Notions de sÃ©curitÃ© pour un serveur informatique

Description

Les pirates informatiques devenant de plus en plus malins, il est dâ??autant plus nÃ©cessaire de protÃ©ger vos actifs numÃ©riques et vos pÃ©riphÃ©riques rÃ©seau.

Pourquoi la sÃ©curitÃ© informatique est-elle nÃ©cessaire ?

Si la sÃ©curitÃ© informatique peut Ãªtre coÃ»teuse, une violation importante coÃ»te beaucoup plus cher Ã une organisation.

Quâ??est-ce que la sÃ©curitÃ© informatique ?

Les brÃ¨ches importantes peuvent mettre en pÃ©ril la santÃ© dâ??une petite entreprise. Pendant ou aprÃ¨s un incident, les Ã©quipes de sÃ©curitÃ© informatique peuvent suivre un plan de rÃ©ponse aux incidents en tant quâ??outil de gestion des risques pour prendre le contrÃ´le de la situation.

Quelle est la diffÃ©rence entre la sÃ©curitÃ© informatique et la sÃ©curitÃ© de lâ??information (InfoSec) ?

Bien que la sÃ©curitÃ© informatique et la sÃ©curitÃ© de lâ??information se ressemblent, elles font rÃ©fÃ©rence Ã des types de sÃ©curitÃ© diffÃ©rents. La sÃ©curitÃ© de lâ??information fait rÃ©fÃ©rence aux processus et aux outils conÃ§us pour protÃ©ger les informations commerciales sensibles contre les intrusions, tandis que la sÃ©curitÃ© informatique fait rÃ©fÃ©rence Ã la sÃ©curisation des donnÃ©es numÃ©riques, par le biais de la sÃ©curitÃ© des rÃ©seaux informatiques.

Quelles sont les menaces pour la sÃ©curitÃ© informatique ?

Les menaces pour la sÃ©curitÃ© informatique peuvent prendre diffÃ©rentes formes. Une menace courante est le malware, ou logiciel malveillant, qui peut se prÃ©senter sous diffÃ©rentes formes pour

infecter les pÃ©riphÃ©riques rÃ©seau, notamment :

- Ransomware
- Logiciels espions
- Virus

Ces menaces rendent encore plus importante la mise en place de pratiques de sÃ©curitÃ© fiables. Apprenez-en davantage sur les logiciels malveillants pour rester protÃ©gÃ©.

Quels sont les avantages de la sÃ©curitÃ© informatique ?

La sÃ©curitÃ© informatique prÃ©vient les menaces malveillantes et les failles de sÃ©curitÃ© potentielles qui peuvent avoir un impact considÃ©rable sur votre entreprise. Lorsque vous entrez dans le rÃ©seau interne de votre entreprise, la sÃ©curitÃ© informatique veille Ã ce que seuls les utilisateurs autorisÃ©s puissent accÃ©der aux informations sensibles qui sâ??y trouvent et les modifier. La sÃ©curitÃ© informatique permet de garantir la confidentialitÃ© des donnÃ©es de votre entreprise.

Types de sÃ©curitÃ© informatique

SÃ©curitÃ© du rÃ©seau

La sÃ©curitÃ© du rÃ©seau est utilisÃ©e pour empÃªcher les utilisateurs non autorisÃ©s ou malveillants de pÃ©nÃ©trer dans votre rÃ©seau. Elle garantit que la convivialitÃ©, la fiabilitÃ© et lâ??intÃ©gritÃ© ne sont pas compromises. Ce type de sÃ©curitÃ© est nÃ©cessaire pour empÃªcher un pirate dâ??accÃ©der aux donnÃ©es du rÃ©seau. Il les empÃªche Ã©galement dâ??affecter nÃ©gativement la capacitÃ© de vos utilisateurs Ã accÃ©der au rÃ©seau ou Ã lâ??utiliser. La sÃ©curitÃ© du rÃ©seau est devenue de plus en plus difficile Ã mesure que les entreprises augmentent le nombre de points dâ??extrÃ©mitÃ© et migrent les services vers le cloud public.

SÃ©curitÃ© Internet

La sÃ©curitÃ© Internet implique la protection des informations qui sont envoyÃ©es et reÃ§ues dans les navigateurs, ainsi que la sÃ©curitÃ© du rÃ©seau impliquant des applications Web. Ces protections sont conÃ§ues pour surveiller le trafic Internet entrant Ã la recherche de logiciels malveillants et de trafic indÃ©sirable. Cette protection peut prendre la forme de pare-feu, de logiciels anti-malware et de logiciels anti-spyware.

SÃ©curitÃ© des points dâ??extrÃ©mitÃ©

La sÃ©curitÃ© des points dâ??accÃ¨s fournit une protection au niveau du dispositif. Les appareils qui peuvent Ãªtre sÃ©curisÃ©s par la sÃ©curitÃ© des points finaux comprennent les tÃ©lÃ©phones cellulaires, les tablettes, les ordinateurs portables et les ordinateurs de bureau. La sÃ©curitÃ© des points finaux empÃªchera vos appareils dâ??accÃ©der Ã des rÃ©seaux malveillants qui pourraient constituer une menace pour votre organisation. Une protection avancÃ©e contre les logiciels malveillants et un logiciel de gestion des appareils sont des exemples de sÃ©curitÃ© des points finaux.

SÃ©curitÃ© du cloud

Les applications, les donnÃ©es et les identitÃ©s se dÃ©placent vers le cloud, ce qui signifie que les utilisateurs se connectent directement Ã Internet et ne sont pas protÃ©gÃ©s par la pile de sÃ©curitÃ© traditionnelle. La sÃ©curitÃ© du cloud peut contribuer Ã sÃ©curiser lâ??utilisation des applications SaaS (Software-as-a-Service) et du cloud public. Un CASB (cloud-access security broker), une passerelle Internet sÃ©curisÃ©e (SIG) et un UTM (cloud-based unified threat management) peuvent Ãªtre utilisÃ©s pour la sÃ©curitÃ© du cloud.

SÃ©curitÃ© des applications

Avec la sÃ©curitÃ© des applications, les applications sont spÃ©cifiquement codÃ©es au moment de leur crÃ©ation pour Ãªtre aussi sÃ»res que possible, afin de sâ??assurer quâ??elles ne sont pas vulnÃ©rables aux attaques. Cette couche supplÃ©mentaire de sÃ©curitÃ© implique lâ??Ã©valuation du code dâ??une application et lâ??identification des vulnÃ©rabilitÃ©s qui peuvent exister dans le logiciel. Voir https://evok.com/fr/netpro-maintenance/ pour en savoir plus sur la maintenance et le dÃ©pannage des serveurs informatiques

Categorie

1. informatique

Date
2026/05/28
date crÃ©Ã©e
2022/03/01
Auteur
blogueur