul computer, controllare che il dispositivo wireless possa rilevare reti wireless.
6. Usare il Device Manager di Windows per testare il modem. Verificare che il test automatico del dispositivo abbia avuto successo.

8 Copyright

Copyright © 2009 Sophos Group. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos e Sophos Anti-Virus sono marchi registrati di Sophos Plc e Sophos Group. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

Alcuni programmi software sono concessi in licenza (o in sottolicenza) all'utente secondo i termini della GNU General Public License (GPL) o licenze similari per il software libero che, tra gli altri diritti, permettono all'utente di copiare, modificare e redistribuire determinati programmi, o porzioni di programma, e di accedere al codice sorgente. La GPL richiede, per

qualsiasi software concesso in licenza secondo i termini della stessa e distribuito a un utente in formato binario eseguibile, che il codice sorgente venga messo a disposizione anche degli altri utenti. Per qualsiasi di tale software che sia distribuito insieme a questo prodotto Sophos, è possibile ottenere il codice sorgente tramite ordine postale inviandone richiesta a Sophos.

E-mail: savlinuxgpl@sophos.com

Indirizzo: Sophos Plc, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Regno Unito.

Copia dei termini della GPL è reperibile all'indirizzo www.gnu.org/copyleft/gpl.html

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.it/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>