TOP 5 DES MEILLEURES PRATIQUES DE SÉCURITÉ SUR IBM i

Pour IBM, rien n'est plus sécurisé (et sécurisant) qu'un IBM i, notamment parce que le système s'appuie sur une architecture orientée objet qui encapsule les données dans des conteneurs typés « data » et les exécutables dans des conteneurs étiquetés « programs ». Comme chaque conteneur identifie très précisément ce qu'il est autorisé à réaliser et qui peut y accéder, les portes d'entrée pour les virus et Worms comme on en trouve sur Windows ou Linux sont belles et bien verrouillées.

Pour autant, enregistrer vos données les plus confidentielles et exécuter vos processus métiers critiques sur IBM i ne suffisent pas à vous mettre à l'abri des fuites de données et autres compromissions.

Ce n'est pas parce qu'on héberge son business sur un tel environnement qu'il faut en oublier pour autant les bonnes pratiques. Voici le TOP 5 des meilleures pratiques de sécurité sur IBM i.

1 LA MENACE VIENT DE L'INTÉRIEUR

En matière de sécurité des systèmes et des données, le premier des risques est celui de la menace interne. C'est particulièrement vrai dans l'univers IBM i où la réputation de solidité du système – notamment face aux menaces Internet - amène bien des administrateurs à négliger les risques internes en utilisant eux-mêmes en permanence des profils à très forts privilèges même pour les consultations les plus basiques et à distribuer trop aisément des profils privilégiés aux utilisateurs. Dès lors, les menaces internes qui modifient, effacent ou s'attribuent des droits qu'ils n'ont pas constituent un risque prioritaire à adresser sur IBM i.

Il est capital d'implémenter et imposer une politique de mots-clés forts - fréquemment renouvelés sur les comptes critiques - mais aussi de systématiquement redéfinir les mots-clés par défaut des servies IBM i. Il est fondamental de limiter le nombre de profils utilisateurs à hautes autorisations. Il est aussi essentiel de procéder régulièrement à un nettoyage des profils inactifs mais aussi à une surveillance permanente des profils disposant de droits d'accès élevés et d'autorisations de contrôles de processus critiques.

Des outils permettent aujourd'hui d'assurer cette gestion avancée et cette surveillance des comptes. Des solutions comme celle de Raz-Lee permettent même d'attribuer dynamiquement des privilèges à tel ou tel utilisateur en fonction du contexte, du jour de la semaine ou d'une tranche horaire. Un moyen bien pratique de n'attribuer des droits supplémentaires à un utilisateur que pendant une période définie ou de verrouiller automatiquement des profils susceptibles d'être utilisés à mauvais escients. Et un bon moyen aussi d'être alerté de comportements douteux.

2 SURVEILLEZ ET SOYEZ ALERTÉ

« Savoir qui fait quoi » est un corollaire du premier point. Le système IBM i crée et maintient de nombreux journaux d'activité sur à peu près toutes les opérations possibles, pour peu qu'on le paramètre ainsi. Mais, même ainsi paramétré, rares sont les entreprises qui utilisent et surveillent ensuite ces journaux pour détecter les comportements anormaux et les tentatives d'accès avortées. Car ces journaux sont souvent illisibles pour l'être humain et bien trop riches en informations inutiles d'un point de vue sécurité.

D'où l'importance de disposer d'outils de surveillance et d'audit capables de générer des vues graphiques et statistiques mettant spécifiquement en évidence les anomalies repérées mais également capables de surveiller les évènements en tâche de fond et de vous alerter automatiquement dès qu'un comportement douteux ou une tentative d'intrusion ou d'extraction de données est détectée.

Un outil comme iSecurity Suite de Raz Lee embarque des fonctions d'audit avancées ainsi qu'un puissant module de visualisation (Visualizer) qui ajoute une dimension BI (Business Intelligence) dédiée à la sécurité au-dessus des journaux d'IBM i. La solution utilise même des algorithmes « Best Fit » pour automatiquement mettre en place des actions correctives en cas de détection de « trous » de sécurité.

Conception éditoriale & graphique : Agence Com4Médias www.com4medias.com

3 PROTÉGEZ VOS DONNÉES CRITIQUES

L'erreur ultime serait cependant de focaliser l'attention seulement sur les utilisateurs et leurs comportements. Au-delà de la nécessité de protéger le système contre des accès malveillants, il est impératif d'apporter toute l'attention nécessaire aux données les plus critiques et les plus confidentielles. C'est pourquoi des solutions comme iSecurity Suite surveillent les données que vous désignez comme critiques (des prix, des taux, des numéros de cartes bancaires, etc.) et génèrent des alertes en fonction de règles métiers définies par les administrateurs (par exemple lorsqu'un prix évolue de plus de 10%).

