Communiqués de presse

IBM sécurise l’usage au travail des applications cloud externes

Un tiers des employés des entreprises du classement Fortune 1000 partage les données sensibles de leur société via des applications cloud externes à l’entreprise

IBM Cloud Security Enforcer aide les entreprises à voir, gérer et sécuriser l’utilisation de ces applications

Paris - 22 sept. 2015: IBM annonce aujourd'hui une nouvelle technologie de sécurité cloud qui protège l'utilisation professionnelle croissante d’applications cloud externes à l’entreprise. Cloud Security Enforcer est la première technologie combinant gestion des identités via le cloud (Identity-as-a-Service) et possibilité pour les entreprises d’avoir une visibilité sur toutes les applications cloud tierces utilisées par leurs employés, y compris celles qui proviennent de leurs appareils mobiles. Cela permet aux entreprises d’offrir à leurs employés un moyen sécurisé d’accéder à ces applications et d’utiliser celles qu’ils souhaitent.

Cloud Security Enforcer aide les entreprises à répondre à une exposition importante de leur sécurité, car elles n’ont actuellement qu’une faible visibilité sur les applications cloud utilisées par leurs employés. Une nouvelle étude d’IBM a révélé qu'un tiers des employés des entreprises du classement Fortune 1000 partage et télécharge les données de l'entreprise via des applications cloud externes. Aujourd’hui, les employés sont de plus en plus impliqués dans des pratiques à risque avec ces applications, par exemple en s’identifiant avec leurs adresses e-mail personnelles, en utilisant des mots de passe peu sécurisés ou en réutilisant les identifiants de connexion de l’entreprise. L'utilisation croissante des applications mobiles comporte également un risque de sécurité : près de 40% des applications mobiles développées aujourd'hui ne sont pas correctement sécurisées lorsqu’elles arrivent sur le marché1.

Alors que le cloud offre une plus grande productivité, le fait que des employés aient des activités illicites via des applications non-approuvées, connu sous le nom de "Shadow IT", a pour conséquence une perte de contrôle et de visibilité des entreprises sur leurs données sensibles et une incapacité de leur part à protéger l’identité de leurs employés. Cela peut être aggravé par des circonstances exacerbant cette perte de contrôle.

Par exemple, un employé pourrait utiliser son email personnel pour créer un compte sur une application cloud de partage de fichiers externe à l’entreprise, sur laquelle il téléchargerait ensuite ses contacts commerciaux afin de pouvoir les consulter sur son appareil mobile. Bien que cette utilisation abusive lui donne un accès flexible à ses données, cela représente un problème majeur s’il décide d’aller travailler pour la concurrence. Car bien qu'il n’ait plus accès aux données et aux réseaux contrôlés par l'équipe IT de son ancien employeur, il aura encore une visibilité sur les données téléchargées dans cette application – ce qui peut représenter un problème concurrentiel et de sécurité.

IBM Cloud Security Enforcer sécurise l'utilisation des applications non-approuvées

La nouvelle solution IBM Cloud Security Enforcer est un outil, basé sur le cloud IBM, qui scanne les réseaux d'entreprise, trouve les applications que les employés utilisent, et fournit un moyen plus sécurisé d'y accéder. Fondé sur le partenariat existant entre IBM et Box, qui offre aux utilisateurs une sécurité renforcée lors du partage de fichiers via des appareils mobiles et sur le Web, IBM a également conçu des connecteurs sécurisés pour Cloud Security Enforcer dans la plateforme collaborative et de gestion de contenu basé sur le cloud de Box.

En plus de l'application de Box, IBM a conçu des connecteurs sécurisés pour d'autres applications populaires et couramment utilisées au travail, dont les outils de Microsoft Office 365, Google Apps, Salesforce.com et d'autres. Ce catalogue de connecteurs d'applications est en croissance constante, et sécuriser l'accès à ces applications va devenir de plus en plus important au fur et à mesure de l'évolution démographique de la main d'œuvre. L'étude d'IBM a également révélé que les employés issus de la génération Y, qui représenteront la moitié de la main-d'œuvre dans le monde entier en 20202, sont les plus grands utilisateurs d'applications cloud. Selon l'étude, plus de la moitié (51%) de ce groupe démographique utilise des services cloud au travail.

Cloud Security Enforcer comprend également des contrôles de sécurité supplémentaires concernant l'intégrité et la sécurité des applications utilisées par les employés. Ces contrôles sont basés sur l'analyse en profondeur des menaces issue d'IBM X-Force Exchange et du réseau mondial d'analyse des menaces avancées d'IBM. Cette plate-forme est gérée par un vaste réseau mondial de spécialistes de la sécurité qui surveillent Internet pour découvrir les activités malveillantes et les attaques émergentes. Ils analysent plus de 20 milliards d'événements de sécurité quotidiennement. Cette analyse permet aux équipes informatiques et de sécurité de réagir rapidement aux menaces qui émergent d'applications cloud utilisées par les employés, en bloquant et en prenant les mesures nécessaires contre celles qui présentent un risque.

