PLOUFTECH	PRI : Plan de Réponse à un Incident *PRI : Ensemble du système informatique*	Date création 25/10/2024	Référence 09PS.001
		Dernière modification 25/10/2024	2 pages

Auteurs :

- Etienne PAQUELET - Ardy OCKANDJI - GREDER Guillaume - LEGELEUX Keryan

Plan de réponse à incident

Ce plan résume les acteurs et les actions à mener afin de prévenir d'une potentielle attaque cyber. Mais cela permet aussi de réagir efficacement et rapidement à un incident en cours.

Dans cette optique, notre objectif est de minimiser l'impact de l'attaque. D'être en mesure de restaurer les systèmes, de sécuriser les données et d'éviter que l'incident ne se reproduise.

Ce plan est applicable à l'ensemble des systèmes, réseaux et données de l'hôpital, y compris les applications critiques. Certains serveurs cités ci-dessous sont inexistants dans notre infrastructure actuelle mais pourraient être installés à la suite de la remise du système informatique aux services informatiques de l'Hôpital Public de Belfort Montbéliard. Ce plan de réponse à un incident explique les mesures à la fois générales et précises à mettre en œuvre lors d'une cyberattaque.

Les services administratifs seront chargés de procéder à la création d'une cellule de crise en lien avec les acteurs chargés de répondre à l'incident : Service Informatique, Service Juridique, Service de communication.

1) Acteurs du plan (Équipe de réponse à incident)

Les acteurs sont les membres clés de cette réponse. Nous sélectionnons deux personnes parmi chaque service pour participer à la cellule de crise. Les autres membres continuerons de travailler sur la résolution de l'incident concernant le service informatique.

Ce sont :

Pour le service informatique

Le service est composé de différents sous-services notamment les services Systèmes et Réseaux, SOC et Support.

Pour la cellule de crise, les membres suivants seront engagés :

- Le **responsable de la réponse à incident** qui peut être en réalité le **DSI**.
- Le **responsable des systèmes** pour superviser la remise en service des systèmes affectés.
- Deux **analystes de sécurité** : qui vont identifier les vecteurs d'attaque et limiter l'impact.

Le service Support quant à lui, fera le relais des informations récoltées par les employés au responsable de l'ERI.

Un pôle communication

Un **expert en communication** sera désigné comme responsable des communications internes et externes. Il sera l'interlocuteur principal et s'occupera des échanges avec l'extérieur.

Il travaille en étroite collaboration avec les **relations publiques** qui vont gérer l'image publique et la presse en cas de médiatisation de l'incident.

Un pôle juridique

Le **responsable juridique** a pour rôle de gérer les obligations légales en cas d'incident et d'assurer la conformité des démarches avec les réglementations en vigueur (RGPD, ANSSI, etc.). Il gèrera en cas d'incident les aspects légaux comme la violation des données, les rapports aux autorités.

2) Inventaire de l'infrastructure

L'infrastructure informatique actuelle est constitué des équipements serveurs suivants :

- 1 Serveurs Windows Server 2022
- 4 Serveurs sous Linux
- 2 pare-feux
- 2 switchs

Les services suivants ont été installé et seront mis en redondance sur les serveurs :

- Logiciel de gestion hospitalière (OpenEMR)
    - Données patientes et médecins
- Logiciel de bureau à distance : Terminal Server
- Active Directory : Annuaire LDAP.
- Veeam : Serveur de sauvegarde
- Serveur DNS
- Serveur DHCP
- Serveur RADIUS
- Serveur Apache2
- Serveur NextCloud
- Serveur Mail
- Pare-feu Stormshield
- Serveur de supervision
- Serveur IDS
- Serveur de télécommunication

Cependant, l'infrastructure informatique pourrait être amélioré dans le futur avec l'ajout de certains serveurs :

- Serveur de log
- Serveur cache
- Serveur proxy
- Serveur ERP
- Serveur de systèmes d'imagerie médicale
- Serveur de Gestion des ordonnances médicales
- Serveur RIS
- Serveur Dossiers médicaux

En dehors de cela, des mises à jour et correctifs sont régulièrement faits afin de corriger des vulnérabilités connues.

