La protection antivirus dans les PME

L'antivirus fait partie de l'équipement de base de toute entreprise, car les logiciels malveillants représentent une menace croissante dans notre monde numérique, surtout pour les PME. Une bonne protection antivirus et de bons comportements sont la meilleure façon de s'en prémunir.

Principales informations à connaître :

- Définissez et mettez en place un système de **protection antivirus** dans votre PME.
- Créez un support permettant d'illustrer la façon dont les malwares peuvent entrer et **se diffuser** dans l'entreprise.
- Établissez un **plan antivirus** dans lequel vous définirez les points de contrôle antivirus les plus efficaces pour votre réseau.
- **Sensibilisez** les salariés aux dangers que comportent les malwares.

Les processus de protection antivirus

De nombreux fabricants proposent aujourd'hui de très bons systèmes de protection antivirus qui s'adaptent très bien aux différents besoins et contextes des réseaux informatiques des PME. Une première analyse doit cependant être effectuée pour permettre d'identifier la meilleure solution qui sera ensuite mise en œuvre par du personnel expert.

Mais la question ne s'arrête pas là. Les mesures de sécurité adoptées doivent en effet être constamment actualisées pour suivre l'évolution de la cybercriminalité et des logiciels malveillants. L'antivirus par exemple doit être constamment mis à jour avec les derniers modèles de virus.

Il convient donc de mettre en place un processus de protection antivirus en mesure de surveiller correctement les flux de données, de détecter et supprimer les logiciels malveillants (https://www.ebas.ch/fr/les-infections-par-malware/), ainsi que d'assurer la maintenance des systèmes informatiques. Dans ce cadre, il est tout aussi important de sensibiliser régulièrement les salariés à ce type de menace.

Les modes de diffusion

La complexité des réseaux dans les PME ne cesse d'augmenter. En effet, il n'y a pratiquement pas un jour qui passe sans que de nouvelles solutions logicielles ne soient implémentées, sans que de nouvelles connexions de données ne soient créées ou que des améliorations ne soient apportées à l'infrastructure. Les cybercriminels profitent de cette complexité croissante pour mettre au point de nouvelles attaques et de nouveaux modes de diffusion pour leurs malwares.

Une bonne stratégie de protection antivirus (#concept) doit donc se baser sur l'identification – la plus complète possible – des vecteurs potentiels d'entrée et de diffusion des maliciels. Pour ce faire, une bonne approche consiste à imaginer plusieurs scénarios possibles :

1. « Comment et par quel moyen un hacker pourrait-il introduire un malware dans le réseau » ?
2. « Comment ce malware pourrait-il ensuite se diffuser dans le réseau » ?

Pour s'introduire dans les réseaux, les logiciels malveillants utilisent principalement les canaux suivants :

- les connexions Internet, WLAN et VPN
- les pièces jointes aux supports de communication comme les courriels par exemple
- les dispositifs mobiles des salariés et des visiteurs
- les applications de contrôle à distance (RDP) et de configuration de terminal (Terminal Server)
- Les échanges de supports physiques de stockage des données
- Des environnements IoT mal protégés

Une fois qu'ils ont pénétré dans le réseau, les malwares peuvent profiter des vulnérabilités du système pour se diffuser. Il suffira ensuite d'un comportement imprudent d'un salarié pour lui permettre de s'activer et de déployer son action néfaste. Dans ce cas, il est important de limiter le plus possible les dégâts et d'empêcher une diffusion à large échelle.

La stratégie antivirus

Une fois que l'on a identifié les vecteurs d'entrée et de diffusion des malwares, il est possible de déterminer les secteurs où les mesures antivirus seront les plus efficaces dans le réseau.

En raison de leur exposition, les connexions réseau entrantes et sortantes à Internet devraient faire l'objet d'une attention toute particulière dans la chasse aux malwares. Cette surveillance peut se faire au moyen d'un pare-feu ou de serveurs de communication et serveurs proxy, en veillant à ce que les contenus soient toujours vérifiés avant le cryptage et après le décryptage.

À cet égard, les dispositifs mobiles des salariés et des visiteurs représentent un danger important, dans la mesure où ils sont souvent utilisés dans des environnements non sécurisés Ces dispositifs ne devraient donc jamais pouvoir accéder sans surveillance au réseau interne de l'entreprise. Cette règle vaut notamment pour les connexions VPN vers l'extérieur, dans le cadre du télétravail (https://www.ebas.ch/fr/5-precautions-quand-on-travaille-a-la-maison/) par exemple. Dans de tels cas, le recours à un logiciel antivirus géré de manière centralisée pour les terminaux peut s'avérer une bonne solution.

Enfin, les ordinateurs fixes, mais auxquels on connecte régulièrement des supports de données externes, doivent être équipés d'un logiciel antivirus approprié.

La stratégie de protection antivirus doit définir l'ensemble du système de protection antivirus et sa configuration.

Les suites antivirus pour les entreprises

De nombreux éditeurs proposent des solutions antivirus adaptées aux réseaux plus importants, où le déploiement, la configuration et la maintenance de la protection antivirus peuvent être gérés de manière centralisée sur l'ensemble des plateformes et des lieux de travail. Ce type de solution permet de garantir que la politique de sécurité des PME soit respectée à chaque fois qu'un dispositif se connecte au réseau.

Les statistiques de la cybercriminalité sont sans appel : le nombre d'attaques de malwares ayant fait des ravages a augmenté de manière significative au cours de ces dernières années. En particulier, les ransomwares représentent un danger de plus en plus sérieux pour les PME.