En outre, de telles solutions permettent de mettre en œuvre, avec beaucoup plus de simplicité mais aussi de granularité et de contrôle, les fonctions de chiffrement des données sensibles d'IBM i. Elles complètent ces fonctionnalités avec du chiffrement PGP pour les données en mouvement qui doivent transiter hors des murs de l'entreprise.

4 LES MENACES EXTÉRIEURES EXISTENT

En matière de sécurité, il n'existe qu'une approche payante : la défense en profondeur qui consiste à empiler les couches de sécurité pour rendre toute attaque beaucoup plus complexe à mettre en œuvre (la suite Raz-Lee incorpore plus de 15 modules différents par exemple). Autrement dit, il ne faut négliger aucune piste ni aucun vecteur d'attaques. Dès lors, il faut aussi prévoir les attaques portées de l'extérieur des murs de l'entreprise. D'autant qu'il y a bien longtemps que les systèmes IBM i ne sont plus simplement reliés à des terminaux passifs directement connectés. Bien au contraire, l'IBM i s'est ouvert au monde qui l'entoure pour s'intégrer dans un système d'information hétérogène.

Les données de l'univers IBM i sont désormais accessibles en TCP/IP que ce soit au travers d'accès FTP, au travers d'accès ODBC, qu'au travers de services les exposant. Les outils iSecurity Suite de Raz-Lee ne se contentent pas de surveiller les points d'entrée et de sortie. Ils créent aussi de vrais pare-feux (Firewalls) pour chaque protocole. Ils repèrent les volumétries anormales qui sortent de l'entreprise et peuvent témoigner d'une tentative d'extraction, vous alertant immédiatement de l'anomalie. Ils incorporent même un anti-virus afin d'éradiquer les menaces PC, l'IBM i pouvant servir de point de contournement des protections « End Point » mises en œuvre.

5 INTÉGREZ L'IBM I DANS VOTRE INFRASTRUCTURE SIEM

Toute sécurisation d'un système d'information passe par une analyse de risques. Celle-ci est indispensable afin de bien comprendre les éléments, les profils et les données à protéger. Pour vous aider, Raz Lee propose un outil gratuit, dénommé Security Assessment qui permet rapidement de mettre en exergue les bonnes pratiques non respectées, les sécurités IBM i non mises en œuvre, les anomalies dans les profils et l'exploitation des données, les problèmes de connectivité, etc.

Cependant, il ne faut pas perdre de vue que protéger l'IBM i n'est pas une fin en soi. Le système n'est qu'une composante de votre système d'information. Aujourd'hui, une nouvelle génération d'outils SIEM (Security Information Event Manager comme Arcsight, IBM SIEM, Splunk, etc.) embarque de l'intelligence artificielle pour repérer les signaux faibles et trouver des patterns d'attaques en rapprochant les données provenant de toutes les composantes du système d'information.

C'est pourquoi des outils comme iSecurity Suite sont aujourd'hui capables de transférer vers ces systèmes SIEM les données essentielles permettant une approche vraiment globale de la gestion des événements, une meilleure détection des attaques et une meilleure investigation d'éventuelles compromissions.

La sécurité n'est pas une destination, c'est un cheminement infini nécessitant une attention permanente et des capacités de surveillance, d'alertes et d'audit que seuls des outils comme iSecurity Suite de Raz-Lee peuvent offrir à votre IBM i.

Conception éditoriale & graphique : Agence Com4Médias www.com4medias.com

RAZ-LEE
Experts @ Security and Compliance

RazLee Security est l'un des leaders en matière de solutions de sécurité pour les serveurs iSeries (AS/400 ou Power i). La famille de produits Raz-Lee iSecurity apporte une aide précieuse pour éviter les malversations internes et les accès non autorisés venant de l'extérieur. iSecurity offre des solutions complètes pour sécuriser votre IT et rendre vos systèmes Power i plus transparents. Les solutions Raz-Lee permettent aux entreprises de contrôler et prouver leur conformité aux réglementations telles que PCI, Sarbanes-Oxley (SOX) et HIPAA. Pour aller plus loin : http://www.razlee.de/fr/