La sécurité de l'accès

Le télétravail à été promu à raison de la pandémie de COVID-19 par le gouvernement Français pour toutes les entreprises où leurs employées pouvaient effectuer leur travail à distance durant le confinement de mars-mai 2020 ainsi que d'octobre à décembre 2020. Le télétravail consiste à pouvoir travailler en dehors des locaux de l'entreprise tout en ayant accès au réseau de celle-ci. Ce changement massif et rapide d'organisation du travail pour de nombreuses entreprises pose alors des questionnements ainsi que de potentiels et réels problèmes sur la sécurité des accès au réseau des entreprises par les employées alors distants de celui-ci. La sécurisation de l'accès est un aspect important pour le système d'information car celui-ci est le patrimoine essentiel d'une organisation. Cette sécurisation peut se découper en 3 grands piliers qui sont la confidentialité, l'authentification et les habilitations.

La confidentialité :

La confidentialité est le fait de s'assurer que l'information n'est accessible qu'à ceux donc l'accès est autorisé pour ce faire de nombreuses solutions existent pour se connecter au réseau et système de l'entreprise de manière sécurisée.

- Le chiffrement des données transmises entre le poste de travail et le réseau de l'entreprise peut être effectué avec un réseau privé virtuel (VPN). Un VPN permet de cryptées les données qui circulent sur un réseau de télécommunications publiques afin que si une personne non autorisée intercepte celle-ci, il ne pourras pas les exploiter.
- La connexion d'un utilisateur à distance peut aussi s'effectuer sans avoir besoin de VPN traditionnelles comme avec le DirectAccess. Le DirectAccess permet à un ordinateur d'être toujours connectés à l'organisation au quelle elle appartient. L'utilisateur n'as pas besoin de faire de manipulation afin de se connecter à celui-ci. Direct Access est protégé au niveau réseau par SSL en cas d'utilisation IP-HTTPS, d'IPsec dans tous les cas. Mais aussi au niveau des authentification avec des comptes AD pour authentifier l'utilisateur, des certificat pour authentifier l'ordinateur.
- Le cloud computing est une technologie qui permet à chaque employé au sein d'une entreprise de travailler de n'importe quel endroit à partir du moment où il dispose d'une connexion internet suffisante. Le cloud computing permet de renforcer la sécurité des données de l'entreprise. Cette technologie est même plus sécuritaire qu'un serveur physique (de type NAS par exemple). Le cloud peut permettre aussi d'avoir un serveur non matériel, évitant tout risque de pertes de données lors d'incendies ou d'accidents physiques.
- Mais aussi divers équipement physique comme un pare-feu permettent de garantir le respect d'une politique de traitement des flux de données prédéfinies au niveau protocolaire TCP/IP, mais aussi l'utilisation de composant logique comme un proxy afin de traiter les données au niveau applicatif.

L'authentification et l'habilitation :

L'authentification est un processus permettant au système de s'assurer de la légitimité de la demande d'accès faite par quelqu'un ou un autre système afin d'autoriser l'accès de cette entité à

des ressources du système. A celle ci ce couple l'habilitation qui est un ensemble de droit donnés à certains comptes utilisateurs afin de s'assurer qu'il n'est accès seulement à ce qu'ils ont besoin.

- L'utilisation de compte identifiant ainsi que de mot de passe pour pouvoir se connecter doit pour être efficace utilisé une stratégie de mots de passe forte afin que les exigences en matière de longueur et complexité soit respecter et ainsi rendre difficiles le cassage des mots de passe.
- L'utilisation de connexion à double facteur afin de pouvoir augmenter le niveau de certitude que l'utilisateur qui essaye de se connecter et bien l'utilisateur légitime.
- Au niveau des habilitations, il faut s'assurer qu'il n'y est aucuns comptes périmés ou inutilisés, que les droits attribués aux comptes ne soit pas excessifs et régler au mieux les stratégies de groupe afin d'être adaptées aux besoins.

Chaque entreprise doit donc sécuriser ses connexions qui viennent des employées à l'extérieur du réseau afin de réduire les risques de cybercrimes contre le patrimoine informatique de l'entreprise lié au télétravail pour éviter que l'entreprise ne subissent d'impact négatif.

Sources :

https://www.netwrix.fr/remote_access_security_best_practices.html

https://docs.vmware.com/fr/VMware-Horizon-7/7.13/horizon-administration/GUID-D85363FF-D343-4853-AAD0-D4ACB2255C3B.html

https://alexis-bonnecaze.pedaweb.univ-amu.fr/HUGo/Cours6.pdf

https://cloud.unova.fr/cloud-teletravail/

https://docs.microsoft.com/fr-fr/windows-server/remote/remote-access/remote-access

https://docs.microsoft.com/fr-fr/windows-server/remote/remote-access/directaccess/directaccess

SIO 1 2022 - LEROY Alexandre & ADEKOYA Esther

From:
https://wiki.sio.bts/ - **WIKI SIO : DEPUIS 2017**

Permanent link:
https://wiki.sio.bts/doku.php?id=tt_secu_acces

Last update: **2021/01/04 15:36**