Secure Computing : « les hackers adorent le SaaS »

Présent depuis plus de 20 ans sur le marché de la sécurité, et plus précisément dans les domaines de les appliances de sécurité et de la sécurisation des passerelles d'entreprises, le vice-président du groupe, Paul A.Henry, -qui est aussi un passionné et un expert reconnu dans l'univers du hacking- expose à *silicon.fr* sa vision de la sécurité et répond à nos questions…

-Pouvez-vous nous dire quelques mots sur l'histoire et l'actualité de Secure Computing?

« Tout commence il y a une vingtaine d'années, avec la signature d'un contrat avec le gouvernement américain et Honeywell pour mettre au point un système d'exploitation hautement sécurisé, et un pare-feu impénétrable. Une fois ce contrat mené à terme, nous avons réalisé le potentiel commercial d'une telle application et Honeywell a créé une nouvelle entité : Secure Computing; dont le cœur de métier allait être la sécurité informatique. Nous sommes à l'origine de la charte Rainbow Orange Book qui pendant très longtemps a été une référence dans la sécurisation du système d'information. »

« Depuis tout ce temps, Secure Computing a pris une autre dimension et a multiplié les acquisitions. Par exemple, nous avons racheté Cyberguard qui nous a permis de développer notre appliance de Gateway Security : WebWasher. Beaucoup de nos technologies actuelles sont la conséquence directe de cette acquisition. Dans les faits, nous sommes présents dans de nombreux pays, notamment en Europe, le bureau de développement de Webwasher se trouve en Allemagne, et nous avons également des bureaux en Grande-Bretagne. Nous disposons de locaux en France, plutôt spécialisés dans la lutte anti-malware. En réalité, **nous estimons que les développeurs français sont très bons dans le domaine de l'Open Source**. Qui plus est, ils ont une très bonne connaissance de la sécurité des réseaux et donc une importante capacité d'expertise. Nous avons envie de travailler davantage avec des ingénieurs français. »

-A propos des nouvelles menaces quelle a été la tendance en 2007, et que voyez-vous venir pour 2008?

« D'abord, nos équipes ont remarqué une nouvelle tendance. Les malwares dans les emails utilisent de moins en moins la technique des pièces jointes. D'ailleurs, cela fait longtemps qu'il n'y a pas eu de diffusion massive d'un nouveau virus par ce biais. Désormais, les hackers placent les malwares directement dans le corps du mail, dans un lien. Le code malveillant est hébergé sur une page Web. Nous appelons ces menaces les « Web Born Malware ». Ce mouvement a commencé en 2007, et nous pensons qu'il va s'accélérer en 2008. »

« Personnellement, j'estime qu'il s'agit de la tendance la plus dangereuse d'autant qu'il y a énormément d'entreprises qui ne sont absolument pas protégées contre ces menaces. Si vous parlez de menace de sécurité à un CEO, il va immédiatement penser à la mise en place d'un pare-feu au niveau du serveur, les responsables des entreprises ne réalisent pas qu'il faut également agir au niveau individuel. Il n'y a pas si longtemps, le chef de la sécurité avait une formation très technique, de nos jours ils ont tous un MBA en poche, et ce changement est un problème, car les

décisions qui sont prises reposent sur le marketing. **Finalement, c'est davantage la popularité d'une solution que sa véritable efficacité qui prime.** C'est un problème très important qui est même confirmé par les statistiques. D'après le CSO Crime report 2007 réalisé par le FBI : 97% des entreprises ont un pare-feu et pourtant 56% d'entres elles ont été la cible d'au moins une intrusion, et la situation est similaire en Europe. »

–**Utiliser un pare-feu n'est donc pas suffisant?**

« Tous les spécialistes de la sécurité savent que les menaces les plus importantes passent par les vulnérabilités dans les applications, dans le jargon c'est ce que l'on appelle le layer 7 (le niveau 7 de sécurité). Pourtant, la grande majorité des entreprises ne déploient que des pare-feu de niveau 4, ce qui est incroyable quand on connaît les risques. Comment pouvez-vous vous protéger lorsque les menaces passent au dessus de votre tête? Il faut que les entreprises utilisent des firewalls qui protègent les applications. »

