Microsoft

L'optimisation de la sécurité commence par le système d'exploitation

avec Windows Server 2016

La sophistication accrue des attaques nécessite de nouvelles couches de sécurité.

L'évolution des menaces virtuelles complique plus que jamais la sécurisation des données et des applications. Les utilisateurs malveillants font appel à des méthodes plus sophistiquées et utilisent fréquemment des identifiants d'administrateur hautement privilégiés pour contrôler l'accès. Ces identifiants permettent d'échapper à toute détection pendant une longue période ou de créer une attaque instantanée dévastatrice.

Les environnements virtualisés sont les plus à risque. Les machines virtuelles ne disposent pas des fonctionnalités de sécurité liées au matériel des serveurs physiques. Étant donné que les machines virtuelles sont instanciées à partir de fichiers qui peuvent être copiés et modifiés, n'importe quel utilisateur malveillant en mesure d'accéder au stockage, au réseau ou aux ressources de calcul de l'infrastructure dispose immédiatement de privilèges non vérifiés pour l'ensemble des machines virtuelles. Un utilisateur malveillant peut se contenter de copier vos machines virtuelles SQL et de contrôleur de domaine sur une clé USB avant de filer à l'anglaise avec le butin.

Protection, détection, réaction

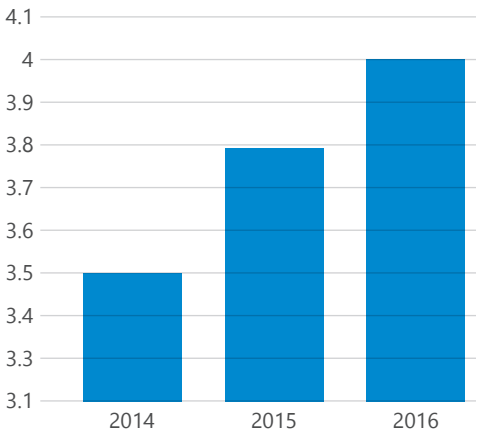
Windows Server 2016 inclut des mécanismes de résistance aux violations intégrés qui permettent de contrer les attaques sur vos systèmes et de répondre aux objectifs de conformité. Même si un utilisateur malveillant se fraie un chemin vers votre environnement, les couches de sécurité intégrées dans chaque système Windows Server 2016 limitent les dommages possibles. Certaines fonctionnalités d'isolation des identifiants et de défense contre les menaces sont activées au moment du déploiement. D'autres fonctionnalités peuvent être activées au besoin pour :

- Bloquer des attaques pass-the-hash et d'autres tentatives visant à compromettre les identifiants d'administrateur.
- Empêcher les programmes malveillants et les ransomware d'être injectés dans vos serveurs.
- Identifier rapidement le comportement qui suggère une violation du serveur.
- Développer la protection qui existe pour vos serveurs physiques vers vos machines virtuelles.

« Les machines virtuelles protégées éliminent un obstacle empêchant l'hébergement et constituent un avantage concurrentiel de taille. Microsoft propose cette technologie en exclusivité. »

– Philip Moss
Chief Product Officer,
Acuutech

Coûts relatifs aux violations de données par entreprise dans le monde (en milliards de dollars)



Le coût relatif aux violations de données continue d'augmenter chaque année pour atteindre 4 milliards de dollars en moyenne par incident.

Source : Cost of Data Breach Study, IBM, Ponemon

L'optimisation de la sécurité commence par le système d'exploitation

Windows Server 2016 garantit une sécurité à l'échelle de l'entreprise, ce qui permet aux organisations de se conformer aux critères organisationnels et sectoriels les plus stricts. L'infrastructure et les applications sont protégés sur site et dans le cloud, sur des serveurs physiques et virtuels.

« Les machines virtuelles protégées simplifient la sécurisation des scénarios d'usage de machine virtuelle. Auparavant, la tâche était complexe, voire impossible. Aujourd'hui, nous parvenons à les protéger. »

– Rand Morimoto, Président de Convergent Computing

Les entreprises doivent :	Exemple de menace :	Windows Server 2016 offre les avantages suivants :
Protéger les identifiants d'administrateur	Une attaque pass-the-hash fournit à l'utilisateur malveillant des identifiants d'administrateur sur un réseau d'hôpital, que l'utilisateur malveillant utilise pour accéder aux données confidentielles des patients.	Proposez **Just Enough Administration** et **Just-in-Time Administration** pour avoir la certitude que les utilisateurs malveillants ne peuvent pas accéder à des données critiques, même s'ils se sont emparés d'identifiants d'administrateur. **Credential Guard** permet d'empêcher le vol d'identifiants d'administrateur par des attaques pass-the-hash et pass-the-ticket. **Credential Guard à distance** propose une authentification unique pour les sessions de Bureau à distance (RDP), ce qui élimine la nécessité de transfert d'informations d'identification à l'hôte RDP.
Protéger les serveurs, détecter les menaces et répondre à temps	Les ransomware sur les serveurs d'université empêchent les utilisateurs d'accéder aux données critiques de recherche et liées aux étudiants, jusqu'à ce qu'une rançon ait été payée à l'attaquant. Un développeur d'applications métier télécharge du code depuis l'Internet public pour l'intégrer à son application. Le code téléchargé inclut des programmes malveillants qui peuvent suivre l'activité dans d'autres conteneurs via le noyau partagé.	Assurez-vous que seuls les binaires autorisés sont exécutés avec **Code Integrity**. Protégez-vous contre les vulnérabilités inconnues avec la **protection du flux de contrôle**. **Windows Defender** permet également d'assurer une protection contre les vulnérabilités connues, sans aucune incidence sur les rôles serveur (tels que les serveurs web). Isolez les applications conteneurisées qui utilisent des **conteneurs Hyper-V**, sans qu'aucune modification au niveau du conteneur ne soit nécessaire. Limitez un peu plus la surface d'exposition aux attaques grâce à des possibilités de déploiement de système d'exploitation « sur mesure » de **Nano Server**.
Identifier rapidement les comportements malveillants	Un programme malveillant basé sur le noyau injecté dans le serveur d'un cabinet d'avocats a permis à un utilisateur malveillant d'accéder aux fichiers des clients sans être détecté.	Optimisez les contrôles de sécurité grâce à la **journalisation améliorée** en matière de détection des menaces. Cela inclut le contrôle de l'accès au noyau ainsi que d'autres processus sensibles, et par conséquent, à des informations détaillées qui permettent à **Microsoft Operations Management Suite (OMS)**, un système de sécurité et de gestion des événements relatifs aux informations, de fournir des renseignements sur les violations potentielles, grâce à sa fonctionnalité **Log Analytics**.
Virtualiser sans aucun compromis en termes de sécurité	Un utilisateur malveillant compromet les identifiants d'administrateur de l'infrastructure d'une banque, ce qui lui donne accès à des contrôleurs de domaine Active Directory virtualisés ainsi qu'à des bases de données SQL où des informations de compte client sont stockées.	Créez **des machines virtuelles protégées** (machines virtuelles de deuxième génération équipées d'un TPM), qui sont chiffrées à l'aide de BitLocker et qui ne peuvent fonctionner que sur des hôtes approuvés dans l'infrastructure. **Le service Guardian hôte** oblige chaque hôte à faire état de sa sécurité, avant que des machines virtuelles protégées puissent être démarrées ou migrées.

Passez à l'étape supérieure. Pour en savoir plus, consultez le site www.Microsoft.com/WindowsServer2016

Microsoft