

PROTECTION DES CENTRES DE DONNÉES

Epsilon après la compromission

En 2011, les noms et adresses e-mail de millions de clients ont été exposés suite à une divulgation de données dans la société de marketing par e-mail Epsilon. Comme de nombreuses entreprises en vue utilisent les services d'Epsilon, une foule de notifications ont été envoyées pour avertir les clients de la fraude potentielle. Parmi les entreprises qui ont dû avertir leurs clients figurent Barclaycard US, Capital One, Best Buy, JPMorgan, Citigroup, Tivo, Disney Destinations, New York & Company, Walgreens, Marriott et bien d'autres encore. (Source : <http://mcaf.ee/5342e>)

Security Connected

Le cadre d'implémentation McAfee Security Connected permet l'intégration de plusieurs produits, services et partenariats dans le but d'assurer une réduction des risques efficace et centralisée. Fondée sur plus de vingt ans de pratiques éprouvées en matière de sécurité, l'approche Security Connected apporte une assistance précieuse à toutes les entreprises, indépendamment de leur taille, de leur secteur d'activités ou de leur situation géographique. Ainsi, elle permet d'améliorer l'état de sécurisation général, d'optimiser les systèmes de protection pour une meilleure rentabilité de l'investissement en sécurité et d'aligner les stratégies de sécurité sur les initiatives d'ordre commercial. L'architecture de référence McAfee Security Connected vous mène des idées jusqu'à l'implémentation. Faites-en bon usage et adaptez ses concepts aux risques, à l'infrastructure et aux objectifs spécifiques de votre entreprise. McAfee consacre tous ses efforts à trouver des solutions novatrices afin d'assurer à ses clients une protection irréprochable.

Une sécurité renforcée pour un centre de données plus agile

Défis

Le centre de données est le centre névralgique de l'entreprise. Il a pour principales fonctions de générer des revenus, de stocker des données sensibles et de fournir des services stratégiques. Sa nature critique et sa grande valeur en font une cible idéale. Depuis longtemps déjà, les données sensibles, les applications métiers, les bases de données, les équipements réseau, les dispositifs de stockage et l'infrastructure sous-jacente sont dans la ligne de mire des auteurs d'attaques externes et internes, mais aussi des auditeurs qui leur imposent une multitude de contraintes réglementaires.

Pratiquement tout impératif réglementaire ou problème de sécurité pesant sur les centres de données a donné naissance à une solution ponctuelle. En vertu de ce processus réactif, par lequel de nouvelles solutions individuelles sont ajoutées à la moindre occasion, les contrôles des centres de données sont devenus à la fois complexes, trop nombreux, coûteux et isolés, ce qui finit par submerger la plupart des entreprises. Aux demandes existantes vient s'ajouter un flot incessant de nouvelles menaces et tendances. Ainsi, les entreprises exigent que les centres de données prennent en charge la mobilité et les environnements web 2.0 et qu'ils contrent les attaques ciblées et opportunistes. Cela tout en limitant au maximum les temps d'indisponibilité et en produisant des rapports fréquents apportant la preuve de leur conformité.

Le modèle traditionnel de sécurité des centres de données n'offre ni l'agilité attendue pour se conformer de façon rapide et transparente aux nouvelles exigences, ni les fonctions de gestion de la sécurité permettant de garantir efficacité et performances, ni la disponibilité et l'intégrité indispensables aux opérations stratégiques actuelles, pas plus que la conception optimisée nécessaire pour assurer la rentabilité. Or, les centres de données sont plus vitaux que jamais pour les activités de l'entreprise. Aujourd'hui, les départements informatiques tracent de nouvelles voies. Nous ne pouvons certes que formuler des hypothèses quant à la prochaine tendance qui émergera dans cinq ans, mais au regard de ces cinq dernières années, il est clair que la protection informatique que nous pensions efficace ne suffira pas à garantir notre sécurité. Un cadre stratégique destiné à relier des éléments jusqu'ici disparates est désormais indispensable.

D'après l'étude Cost of a Data Breach (Coût des divulgations de données) du Ponemon Institute parue en mars 2011, chaque enregistrement compromis coûte 214 dollars, ce qui porte le coût moyen d'une fuite de données à 7,2 millions de dollars².

