Microsoft Azure

Cinq pratiques exemplaires pour la sécurité infonuagique

Pour de nombreuses entreprises, la sécurité infonuagique est un territoire inconnu. Si bon nombre de principes de sécurité infonuagiques sont les mêmes que pour la sécurité sur place, leur mise en œuvre est souvent bien différente. Cet aperçu présente cinq pratiques exemplaires en matière de sécurité infonuagique : le contrôle des identités et des accès, la gestion du niveau de sécurité, la sécurité des applications et des données, la protection contre les menaces et la sécurité du réseau.

Renforcez le contrôle des accès

Améliorez le niveau de sécurité

Assurez la sécurité des applications et des données

Réduisez les menaces

Protégez le réseau

01 Renforcez le contrôle des accès

Les pratiques de sécurité classiques ne suffisent pas à se défendre contre les atteintes à la sécurité modernes. Par conséquent, l'approche de sécurité moderne consiste à toujours présumer qu'il y a une violation : protégez-vous comme si l'attaquant avait déjà infiltré le périmètre du réseau. De nos jours, les utilisateurs travaillent à partir de nombreux emplacements au moyen de plusieurs appareils et applications. La seule constante est l'identité de l'utilisateur; c'est pourquoi cette dernière est le nouveau point focal du contrôle de sécurité.

Mettez en place l'authentification multifacteur

Ajoutez une couche de sécurité en exigeant deux ou plusieurs des méthodes d'authentification suivantes :

- Un élément que vous connaissez (généralement un mot de passe)
- Un élément dont vous *disposez* (un appareil de confiance difficile à dupliquer, comme un téléphone)
- Un élément vous concernant (biométrie)

Profitez de l'accès conditionnel

Maîtrisez l'équilibre entre la sécurité et la productivité en tenant compte de la *manière* dont une ressource est accessible pour parvenir à une décision de contrôle d'accès. Mettez en place des décisions de contrôle d'accès automatisées fondées sur des conditions pour permettre ou refuser l'accès à vos applications sur le nuage.

Employez un modèle de confiance zéro

Vérifiez l'identité de tout élément et de toute personne qui tentent de s'authentifier ou de se connecter avant d'accorder l'accès.

02 Améliorez le niveau de sécurité

En raison du nombre sans cesse croissant de recommandations et de vulnérabilités informatiques relevées, il est devenu difficile de déterminer les priorités en cas de problème. Assurez-vous de disposer des outils dont vous avez besoin pour évaluer vos environnements et vos actifs actuels et relever les problèmes de sécurité potentiels.

Améliorez vos conditions actuelles

Utilisez un outil comme Secure Score dans le Centre de sécurité Azure pour comprendre et améliorer votre niveau de sécurité en suivant des pratiques exemplaires.

Sensibilisez les intervenants

Faites part de l'amélioration de votre niveau de sécurité aux intervenants pour démontrer la valeur que vous fournissez à l'organisation au fur et à mesure que vous améliorez la sécurité organisationnelle.

Collaborez avec votre équipe d'opérations de développement pour formuler des politiques

Pour vous sortir de votre modèle réactif, vous devez travailler de concert avec vos équipes d'opérations de développement pour appliquer les stratégies de sécurité essentielles dès le début du cycle d'ingénierie pour assurer des opérations de développement sécurisées.

03 Assurez la sécurité des applications et des données

Protégez les données, les applications et l'infrastructure au moyen d'une stratégie de défense en profondeur en couches appliquée à l'ensemble des identités, des données, des hôtes et des réseaux.

Chiffrement

Chiffrez les données pendant leur *stockage* et les transferts. Pensez à chiffrer les données en cours d'utilisation avec des technologies informatiques confidentielles.

Suivez les pratiques exemplaires en matière de sécurité

Assurez-vous que vos dépendances en code source libre ne présentent pas de vulnérabilités. De plus, formez vos développeurs aux pratiques exemplaires en matière de sécurité comme l'approche Security Development Lifecycle (SDL).

Partagez la responsabilité

Lorsqu'une entreprise mène la majorité de ses activités sur place, elle est propriétaire de l'ensemble de la pile et est responsable de sa propre sécurité. Selon la façon dont vous utilisez le nuage, vos responsabilités changent, et certaines responsabilités relèvent désormais de votre fournisseur infonuagique.

- IaaS : en ce qui concerne les applications exécutées dans des machines virtuelles, c'est au client que revient une grande part de la responsabilité de s'assurer que l'application et le système d'exploitation sont sécurisés.
- PaaS : au fur et à mesure que vous migrez vers un service PaaS natif au nuage, les fournisseurs infonuagiques comme Microsoft assumeront davantage de responsabilités relativement à la sécurité au niveau du système d'exploitation lui-même.
- SaaS : avec un service SaaS, le client a encore moins de responsabilités à assumer. Consultez le modèle de responsabilité partagée.

04 Réduisez les menaces

Le niveau de sécurité opérationnelle (protection, détection et réaction) doit se fonder sur des renseignements de sécurité ultrafiables pour que vous puissiez détecter rapidement les menaces en constante évolution et réagir à celles-ci rapidement.

Instaurez une détection pour tous les types de ressources

Assurez-vous que la détection des menaces est activée pour les machines virtuelles, les bases de données, le stockage et l'IdO. Le Centre de sécurité Azure dispose d'une détection intégrée des menaces qui prend en charge tous les types de ressources Azure.

Intégrez les renseignements sur les menaces

Faites appel à un fournisseur infonuagique qui intègre les renseignements sur les menaces pour vous fournir le contexte, la pertinence et la hiérarchisation nécessaires pour que vous preniez des décisions plus rapides, plus efficaces et plus proactives.

Modernisez votre système de gestion des événements et des informations liés à la sécurité (SIEM)

Envisagez d'adopter un système SIEM natif au nuage qui évolue avec vos besoins, qui utilise l'Intelligence Artificielle pour trier les données pertinentes et qui ne nécessite aucune infrastructure.

05 Protégez le réseau

Nous sommes à une époque où une transformation de la sécurité du réseau est devenue nécessaire. Au fur et à mesure que l'environnement change, vos solutions de sécurité doivent pouvoir se mesurer aux menaces en constante évolution et réduire au maximum la capacité des attaquants à pirater des réseaux.

Renforcez la protection de vos pare-feu

Il demeure essentiel de configurer des pare-feu, même si vous disposez d'une gestion des identités et des accès. Vous devez mettre en place des contrôles permettant de protéger le périmètre, de détecter les activités hostiles et de réagir aux menaces. Un pare-feu d'applications Web (WAF) protège les applications Web contre les attaques courantes, comme l'injection de code SQL et les attaques de script multisite.

Mettez en place une protection contre les attaques informatiques par saturation (DDoS)

Protégez les ressources et les réseaux Web contre le trafic malveillant ciblant les applications et les couches réseau pour préserver la disponibilité et l'efficacité tout en évitant l'explosion des coûts d'exploitation.

Créez un réseau microsegmenté

Les attaquants peuvent se déplacer plus facilement de manière latérale si vous avez un réseau à plat. Familiarisez-vous avec des concepts comme la mise en réseau virtuelle, la mise en service de sous-réseau et l'adressage IP. Utilisez la microsegmentation et adoptez un tout nouveau concept de microprépérimètres pour adopter une approche zéro confiance aux réseaux.

Et après?

Vous cherchez à renforcer la sécurité de vos charges de travail dans le nuage?

En savoir plus sur la sécurité sur Azure

Communiquer avec nous