

Pourquoi la sécurité informatique est-elle insuffisante face à la cybercriminalité ? **Interview**

Posté par : JPilo

Publié le : 23/4/2012 14:00:00

Voici un constat évident : il est plus facile d'attaquer que de se défendre. Partant de ce postulat, nous avons pour usage de sécuriser notre territoire informatique en nous armant d'un ensemble de contre-mesures (ou anti-virus) capables de parer une attaque (ou menace). Nous sommes donc contraints de subir l'attaque avant d'y faire face. Mais à l'heure actuelle, ces systèmes de défense sont-ils réellement au point ? Sommes-nous prêts d'être protégés à 100% ? **Mikaël Masson**, Channel Manager EMEA et co-fondateur de Cyberprotect, nous donne son point de vue sur la question...

Les anti-virus actuels sont-ils efficaces ?

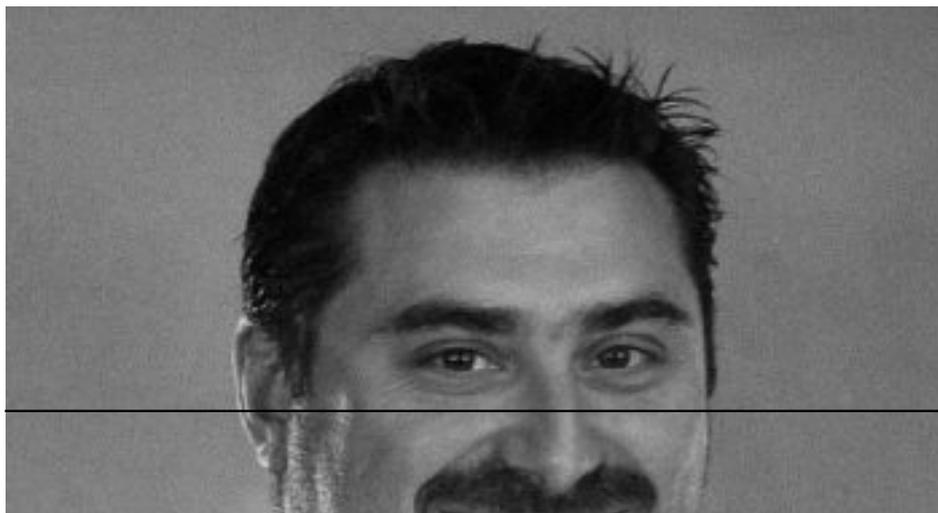
Lorsqu'un virus informatique est découvert, nous créons un vaccin, ou anti-virus, et nous propageons un antidote, ou signature. Si le vaccin est trouvé rapidement, la contamination peut être vite endiguée et le nombre de victimes réduit. Mais plus la fréquence et la virulence des nouvelles malveillances augmente (vers, virus, botnet...), plus il est difficile d'y faire face. Les professionnels de la sécurité se trouvent alors face à une obligation de trouver encore plus rapidement de nouvelles signatures. En parallèle, il leur faut un champ d'action plus large pour détecter, analyser et créer la contre-mesure efficace associée. C'est le phénomène auquel nous sommes confrontés aujourd'hui. Donc, pour répondre précisément à la question, les anti-virus ne peuvent être efficaces que si la découverte de la malveillance, la création de la signature et sa propagation sont très rapides. Ce qui est loin d'être le cas actuellement...

Le marché de la sécurité serait-il en perte de vitesse ?

Non, au contraire, le marché de la sécurité se porte bien. Et pour cause : la quasi-totalité des entreprises françaises (pour ne parler que de la Métropole) possède une sécurité, à savoir un pare-feu et/ou un anti-virus/anti-spam. En outre, l'acquisition d'une sécurité est plus faible d'année en année. Ainsi, une licence pare-feu (et uniquement pare-feu) pour une PME de moins de 100 personnes coûtait environ 5 000 euros HT début 2000. En 2012, un équipement type UTM avec tous les services associés revient à moins 2 500 euros HT environ.

Alors, ne doit-on pas augmenter le prix de la sécurité pour permettre aux éditeurs de la sécurité d'embaucher de nouveaux chercheurs ou virus doctors ?

Cette solution n'est évidemment pas la bonne car elle ne résoudreait le problème que sur le court terme (et impacterait encore davantage le budget des entreprises).



Pourquoi la sécurité informatique n'est-elle pas sûre ?

Parce que la sécurité est uniquement un moyen technique mis en œuvre pour protéger le système d'information contre les dangers connus du cyber-espace. Si l'on veut s'assurer que cette sécurité est efficace à tout moment, il faut la contrôler en permanence. Or, la sécurité ne peut se contrôler elle-même...

Que font les entreprises aujourd'hui pour régler ces problèmes de sécurité ?

Certaines entreprises mettent en place des PCA (Plan de Continuité d'Activité) et/ou des PRA (Plan de Reprise d'Activité) principalement tournés vers les serveurs d'applications/marchés pour résoudre le problème d'indisponibilité de ces ressources en cas de défaillance de la sécurité (attaque virale, intrusion...). En complément, certaines entreprises utilisent un Cloud privé ou public qui permet de déplacer les applications, partiellement ou totalement, dans des environnements dont la sécurité et le maintien ne sont plus à la charge de l'entreprise mais à l'opérateur de ce Cloud.

