
MR ROLIN
[SECURITY] Les anti-virus

2025

Objectifs

À la fin de ce cours, l'apprenant sera capable de :

- Expliquer l'utilité d'un antivirus dans la protection d'un système informatique.
- Décrire les principaux types de logiciels malveillants pris en charge par un antivirus.
- Comprendre les méthodes de détection : signatures, heuristique, analyse comportementale.
- Expliquer le principe de la quarantaine.
- Identifier les limites d'un antivirus et les bonnes pratiques à adopter pour compléter la protection.

Introduction

L'antivirus est un outil indispensable dans tout environnement informatique, que ce soit à la maison, en entreprise ou dans une infrastructure réseau complexe. Les systèmes sont exposés en permanence à des menaces, qu'il s'agisse de virus historiques, de ransomwares modernes ou de logiciels espions. Pour un futur technicien PC et réseaux, comprendre comment fonctionne un antivirus est essentiel afin de diagnostiquer des problèmes de sécurité, conseiller les utilisateurs et mettre en place une protection efficace. Ce cours a pour but d'expliquer de manière claire et concrète les mécanismes internes d'un antivirus et son rôle dans la défense d'un système informatique.

Rôle et utilité d'un antivirus

Un antivirus est un programme informatique conçu pour prévenir, détecter et supprimer les logiciels malveillants (malwares). Il agit comme un système de surveillance qui examine constamment les fichiers, les programmes et les activités du système afin de repérer tout comportement anormal. Grâce à lui, l'ordinateur est protégé contre la perte de données, le vol d'informations personnelles ou les perturbations du système d'exploitation.

Dans un contexte professionnel, l'antivirus joue également un rôle de prévention des arrêts de service, de protection des réseaux et de conformité aux règles de cybersécurité imposées par les entreprises.

Les types de menaces détectées

Les antivirus luttent contre une grande variété de malwares. Les virus traditionnels se propagent en infectant des fichiers légitimes, tandis que les vers se propagent automatiquement à travers les réseaux. Les chevaux de Troie se cachent dans des logiciels en apparence fiables et ouvrent souvent des portes dérobées. Les ransomwares chiffrent les données et exigent un paiement, alors que les spywares collectent des informations sans autorisation. La diversité de ces menaces oblige les antivirus à adopter des stratégies de détection multiples et sophistiquées.

La détection par signatures

La méthode la plus ancienne et la plus répandue est la détection par signatures. Une signature est une sorte d'empreinte unique permettant d'identifier un malware connu. L'antivirus compare les fichiers du système à une base de données régulièrement mise à jour et repère les correspondances. Ce système est très efficace tant que le malware est déjà répertorié. En revanche, il devient moins performant face aux nouvelles menaces, ce qui pousse les éditeurs à publier des mises à jour fréquentes.

Les techniques heuristiques et comportementales

Pour détecter des menaces nouvelles ou modifiées, les antivirus utilisent des techniques heuristiques et comportementales. L'heuristique analyse la structure et le code d'un fichier afin de déterminer s'il ressemble à un malware, même si sa signature est inconnue. L'analyse comportementale, quant à

elle, se concentre sur les actions du programme : modification de fichiers système, tentatives de connexion suspectes, création anormale de processus, etc. Ces méthodes permettent de repérer des malwares encore inconnus, appelés attaques zero-day.

L'analyse en temps réel

Un antivirus efficace surveille en continu les activités du système. Chaque fichier ouvert, téléchargé ou exécuté est analysé instantanément. Cette protection en temps réel empêche qu'un fichier malveillant n'ait le temps d'endommager le système. C'est l'une des fonctionnalités essentielles pour assurer la sécurité d'un poste de travail.

La quarantaine

Lorsqu'un fichier suspect est détecté mais ne peut pas être immédiatement supprimé, l'antivirus le place en quarantaine. Il est alors isolé du reste du système et ne peut plus être exécuté. Cette étape permet au technicien ou à l'utilisateur d'analyser le fichier, de confirmer s'il s'agit bien d'un malware ou d'un simple faux positif, et de décider de sa suppression ou de sa restauration.

Limites d'un antivirus et bonnes pratiques

Même si les antivirus sont très performants, ils ne garantissent pas une sécurité totale. Les attaques sophistiquées, les erreurs humaines et l'absence de mises à jour peuvent compromettre la protection. L'utilisateur joue donc un rôle clé : éviter les téléchargements hasardeux, vérifier l'origine des pièces jointes, maintenir le système et les logiciels à jour, et utiliser un pare-feu. L'antivirus doit être vu comme un outil complémentaire dans une stratégie globale de cybersécurité.

Conclusion

L'antivirus est un élément essentiel de la protection des systèmes informatiques. Grâce à ses mécanismes de détection par signatures, heuristique et analyse comportementale, il permet d'identifier un large éventail de menaces et d'assurer une surveillance continue du système. Toutefois, son efficacité dépend fortement de la mise à jour régulière et de la vigilance de l'utilisateur. Pour un technicien en maintenance PC et réseaux, savoir expliquer et configurer un antivirus fait partie des compétences fondamentales pour garantir la sécurité d'un poste de travail ou d'un réseau.