Jean-Noël de Galzain (Wallix) : « PRISM sert de révélateur aux problèmes de sécurité des comptes à privilèges »

Jean-Noël de Galzain, PDG de Wallix, l'éditeur français de WAB, une solution de PUM (*Privileged User Management*), revient sur les conséquences de l'affaire PRISM sur les choix des donneurs d'ordre, en particulier en matière de gestion des comptes dits à privilèges (administrateurs notamment). Rappelons que Wallix édite la solution WAB (*Wallix AdminBastion*), qui permet le contrôle des utilisateurs à privilèges pour la sécurisation des accès informatiques et la traçabilité.

Silicon.fr : Où en est le marché de la gestion des comptes à privilèges ?

Jean-Noël de Galzain : La sécurisation des comptes à privilèges devient de plus en plus prioritaire. Dès sa création, le suivi de l'origine du comptes est mal, voire pas maitrisé, et ne prend pas en compte l'évolution de la société. Le RSSI est contraint de se retourner vers les directions de la production pour traiter la menace ou l'erreur interne. Pourtant l'entreprise doit être en mesure de contrôler le risque, le visualiser, le rejouer pour savoir ce qui s'est passé et détecter son origine, afin de trouver la meilleure parade. Car les incidents imputables à des comptes à privilèges ont un coût élevé, auquel s'additionne le temps pour les reconstituer.

L'actualité récente ne joue-t-elle pas en votre faveur ?

En effet, nous assistons à une prise de conscience, sous l'effet conjugué des règlementations et des grands incidents médiatiques. Avec la révélation de PRISM, il est difficile de passer à coté ! Nos entreprises sont désormais confrontées à une problématique de choix dans le cloud computing et les solutions informatiques. Ces infrastructures entrent-elles dans le périmètre de PRISM et sont-elles soumises au Patriot Act ? Ai-je le contrôle de mes données ou ne suis-je pas le seul à l'avoir ? Les organisations doivent se poser des questions et faire des choix en conséquence. Le cloud et la mobilité imposent de contrôler et de sécuriser l'accès à l'information.

Sur le volet réglementation, on ne confie plus des données à des tiers dans les environnements critiques, comme la santé, la finance, le secteur public, les telco ou les hébergeurs. Le cadre législatif évolue vers la responsabilité de l'hébergeur, le contrôle des accès aux données et la capacité de remonter à la source en cas d'accident. La responsabilité de tout hébergeur de données est non pas de conserver les logs, mais de disposer de la capacité de séparer les rôles, avec d'un côté l'accès à l'information et de l'autre la gestion des systèmes qui stockent ladite information. S'y ajoutent des règles de contrôle de l'accès et la capacité à retrouver l'origine d'un accident. L'évolution porte vers une plus grande responsabilisation des hébergeurs informatiques, données et système. Et c'est parfaitement normal, car les données appartiennent à chacun d'entre nous. Les hébergeurs doivent protéger les données dès lors qu'ils disposent d'une délégation pour les gérer.

Les phénomènes du cloud et des 'aaS' (as a Service) ne risquent-ils pas de complexifier votre mission ?

C’est un challenge ! Il y a une complexité à gérer des environnements de connexions entrantes et sortantes, d’accès à différentes applications, de gestion d’un grand nombre d’utilisateurs, de contrôle de ressources externes, internes, et maintenant virtuelles. Au niveau du réseau et des protocoles IP, nous avons la capacité de nous adapter assez aisément aux technologies en place, en particulier virtuelles. La version 3.2 de WAB renforce la partie outils, les adapte sur des environnements virtuels avec le même confort et la même transparence. Concernant le volume, avec un plus grand nombre d’accès potentiels, nous travaillons en permanence en R&D sur nos mécanismes de répartition de la charge et d’adaptation aux environnements SaaS.

Notre challenge consiste à permettre à nos clients et partenaires d’intégrer notre produit dans leurs plateformes pour le servir en modèle SaaS. Pour cela, nous adaptons nos technologies avec des outils complémentaires. L’objectif : vendre la sécurité embarquée dans la valeur ajoutée d’une application, afin que les clients achètent la valeur ajoutée en même temps que le réseau de confiance. La fonction sécurité doit donc être intégrée dans les nouvelles plateformes de services web.

Les donneurs d’ordre doivent se montrer exigeants. Et s’assurer de disposer des briques de sécurité fondamentales pour sécuriser les accès au réseau, la bureautique, ou les accès aux données sensibles et externes tout en garantissant la traçabilité de l’information et la résilience.

Voir aussi

Silicon.fr étend son site dédié à l’emploi IT
Silicon.fr en direct sur les smartphones et tablettes