Tester les maliciels et la sécurité dans un nuage de... pluie acide

EDDY WILLEMS
Eddy Willems est malware researcher et a plus de 20 années d'expérience à son actif. Il est security evangelist chez le spécialiste de la sécurité G-Data, mais aussi directeur de l'information et de la presse chez EICAR (European Institute for Computer Anti-Virus Research).

Je me cognai la tête à mon nouveau bureau en rampant par dessous. Résultat: une vilaine bosse me défigura les jours suivants, mais - eurêka! - les quatre réseaux internes de mon habitation étaient entièrement restructurés et dotés des plus récents gadgets de sécurité. C'est là un élément de ma politique de protection, et celle-ci est quasiment ce qu'il y a de plus important pour une entreprise. Manifestement, tel n'est cependant pas encore le cas, nous apprend l'EICAR (European Institute for Computer Anti-Virus Research), à moins de se tourner vers les plus grandes sociétés comme les banques et les compagnies d'assurance. Mais nous sommes bien en Belgique avec ses plus de 90% de petites et moyennes entreprises. Devinez donc combien d'entre elles appliquent une politique de sécurité? Selon les statistiques de l'EICAR, elles sont un peu plus de 10%.

Une politique de sécurité, c'est en effet bien plus qu'installer un progiciel anti-virus et un pare-feu. Du logiciel et du matériel ne sont du reste pas de trop car aujourd'hui, c'est une montagne de 50 millions de maliciels qu'il faut affronter. Un problème vertigineux engendré par le cyber-crime, et cela ne risque pas de s'arranger dans les années à venir.

L'internet permet à tout un chacun de faire des choses défendues. Pour beaucoup, la frontière entre le bien et le mal devient en effet très, très ténue. Quand allez-vous passer la ligne? Si vous faites voir sur Youtube la facilité avec laquelle vous pouvez abuser d'un progiciel de sécurité? Ou si vous avez vous-même acquis une partie d'un botnet pour expédier des mails vers des clients potentiels? Ces deux possibilités sont discutables, mais seules quelques exceptions partagent encore cette opinion, semble-t-il... Actuellement, des dizaines de botnets regroupant des millions de PC sous la coupe de la pègre sont à l'origine de la plupart des difficultés. Et c'est sans parler des maliciels que nombre de centres de 'command-and-control' ont fait ou font tourner chez les ISP d'un pays voisin: les Pays-Bas. Estompage de la norme, laxisme ou liberté, où dont le classer?

L'on me demande souvent comment des infections sont encore possibles, maintenant que tout le monde dispose d'une solide protection. L'exemple suivant suffit à répondre. Lors de trois des cinq événements auxquels j'ai assisté l'an dernier, des sub-sticks contaminés circulaient. A tous points de vue, la clé USB est donc réellement bien le substitut de la disquette et même en prenant des mesures valables, cette clé peut générer pas mal de problèmes. Ici aussi, il est donc important d'appliquer une politique stricte. Canaliser correctement le comportement humain est dès lors un facteur essentiel d'une politique de qualité. Les problèmes de sécurité des sites web de socialisation sont aujourd'hui bien connus et pourtant, ils ne sont pas encore résolus. Acceptez-vous toutes les applications sur votre Facebook? Moi assurément pas! Soyez également prudent avec tous les plugins possibles pour Firefox, avec les anciennes versions de Flash ou avec du software Adobe Acrobat Reader non actualisé.

Nous voulons aussi tous accéder trop vite à l'information. Twitter en est un très bel exemple. La principale menace émane des sites web infectés, même légitimes, par du maliciel tel Gumblar, un fléau qui se propage toujours plus. De piètres mots de passe et une déficiente protection des réseaux en sont coresponsables. Des techniques comme la virtualisation, la protection dans le nuage et le 'whitelisting' s'améliorent certes toujours. Le danger, c'est que nos nuages soient sans cesse davantage agressés jusqu'à ce qu'ils se dissolvent en une pluie 'acide'.

Les problèmes de sécurité des sites web de socialisation sont aujourd'hui bien connus et pourtant, ils ne sont pas encore résolus.

Des testeurs indépendants de tout ce qui précède gagneront dès lors aussi en importance à l'avenir. Beaucoup d'entreprises accorderont en effet un vif intérêt à la réalisation de tests corrects, ainsi qu'à des conseils à propos de ces techniques, logiciels et matériel. C'est précisément l'une des missions de l'AMTSO, l'Anti-Malware Testing Organisation (cf. www.amtso.org). J'estime qu'il y a aujourd'hui trop de tests qui ne suffisent absolument pas à offrir l'image correcte d'une sécurité suffisante. L'ATMSO entend être le fil rouge pour des tests valables permettant une bonne comparaison. Les tests des logiciels ou du matériel ne sont en effet pas les mêmes que ceux d'un progiciel ou d'un applicatif de sécurité. Les journalistes-testeurs doivent passer en revue les directives de l'AMTSO car ils aideront ainsi les entreprises et les futurs utilisateurs à rendre le monde quelque peu plus sûr. Je conseille à tout un chacun de suivre cela de très près. Autre point important: les conseils des consultants en sécurité, même si vous n'êtes pas vraiment certain qu'ils soient tout à fait objectifs. C'est en tout cas recommandé si vous ne voulez pas que votre réseau ou votre entreprise soit défiguré par une vilaine bosse... #