Conçue par la division sécurité d'IBM, cette nouvelle technologie permet aux entreprises de réduire les défis liés au « Shadow IT », de se défendre contre les acteurs malveillants qui cherchent à tirer profit de l'utilisation des applications cloud non sécurisées, et de bénéficier de la productivité et de l'efficacité liées à l'utilisation d'applications cloud sécurisées. Ceci est réalisé par quatre fonctions de base qui :

• Détectent l'utilisation non autorisée d'une l'application cloud par des employés, ce qui permet aux entreprises de déterminer et de configurer de façon sécurisée les applications que leurs employés veulent utiliser. Cela permet également de gérer, visualiser et de diriger la façon dont ils peuvent les utiliser et y accéder.

• Déterminent et imposent quelle donnée de l'entreprise peut ou ne peut pas être partagée par les employés via des applications cloud tierces spécifiques.

• Connectent les employés rapidement à des applications cloud tierces via des connecteurs sécurisés, ce qui inclut l'attribution automatique de mots de passe sophistiqués, et contribue à atténuer les failles de sécurité causées par une erreur humaine (95% de tous les incidents3), telles que les mots de passe peu sécurisés. Selon l'équipe recherche d'IBM, un employé sur quatre utilise son identifiant et son mot de passe d'entreprise pour se connecter à ces applications, laissant ainsi la porte ouverte à de vastes failles à travers lesquelles les

pirates peuvent s’engouffrer.

• Protègent contre les menaces liées au cloud ou causées par les employés grâce à l'analyse des données sur les menaces en temps réel d’IBM X-Force Exchange.

Avec le lancement de Cloud Security Enforcer, IBM poursuit son engagement visant à accroître le contrôle, la visibilité, la sécurité et la gestion des clients dans leurs environnements cloud hybrides. Pour ce faire, IBM fournit une portabilité accrue des données, et une meilleure sécurisation dans ce type d’environnements.

Pour lire les résultats complets de la recherche sur la façon dont les employés utilisent des applications cloud : https://securityintelligence.com/

Pour en savoir plus sur Cloud Security Enforcer : http://www.ibm.com/security/cloud/cloud-security-enforcer.html.

A propos d’IBM Security

La plateforme de sécurité IBM apporte la sécurité intelligente pour aider les organisations à protéger les personnes, les données, les applications et les infrastructures. Les solutions IBM couvrent la gestion des identités et des accès, le SIEM (Security Information and Event Management), la sécurité des données, la sécurité des applications, la gestion du risque, la gestion des terminaux, la nouvelle génération de protection contre les intrusions et d’autres sujets. IBM dispose d’une des plus importantes organisations au monde de recherche et développement et de prestations de services dans le domaine de la sécurité.

Pour plus d'informations sur l’offre sécurité d’IBM : www.ibm.com/security/fr/fr

Suivez notre actualité sur Twitter @IBMSecurityFR

- Etude de l’Institut Ponemon, The State of Mobile Insecurity (l’Etat de l’Insécurité Mobile): https://securityintelligence.com/mobile-insecurity/
- Sondage Gallup : http://www.gallup.com/poll/183074/millennials-trusting-safety-personal-information.aspx
- Rapport IBM X-Force Threat Intelligence trimestriel publié en Q1 2015

À propos du sondage

Ces résultats sont issus d'un sondage Ipsos réalisé pour le compte d'IBM, et ayant eu lieu entre le 27 et le 31 Juillet 2015. Pour cette étude, un échantillon de 1001 adultes américains employés à temps plein dans les entreprises du classement Fortune 1000 ont été interrogés en ligne. La précision des sondages en ligne d'Ipsos est mesurée en utilisant un intervalle de crédibilité. Dans ce cas, le sondage a un intervalle de plus ou moins 3,5 points de pourcentage de crédibilité pour tous les employés. Les données ont été pondérées par les données actuelles de la population des États-Unis par sexe, âge, région et revenu des ménages, et basées sur les données du recensement américain.

Avertissement : Les déclarations d'IBM concernant ses plans, orientations et intentions sont sujettes à modification ou retrait sans préavis à la seule discrétion d'IBM. Les informations sur les produits futurs potentiels sont destinées à décrire l'orientation générale de la stratégie produit d'IBM et ne doivent pas être prises en compte pour prendre une décision d'achat. Les informations mentionnées sur les produits futurs potentiels ne créent pas d'engagement, promesse ou obligation juridique de fournir un quelconque produit, code ou fonctionnalité. Les informations sur les produits potentiels futurs ne peuvent être incorporées dans un contrat. Le développement, la mise sur le marché ou le calendrier associé à des caractéristiques ou fonctionnalités futures décrites pour nos produits restent à notre seule discrétion.x

---