Charpenay Côme Sio 1
26/11/25

B1 TP Compte Rendu

Sécurité Informatique

Sommaire :

Notes:

En Cas d'Incident Suivre le Protocole :

1. **Isoler** le système compromis du réseau
2. **Alerter** le responsable sécurité et la direction
3. **Documenter** tous les détails de l'incident
4. **Préserver** les preuves pour investigation
5. **Appliquer** le plan de reprise d'activité

Contact Urgence :

Responsable Sécurité : x1234
DSI : x5678
Cellule de Crise : x9012

La première étape du traitement d'un incident est de le qualifier

Détections : que détectent les dispositifs de sécurité du système d'informations

journaux : puits de log et SIEM,

antivirus et EDR/xDR,

supervision de la production

Dysfonctionnements informatiques

identifier le niveau de perturbation des applications et de l'infrastructure,

détecter les arrêts de services, de machine, etc.

détecter la disparition ou l'impossibilité de lire des fichiers ;

Perturbation des métiers

Quels dysfonctionnements sont constatés ?

Déterminer la source précise de l'incident, et éventuellement confirmer le plus en amont possible l'interprétation de la détection ou du signalement ;

Déterminer le périmètre concerné.

Des systèmes distincts présentent-ils des anomalies, et si oui sont-elles liées ?

Qu'est-ce qui relie différents sous-systèmes touchés ? Comment une attaque peut s'y être propagée ?

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

Mise en place sécurité des postes informatiques :

- **Prévoir** un mécanisme de **verrouillage automatique** de session en cas de **non-utilisation** du poste pendant un **temps donné**.
- **Installer** un « **pare-feu** » (« *firewall* ») logiciel sur le poste et **limiter** l'ouverture des **ports de communication** à ceux **strictement nécessaires** au bon fonctionnement des applications installées sur le poste de travail.
- **Utiliser** des **antivirus régulièrement mis à jour**.
- **Déployer les mises à jour de sécurité** au plus tôt, après les avoir **testées** sur un **poste informatique isolé** du réseau.

- **Limiter les droits des utilisateurs au strict minimum en fonction de leurs besoins sur les postes de travail.**
- **sensibiliser les utilisateurs aux risques liés à l'utilisation de support amovibles, en particulier s'ils proviennent de l'extérieur ;**
- **limiter la connexion de supports mobiles à l'indispensable ;**
- **désactiver l'exécution automatique (« *autorun* ») depuis les supports amovibles.**

Mise en place des solutions via l'utilisation des clé USB :

ESET SysRescue/ ClamAV

La solution ESET Antivirus fournit la meilleure des solutions pour détecter et supprimer les virus et les fichiers malveillants de votre système informatique ainsi que des clés USB. Si vous rencontrez des problèmes lors du démarrage de votre système, vous pouvez utiliser l'outil Live Rescue d'ESET.

- **Cartographie des menaces à chaques utilisations matériels**
- **Utiliser des authentification à double facteur lorsque possible avec mot de passe robuste**
- **Vérification de l' états hebdomadaire des outils informatiques personnelles et professionnelles**
- **Surveiller personnellement ses outils avec des informations confidentielles/professionnelles**
- **Éviter les réseaux publics, matériels empruntés ou autres outils susceptibles d'être corrompus et non personnels/professionnels.**

En entreprise, il est préférable d'imposer le chiffrement total du supports amovibles usb afin de garantir qu'aucune donnée sensible ne puisse sortir de l'entreprise par ce biais. Une solution de chiffrement de qualité peut proposer différents comportements face à l'introduction d'une clé usb ou d'un disque dur sur un PC du réseau de l'entreprise. Les Données stockées sur clé USB doivent être chiffrées, contenant une méthode de connexion sécurisée par clé d'authentification / mot de passe à usage personnel permettant d'accéder au contenu du fichier de la clé USB. Chiffrement AES (niveau militaire) PRIM'X

Jeux de Rôle:

RQ

Responsable Qualité

Mme Sophie Dubois

Préoccupation : Normes FDA/EMA

Style : Méthodique, procédurier

Soutien : "Il faut être conforme"

Position : "La traçabilité et la conformité aux normes FDA/EMA sont essentielles. Je soutiens des mesures qui renforcent notre conformité réglementaire."

💭 Questions de Préparation

❓ Quels aspects des mesures proposées répondent directement aux exigences FDA 21 CFR Part 11 ?

Conserver les enregistrements dans une base de données (ex: Cloud) pendant minimum 2 ans, garantir la traçabilité / sécurité / intégralité des données pour pouvoir vérifier la similitude des données. Garantir la fiabilité des données au secteur pharmaceutiques et être en conformité avec la CNIL.

❓ Comment allez-vous soutenir l'animateur face aux objections des autres directeurs ?

Il est essentiel de répondre aux risques via des normes aux secteurs pharmaceutiques tel ISO 9001 est une norme qui vise la gestion de la qualité. Il est favorable d'inclure davantage de norme pour la mise en place des solutions pour répondre aux règles et sécurisé de manière supplémentaire les données sensibles de l'entreprise

❓ Quels risques réglementaires évitons-nous avec ces mesures ?

