HIPS : « Host-based Intrusion Prevention System »

Contrairement au simple IPS qui agit au niveau du réseau et sous réseau, l’HIPS agit directement au niveau du poste de travail de chaque utilisateur.

Il s’agit en fait d’une sorte de firewall croisé avec un anti-virus. En effet, son rôle est de contrôler les actions de l’utilisateur, lorsqu’il clique sur un lien, lorsqu’il essaye d’ouvrir un logiciel, …

Attention, le mot « firewall » est à nuancer. Un firewall n’est pas nécessairement un HIPS. En effet, le principe du firewall repose sur le blocage des ports TCP/IP. En revanche, un HIPS est capable de détecter tous types de menaces et, contrairement au firewall, il peut aussi bien le détecter avant qu’il n’arrive dans l’ordinateur, qu’au moment où il est déjà bien ancré dedans.

Dès lors que l’action est considérée comme étant suspecte, l’HIPS ouvre une fenêtre d’alerte en signalant un danger potentiel. Libre à l’utilisateur de poursuivre son action ou non.

La question se pose, pour un simple utilisateur, de savoir quel est le plus rentable entre l’HIPS et un simple Firewall. L’HIPS étant beaucoup plus complexe, le nombre d’alertes est largement supérieur à celui proposé par un Firewall, celui-ci étant prévu pour protéger l’ordinateur, sans pour autant faire couler l’utilisateur sous les alertes. De ce fait, l’HIPS est plutôt destiné à un utilisateur averti.

Comment ça marche ?

* Protection du système de fichiers
* Protection du registre (regedit)
* Contrôle du démarrage
* Filtrage réseau
* …

Avantages :

* Le logiciel ne requiert aucune mise à jour régulière, dans la mesure où il calcule des valeurs de danger en fonction du trafic, qui devient inhabituel. Il n’a pas besoin de connaitre les virus précisément, il lui suffit de détecter qu’un packet inhabituel tente d’accéder au PC.
* Outil de supervision qui permet de consulter les informations d’activité et d’état de l’HIPS.