# 3 préconisations techniques

Pour améliorer la cybersécurité de l'entreprise

# I – Poste d'administration

- En tant que point d’entrée du système d’information pour l’administration, le poste de travail de l’administrateur constitue par nature un composant critique. Il bénéficie d’accès étendus et privilégiés et manipule souvent des informations sensibles, telles que des configurations, des dossiers d’architecture, des versions logicielles déployées ou encore des mots de passe. De plus, il possède la capacité technique d’accéder à certaines données métiers. À ce titre, il doit faire l’objet d’une sécurisation renforcée, tant sur le plan physique que logiciel, afin de limiter au maximum les risques de compromission.
- L’accès à Internet accroît considérablement la surface d’exposition aux menaces et ouvre la voie à de nombreux vecteurs d’attaque : navigation Web, courriels, téléchargement ou exécution de programmes, etc. Dans ce contexte, il est particulièrement difficile de garantir l’intégrité d’un poste connecté à Internet.

- Bloquer tout accès à Internet depuis ou vers le poste d’administration

Le poste d’administration ne doit en aucun cas être relié à Internet. Cette interdiction concerne notamment la navigation Web et l’utilisation de messageries électroniques connectées, même lorsque ces services sont protégés par des passerelles sécurisées.

Ainsi, tout accès à Internet ou aux comptes de messagerie électronique doit être exclusivement réservé aux environnements bureautiques, eux-mêmes protégés par un filtrage via les passerelles d’accès Internet de l’organisation.

Le disque dur d’un poste d’administration peut contenir des informations sensibles permettant l’accès au système d’information. En cas de perte ou de vol de l’équipement, ces données pourraient être compromises, entraînant un risque majeur pour la sécurité.

# II - Réseau d'administration

- Le réseau d’administration correspond au réseau de communication par lequel transitent les flux internes du système d’information d’administration ainsi que les flux nécessaires à la gestion des ressources administrées. Compte tenu de sa sensibilité, ce réseau doit bénéficier de mesures de sécurisation spécifiques, définies en cohérence avec l’analyse de risques et les objectifs de sécurité établis.
- Les ressources d’administration (telles que les postes d’administration et les serveurs outils) doivent être déployées sur un réseau physiquement dédié à cet usage. Lorsque cela est possible, il est également recommandé de mettre en place une authentification des postes d’administration afin de contrôler et sécuriser leur accès au réseau d’administration.
- À défaut de pouvoir disposer d’un réseau physique dédié, les ressources d’administration doivent être isolées sur un réseau logique spécifique, en s’appuyant sur des mécanismes de chiffrement et d’authentification tels que le protocole IPsec. En complément, il est recommandé de mettre en place une segmentation logique (VLAN) ainsi que des règles de filtrage réseau, afin de restreindre l’exposition du concentrateur VPN IPsec aux seuls postes d’administration autorisés.

# III – Sauvegarde, journalisation et supervision de la sécurité

- Comme pour tout système d'information, il est essentiel de définir une politique de sauvegarde spécifique au SI d'administration afin de garantir la continuité du service en cas d'incident ou de compromission. Cette politique doit préciser les éléments à sauvegarder, l'emplacement des sauvegardes ainsi que les droits d'accès associés. Les sauvegardes doivent être effectuées de manière régulière, tandis que les procédures de restauration doivent être documentées, maintenues à jour et testées périodiquement.
- Afin de faire face à une éventuelle corruption ou indisponibilité des données provoquée par un incident ou une compromission, une politique de sauvegarde doit être définie et appliquée au SI d'administration. Pour les éléments les plus critiques, il est recommandé de prévoir des sauvegardes hors ligne, offrant une protection supplémentaire contre les attaques ciblant les systèmes connectés.
- La journalisation des événements techniques, notamment ceux liés à la sécurité, ainsi que leur analyse régulière, constitue un élément essentiel pour détecter une compromission éventuelle du système d'information. L'archivage de ces journaux facilite par ailleurs les investigations numériques visant à comprendre les causes et modalités d'une intrusion.
- Ainsi, les besoins en journalisation du SI administré et du SI d'administration doivent être intégrés dès la phase de conception du SI d'administration. Une zone spécifique doit être dédiée aux services de journalisation afin de garantir la pertinence et l'intégrité des journaux, depuis leur génération jusqu'à leur stockage.
- En cas d'intrusion, un attaquant cherchera généralement à effacer ou modifier ces traces afin de masquer sa présence. Pour limiter ce risque, il est indispensable de cloisonner les services de journalisation et de restreindre strictement l'accès aux journaux aux seules personnes disposant d'un besoin légitime.