Fadi Alouani

BTS SIO 1
groupe 1
ATELIER
26/11/25

Atelier 10 : TP2 Sécurité informatique

Sommaire

Introduction

Dans le cadre de ce TP, nous devions réaliser un compte rendu comprenant le cahier des charges de l'atelier, la préparation d'un jeu de rôle et l'analyse associée. Chaque étudiant doit choisir un rôle parmi ceux proposés, ou intervenir en tant qu'observateur, puis remplir la fiche correspondante. L'objectif de cette activité est de nous entraîner à préparer et animer une réunion, à analyser les interactions entre différents intervenants et à développer nos compétences de communication professionnelle. Ce compte rendu rassemble l'ensemble des éléments nécessaires au déroulement du TP ainsi que les documents complétés.

Fadi Alouani

Analyse et préparation

Notes préparatoires pour la rédaction de la note

. Risques liés aux clés USB chez GSB

Risques identifiés dans le secteur pharmaceutique :
Intrusion / malware via clés USB = risque élevé
Vol de propriété intellectuelle (formules, résultats d'essais, brevets) = risque très élevé.
Perte ou fuite de données sensibles
Non-conformité réglementaire .
Espionnage
Erreur humaine (utilisation de clés non autorisées, absence de chiffrement.)

. **Données sensibles manipulées chez GSB**

Formules chimiques brevetées
Données d'essais cliniques
Prototypes de molécules
Documents réglementaires
Données médicales de patients (RGPD)

. **Métiers impliqués**

RSSI (Responsable sécurité)
Ingénieur cybersécurité
Administrateur systèmes / réseaux
Technicien support
Chef de projet SSI

. **Mesures adaptées au contexte pharmaceutique**

Interdiction stricte utilisation de clés USB personnelles
seulement les clés GSB chiffrées sont autorisées
Contrôle d'accès basé sur les rôles
Traçabilité + journalisation des transferts
Validation DSI obligatoire
Alternative : plateformes sécurisées GSB pour l'échange de données

Fadi Alouani

Note Corporate GSB

Référence :GSB/DSI/SEC-USB/2025-01

Date :26/11/2025

Objet : Renforcement de la politique d'usage des clés USB au sein de GSB

De : FADI ALOUANI

À : Directeur des Systèmes d'Information

Pièces jointes :

1. CONTEXTE ET CONSTAT

Suite à l'incident récent impliquant une clé USB non autorisée ayant potentiellement exposé des données sensibles liées à un nouveau principe actif, une analyse de sécurité a révélé des pratiques hétérogènes concernant l'utilisation des périphériques USB au sein de GSB. Ce type d'incident représente un risque majeur dans un environnement pharmaceutique soumis aux réglementations FDA 21 CFR Part 11, BPF et aux obligations de protection de la propriété intellectuelle. Données d'analyse Les travaux du CNRS, les alertes CERTA ainsi que les enseignements du documentaire La Guerre Invisible confirment la vulnérabilité des entreprises face aux attaques via périphériques amovibles. Les métiers R&D, production et qualité sont particulièrement exposés en raison du volume et de la criticité des données manipulées.

2. ANALYSE

Éléments identifiés

Détailler les éléments identifiés, problèmes ou opportunités...

Risque de fuite de données de recherche Les clés USB non contrôlées facilitent l'exfiltration de formules chimiques, données d'essais cliniques ou documents réglementaires. L'impact potentiel inclut des pertes financières majeures, atteintes à la conformité FDA/EMA et risques pour la propriété intellectuelle.

HAUTE

Décrire le premier point important...

Introduction de malware via périphérique amovible Les clés USB constituent un vecteur d'attaque privilégié pour introduire ransomware ou chevaux de Troie dans les infrastructures R&D et production, pouvant interrompre les processus critiques.

MOYENNE

Décrire le deuxième point important...

Méconnaissance des procédures internes Une partie des collaborateurs n'a pas connaissance des règles strictes de la charte GSB (article 4), augmentant le risque de mauvaise manipulation ou de non-respect involontaire.

FAIBLE

Décrire le troisième point important...

.

3. RECOMMANDATIONS

Propositions d'action Afin de réduire les risques, il est proposé de renforcer la politique d'usage des supports amovibles, en s'appuyant sur les règles existantes et les meilleures pratiques CERTA. Plan d'action proposé

Présenter les recommandations générales et objectifs...

Plan d'action proposé

Action prioritaire 1

Responsable : RSSI Échéance : 30 jours HAUTE

Objet : Interdiction automatique des clés USB non GSB et déploiement de clés chiffrées standardisées. Description : Blocage par défaut via GPO ; attribution de clés AES-256 GSB..

