BTS SIO

2019/2021

VEILLE TECHNOLOGIQUE

La veille technologique consiste à s'informer en continue sur les nouvelles techniques du secteur informatique. L'objectif est d'être toujours à jour sur les dernières avancées technologiques pour être le meilleur dans son domaine professionnel. Aujourd'hui, la veille technologique possède une place majeure dans le travail d'un informaticien.

La veille technologique sert à :

- Se tenir au courant des dernières mises à jour de produits (les nouveaux produits, innovations, nouvelles inventions)
- Découvrir des solutions plus avantageuses
- Anticiper sur la concurrence : on peut ainsi rester à la pointe du marché en acquérant toutes les nouvelles technologiques qui permettent de disposer d'un avantage concurrentiel.
- Se former sur un sujet précis (dans mon cas)

TOFILI Xavier

L’antivirus : principe et fonctionnement

Un antivirus est un programme dont le rôle est de détecter les virus présents sur votre ordinateur. Cette définition est succincte.

Dans l’esprit de nombreux utilisateurs, un antivirus détecte et supprime les virus tout simplement, mais pas seulement.

Lorsqu’il trouve un programme suspect, il a plusieurs vérifications ou décisions à prendre :

- Il doit d’abord s’assurer que c’est un vrai virus ;
- Il doit vérifier que ses agissements sont bien anormaux et dangereux à l’intégrité du Système.
- S’il s’avère que c’est bien un programme nuisible, il doit décider quelle est la meilleure action à envisager en fonction des dégâts causés.
- Si le code malveillant détecté est complexe, semble très dangereux et/ou inconnu et qu’il ne sait pas comment l’éradiquer, il le déplace dans une zone de quarantaine.

Dire qu’un logiciel antivirus sert qu’à analyser des fichiers est donc réducteur. Il surveille aussi en permanence, en tâche de fond, toutes les activités de l’ordinateur, en essayant de minimiser l’impact de cette surveillance sur les performances du système. Le but étant de limiter la gêne occasionnée pour l’utilisateur tout en gardant la possibilité de prendre des décisions importantes voir vitales en cas de besoin.

3 possibilités pour sauver l'ordinateur :

En cas d'anomalie, il avertit l'utilisateur par un message explicite. Cette méthode n'est jamais utilisée seule et vient en complément de l'une des deux premières. Cette protection est indispensable lorsque vous surfez sur internet. Lorsque l'antivirus a détecté un virus, il offre trois possibilités à l'utilisateur.

- Réparer le fichier : l'antivirus doit être capable de réparer un fichier atteint. Mais ce n'est pas toujours possible.
- Supprimer le fichier : si l'antivirus n'est pas capable de supprimer le fichier, vous pouvez le supprimer. Cette option est conseillée si le fichier n'est pas important, sinon il est placé en quarantaine.
- Mise en quarantaine du fichier dans un dossier sur le disque dur. Lorsque l'antivirus sera capable de réparer le fichier, vous pourrez extraire le fichier du dossier et le réparer (ne pas compter dessus si des données sensibles sont en quarantaine).

Types de détection d'un virus

La détection par la signature :

C'est la méthode la plus ancienne, chaque virus a une signature unique. Lorsqu'il rencontre un problème, l'antivirus analyse sa base de données pour savoir à qui il a à faire et prendre les mesures qui s'imposent.

Le problème de cette méthode est que les personnes qui créent les virus ont pensé à contourner ces systèmes, ils ont créé un virus polymorphe. C'est un virus qui dépose une nouvelle signature en se répliquant dans le système, ce qui peut poser un problème à l'antivirus et causer d'éventuelles baisses de performances. Donc l'antivirus doit être mis à jour régulièrement pour être informé des nouvelles menaces qui apparaissent chaque jour (toutes les 24h, voir 2h pour les payants).

La détection par le comportement :

Lorsqu'il y a une tentative de téléchargement ou d'envoi des données sans l'accord du propriétaire ou encore lorsqu'il lance une duplication importante de fichiers (certains virus paralysent le système en remplissant complètement le disque dur).

Alors si cela est possible, l'antivirus répare le fichier ou le programme qui en est à l'origine, sinon il le supprimera.

Suivant l'antivirus et les réglages paramétrés, il prendra seul une décision ou proposera plusieurs possibilités. En indiquant la plus adaptée.

Il a aussi une autre solution, la mise en quarantaine. Le/les fichiers sont placés dans un dossier isolé et sur le disque afin que le programme malveillant ne puisse agir. Au fur et à mesure des mises à jour de sa base virale, il pourra éventuellement le réparer/supprimer et même parfois décider quel fichier incriminé n'est pas dangereux, et le faire sortir de cette quarantaine.

La détection par le contrôle de l'intégrité :

Vérifier l'intégrité d'un fichier consiste à contrôler qu'il n'a pas été modifié ou altéré au cours du temps.

L'antivirus pour contrôler l'intégrité des fichiers, va stocker un fichier central recensant l'ensemble des fichiers présents sur le disque auquel il aura associé des informations qui peuvent changer lorsque le fichier est modifié :

- La taille
- La date et heure de dernière modification
- La somme de contrôle (CRC : code de redondance cyclique) éventuelle.

