



Notions de sécurité pour un serveur informatique

Description

Les pirates informatiques devenant de plus en plus malins, il est de plus en plus nécessaire de protéger vos actifs numériques et vos périphériques réseau.

Pourquoi la sécurité informatique est-elle nécessaire ?

Si la sécurité informatique peut être coûteuse, une violation importante coûte beaucoup plus cher à une organisation.

Qu'est-ce que la sécurité informatique ?

Les branches importantes peuvent mettre en péril la santé d'une petite entreprise. Pendant ou après un incident, les équipes de sécurité informatique peuvent suivre un plan de réponse aux incidents en tant qu'outil de gestion des risques pour prendre le contrôle de la situation.

Quelle est la différence entre la sécurité informatique et la sécurité de l'information (InfoSec) ?

Bien que la sécurité informatique et la sécurité de l'information se ressemblent, elles font référence à des types de sécurité différents. La sécurité de l'information fait référence aux processus et aux outils conçus pour protéger les informations commerciales sensibles contre les intrusions, tandis que la sécurité informatique fait référence à la sécurisation des données numériques, par le biais de la sécurité des réseaux informatiques.

Quelles sont les menaces pour la sécurité informatique ?

Les menaces pour la sécurité informatique peuvent prendre différentes formes. Une menace courante est le malware, ou logiciel malveillant, qui peut se présenter sous différentes formes pour

infecter les périphériques réseau, notamment :

- Ransomware
- Logiciels espions
- Virus

Ces menaces rendent encore plus importante la mise en place de pratiques de sécurité fiables. Apprenez-en davantage sur les logiciels malveillants pour rester protégé.

Quels sont les avantages de la sécurité informatique ?

La sécurité informatique prévient les menaces malveillantes et les failles de sécurité potentielles qui peuvent avoir un impact considérable sur votre entreprise. Lorsque vous entrez dans le réseau interne de votre entreprise, la sécurité informatique veille à ce que seuls les utilisateurs autorisés puissent accéder aux informations sensibles qui s'y trouvent et les modifier. La sécurité informatique permet de garantir la confidentialité des données de votre entreprise.

Types de sécurité informatique

Sécurité du réseau

La sécurité du réseau est utilisée pour empêcher les utilisateurs non autorisés ou malveillants de pénétrer dans votre réseau. Elle garantit que la confidentialité, la fiabilité et l'intégrité ne sont pas compromises. Ce type de sécurité est nécessaire pour empêcher un pirate d'accéder aux données du réseau. Il les empêche également d'affecter négativement la capacité de vos utilisateurs à accéder au réseau ou à l'utiliser. La sécurité du réseau est devenue de plus en plus difficile à mesure que les entreprises augmentent le nombre de points d'extrémité et migrent les services vers le cloud public.

Sécurité Internet

La sécurité Internet implique la protection des informations qui sont envoyées et reçues dans les navigateurs, ainsi que la sécurité du réseau impliquant des applications Web. Ces protections sont conçues pour surveiller le trafic Internet entrant à la recherche de logiciels malveillants et de trafic indésirable. Cette protection peut prendre la forme de pare-feu, de logiciels anti-malware et de logiciels anti-spyware.

Sécurité des points d'extrémité

La sécurité des points d'accès fournit une protection au niveau du dispositif. Les appareils qui peuvent être sécurisés par la sécurité des points finaux comprennent les téléphones cellulaires, les tablettes, les ordinateurs portables et les ordinateurs de bureau. La sécurité des points finaux empêchera vos appareils d'accéder à des réseaux malveillants qui pourraient constituer une menace pour votre organisation. Une protection avancée contre les logiciels malveillants et un logiciel de gestion des appareils sont des exemples de sécurité des points finaux.

S curit  du cloud

Les applications, les donn es et les identit s se d placent vers le cloud, ce qui signifie que les utilisateurs se connectent directement   Internet et ne sont pas prot g s par la pile de s curit  traditionnelle. La s curit  du cloud peut contribuer   s curiser lâ utilisation des applications SaaS (Software-as-a-Service) et du cloud public. Un CASB (cloud-access security broker), une passerelle Internet s curis e (SIG) et un UTM (cloud-based unified threat management) peuvent  tre utilis s pour la s curit  du cloud.

S curit  des applications

Avec la s curit  des applications, les applications sont sp cifiquement cod es au moment de leur cr ation pour  tre aussi s res que possible, afin de s assurer qu elles ne sont pas vuln rables aux attaques. Cette couche suppl mentaire de s curit  implique lâ  valuation du code d une application et lâ identification des vuln rabilit s qui peuvent exister dans le logiciel. Voir <https://evok.com/fr/netpro-maintenance/> pour en savoir plus sur la maintenance et le d pannage des serveurs informatiques

Categorie

1. informatique

Date

2026/04/12

date cr  e

2022/03/01

Auteur

blogueur