Nous pouvons éviter des problèmes avec les clients (manque confiance), Sans normes, les processus, la production et les contrôles pourraient ne pas répondre aux attentes des autorités (ANSM, EMA, FDA).
Risque évité : inspection défavorable, lettres d'avertissement, demande retrait de produits, refus AMM (Autorisation mise sur le marché)

Lettre:

Référence :
?
Date :
26/11/2025
Objet :
Les Risques liées à la clé USB
De :
Charpenay Côme
À :
M. Patron
Pièces jointes :
Aucune

1. CONTEXTE ET CONSTAT

Situation actuelle

Dans un contexte où les menaces informatiques ne cessent d'évoluer, il est essentiel pour l'ensemble des collaborateurs GSB de connaître les réflexes à adopter en cas d'incident et de respecter les bonnes pratiques de sécurité au quotidien. Cette note rassemble les points essentiels pour savoir comment réagir rapidement et limiter les risques.

Données d'analyse

Les analyses montrent :

- **une augmentation des détections issues des journaux (puits de logs, SIEM), des antivirus et des solutions EDR/xDR ;**

- **plusieurs dysfonctionnements mineurs constatés sur certains postes ;**

- **des anomalies isolées dans les services métiers, nécessitant une qualification plus fine ;**

- **un besoin renforcé de sécurisation des postes et d'encadrement de l'usage des supports amovibles.**

2. ANALYSE

Éléments identifiés / Qualification de l'incident

La première étape lors de tout incident consiste à le qualifier, c'est-à-dire :

- **analyser ce que détectent les dispositifs de sécurité (journaux, antivirus, EDR/xDR, supervision) ;**

- **identifier les dysfonctionnements informatiques (arrêt de services, machines, pertes de fichiers) ;**

- **évaluer la perturbation des métiers (quels services sont touchés, quelles actions bloquées ?) ;**

- **déterminer la source précise de l'incident, et confirmer la validité du signalement ;**

- **définir le périmètre impacté et voir si plusieurs systèmes touchés présentent un lien logique entre eux ;**

- **comprendre comment une attaque pourrait se propager d'un sous-système à l'autre.**

Point important 1 — HAUTE

Réaction immédiate en cas d'incident:

Il est indispensable de couper rapidement la propagation d'un incident pour limiter son impact. L'isolement réseau doit être effectué sans délai.

Point important 2 — MOYENNE

Organisation et communication:

Alerter les bonnes personnes rapidement permet d'éviter les mauvaises manipulations et de préserver les preuves nécessaires à l'enquête.

Point important 3 — FAIBLE

Documentation et suivi:

Noter les anomalies, messages d'erreur ou comportements inhabituels facilite le travail des équipes techniques et permet un retour rapide à la normale.

3. RECOMMANDATIONS

Propositions d'action

Pour renforcer la sécurité au quotidien, plusieurs actions doivent être appliquées de manière systématique :

- **garder les postes protégés, à jour et verrouillés ;**
- **limiter les droits utilisateurs et les accès non nécessaires ;**

- **sensibiliser chacun aux risques liés aux supports amovibles ;**

- **privilégier le chiffrement et l'authentification renforcée ;**

- **surveiller régulièrement l'état des outils personnels/pro ;**

- **éviter les réseaux publics ou matériels inconnus.**

Plan d'action proposé

Action prioritaire 1 : HAUTE

En cas d'incident, suivre le protocole immédiatement

1. **Isoler le système compromis du réseau**

2. **Alerter la sécurité et la direction**

3. **Documenter tous les détails observés**

4. Préserver les preuves pour l'investigation

5. Déclencher le plan de reprise d'activité

Contacts urgence :

- Responsable Sécurité : **x1234**
- DSI : **x5678**
- Cellule de Crise : **x9012**

Action prioritaire 2 : MOYENNE

Sécurisation renforcée des postes de travail

- **Verrouillage automatique après inactivité**
- **Installation d'un firewall logiciel**
- **Antivirus à jour**
- **Mise à jour des correctifs après test isolé**

- **Limitation stricte des droits utilisateurs**
- **Sensibilisation aux supports amovibles**
- **Désactivation de l'autorun**

Action complémentaire : FAIBLE

Sécurisation des clés USB et utilisation contrôlée

- **Utilisation d'outils de nettoyage (ESET SysRescue, ClamAV)**
- **Cartographie des menaces pour chaques matériels utilisés**
- **Activation d'une authentification forte (A2F) et mots de passe robustes**
- **Vérifications hebdomadaires des équipements**
- **Éviter tout réseau public ou matériel emprunté**

- **Imposer en entreprise le chiffrement total des supports USB (ex. AES — niveau militaire)**

- **Accès aux données via clé d'authentification ou mot de passe personnel**
  Ex : solutions de chiffrement type PRIM'X

4. CONCLUSION

Cette note rappelle les réflexes essentiels pour réagir efficacement lors d'un incident et les bonnes pratiques à appliquer pour limiter les risques au quotidien. Chacun a un rôle à jouer dans la sécurité du système d'information : vigilance, réactivité et respect des consignes permettront de protéger l'entreprise et les données sensibles.

Les prochaines étapes :

- **la diffusion du protocole incident au sein de l'entreprise ;**

- **des rappels réguliers de sensibilisation ;**

- **un suivi des actions de sécurisation sur l'ensemble des manipulations liées à l'informatiques.**

Pour le service émetteur	Vu et approuvé
Charpenay Côme	**M.Patron**
Stagiaire	**Patron**

CONFIDENTIEL - Usage interne GSB uniquement