Action prioritaire 2

Responsable : Chef de projet SSI Échéance : 60 jours MOYENNE

Objet : Mise en place d'une plateforme interne sécurisée pour le transfert de données entre chercheurs et techniciens. Description : Partage sécurisé évitant le recours aux périphériques amovibles..

Action complémentaire

Responsable : RH + DSI Échéance: 90 jours FAIBLE

Objet : Formation obligatoire R&D et production sur l'usage sécurisé des supports et la cybersécurité. .

4. CONCLUSION

Les risques liés à l'usage de clés USB présentent un impact critique pour GSB, particulièrement en matière de propriété intellectuelle, conformité réglementaire et intégrité des données de recherche. La mise en place de mesures renforcées (interdiction des périphériques non autorisés, chiffrement systématique, alternatives sécurisées et formation) permettra d'assurer la protection des données sensibles et le respect des normes FDA/EMA. Les prochaines étapes consistent à valider ce plan d'action, lancer le déploiement des mesures techniques et organiser les sessions de sensibilisation. .

Pour le service émetteur	Vu et approuvé
[un autre eleve]	**[un autre eleve]**
[Fonction]	[Fonction]

Fadi Alouani

Jeu de rôle fiche préparatoire :

Introduction: j'ai choisi animateur de réunion(role1)

Bonjour à tous, merci d'avoir pris le temps pour cette réunion.
Si nous sommes réunis aujourd'hui, c'est suite à l'incident de la semaine dernière : un poste de production a été compromis après l'utilisation d'une clé USB non autorisée.
Même si les conséquences ont pu être contenues rapidement, l'incident a mis en lumière plusieurs vulnérabilités dans nos pratiques internes.
Dans un groupe pharmaceutique comme Galaxy Swiss Bourdin, la sécurité informatique est directement liée à trois enjeux majeurs :

- la protection de notre propriété intellectuelle, notamment sur les molécules en développement,
- la conformité FDA/EMA, qui impose une traçabilité stricte,
- la continuité de nos opérations, particulièrement en R&D et en production.

Je vais aujourd'hui vous présenter trois recommandations pour éviter que ce type d'incident ne se reproduise, tout en respectant vos impératifs métiers.

Présentation des 3 recommandations
Voici les trois mesures que je propose :
1 Blocage des périphériques USB non autorisés
Les ports USB resteront actifs uniquement pour des clés chiffrées et enregistrées.
Objectif : empêcher toute introduction de malware ou fuite de données.
2 Mise en place d'une plateforme sécurisée pour les échanges de fichiers
Un espace dédié, chiffré et synchronisé avec nos partenaires externes.
Objectif : remplacer les transferts USB par un canal conforme et traçable.
3 Sensibilisation obligatoire pour les équipes R&D et Production
Une courte formation (30 min) pour comprendre les risques concrets et les bonnes pratiques.
Objectif : réduire les erreurs humaines, qui représentent 80 % des incidents.
Ces mesures peuvent être déployées progressivement pour limiter l'impact sur la productivité.

Objections des Directeurs & Réponses... (fait en classe)

Négociation & Compromis (idem)

. Conclusion & Décision
Pour résumer :

- Nous avons identifié un risque réel suite à l'incident USB.
- Trois mesures simples et réalistes sont proposées :
  contrôle des USB, plate-forme sécurisée, sensibilisation.
- Les compromis proposés permettent d'intégrer vos contraintes spécifiques.

Je vous propose donc de valider le déploiement progressif des trois mesures, avec un pilote dès la semaine prochaine.

Fadi Alouani

Émail

Objet : Mise en place de nouvelles mesures de sécurité liées à l'utilisation des périphériques USB

Chers collaborateurs,
Suite à un incident récent impliquant l'utilisation d'une clé USB non autorisée, Galaxy Swiss Bourdin renforce ses mesures de sécurité informatique afin de protéger nos données, nos activités de recherche et notre conformité réglementaire.
À partir du [date convenu], les règles suivantes entreront progressivement en vigueur :

1. Blocage des périphériques USB non autorisés
   Seules les clés USB chiffrées et enregistrées par la DSI seront utilisables sur les postes GSB.
2. Mise à disposition d'une plateforme sécurisée de partage de fichiers
   Elle permettra les échanges internes et externes dans un cadre traçable et conforme aux normes FDA/EMA.
3. Sensibilisation obligatoire des équipes
   Une courte formation en ligne sera déployée afin de présenter les bonnes pratiques et les solutions alternatives.

Ces mesures visent à garantir la protection de nos données et la continuité de nos activités, sans compromettre l'efficacité de nos opérations.

