Comprendre les solutions de sécurité : antivirus, pare-feu, VPN...

Dernière modification : 06 avril 2022

Tags

#antivirus #parefeu #vpn #sécurité #misesajour

Résumé

Ce tutoriel a pour objectif de présenter les catégories de solutions de sécurité et les fonctionnalités que l'on peut y retrouver.

Prérequis

Aucun - Contenu approprié pour tous les supports

Des antivirus aux solutions de sécurité

Des solutions différentes selon les menaces

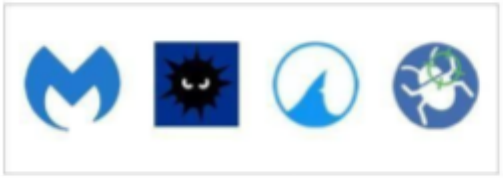
Un antivirus est un logiciel qui permet de mettre en quarantaine / supprimer des virus (ou vers informatiques).

D'autres outils sont apparus pour contrer de nouveaux types de logiciels malveillants. Ces logiciels sont complémentaires aux antivirus. Parmi ces nouvelles catégories de logiciel, on retrouve :

- **l'anti-malware** protège **contre les logiciels publicitaires** et les logiciels malveillants plus sophistiqués ;
- le **pare-feu (firewall)** protège l'ordinateur des **intrusions extérieures** via le réseau Internet ou local ;
- les **nettoyeurs** qui suppriment les fichiers temporaires et non essentiels pour le bon fonctionnement de l'ordinateur.

Les antivirus

Les pare-feu



Les antivirus par défaut sont très efficaces.

Des **solutions de sécurité** sont **intégrées** dans les systèmes d'exploitation : par exemple **Windows Defender** sur **Windows 10**. Elles sont considérées comme efficaces, voire plus performantes que des antivirus dédiés, selon des tests réalisés par des instituts indépendants, tels qu'AV-TEST.

Aujourd'hui, les antivirus sont de véritables solutions de sécurité avec une panoplie de fonctionnalités différentes du fait de **cyber attaques plus sophistiquées**.

Les fonctionnalités d'une solution de sécurité

L'antivirus

L'antivirus réalise des analyses ("scans") à des moments programmés, ou lorsqu'un fichier est transféré ou téléchargé sur l'ordinateur.

Une fois détectés, les fichiers dangereux sont supprimés, mis en quarantaine, ou conservés dans le cas de faux-positifs.

Le filtrage (pare-feu, proxy ou serveur mandataire…)

Le filtrage du trafic Internet entrant et sortant s'impose pour éviter les intrusions sur un réseau informatique, et sur les postes de ce réseau : c'est le **rôle du pare-feu.**

Certaines solutions de sécurité permettent de contrôler la navigation sur Internet, en limitant l'accès à des sites. Ces logiciels peuvent aussi enregistrer les connexions réalisées.

Le pare-feu permet aussi de cloisonner le réseau en plusieurs sous-réseaux. Cela est utile si vous souhaitez **dissocier un réseau public, accessible par vos clients, d'un réseau privé interne par exemple.**

La protection du noyau du système d'exploitation

Certains logiciels malveillants modifient des fichiers vitaux de l'ordinateur.

La suppression ou la mise en quarantaine **de ces fichiers peut empêcher le bon fonctionnement du système d'exploitation.**

Pour limiter ce risque des **mécanismes de protection** peuvent être mis en place. Ils **stoppent également les actions de certains rançongiciels** (ransomwares).

La gestion des vulnérabilités (mises à jour)

Les cybercriminels exploitent les failles des logiciels ou des systèmes pour réaliser leurs attaques.

Ce type d'attaque peut être évité par la mise à jour de son système et de ses logiciels.

Les solutions de sécurité proposent ainsi d'analyser les vulnérabilités et de réaliser les mises à jour nécessaires pour combler les failles détectées.

La détection des fraudes

Le phishing (ou hameçonnage), les pages Internet piégées et le spam constituent autant de fraudes qui parasitent votre confort de navigation et la sécurité de votre équipement.

Les solutions de sécurité embarquent des outils qui permettent d'alerter l'utilisateur en cas de suspicion de danger d'une page Internet ou d'un email reçu.

La gestion de flotte

On retrouve généralement plusieurs appareils connectés au réseau d'un foyer ou d'une entreprise. S'ils sont vulnérables, ils peuvent **devenir la porte d'entrée d'un pirate, et propager une attaque sur les autres appareils du réseau.**

Dans le cadre familial, on retrouve cet usage pour le contrôle parental, qui permet de bloquer certaines fonctionnalités, l'accès à certains sites, ou de verrouiller automatiquement la machine sur une période de temps.

Dans un cadre professionnel, on peut aussi contrôler des paramètres à distance à des fins de sécurité et de productivité.

