

# Modèle de Note Corporate GSB

Référence :

GSB/SI/USB-1546

Date :

12/04/2023

De :

Stagiaire SI

À :

DSI

Pièce jointe :

...

Objet :

RAPPORT D'INCIDENT LOG N°437 - Risque brèche de sécurité

## 1. Contexte et Constat

### 📌 Situation actuelle

Le 12/04/2023 à 16h42, une alerte de sécurité s'est produit et a détecter un risque de connexion non identifie a été détectée sur le poste de travail au département R&D, au poste N°42.

Un collaborateur a connecter une clé USB qui s'affaire une clé USB personnelle non déclaré dans le département R&D connecter aux poste pour se connecter au projet "domaine numérique". Due a cette alerte, le serveur du département R&D a été mis en isolation c du réseaux afin que aucun donnée ne fuite.

Fort heureusement, aucun risque de malware a été trouve et aucun fuite de données aussi mais cela a constitue une violation dans la politique de sécurité dans l'entreprise GSB.

### 📌 Domaine d'analyse

Voici les recommandation après l'enquête interne avec plusieurs collègue enquêteur :

- Interdire l'utilisation de tout support USB personnelle dans l'ensemble de l'établissement GSB ou faire une demande au préalable à son supérieur pour obtenir l'autorisation et devra être contrôlé régulièrement.
- Déployer des clé USB sécurisées et chiffrée fournis par l'entreprise afin que plus personnes l'emporte leur clé USB personnelle, ce-qui pourra mieux grandir la sécurité des serveurs des différent département.
- Procédé à l'installation d'un outil de blocage automatique aux ports USB, si une clé USB est braché mais qui est non identifié, l'outil bloque tout accès à la clé. En cas il s'agit d'une clé USB fournis par l'entreprise, doit être signalé à son supérieur hiérarchique.

## 2. Analyse

---

### 📌 Éléments identifiés

Les éléments identifiés sont les suivants:

- Présence de support/clé USB personnel non identifié sans demande préalable.
- Absence de chiffrement et sécurité au périphérique.
- Manque de formation aux risques liés aux supports (clé USB)
- Non respect de la conformité aux exigences de protection des données du département R&D (BPF, EMA).

#### Point important 1

Risque élevé : infection.

Les clé USB non contrôlée peuvent contenir un malware, cheval de Troie ou autre type dormant capable d'infecter le serveur et le réseau interne du département R&D jusqu'à la paralysie.

#### Point important 2

Risque moyen : Fuite de données.

Les fichiers présents sur le poste de travail peuvent être copiés sans trace par un employé révoltant cherchant à faire du chantage, ce qui peut compromettre les documents ou données qui sont à la propriété intellectuelle de l'entreprise GSB.

#### Point important 3

Risque faible : Non respect des conformités réglementaires.

L'absence de contrôle régulier concernant les supports de type amovible (clé USB) peut entraîner des risques non favorables pour l'entreprise (FDA, EMA).

## 3. Recommandations

---

### 📌 Proposition d'action

Voici les recommandation après l'enquête interne avec plusieurs collègue enquêteur :

- Interdire l'utilisation de tout support USB personnelle dans l'ensemble de l'établissement GSB ou faire une demande au préalable à son supérieur pour obtenir l'autorisation et devra être contrôlé régulièrement.
- Déployer des clé USB sécurisées et chiffrée fournis par l'entreprise afin que plus personnes l'emporte leur clé USB personnelle, ce-qui pourra mieux grandir la sécurité des serveurs des différent département.
- Procédé à l'installation d'un outil de blocage automatique aux ports USB, si une clé USB est braché mais qui est non identifié, l'outil bloque tout accès à la clé. En cas il s'agit d'une clé USB fournis par l'entreprise, doit être signalé à son supérieur hiérarchique.

#### Action prioritaire 1

**HAUT PRIORITAIRE** : Mise en place du blocage des clé USB

Niveau : Haut

Responsable : RSI (Responsable Service Informatique)

Délai : 30 jours

Détail : Installer un système de contrôle aux ports USB permettant d'autoriser uniquement les clé USB fourni par l'entreprise USB.

#### Action prioritaire 2

**MOYENNE PRIORITAIRE** : Fourniture de clés USB sécurisées

Niveau : Moyen

Responsable : SI (Service Informatique)

Délai : 45 jours

Détails : Fournir des support de type clé USB sécurisé aux employé dans l'entreprise GSB ou au membre affecte a des projet sensible. Mais a en fournir en premier au département R&D.

#### Action complémentaire

**FAIBLE PRIORITAIRE** : Sensibilisation du personnel

Niveau : Faible

Responsable : SF (Service Formation)

Délai : 60 jours

Détail : Mettre en place une formation pour sensibilise les risques de sécurité et mettre en place un atelier internes sur les donnees pratique cyber.

## 4. Conclusion

L'incident LOG N°437 à représenter une alerte majeur concernant la protection des données au sein de l'établissement GSB. Même si aucun dommage à été détecter et constaté, l'usage de clé USB personnelle non autorisé peut constitué un risque haute pour la sécurité du SI (Service Informatique) et pour la propriété intellectuelle de l'entreprise GSB.

Cela permettra de :

- Renforcer la sécurité dans le département R&D.
- Limiter les risques d'infections par malware ou/et aux fuites de données
- Grandir la conformité des pratique interne et aux standards du règlement du EMA, CFR et CERTA

**Pour le service émetteur**

**Vu et approuvé**

Nom et prénom

Nom et prénom

Fonction

Fonction

CONFIDENTIEL – Usage interne GSB uniquement