

FOIRE AUX QUESTIONS ESA : Est-ce que je néanmoins ai besoin d'antivirus de bureau si j'active Sophos ou l'antivirus de McAfee sur mon ESA ?

Contenu

[Introduction](#)

[Est-ce que je néanmoins ai besoin d'antivirus de bureau si j'active Sophos ou l'antivirus de McAfee sur mon ESA ?](#)

Introduction

Ce document décrit des exemples de la façon dont des virus sont introduits dans un réseau d'entreprise et la recommandation de Cisco pour avoir l'antivirus local pour des utilisateurs.

Est-ce que je néanmoins ai besoin d'antivirus de bureau si j'active Sophos ou l'antivirus de McAfee sur mon ESA ?

Oui. L'antivirus autorisé et étant activé sur l'appliance de Sécurité d'email (ESA), ceci seulement une première défense de couche à empêcher des virus d'atteindre des utilisateurs. Les pratiques recommandées dans l'appel de Sécurité de réseau d'entreprise pour une défense en profondeur posée s'approchent. C'est pour cette raison que beaucoup de réseaux d'entreprise ont choisi d'implémenter non seulement l'antivirus de côté serveur, tel que l'ESA prévoit, mais également antivirus de bureau localement des utilisateurs.

Des virus sont portés dans un réseau d'entreprise de plusieurs manières sans compter que par l'intermédiaire de l'email. Les pages Web malveillantes peuvent injecter des virus. Un ordinateur portable infecté peut être apporté dedans d'un réseau extérieur. Les fichiers infectés apportés dedans sur des supports amovibles et chargés à un ordinateur d'entreprise sont une occurrence quotidienne pour les utilisateurs inconscients. Les auteurs de malware emploient l'ingénierie sociale pour avoir leurs attachements infectés, la codent, et des messages activement avertis et trouvent des moyens de sauter des mesures de sécurité standard. Ce sont juste quelques uns, des méthodes simples qu'un virus peut être introduit dans un réseau d'entreprise.

Non chaque scanner de virus attrapera chaque virus, et non chaque constructeur d'antivirus met leurs dossiers à jour de définition de virus en même temps. En outre, selon la façon dont les virus entrent dans le réseau d'entreprise, non chaque scanner de virus verra tous les virus. Par exemple, un virus basé sur le WEB ne traverserait pas le système de courrier électronique d'entreprise, ou un ordinateur intérieurement infecté peut envoyer les virus email-soutenus de votre réseau et évite de traverser par l'ESA.

Cisco recommande que vous ayez une suite locale à jour d'application ou de Sécurité d'antivirus qui assurera une couche supplémentaire de protection pour tous les utilisateurs dans un réseau d'entreprise. Il est essentiel de mettre à jour un système de défense multicouche de virus pour garder contre l'entrée de virus sur tous les avants pour votre réseau.