Heartland Payment Systems après la compromission

En 2010, Heartland a conclu un accord avec VISA fixant le montant des réparations à 60 millions de dollars pour toutes les plaintes potentielles liées à la fuite de données survenue en 2009. L'année précédente, Heartland avait conclu un accord similaire avec Amex pour un montant de 3,5 millions de dollars¹.



Solutions

Agilité de l'entreprise

L'équipe en charge des opérations du centre de données ne manque pas de responsabilités : développement de solutions destinées au maintien de la conformité, virtualisation, consolidation ou mise en œuvre de l'informatique dématérialisée (*cloud computing*). Un cadre d'implémentation de la sécurité doit être suffisamment agile pour permettre l'exécution rapide de modifications et l'adoption de nouvelles tendances, sans engendrer de risques supplémentaires. S'il offre la robustesse nécessaire pour un tel niveau d'agilité, il aura un impact positif sur les opérations de sécurité et les activités de l'entreprise.

Gestion de la sécurité

Les compromissions de sécurité entraînent des coûts élevés : sanctions réglementaires, actions collectives, détérioration de l'image de l'entreprise, préjudice porté à la marque, perte de clientèle et, en fin de compte, diminution des revenus. Etant donné la complexité des centres de données, conjuguée à certaines des tendances et menaces mentionnées précédemment, la réduction des risques nécessite, pour être efficace, une approche globale de la sécurité. La gestion des centres de données, quels que soient leur taille et leur niveau de complexité, exige une solution centralisée de gestion de la sécurité qui relie les solutions disparates de protection des données, des postes clients, du réseau et des environnements dématérialisés. Une gestion de la sécurité évolutive est vitale pour garantir une visibilité sur les applications et les bases de données qui traitent les transactions et sur les équipements de stockage qui contiennent ces données.

Disponibilité et intégrité

Garantir la disponibilité et l'intégrité face à des menaces internes et externes, s'ouvrir à de nouvelles tendances telles que les versions mobiles des sites web, assurer l'intégration avec des services web 2.0 d'autres entreprises ou encore tirer parti de diverses infrastructures dématérialisées : les défis ne manquent pas. Il est impératif de mettre en place un système de défense robuste qui ne se focalise pas aveuglément sur la protection du contenu et du réseau, mais englobe et intègre à la fois la sécurisation des postes clients, du contenu et du réseau, sans oublier le nuage Internet. Le cadre de sécurité doit réduire autant que possible la latence, limiter le risque d'erreurs de configuration

manuelles, interdire l'installation de logiciels malveillants et protéger les informations du centre de données, quelle que soit sa taille et sa nature (consolidé, virtualisé ou dématérialisé). La protection des environnements virtualisés, tant au niveau des serveurs que des postes de travail virtuels, revêt une importance capitale. Des infrastructures de postes de travail virtuels sont installées partout, depuis les smartphones jusqu'aux ordinateurs portables ou aux serveurs virtuels, et elles constituent la norme dans les centres de données. Les solutions actuelles doivent être optimisées pour permettre l'adoption des nouvelles tendances de la virtualisation, mais sans négliger les fondamentaux. Ainsi, la latence ou les indisponibilités non planifiées ne sont tout simplement pas acceptables dans les environnements stratégiques. Les opérations réseau, le contrôle d'accès, la protection des postes clients et les pare-feux doivent être conçus de manière à satisfaire les besoins des opérations informatiques, et pas uniquement en termes de sécurité, car les solutions de sécurité médiocres qui engendrent une latence peuvent occasionner autant de dommages qu'une attaque.

Optimisation de la sécurité

L'optimisation de la sécurité permet aux entreprises de dépasser la question purement technique de la faisabilité des contrôles pour les envisager du point de vue de l'efficacité. Il existe de nombreuses solutions de sécurité sur le marché et la plupart sont assez performantes. Néanmoins, d'une manière générale, elles sont sources de complexité, le pire ennemi de la sécurité. Les solutions disparates et isolées, sans interconnectivité et nécessitant toujours plus de ressources pour fonctionner ne constituent pas une option viable. Les cadres de conception modernes doivent en revanche se centrer sur un modèle de protection optimisé visant à centraliser la gestion des contrôles de sécurité et leur enrichissement mutuel, qui aligne les solutions sur les priorités de l'entreprise tout en réduisant les coûts des opérations de sécurisation. A mesure que les menaces évoluent et que les nouvelles tendances sont adoptées à un rythme soutenu, un tel cadre optimisé s'imposera comme une nécessité pour garantir rentabilité, efficacité et sécurité des opérations d'entreprise. Les solutions optimisées doivent faire partie intégrante de l'automatisation du processus de conformité, de façon à permettre une convergence des processus et des tâches de sécurité liés aux obligations réglementaires sans accroître la charge d'administration.