Lorsqu'une analyse est effectuée (ou à l'ouverture du fichier si l'antivirus réside en mémoire), l'antivirus calcule la somme de contrôle et vérifie que les autres paramètres n'ont pas été modifiés. Si une anomalie se présente, l'utilisateur est informé. Pour contrer en partie cette méthode, les virus ne modifient pas forcément la date de modification du fichier ou la rétablissent.

La détection par l'analyse heuristique :

Cette méthode de détection est une nouvelle méthode permettant de détecter des nouveaux virus ou de nouvelles variantes de virus déjà connues. Son principe est assez simple, l'antivirus va isoler le programme inconnu dans un environnement dit « virtuel » et va ensuite analyser son comportement et voir ce qu'il pourrait éventuellement se passer.

Le point faible est que ces tests provoquent parfois de fausses alertes, on appelle cela des faux positifs. C'est parce que les virus informatiques, tout comme les virus biologiques, changent constamment et évoluent. Comme l'analyse heuristique repose sur la comparaison du fichier suspect avec les autres virus déjà connus, il est fréquent qu'elle rate certains virus qui contiennent de nouveaux codes ou de nouvelles méthodes de fonctionnement.

C'est à ce jour la méthode la plus puissante et la plus récente. Toutes ses méthodes se complètent les unes des autres pour identifier, traiter et supprimer une menace.

La sécurité information en entreprise

Dans le cadre de la sécurité informatique du SI, on discerne 3 piliers : La prévention, la détection et la remédiation.

- La prévention est le fait de protéger son SI de tous les dommages possibles.
- La direction est la capacité de l'entreprise à détecter ses failles et ses vulnérabilités.
- La remédiation est la capacité de l'entreprise à corriger ces failles de sécurité.

<u>La prévention :</u>

On distingue deux sous-niveaux de prévention :

- Le niveau des utilisateurs : on forme les utilisateurs aux bonnes pratiques (téléchargements, mails suspects, comportements inhabituels du poste de travail). Cela permet de réduire nettement les intrusions de pirates dans le SI par le biais d'un virus, ransomware, trojan, etc…
- Les antivirus : on installe des antivirus sur toutes les machines connectées au réseau de l'entreprise, aux postes de travail, serveurs, équipements réseaux, etc.

L'objectif ici est d'avoir un second niveau de protection. Si un assaillant parvient à atteindre une machine du réseau, l'antivirus peut alors automatiquement supprimer les fichiers dangereux.

<u>La détection :</u>

Utiliser un antivirus et former les utilisateurs ne suffit pas pour les grandes entreprises. Il faut utiliser des outils qui permettent de détecter les failles et vulnérabilités du système d'information entier. Un serveur ou un logiciel non mis à jour peut tout aussi bien représenter une menace qu'un virus informatique.

Pour pallier ce problème, on utilise des outils appelés « scanner de vulnérabilités ». Ces outils fonctionnent à partir d'une base de connaissances qui est mise à jour continuellement avec les

dernières vulnérabilités et failles de sécurité publiées par les grands éditeurs. Ces outils vont aller se connecter aux équipements connectés sur le réseau d'entreprise et les tester pour chaque vulnérabilité qu'ils connaissent. A la fin des scans de sécurité, les logiciels produisent un rapport de sécurité. L'avantage de ces outils est aussi qu'ils permettent de détecter les équipements inconnus connectés sur le réseau, même si ceux-ci ne constituent pas une faille de sécurité.

Ces rapports de sécurité sont généralement des fichiers Excel. A chaque ligne on retrouve principalement : L'adresse IP de la machine, le nom de la machine, la référence de la vulnérabilité, l'impact et la menace que représente cette vulnérabilité. Enfin pour chaque vulnérabilité, on retrouve une solution de contournement où le lien mène vers un patch de sécurité qui permet de remédier la vulnérabilité.

La remédiation :

Une fois détecté, il faut s'assurer que toutes les failles de sécurité soient clôturées :

La plupart du temps, la remontée d'une vulnérabilité est causée par une mise à jour d'application manquante. Pour remédier à cela, il suffit de télécharger la dernière version du logiciel ou de télécharger le dernier patch de sécurité s'appelant des « KB ».

Pour une petite entreprise, la gestion de la vulnérabilité doit se faire manuellement par les techniciens du système d'information. En revanche, pour les grandes entreprises qui comptent parfois plusieurs centaines de milliers de machines à travers le monde, on utilise ce qu'on appelle des patchs manager. Ce qui consiste à industrialiser les processus de détection, d'analyse et de déploiement des mises à jour de sécurité logicielle.

Ces outils permettent de déployer à partir d'une seule interface, des patchs de sécurité que ce soit pour les serveurs, les postes de travail ou d'autres types d'équipements.

En conclusion :

Un antivirus est un logiciel utilitaire qui détecte les programmes malveillants pour le système et les détruit. Afin d'identifier une menace, il utilise différentes méthodes de détection :

- Détection par le comportement
- Détection par l'intégrité
- Détection par l'analyse heuristique

Pour contrer une menace, l'antivirus vous propose trois choix : réparer ; supprimer ; déplacer en zone de quarantaine.

En entreprise, les risques de sécurité sont gérés par 3 étapes : la prévention, la détection, la remédiation