Nous vous remercions pour votre collaboration.
Cordialement,
La Direction des Systèmes d'Information – Galaxy Swiss Bourdin

Fiche récapitulative – Modifications à apporter à la Charte Informatique

Modifications à intégrer dans la Charte Informatique GSB

Thème	Modification	Justification
Périphériques USB	Interdiction des clés USB personnelles ; usage limité aux dispositifs chiffrés fournis par GSB	Prévention des intrusions, protection PI
Traçabilité des échanges	Obligation d'utiliser la plateforme sécurisée pour tout transfert de fichiers sensibles	Conformité FDA/EMA, auditabilité
Responsabilités des utilisateurs	Engagement à respecter les procédures de sécurité ; signalement obligatoire d'incidents USB	Réduction des risques humains
Utilisation des postes de travail	Blocage des ports USB sur certains environnements critiques (production, recherche)	Protection des instruments et environnements GMP
Partenaires externes	Interdiction d'utiliser des supports non validés par GSB lors de collaborations	Protection des données R&D
Formation obligatoire	Ajout d'un module annuel sur la sécurité des données et des pratiques USB	Conformité interne + régulation

Fadi Alouani

Plan de déploiement progressif – Adapté aux sites GSB

Phase 1 – Préparation (Semaine 1)

- Inventaire des usages USB par site (R&D, Production, Siège).
- Distribution des clés USB chiffrées.
- Paramétrage des règles de blocage sur un échantillon représentatif.

Phase 2 – Pilote (Semaines 2–3)
Sites concernés :

- R&D Lyon
- Production Reims

Actions :

- Activation du blocage USB sur 20 % des postes.
- Formation ciblée des utilisateurs pilotes.
- Collecte des retours métiers (contraintes, ajustements techniques).

Phase 3 – Déploiement global (Semaines 4–6)

- Blocage USB généralisé.
- Activation de la plateforme sécurisée pour toutes les directions.
- Mise à jour de la charte informatique + signature des utilisateurs.
- Assistance renforcée (hotline + référents sécurité locaux).

Phase 4 – Stabilisation (Semaine 7)

- Audit interne de conformité.
- Ajustements des règles par direction (R&D, production, siège).
- Bilan global présenté au Comité de Direction.

Auto-évaluation de la séance

Points positifs
Une communication claire et structurée.La capacité à vulgariser les risques cyber pour des non-techniciens.Gestion constructive des objections (Recherche / Opérations).
Recherche de compromis réalistes pour garantir la productivité.

Points à améliorer
Mieux préparer des exemples concrets propres aux instruments de production.
Utiliser plus de supports visuels pour faciliter la compréhension,.
Gérer le timing pour garder plus de temps pour les questions.
Impliquer plus le Directeur des Opérations dans la phase de négociation.
Axe d'amélioration personnel
Développer la confiance en leadership lors de réunions décisionnelles.
Renforcer la capacité à anticiper les objections métier.

Fadi Alouani

Réflexion – Sécurité et l'industrie pharmaceutique

Dans l'industrie pharmaceutique, la sécurité informatique n'est pas un élément périphérique, mais un levier stratégique.
Cependant, elle doit s'articuler intelligemment avec les besoins métiers.
Enjeux sécurité :

- Protection des données de R&D (molécules brevetables).
- Conformité FDA/EMA (traçabilité).
- Prévention des arrêts de production.

Enjeux métiers :

- Rapidité de la recherche scientifique.
- Efficacité opérationnelle des instruments.
- Collaboration avec des partenaires externes (universités, biotech).

Le bon équilibre repose sur :

1. La co-construction avec les équipes métiers
   Les règles doivent s'adapter au terrain, pas l'inverse.
2. La flexibilité encadrée
   Autoriser certains usages, mais dans un cadre sécurisé.
3. La pédagogie
   Les utilisateurs adhèrent mieux lorsqu'ils comprennent le "pourquoi".
4. La progressivité
   Déployer petit à petit, avec retours d'expérience.
5. La transparence
   Expliquer clairement l'impact, les bénéfices et les alternatives.

?Conclusion
La sécurité ne doit pas être perçue comme un frein, mais comme un garant de l'innovation :
on protège mieux pour travailler mieux.

Conclusion

Ce TP m'a permis de mieux comprendre l'importance de la préparation avant une réunion ainsi que le rôle de chacun dans un échange structuré. Que ce soit à travers l'interprétation d'un personnage ou l'observation d'un intervenant, l'exercice met en avant des compétences essentielles : communication, organisation, écoute et analyse. Le travail réalisé, incluant les fiches préparatoires et l'évaluation, reflète l'ensemble des apprentissages tirés de cette activité.