26/11/2025

Atelier - TP2

Sécurité informatique

Sommaire

Fait par : Mattéo Mouranchon – Groupe 2

Compte-rendu numéro 2

Introduction

L'objectif de cet atelier est de nous immerger dans le rôle d'un stagiaire au sein de l'entreprise GSB à la suite d'un incident de sécurité informatique. Il s'agit d'analyser la situation, de rédiger un rapport professionnel et d'en tirer une conclusion permettant de renforcer la politique de sécurité.

Dans ce cadre, le travail consiste à répondre aux questions suivantes :

- **Quelle est la cause de l'incident ?**
- **Quelles en sont les conséquences pour l'entreprise ?**
- **Quelles contre-mesures doivent être mises en place pour éviter qu'un tel incident ne se reproduise ?**
- **Quelle conclusion générale peut-on tirer de l'analyse réalisée ?**

Phase 1 : Analyse et préparation

Au cours de cette première phase, l'analyse de l'ensemble des ressources ont été fournies afin de comprendre les enjeux de la sécurité informatique dans le contexte spécifique du laboratoire pharmaceutique GSB.

La phase d'analyse montre que l'entreprise GSB est sous plusieurs directive de plusieurs organisation ou agence des pays comme le **CNRS** (**C**entre **N**ational de la **R**echerche **S**cientifique) qui ont comme principes fondamentaux de la sécurité des systèmes d'information en termes de :

- Confidentialité,
- intégrité,
- disponibilité,
- traçabilité,
- Preuve.

Ces principes s'appliquent particulièrement au secteur pharmaceutique, notamment pour la protection des résultats d'essais cliniques ou des formules brevet, car sans ses protection, l'entreprise serais exposer aux risques comme :

- Risque de cyberattaque
- Facilité qu'une entreprise concurrente infiltre GSB
- Le risque d'espionnage et pillage industriel qui arrive souvent à l'entreprise GSB

Ce contexte est connu sous le nom de « la guerre invisible ». C'est simple, de l'extérieur, les gens auront impression que tout est normal mais en interne c'est autre chose, c'est une bataille, une guerre sans merci. Les ressources de haute valeur de l'entreprise GSB souligne que la menace vient souvent.

Phase 2 : Rédaction et validation

La Phase 2 consiste à **rédiger une note professionnelle** sur les risques liés qui peuvent se produire chez GSB.

Les principal menace que GSB peut subir le plus sont :

Risque	Impact	Probabilité	Mesures de Protection
Perte de données de recherche	Très élevé	Élevée	Sauvegardes régulières, chiffrement
Vol de propriété intellectuelle	Très élevé	Moyenne	Contrôle d'accès strict, monitoring
Intrusion via périphériques USB	Élevé	Élevée	Politique d'usage, antivirus, contrôle
Erreur humaine	Élevé	Élevée	Formation, procédures, double validation
Panne système	Élevé	Faible	Redondance, plan de reprise

Pour en faire un exemple, un rapport interne a été rédiger sous forme d'incident aux risques de la sécurité des serveurs au département R&D. En cause ? Une clé USB personnelle non autorisé.

Le rapport : Rapport_interne_incident_GSB.pdf

Phase 4 : Communication et formation

Dans cette quatrième et dernière phase, il s'agit de finaliser le travail réalisé tout au long de l'analyse et de montrer que l'incident a été compris dans toute sa dimension et entourage. Cette étape consiste plus à regrouper l'ensemble des livrables et à prendre du recul sur l'analyse menée.

Dans le cadre de mon rapport, la phase 4 a permis de :

1. Finaliser la note professionnelle

Validé la note interne portant sur les risques liés aux clés USB non autorisées et les mesures de sécurité à mettre en place chez GSB.
Cette version finalisée est destinée à être diffusée sur l'intranet de l'entreprise.

2. Préparer la communication aux collaborateurs

Le tout en rédigeant un email type destiné à informer l'ensemble des employés de GSB de la nouvelle procédure concernant l'utilisation des périphériques USB.
L'objectif est d'assurer une diffusion claire et professionnelle des consignes de sécurité.

3. Récapituler les modifications à apporter à la charte informatique

À partir de l'analyse de l'incident, j'ai identifié les points de la charte informatique devant être mis à jour, notamment :

- L'interdiction des supports USB personnels
- L'obligation de chiffrement
- La traçabilité
- La formation régulière des employés

4. Proposer un plan de déploiement

On a conçu un plan de mise en œuvre progressif tenant compte :

- Du siège
- Du département R&D ou aux ensembles des départements

Ce plan permet d'introduire les nouvelles mesures sans perturber les activités critiques.

5. Réaliser une auto-évaluation

L'auto-évaluation pourra être utile pour le personnels qui s'auto-évaluerons après suite ils prendront conscience de leur erreur pour ne plus le reproduire :

- Ce que j'ai réussi dans l'analyse et la rédaction du rapport,
- Les points que je pourrais améliorer (par exemple approfondir certaines mesures techniques),
- Ce que j'ai appris concernant la sécurité dans un laboratoire pharmaceutique.

Conclusion

En conclusion, ce TP m'a permis de comprendre l'importance de la politique de sécurité rigoureuse au sein du laboratoire GSB, particulièrement face aux risques liés à l'utilisation de périphériques USB non autorisés.
L'analyse de l'incident, la rédaction de la note professionnelle et la préparation des actions de communication ont montré la nécessité de renforcer les procédures internes et de sensibiliser l'ensemble des collaborateurs.
Ce travail m'a également permis de développer mes compétences en analyse, en communication professionnelle et en sécurité informatique, compétences essentielles dans un environnement pharmaceutique exigeant.