Et ces mesures sont-elles réellement efficaces ?

Non, ces mécanismes de disponibilité visent à protéger essentiellement les serveurs d'applications/marchés qui, dans la quasi majorité des cas, ne prennent aucunement en compte les ressources utilisateurs, à savoir le périphérique client. Or, si les serveurs de l'entreprise sont en permanence accessibles mais que les utilisateurs ne peuvent pas y accéder car leurs outils informatiques (PC, MAC, tablette, smartphone) ont été compromis par une défaillance de la sécurité, la perte d'exploitation pour l'entreprise peut être aussi forte, voire plus, que celle engendrée par la perte des applications marchés.

Pour combattre ce risque, d'autres entreprises multiplient les couches de sécurité : double pare-feu périmétrique, IPS, anti-virus de postes/serveurs, authentifications des périphériques ou des utilisateurs.... Sauf qu'ajouter les mécanismes de sécurité engendre un phénomène connu : le contournement de cette sécurité par son propre utilisateur. C'est ce qu'on appelle un contournement passif, c'est-à-dire qui est initié sans vouloir nuire volontairement à l'entreprise. Il peut revêtir différentes formes : le partage de mot de passe entre utilisateurs (un utilisateur ayant plus de privilèges qu'un autre), l'inscription des mots de passe sur un pense-bête, l'utilisation de son smartphone personnel pour accéder à une application/site interdit...

Alors, que peut-on faire pour augmenter la performance de la sécurité ?

Contrôler en permanence les menaces et les vulnérabilités pour limiter les chances d'être infecté par une malveillance et réduire fortement les risques de perdre le SI. Ainsi, l'entreprise sera mieux protégée face aux défaillances de sa propre sécurité et de celle de tiers.

Contrôler en permanence sa sécurité, c'est aussi s'assurer que le comportement des utilisateurs ne va pas à l'encontre des règles établies par l'entreprise (ce que l'on nomme PSSI ou Politique de Sécurité du Systèmes d'Information).

Contrôler en permanence sa sécurité, c'est également pouvoir transférer son risque résiduel vers une compagnie d'assurance. Cette dernière pourra alors intervenir financièrement pour aider l'entreprise à régler un dommage lié à une malveillance informatique et prendre en charge, si nécessaire, la perte d'exploitation liée à cet acte de malveillance. Ce transfert vers l'assureur est essentiel car il garantit financièrement au DSI la sécurité qu'il a mis en œuvre et permet au chef d'entreprise de conserver une réserve d'argent pour couvrir un sinistre informatique sans toucher à la trésorerie de l'entreprise.

Mais attention, contrôler en permanence sa sécurité est un travail continu qui nécessite d'avoir au moins une ressource dédiée 7 jours sur 7 et 24 heures sur 24 ! Les menaces et les vulnérabilités augmentent, évoluent chaque jour et ne s'arrêtent malheureusement pas le vendredi à 18h...

Ne peut-on pas se contenter d'une surveillance ponctuelle ?

Faire une évaluation de ces risques une à deux fois par an c'est bien, mais largement insuffisant. Quel DSI ne s'est pas retrouvé, suite à un audit ponctuel de sécurité (audit souvent de vulnérabilités mais très rarement de risques), à appliquer un nombre conséquent de corrections critiques lui imposant une mobilisation de l'ensemble de son équipe pour finalement s'entendre dire, lors de l'audit suivant, que les problèmes n'étaient toujours pas résolus ?

Connaître ses risques en temps réel permet non seulement d'apporter des recommandations applicables immédiatement, mais aussi de ne pas surcharger les équipes d'exploitations et surtout, de réduire considérablement toute menace.

Cependant, contrôler ces risques impose des ressources humaines supplémentaires, chose impensable pour 98% des sociétés françaises qui sont des TPE/PME n'ayant généralement pas les moyens de gérer nativement leur sécurité (heureusement que la plupart d'entre elles peuvent faire confiance à leur prestataire informatique pour les accompagner dans les problèmes de sécurité).

C'est pour pallier ces problèmes que des solutions de service comme Cyberprotect existent. Elles permettent d'externaliser la fonction de gestion des risques (et de transfert automatique vers l'assureur dans le cas de Cyberprotect) et d'éviter ainsi la constitution d'une équipe dédiée en interne sans surcharger les équipes de production, qui peuvent alors continuer leur propre travail.

En conclusion pourriez-vous affirmer que la sécurité informatique est insuffisante face à la cybercriminalité ?

Oui, la sécurité informatique est insuffisante pour faire face à l'expansion de la cybercriminalité. Mais ce n'est pas pour autant qu'elle n'est pas nécessaire, bien au contraire.

Pour qu'elle soit réellement efficace, il faut que les entreprises la contrôlent en permanence et surtout, qu'elles puissent gérer leurs risques informatiques et que le poste alloué à la sécurité informatique et donc au bon fonctionnement du SI soit enfin couvert par une garantie financière. La sécurité deviendra alors efficace et le système d'information enfin sûr.