

Renforcement de la Sécurité du Système d'Information de GSB



Introduction:

Dans le cadre de la mission du service informatique de GSB, nous sommes amenés à proposer des solutions renforçant la sécurité des systèmes d'information. Le laboratoire dispose de plusieurs serveurs équipés du système d'exploitation Windows Server 2019, ainsi que de postes de travail fonctionnant sous Windows 7/10. Ce document décrit différentes solutions de sécurité existantes pour atteindre cet objectif.

Solution de sécurité:

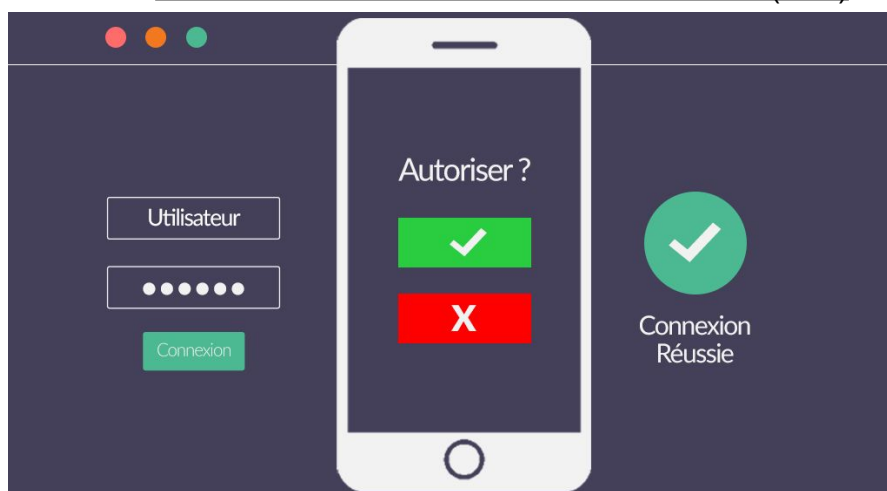
Solution 1: Antivirus



L'installation d'un logiciel antivirus et anti-malware sur tous les postes de travail et serveurs peut aider à détecter, neutraliser ou éradiquer les logiciels malveillants des ordinateurs, notamment les virus et les chevaux de Troie. Les logiciels antivirus et anti-malware sont disponibles auprès de nombreux fournisseurs, tels que McAfee, Norton et Microsoft Defender.

<https://www.netexplorer.fr/blog/a-quoi-sert-antivirus-comment-utiliser/>

Solution 2: Authentification à deux facteurs (2FA)

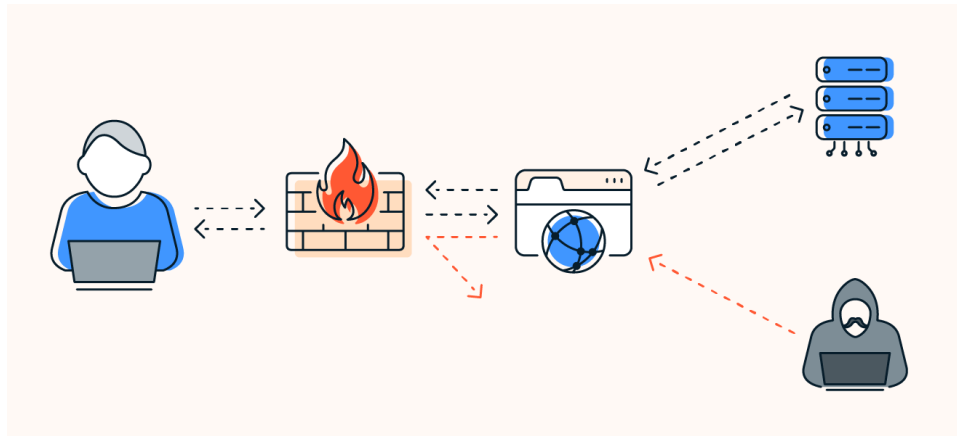


La mise en œuvre de l'authentification à deux facteurs augmente considérablement la sécurité des comptes utilisateur en nécessite non seulement un mot de passe robuste (minuscules, majuscules, chiffres, caractères spéciaux) mais une deuxième forme d'authentification (telle qu'un code PIN ou une empreinte

digitale). Les méthodes d'authentification à deux facteurs sont de plus en plus courantes dans les pratiques modernes de sécurité informatique.

<https://www.blogdumoderateur.com/double-authentification-definition-methodes-connaître/>

Solution 3: Par-feu



L'installation d'un pare-feu matériel ou logiciel, de type SaaS (logiciels utilisés comme un service), ou hébergé dans un cloud public ou privé (virtuel). dédié peut aider à filtrer le trafic entrant et sortant afin de prévenir les intrusions. Le pare-feu peut être configuré pour bloquer les ports inutilisés et surveiller le trafic réseau en temps réel.

https://www.cisco.com/c/fr_fr/products/security/firewalls/what-is-a-firewall.html

Solution 4: Mise à jour



S'assurer que tous les serveurs Windows Server 2019 et les postes de travail Windows 7/10 sont régulièrement mis à jour avec les derniers correctifs de sécurité est essentiel pour se protéger contre les vulnérabilités connues et moins vulnérable en cas d'attaque la mise à jour est une règle de sécurité à ne pas négliger.

<https://www.exodata.fr/blog/renforcer-securite-informatique-entreprise#a>

Solution 5: Sensibiliser les employés à la sécurité informatique

Charte Informatique



S'assurer que tous les employés doivent être largement sensibilisés aux bonnes pratiques de la cybersécurité, pour informer qui faudrait pas utiliser par exemple ces données personnels sur les pc professionnels, ne pas cliquer sur des liens suspects qui pourraient causer des failles sur le pc.

<https://www.exodata.fr/blog/renforcer-securite-informatique-entreprise#b>

Conclusion

Pour conclure, il est essentiel pour GSB de mettre en place des mesures de sécurité pour protéger son système d'information contre les intrusions. Chaque solution présentée ci-dessus apporte une couche supplémentaire de sécurité, et la combinaison de plusieurs de ces solutions peut renforcer de manière très importante la sécurité globale du réseau.

Je recommande à GSB de faire une approche pour toutes les solutions que j'ai indiquées qui pourraient éviter des menaces importantes car les solutions présentées sont gratuites après il y a les versions payantes mais les versions gratuites pourraient nous servir si les employés respectent la charte informatique.