Annexe 5 - Exigences de sécurité pour l'hébergement des données

Ces exigences concernent l'hébergement de toutes les applications et données **« Confidentielles » (IC)** ou **« Strictement confidentielles » (ISC)** se trouvant dans n'importe quel lieu qui n'est pas la propriété de BT ou qui n'est pas géré par BT. Il s'agit notamment, sans exclusivité, des Services Cloud où a) les données en transit sont sécurisées et protégées contre une interception, généralement grâce à un protocole chiffré et b) les données de BT sont chiffrées pendant leur stockage dans le service Cloud.

Les conditions suivantes concernent les applications et les données Confidentielles hébergées en dehors des locaux de BT :

- Le Centre de données doit détenir une certification ISO 27001 en cours de validité (ou une (des) certification(s) prouvant des contrôles équivalents) pour la gestion de la sécurité ou devra se conformer aux Exigences de sécurité de la certification ISO 27001 ou de politiques de sécurité conformes à ISO 27001 et/ou travailler à l'élaboration d'une politique conforme à ISO 27001 dans des délais convenus avec BT.
- Les données en cours de transfert doivent être fortement cryptées, afin de protéger les données de BT entre le point où elles quittent BT et la frontière du contrôleur de domaine (généralement l'équilibreur de charge et le dispositif de déchiffrement situé derrière le pare-feu de la frontière du contrôleur de domaine).
- Les techniciens du contrôleur de charge qui disposent d'un accès physique aux serveurs ne doivent pas avoir d'accès logique à l'environnement de production et les administrateurs possédant un accès logique aux systèmes ne doivent pas avoir d'accès physique au contrôleur de domaine.
- Tous les accès logiques doivent être contrôlés par un système de sécurité des comptes, afin de s'assurer que la gestion des mots de passe est contrôlée et que le processus approprié d'autorisation est mis en œuvre, permettant de valider l'identité du demandeur, par ex. CyberArk.
- Pour un accès privilégié (notamment, mais sans exclusivité, DBA), la gestion des mots de passe doit être limitée dans le temps et, dans la mesure du possible, mettre en œuvre des restrictions supplémentaires sur l'adresse IP source.
- Tout accès privilégié, par ex. DBA, ASG etc. aux systèmes qui traitent des informations de BT doit être conforme aux exigences de l'Annexe 1 - Classification des informations.
- Pour un accès à distance, il faut impérativement utiliser un Réseau privé virtuel associé à une authentification par profil à deux facteurs. En outre, tous les accès privilégiés à distance de tiers ne doivent permettre d'accéder qu'aux systèmes où les données de BT sont en cours de transfert ou sont stockées, dans le même pays que le contrôleur de domaine, ou un pays ou un territoire qui garantit un degré de protection adéquat pour les données de BT.
- Mettre en œuvre des processus de gestion des clés cryptographiques sur la totalité du cycle de vie, qui sont compatibles avec les bonnes pratiques du secteur.
- Tout accès physique à des lieux ou des équipements où sont stockées ou traitées des informations de BT doit bénéficier d'un processus permettant un audit, par ex. demande de modification, pour s'assurer que l'accès n'est accordé que pour la durée minimum requise, c.-à-d. pas d'accès permanent.
- Les données de sauvegarde stockées hors site doivent être chiffrées conformément aux exigences de l'Annexe 1.

- Des contrôles doivent être en place afin de minimiser, détecter et prévenir les accès non autorisés. Ces contrôles doivent créer une piste d'audit, en se basant sur le principe « Qui, quoi, quand, où ».
- Qui était l'utilisateur, par ex. identifiant du compte utilisateur.
- À quel actif il a accédé, par ex. des données.
- Depuis où il a accédé à l'actif, par ex. adresse IP.
- Quand, par ex. horodatage.
- Tous les accès physiques et logiques doivent être enregistrés, avec des fichiers journaux qui sont conservés pendant 1 an (au moins).
- En cas de violation où les données de BT sont compromises, volées ou modifiées, un processus doit être en place afin de s'assurer que BT est informé dans un délai raisonnable et avec un degré de détail suffisant.

Pour les informations Strictement confidentielles, les principes suivants s'appliquent :

- Le centre de données doit subir une inspection de sécurité sur site.
- Les serveurs d'applications, les bases de données, etc. doivent être sur des infrastructures dédiées, qui n'ont pas plusieurs locataires, et doivent être hébergés sur un bâti dédié, dans une cage sécurisée. Si cette exigence n'est pas satisfaite, une Évaluation des risques de BT devra permettre de garantir la séparation adéquate des données de BT de celles des autres clients partageant le même environnement, en veillant à ce que les Administrateurs des bases de données ne puissent pas se connecter aux instances des clients et ne puissent pas voir les données des clients sous forme compilée. Les tables et les rangées des bases de données ne doivent pas refléter la vue d'une instance d'un seul client.
- Des processus doivent être en place pour s'assurer que les données strictement confidentielles sont supprimées de manière sécurisée à la fin de leur cycle de vie sur le cloud. Toutes les données strictement confidentielles que contiennent les supports de stockage doivent être effacées/supprimées conformément à l'Annexe 1.