Photo : Annie Tremblay

Mario Audet est éditeur et copropriétaire du magazine SÉCUS. Il compte dix-sept années d'expérience en technologies dont dix en sécurité de l'information. Son intérêt pour la veille en sécurité l'a amené à développer l'agrégateur automatisé de nouvelles de sécurité informatique SecurNews.com.

Gestion de la faille de RSA au Québec

PAR MARIO AUDET, éditeur et copropriétaire de *SÉCUS*

En mars dernier, RSA[1] a reconnu avoir subi une cyberattaque. L'intégrité de ses solutions technologiques de sécurité est-elle menacée ? D'un côté, plusieurs articles en ligne sont alarmants. De l'autre, les responsables de RSA se font rassurants. La crainte des utilisateurs est-elle légitime ? L'avenir le dira.

Un *jeton d'authentification* est un « dispositif électronique que l'on transporte avec soi et qui sert à produire des codes ou des mots de passe à partir desquels l'appareil qui les reçoit peut reconnaître l'identité de la personne qui désire obtenir l'accès à un réseau, à un système ou à un ordinateur ». (OQLF)

À ce jour, dans le monde, RSA affirme avoir vendu 250 millions de jetons d'authentification SecurID en format logiciel et 40 millions de SecurID en format matériel. SecurID est un système d'authentification à deux facteurs. Les organisations l'utilisent pour fournir une protection à leurs données sensibles et à leurs réseaux plus efficace qu'un simple mot de passe.

RSA EXPLIQUE LA FAILLE

Les responsables de RSA ont analysé rigoureusement la cyberattaque dont ils ont été victimes. D'abord, les pirates ont utilisé l'hameçonnage par courriel en visant différents employés de l'organisation. Ces derniers, en cliquant sur des liens malveillants ont permis aux attaquants de prendre le contrôle à distance des machines. Les postes de personnes plus « stratégiques » ont donc pu être compromis. Les cyberpirates ont alors atteint des données critiques qu'ils ont cryptées et transmises à un serveur sur le Web.

RSA INFORME ET RASSURE

Les responsables de RAS ont rencontré les gens de la presse surtout spécialisés en technologie pour répondre à leurs questions au sujet de la faille. Au Québec, *SÉCUS* a appris de certains clients de la firme américaine qu'elle les a joints par courriel, par téléphone ou qu'elle les a rencontrés afin de leur expliquer l'attaque et de les rassurer. Confiante, RSA a affirmé que l'information dérobée ne permet pas aux attaquants de compromettre les jetons d'authentification de leurs clients. Dans les jours suivant l'incident, Art Coviello, le président de RSA, a

Suite en page

Suite de la page 4

également répondu à plusieurs questions qui ont entraîné la rédaction de certains articles informatifs[2,3].

Cette gestion de crise n'a pas été de tout repos. Cependant, pour le moment, elle semble satisfaisante.

LE MALHEUR DE RSA FERA-T-IL LE BONHEUR DES AUTRES ?

Dans un tel contexte, il est normal que des concurrents de RSA veuillent profiter de l'occasion pour gruger les parts importantes de marché de l'organisation dans le domaine des solutions d'authentification à mot de passe unique. D'ailleurs, CA Technologies et SafeNet ont lancé des programmes d'échange de jetons en mettant à profit leurs solutions. Avant d'envisager leurs possibilités, vous pouvez lire le billet de Mark Diodatti de Gartner intitulé *Perspectives on OTP Authentication and Migration*[4].

L'AVENIR LE DIRA

Apparemment, RSA a bien réussi la gestion de la faille. Cependant, seuls les prochains mois révéleront ce que fera le marché quant à cet incident. Dans ce secteur de sécurité en expansion, comment les clients réagiront-ils envers RSA et les autres fournisseurs de solutions similaires ? Souvent, les gens oublient et pardonnent rapidement. Cette fois, est-ce que ce sera le cas ? ■

1. La firme américaine RSA est la division de la sécurité d'EMC[2] (voir article *EMC/RSA piratée, la solution SecurID compromise* au www.silicon.fr/emcrsa-piratee-la-solution-securid-compromise-47810.html).
2. The RSA Hack FAQ (http://www.cio.com/article/677561/The_RSA_Hack_FAQ?source=rss_security&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+cio%2Ffeed%2Fdrilldowntopic%2F3089+%28CIO.com+-+Security%29).
3. What the RSA breach means for you (FAQ) (http://news.cnet.com/8301-27080_3-20044775-245.html?part=rss&tag=feed&subj=News-Security).
4. CA Capitalizes on RSA SecurID Breach with a Token Trade-in Program (http://www.eweek.com/c/a/Security/CA-Capitalizes-on-RSA-SecurID-Breach-with-a-Token-Tradein-Program-391611/?kc=rss&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+RSS%2Feweeksecurity+%28eWEEK+Security%29).