Meilleures pratiques

- Comprendre que les centres de données évoluent rapidement : consolidation, virtualisation et dématérialisation (*cloud computing*)
- Mettre en œuvre des solutions qui répondent aux besoins dans des domaines tels que l'agilité, la gestion de la sécurité, la disponibilité, l'intégrité et l'optimisation de la sécurité
- Déployer des solutions qui centralisent les opérations de sécurité pour les composants essentiels du centre de données : réseaux, solutions virtuelles, bases de données, serveurs et équipements de stockage
- Faire en sorte que les solutions de sécurité utilisées contribuent également à l'automatisation de la conformité
- Tout en répondant aux exigences de sécurité, garantir la prise en compte des principaux facteurs opérationnels en termes de disponibilité et de latence

D'après des études du projet DataLossDB de l'Open Security Foundation, à partir d'avril 2011, 75 % des fuites de données étaient le résultat d'activités malveillantes alors que le reste était attribuable à de la négligence³.

Générateurs de valeur

Vos initiatives en matière de centre de données doivent tirer parti de technologies de sécurité pour favoriser l'efficacité opérationnelle. Voici divers domaines susceptibles de permettre une optimisation des centres de données :

- *Consolidation* — Les solutions de consolidation doivent être déployées au niveau du matériel, des logiciels et de l'infrastructure sous-jacente.
- *Standardisation* — Les solutions doivent favoriser la standardisation des fonctionnalités de protection des postes clients, des données et du réseau. Ceci permettra de garantir l'efficacité de l'analyse des menaces et des réponses à celles-ci.
- *Réduction des coûts d'audit, de conformité et de surveillance* — Les solutions doivent assurer (ou se justifier par) une diminution des coûts de mise en conformité et des audits informatiques, en permettant de vérifier les systèmes et les processus plutôt que les postes individuels.
- *Baisse du trafic réseau* — Les solutions pouvant résider au cœur du réseau ont pour but d'assurer une protection et doivent également contribuer à éliminer le spam et le trafic réseau inutile.
- *Réduction des coûts des interventions du centre d'assistance* — La sécurisation du cœur du centre de données doit entraîner une diminution des appels au centre d'assistance liés à des incidents de sécurité.

Architecture de référence McAfee Security Connected — Documents connexes

Niveau II

- Protection des informations
- Contrôle et surveillance des modifications

Niveau III

- Evaluation des vulnérabilités
- Mise en œuvre de la conformité sur les postes clients
- Prévention des attaques par déni de service et par déni de service distribué
- Protection des serveurs

Pour plus d'informations sur l'architecture de référence McAfee Security Connected, consultez notre site à l'adresse : www.mcafee.com/fr/entreprise/reference-architecture/.

L'auteur



Brian Contos, spécialiste certifié en sécurité des systèmes d'information (CISSP), est Directeur de la stratégie de sécurité à l'échelle mondiale de McAfee. Fort de plus de vingt ans d'expérience en gestion et en ingénierie de sécurité, expert éminent en matière de sécurité informatique, il est l'auteur de divers ouvrages, dont *Enemy at the Water Cooler* (L'ennemi au sein même de l'entreprise) et *Physical and Logical Security Convergence* (Convergence de la sécurité physique et logique). Brian Contos a travaillé avec des organisations gouvernementales et des sociétés du classement Forbes Global 2000 en Amérique du Nord, en Amérique Centrale et en Amérique du Sud, ainsi qu'en Europe, au Moyen-Orient et en Asie. Il a participé en qualité d'orateur invité à des événements majeurs du secteur de la sécurité tels que RSA, Interop, SANS, OWASP et SecTor. Il collabore à des publications informatiques spécialisées et à des revues économiques dont *Forbes*, le *New York Times* et *The Times of London*. Il est un membre distingué du Ponemon Institute et est diplômé de l'Université de l'Arizona.

brian_contos@mcafee.com || <http://siblog.mcafee.com/author/brian-contos/> || @BrianContos

¹ <http://mcaf.ee/gvxkh>

² <http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2010%20Global%20CODB.pdf>

³ <http://datalossdb.org/>

