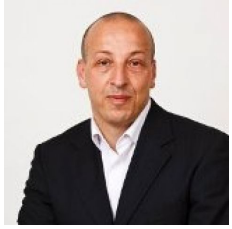
Écrit par Jean-Christophe Perney
Lundi, 20 Avril 2015 20:27



Voici 5 tendances qui auront un impact majeur sur les entreprises au sein de l'économie des applications. Dans ce contexte les professionnels de la sécurité seront confrontés à une double-équation : faire face aux cyber-risques dont l'actualité s'est déjà largement fait l'écho en 2014 et 2015 et répondre aux enjeux de l'économie des applications, en facilitant le déploiement de services innovants (Cloud, Mobile, Social, Big Data) via des canaux multiples (laptop, smartphone, tablette, kiosques, centres d'appels, ...) :

Nous savons que la résolution de cette double équation réside à la fois dans la gestion de l'identité numérique, nouveau périmètre des organisations pour authentifier les utilisateurs ; et la gestion des accès pour adapter et personnaliser les services déployés aux utilisateurs. C'est tout l'enjeu auquel ces professionnels de la sécurité seront confrontés en 2015.

5 tendances clés dans le domaine de la cybersécurité pour 2015, Par Mostafa Amokhtari, Directeur Technique de CA Technologies France :

Prédictions de CA Technologies pour la gestion des identités et des accès en 2015 :

1. Une authentification universelle à portée de main :

l'authentification multi-facteurs, les cartes à puce, la signature électronique, la biométrie et les nouveaux modes de paiement électronique vont stimuler la demande de nouvelles solutions d'authentification plus simples et adaptées au contexte de l'utilisateur. Les entreprises chercheront à implémenter un système d'authentification sans mot de passe et sans contact, où les terminaux mobiles (smartphone, tablette, objets connectés, etc.) seront utilisés comme moyen d'authentification universelle.

2. Un identifiant numérique unique :

l'économie des applications et l'utilisation croissante d'applications mobiles nécessitent un mode d'accès centralisé aux identités et aux droits d'accès. Les entreprises devront établir un identifiant numérique unique qui sera utilisé pour authentifier les utilisateurs, simplifier le développement, le déploiement et l'adoption d'applications tout en favorisant l'innovation. Cet identifiant unique couvrira toutes les applications, via tous les canaux, et sera facilement accessible via des API de gestion des identités.

3. De la gestion des identités vers la sécurité d'accès aux identités :

un changement d'orientation va se produire sur le marché de la gestion des identités, en raison

des cyber- menaces qui ont défrayé la chronique en 2014. L'accent ne sera plus mis sur l'administration de base des identités, mais sur leur sécurité. La majorité des piratages perpétrés en 2014 était liée à l'usurpation d'identités d'utilisateurs internes exposant les entreprises au vol de données et à l'utilisation malveillante d'applications. La protection des entreprises contre l'usurpation d'identité exigera de nouveaux systèmes de protection à la fois intelligents, contextuels et vérifiables.

4. La mobilité et l'Internet des objets entraîneront l'émergence d' « architectures orientées API » :

la croissance exponentielle des applications mobiles et de l'Internet des objets entraîneront une migration vers des architectures orientées API plus légères, afin de faciliter les connexions au sein des écosystèmes
numériques. Ces architectures seront mieux à même de prendre en charge le large éventail d'utilisateurs ayant besoin d'accéder à des applications et des données sur site ou dans le Cloud et via divers types de terminaux. C'est en fait l'architecture orientée API qui apportera l'agilité et la flexibilité nécessaires pour réussir dans l'économie des applications.

5. La direction aux commandes de la stratégie de sécurité interne :

La direction sera de plus en plus impactée par les actions de piratage portant atteinte à l'image de marque de l'entreprise. En conséquence, elle s'impliquera davantage dans la stratégie de sécurité de l'entreprise et la gouvernance de la sécurité. La sécurité ne sera plus un « problème informatique », mais un « problème stratégique ». Les inquiétudes relatives aux attaques de type DoB (Denial of Business) se traduiront pas une surveillance accrue des instances de direction.