« Le niveau 4 a rencontré un grand succès auprès des entreprises parce qu'ils sont très simples à installer, il ne requiert pas de connaissances techniques ce sont des solutions « plug and play ». Avant d'installer un pare-feu de niveau 7, il faut d'abord comprendre les besoins spécifiques d'une entreprise en fonction des données qu'elle stocke et des applications qu'elle utilise, mais aussi des règles de sécurité déjà en place. Avec un pare-feu qui surveille les applications, l'on réduit considérablement la probabilité d'une intrusion et l'on peut exercer un contrôle plus précis sur l'usage qui est fait des données de l'entreprise, l'on construit des zones de confiance selon l'activité de chaque département. On peut utiliser ces firewalls sur un Intranet ou sur Internet. »

-Quel avenir pour la protection des données? Que pensez-vous de l'externalisation de la sécurité?

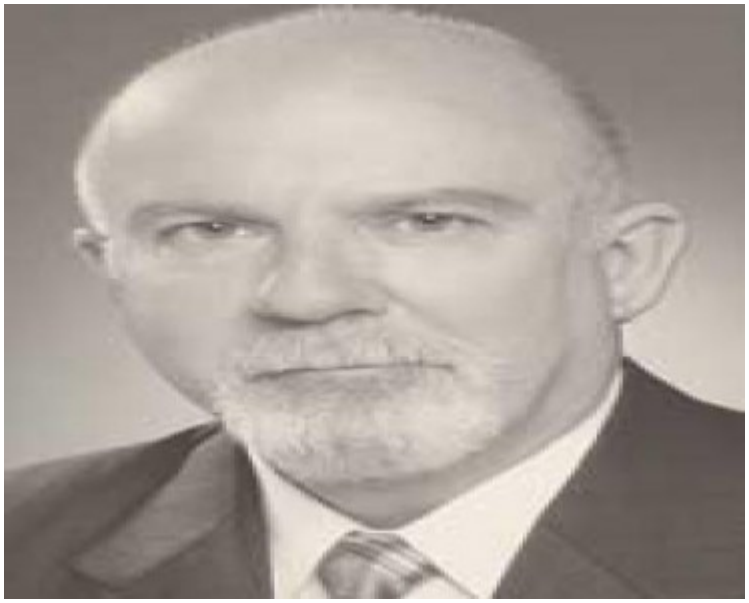
« Les solutions de DLP (Data Leak Protection) sont très à la mode aux États-Unis. Notamment en raison de la régulation. Mais c'est surtout la multiplication des litiges qui inquiète les entreprises. Elles sont de plus en plus conscientes des risques parce qu'ils ont un impact financier de plus en plus important, dans certains cas elles risquent même la banqueroute. »

« Avec le Web 2.0, et les risques associés, les malwares sont encore plus puissantes et le risque est énorme.**L'externalisation de la sécurité n'est pas une bonne approche**, car il faut pouvoir déterminer les responsabilités. Et les prestataires de ce type de services s'engagent rarement. C'est une question de confiance. Si je me mets dans la peau d'un « black Hat », alors là oui je trouve cette idée formidable, car je n'ai plus à cibler de petites entreprises, désormais je peux en cibler vingt, qui sont toutes hébergées chez un même prestataire. Les risques de fuite d'information sont donc encore plus grands avec l'externalisation de la sécurité. Aux USA, les entreprises qui proposent du SaaS (Software as a service) sont surtout intéressées par les profits ce sont rarement des spécialistes de la sécurité, c'est pour cette raison que les hackers adorent le SaaS. »

-Une question plus personnelle? Est-ce que vous utilisez votre service de banque en ligne

« Oui, mais le président de ma banque m'a rédigé un courrier dans lequel il s'engage a me rembourser si jamais je suis victime d'une fraude. Je vais être sincère, sans ce papier je n'utiliserais pas les services en ligne des banques. À mon avis, dans un avenir proche les banques ne rembourseront plus les victimes, car le phishing augmente très rapidement et elles ne vont plus

pouvoir supporter le coût du piratage. »



(Paul A.Henry vp de Secure Computing (Crédits : GCN))