La protection de la vie privée

La vie privée des utilisateurs représente un enjeu important. Les solutions de sécurité peuvent intégrer :

- **un VPN** : chiffre le transport des données de votre ordinateur vers un site Internet lorsque vous utilisez un réseau public ou peu sécurisé ;
- **un anti-tracker** : brouille les pistes des mouchards installés sur un site Internet pour espionner votre comportement et votre navigation afin de vous proposer de la publicité personnalisée ;
- **une protection webcam et micro** : demande votre autorisation si un logiciel doit accéder à ces éléments, afin d'éviter de vous espionner.

La protection contre vols et pertes de matériel

Localise voire bloque un ordinateur et supprime les données à distance.

Le gestionnaire de mots de passe

Stocke de manière sécurisée. Certains génèrent des mots de passe robustes.

La destruction sécurisée de fichiers

Les fichiers supprimés de façon standard peuvent laisser des traces sur le disque dur et être récupérés par des personnes malveillantes. Cela peut poser problème, notamment si vous revendez votre ordinateur à une personne, et que cette dernière essaie de restaurer des données de cette manière.

Certaines solutions de sécurité disposent d'outils pour détruire de manière sûre et durable les fichiers que vous souhaitez éliminer…

Les choix possibles selon son système d'exploitation

Sur Windows

Sous Windows, la suite **Windows Defender** offre par défaut un antivirus, un pare-feu et des protections complémentaires, notamment contre les ransomwares. Cette suite suffit pour assurer raisonnablement votre sécurité personnelle (surf, e-mail, bureautique).

Si vous devez gérer un parc informatique de plusieurs machines, il est recommandé de recourir à des solutions professionnelles payantes afin de disposer d'**une interface d'administration permettant de surveiller le niveau de sécurité** de l'ensemble des équipements de ce réseau.

Les solutions de sécurité gratuites (et propriétaires) ne sont pas forcément recommandées. En effet, certaines solutions peuvent utiliser vos données personnelles en contrepartie. Attention, cela ne vaut pas pour les

versions d'essai de solutions payantes, pour des scanners antivirus dits "ponctuels".

Sur Mac OS

Les ordinateurs sous Mac OS **ne sont pas moins vulnérables** à des attaques plus perfectionnées.

En effet, la part de marché des Mac étant croissante et le pouvoir d'achat des utilisateurs Apple étant important, ces derniers deviennent des cibles intéressantes pour les cybercriminels.

Le système Mac OS intègre des mécanismes internes de protection contre les logiciels malveillants (par exemple, la vérification des applications).

Si votre version de Mac OS est plus ancienne et qu'elle **n'est plus mise à jour**, ou si vous avez des usages plus sensibles, **alors l'installation d'une solution de sécurité est recommandée**.

Sur Linux

Comme pour Mac OS, l'architecture des distributions Linux explique sa moindre perméabilité aux malwares classiques. Néanmoins, face à des cyberattaques sophistiqués, **la présence de vulnérabilités non corrigées sur un système Linux expose leur utilisation à des risques.**

Dans le cas de Linux, le paramétrage maîtrisé du système et les bonnes pratiques de sécurité élémentaires sont préconisés. **L'installation d'une solution de sécurité n'est pas spécialement recommandée**. Elle reste néanmoins intéressante en cas d'interconnexion avec des PC sous Windows (par exemple des ordinateurs Windows connectés à un serveur de fichier Linux).

En effet, ces serveurs peuvent servir de relais à des attaques sur des réseaux informatiques (réplication de virus).

Sur Android (smartphone, tablette)

Par défaut, les équipements Android embarquent Play Protect qui analyse les applications que vous utilisez sur votre smartphone ou sur votre tablette.

L'installation d'un antivirus peut apporter une sécurité complémentaire. Il est recommandé de
choisir une solution connue et rester **vigilant sur les applications que vous installez et les liens que vous ouvrez sur votre téléphone ou sur votre tablette**.

Sur iOS (iPhone, iPad)

Le système d'Apple iOS est moins sensible aux logiciels malveillants pour deux raisons :

- les applications sont exécutées dans un environnement hermétique, laissant moins de possibilités à la prise de contrôle d'un iPhone ou d'un iPad par des malwares ;
- celles qui sont téléchargées depuis l'App Store suivent une procédure stricte avant d'être publiées. Ce qui limite le risque de tomber sur des programmes malveillants.

Toutefois, le risque zéro n'existe pas. Des problèmes de sécurité sont déjà apparus sur des iPhone et des iPad (site internet piégé qui exploite des failles logicielles non corrigées ou application malveillante ayant réussi à passer les barrières d'Apple).

Bon à savoir

Apple interdit les applications d'antivirus sur son App Store.

Les applications de sécurité qui existent proposent des fonctionnalités tels que les VPN, la localisation du téléphone à distance, ou encore des gestionnaires de mots de passe. C'est pourquoi les bonnes pratiques restent de mise : **vigilance sur les applications que vous installez et sur les liens que vous ouvrez**.

Pour aller plus loin - liens utiles

Guide Que Choisir pour sélectionner son antivirus

Logiciels préconisés par l'ANSSI

Licence