Microsoft TechDays : Bernard Ourghanlian, « C'est quand même incroyable d'imaginer que les particuliers sont mieux protégés que les entreprises ! »

Silicon.fr : ***Qu'en est-il aujourd'hui de la sécurité dans le cloud ?***

Avec l'avènement du *cloud computing*, de nouveaux sujets sont à traiter. C'est la seconde dimension de la problématique sécuritaire associée au système d'information aujourd'hui *(lire notre précédent article, NDLR)*. La plupart de nos clients grandes entreprises ont une démarche pour le *cloud* qui est souvent subjective. La seule démarche, à mon sens, pour aller ou non vers le *cloud*, c'est de regarder les risques supplémentaires, comment les atténuer et s'assurer que le risque résiduel soit suffisamment limité pour que l'on accepte d'aller dans cette direction. C'est un sujet dont on continuera de parler encore longtemps. Nous prolongeons l'initiative de l'informatique de confiance et nos travaux de « *secure development lifecycle* » (SDL) pour nos services dans le *cloud* afin de nous assurer que nous ne mettons pas en fonction des services qui ne sont pas suffisamment sécurisés. Notre initiative n'est pas remise en cause, mais le monde dans lequel elle opère est très différent, avec une perspective nouvelle, le *cloud*, qui nécessite d'étendre des concepts non plus aux logiciels que nos clients opèrent, mais à des logiciels instanciés sous forme de services.

Silicon.fr : ***Le positionnement de Microsoft vous place au cœur des problématiques de sécurité alors que la plupart de ces dernières ne vous sont pas imputables. Comment gérez-vous cela ?***

Nous avons l'habitude… Nos logiciels affichent un nombre de vulnérabilités qui aujourd'hui est infiniment moindre qu'il y a dix ans. Nos méthodologies, comme SDL, ont été adoptées par d'autres, comme Cisco ou Adobe, ce qui est la preuve que nous avons fait des progrès importants et que nous montrons le chemin. Il ne faut pas résumer la sécurité à la technologie. Elle repose sur un trépied, la technologie, des processus et des hommes, et ce n'est pas près de changer. Lorsque l'on observe les APT (*Advance Persistent Threats*), souvent les personnes visées par ces attaques sont haut placées dans la hiérarchie des organisations, et les *mails* qui servent de vecteur d'attaque sont très bien faits. Honnêtement pour en avoir lu quelques-uns, il est difficile de ne pas se faire avoir ! Certes il faut continuer de faire de la pédagogie, mais ce n'est plus suffisant. Il faut comprendre que la sécurité n'est pas une accumulation de technologies, ce qui n'aboutit qu'à complexifier le SI et le rend plus difficile à protéger. Sécurité et complexité ne vont pas ensemble.

Silicon.fr : ***La responsabilité des RSSI et des DSI est-elle en cause ?***

Il y a certainement un gros travail de pédagogie à faire auprès des RSSI, des responsables sécurité et des DSI, qui sont en retrait. Ils se rendent compte que le monde qui les entoure a beaucoup changé, mais ils n'en tirent pas les conséquences sur l'architecture du SI. Le rôle du périmètre n'a plus vraiment de sens. Aujourd'hui, 90 % à 95 % des entreprises se replient derrière leurs pare-

feux. Il faut extirper cette idée de la tête des gens. Tant que ce ne sera pas fait, et qu'ils continueront de raisonner avec des idées dépassées, ça ne marchera pas ! Les menaces ont changé, les façons de s'en prémunir doivent suivre le même chemin. On arrive au paradoxe, à la lecture de nos études, que les particuliers sont bien souvent mieux protégés que les entreprises sur beaucoup de scénarios. Pourquoi ? Ils ont mis à jour leur système, mis en route Microsoft Update, téléchargé les mises à jour de manière automatique, sans se poser de question, et dans l'ensemble ça les protège bien. C'est quand même incroyable d'imaginer que les particuliers sont mieux protégés que les entreprises !

Silicon.fr : ***Dans ces conditions, la solution ne serait-elle pas de prendre du tout Microsoft ?***

Effectivement, un SI entièrement Microsoft assure une large homogénéité, il est plus simple et donc plus facile à gérer et à sécuriser. En revanche, mettre tous ses œufs dans le même panier c'est prendre un risque. La solution est peut-être dans l'adoption d'un juste milieu, et ce n'est pas la question de prendre ou non un système tout Microsoft, mais plutôt d'adopter des technologies standards. C'est le cas de la généralisation d'IPsec (*Internet Protocol Security*) dans les entreprises, par exemple, avec des règles d'isolation de domaines, dont certains que l'on va particulièrement protéger. Cela ferait franchir un saut quantique à la sécurité des SI. Et cela ne nécessiterait pas la mise en oeuvre de produits Microsoft, mais d'outils standardisés par l'IETF et présents dans IPv6. C'est plus une question de compréhension de ce que doit être l'architecture du SI et de progrès à appliquer pour changer la donne, que de se dire *« il faut du Microsoft partout ! »*.

Silicon.fr : ***Microsoft n'a pas pris position dans l'affaire Megaupload…***

C'est un sujet quelque peu compliqué. Nous avons pris position contre les propositions de l'administration américaine. Concernant Megaupload, nous avons des réflexions qui sont contradictoires. Microsoft, en tant que société éditrice de logiciels, considère qu'il est normal de respecter la propriété intellectuelle et d'éradiquer des phénomènes de piratage industriel. Rappelons qu'en France il y a 39 % de piratage établi. Certes on peut imaginer qu'une partie du piratage soit « normale », mais quand en Allemagne ou Angleterre il y a 25 %, cela représente beaucoup d'argent. Sur la question de garantir la liberté d'expression sur Internet, nous devons rester vigilants, nous ne pouvons interdire l'expression d'opinions concurrentes, la liberté de la presse, et plus généralement la liberté d'expression. C'est complexe, car à l'échelle de l'Internet il n'y a pas vraie régulation, ni de puissance étatique comme on peut l'imaginer dans un système géographique avec des frontières.

De notre côté, nous sommes partagés entre la nécessaire propriété intellectuelle et son respect, et le fait de pouvoir garantir la liberté d'expression en toute circonstance. Cela rejoint des sujets importants, comme la garantie de l'anonymat lorsque c'est nécessaire, tout en considérant que parfois il n'est pas possible. Par exemple, heureusement que je ne suis pas anonyme lorsque je me connecte à ma banque, sinon n'importe qui pourrait aller sur mon compte. Nous l'avons vue au Moyen-Orient, la garantie de l'anonymat est également une nécessité pour les opposants. C'est compliqué.


a-t-il besoin de nous ?
RSLN