Sécurisation de l'accès à distance des prestataires

Un prestataire doit disposer d'un accès à distance sécurisé pour **assurer la maintenance, l'administration** (**télémaintenance**) ou pour **assister les utilisateurs** (**téléassistance**) des solutions dont il est contractuellement responsable au sein des structures. **Il doit ainsi utiliser le bastion ou l'accès VPN de la structure**. Le CERT Santé recommande la contractualisation de clauses de sécurité basées sur les exigences présentées dans cette fiche.

Exigences spécifiques à un accès par bastion unique ou par VPN

- Le prestataire **s'engage à réaliser des connexions au travers de son adresse IP publique** (afin d'avoir une traçabilité des connexions vers les structures en particulier dans le cas de comptes génériques). La structure devra appliquer un filtrage pour que seule l'adresse IP publique du prestataire soit autorisée à se connecter avec le compte donné.
- Le VPN/bastion ainsi que les solutions administrées **doivent être à jour au niveau des correctifs de sécurité** ;
- Le prestataire utilise **des comptes locaux sans lien avec l'Active Directory (AD) de la structure** et avec une authentification forte (privilégier l'utilisation d'algorithmes de chiffrement asymétriques tel que préconisée par l'ANSSI) ; Dans le cas où le prestataire est contraint d'utiliser un compte AD, il doit impérativement mettre en place une authentification à deux facteurs dont le secret qui permet la génération du second facteur ne soit pas dans l'AD. De plus, ce compte AD ne doit avoir aucun privilège sur le SI.
- Lorsque les connexions vers les machines à administrer par le prestataire sont configurées pour être activées automatiquement, **elles doivent de préférence utiliser le compte administrateur local de la machine cible. En aucun cas, il ne faut utiliser un compte à privilèges sur l'ensemble du SI (ex : admin domaine).**
- **La structure désactive par défaut le compte du prestataire.** Ce dernier doit contacter la structure afin de lui indiquer qu'il va réaliser une opération de maintenance afin de l'activer pour la durée nécessaire. Si cela n'est pas possible, alors le prestataire appelle la structure lorsqu'il veut se connecter et la structure qui est seule à connaître le second facteur d'authentification (OTP), qui est unique et avec une durée de vie limitée, lui communique à ce moment-là. Si ces modes opératoires ne sont pas possibles, la structure paramètre des règles de filtrage pour bloquer les accès en dehors des heures ouvrables.
- **La structure génère des logs permettant d'identifier les connexions** (login), depuis où (adresse IP), l'heure, ainsi que la durée de la session. Ces journaux doivent être conservés pendant un délai de rétention (6 mois de préférence en les centralisant). Cela s'applique également au prestataire dans le cas de l'utilisation de compte générique.

Exigences générales pour la télémaintenance

- **Le prestataire ne doit avoir accès qu'aux machines dont il a la charge avec les droits appropriés** (simple utilisateur à admin local maximum) **de préférence avec une authentification forte**. La structure doit mettre en place des règles de filtrage réseau (micro-segmentation), authentification composée (compound authentication) dans les politiques AD, afin que le prestataire ne puisse en aucun cas accéder aux canaux d'administration (ssh, rdp, psexec, winrm, wmi, vnc...) des ressources dont il n'a pas la charge.
- **Le prestataire doit protéger le stockage de tous les secrets de la structure avec une solution sécurisée** (ex : keepass) et ils ne doivent jamais être enregistrés dans les applications utilisées pour l'administration du SI (ex : navigateur, putty, cloud, ...);
- **Les serveurs administrés ne doivent pas avoir accès à internet en sortie à l'exception des flux strictement nécessaires par le biais d'une liste blanche** ;
- **En cas de supervision de ses serveurs par le prestataire, il doit utiliser un canal différent de celui de la télémaintenance.** Celui-ci doit fournir la matrice de flux vers internet. Une inspection TLS pourra être réalisée par la structure afin d'éviter la création d'un tunnel de contrôle et vérifier la légitimité du flux. La configuration de l'agent de supervision doit être statique (aucune demande dynamique depuis le serveur vers l'agent ne doit pouvoir avoir lieu).

Sécurisation de l'accès à distance des prestataires

Exigences pour la téléassistance

- **La téléassistance doit être uniquement activée lorsque l'informaticien de la structure a besoin d'un appui** dans une tâche qu'il ne maîtrise pas ou afin de le former. Elle ne doit pas être mise en œuvre pour réaliser des opérations de télémaintenance.
- **Dans le cadre de l'administration avec des machines dédiées, il ne doit pas être possible pour un poste d'administration du SI (dans la structure) d'installer un outil de prise en main à distance** (ex : Teamviewer, Anydesk, ...) ou d'utiliser un partage d'écran via une application de bureautique non dédiée à l'administration (ex : Teams). Il faut donc mettre un outil de partage d'écran en DMZ (comme indiqué dans la documentation de l'ANSSI). Il existe des outils « légers » en open-source basés sur « webrtc » (webrtc screen sharing) pour réaliser ce type de solution.
- **La solution de prise en main à distance ou de partage de bureau devra respecter les règles suivantes :**
    - On privilégiera le partage d'écran à la prise de main à distance quand cette dernière n'est pas nécessaire ;
    - **Le poste de téléassistance n'est pas dans le VLAN d'administration et n'a pas accès aux canaux d'administration du SI** ;
    - **Aucun compte à privilèges sur le SI ne doit être utilisé sur le poste** (seulement utilisateur simple à admin local maximum) ;
    - L'outil de téléassistance doit obligatoirement être activé suite à une validation manuelle de l'utilisateur pour ouvrir la session d'assistance ;
    - Si les opérations d'assistance ne sont pas fréquentes, l'outil de téléassistance sera désinstallé après utilisation, dans le cas contraire, on vérifiera que celui-ci n'est pas lancé par défaut au démarrage de la machine (autorun) ;
    - La structure doit rester derrière son écran pour contrôler les actions de l'intervenant ;
    - La solution de téléassistance doit permettre à la structure d'identifier avec certitude la personne qui demande l'ouverture d'une session ;
    - La solution de téléassistance doit être maintenue à jour des correctifs de sécurité durant tout le temps où elle sera mise en œuvre sur le poste de l'utilisateur.

- La solution de téléassistance doit permettre une traçabilité des connexions ainsi que des actions réalisées lors des connexions.

Références

1. https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-la-tele-assistance/
2. https://esante.gouv.fr/sites/default/files/media_entity/documents/pgssi_regles_intervention_distance_v1.0.pdf
3. https://us-cert.cisa.gov/ncas/alerts/aa21-042a
4. https://learn.microsoft.com/fr-fr/windows-server/identity/ad-fs/operations/ad-fs-compound-authentication-and-ad-ds-claims