3) Inventaire de la surface d'attaque de l'infrastructure

La surface d'attaque de l'infrastructure peut se présenter sous différentes formes. Que ce soit par le réseau :

1) **Accès VPN** : Utilisé par les employés pour se connecter à distance au réseau interne. S'il est mal configuré ou non protégé, il pourrait être utilisé comme vecteur d'attaque.
2) **Ports ouverts sur les serveurs** : Certains services (DNS, SMTP, RDP) pourraient être exploités s'ils sont exposés sans protection.
3) **Pare-feux mal configurés** : Une mauvaise configuration peut permettre des accès non autorisés aux services internes. Une règle de filtrage directement déployée en production sans avoir été testée.
4) **Switchs et routeurs vulnérables** : Ces équipements peuvent être exploités via des failles non corrigées ou des mots de passe par défaut. Par exemple du port mirroring sur des Switchs.
5) **Serveurs exposés à Internet** : Serveurs web, proxy, et systèmes accessibles depuis Internet peuvent être ciblés par des attaques de type DDoS, exploitation de vulnérabilités, ou injection SQL. Une escalade de privilèges peut également intervenir sur des serveurs Web.
6) **Authentification faible ou non sécurisée** : Manque de protection multi-facteurs (MFA) ou mots de passe faibles sur des comptes administratifs critiques (Active Directory, systèmes de sauvegarde, serveurs).
7) **Systèmes non patchés** : Des vulnérabilités non corrigées dans des logiciels et systèmes d'exploitation (Windows Server, Linux, Apache2, etc.).
8) **Accès utilisateurs internes non restreints** : Utilisateurs avec des droits excessifs ou mal gérés.

9) **Interfaces de gestion à distance (RDP, SSH)** : Si elles sont mal sécurisées, ces interfaces peuvent être exploitées pour un accès non autorisé. Un oubli de configuration peut laisser actif des accès Telnet.

Mais cela peut aussi provenir des utilisateurs :

1) **Phishing et emails malveillants** : Attaques ciblant les employés avec des emails contenant des liens ou pièces jointes malveillants.
2) Accès à des sites non sécurisés et téléchargement depuis celui-ci.
3) **La fraude au président** : un employé peut se laisser influencer par un cybercriminel se faisant passer pour le PDG ou un cadre de service.
4) Des discussions non contrôlées en public qui peuvent laisser échapper des informations sensibles.

4) Inventaire des zones critiques

Les zones critiques sont les systèmes et services auraient un impact majeur sur les opérations de l'hôpital s'ils venaient à être compromis.

Données sensibles :

1. **Dossiers médicaux électroniques (DME)** : La compromission des données patient serait catastrophique (vol de données, rançongiciels).
2. **Systèmes de gestion hospitalière** : Impact direct sur la capacité à gérer les soins, les admissions, et les traitements.
3. **Données des prescriptions et ordonnances** : Affecte la sécurité des patients en cas de manipulation ou de perte.

Infrastructure critique :

1. **Serveurs RIS** : Les images médicales sont vitales pour le diagnostic. Leur perte ou inaccessibilité aurait un impact direct sur les soins aux patients.
2. **Serveur de supervision** : Compromettre le serveur de supervision pourrait empêcher l'identification et la résolution rapide des incidents.
3. **Serveur de messagerie** : La communication interne et externe (notamment avec d'autres hôpitaux ou services médicaux) repose sur le serveur de mail.
4. **Serveur Active Directory** : Compromettre l'AD compromettrait l'ensemble du contrôle d'accès aux systèmes de l'hôpital.
5. **Serveurs de sauvegarde (Veeam)** : Si ces serveurs sont affectés, il sera difficile de restaurer les données après un incident.

Équipements et systèmes vitaux :

1. **Systèmes d'imagerie médicale** : Leur bon fonctionnement est essentiel pour des diagnostics rapides et précis.
2. **Réseau de télécommunication (VoIP)** : La communication entre les services médicaux, les urgences et les administrateurs est essentielle en cas de crise.
3. **Systèmes de supervision et IDS** : Ce sont des outils de détection et de réponse aux incidents qui, s'ils sont affectés, laisseraient l'hôpital vulnérable à d'autres attaques.

5) Inventaire des vulnérabilités

Les différentes vulnérabilités qui pourraient être présente sont les suivantes :

1. Logiciels non patchés

- Description : Certains serveurs ou logiciels hospitaliers ne sont pas régulièrement mis à jour, laissant des vulnérabilités connues non corrigées.
- Impact : Exploitation des failles pour accéder aux systèmes sensibles ou exécuter du code malveillant.

2. Absence de multi-factor authentication (MFA)

- Description : Les systèmes critiques (Active Directory, VPN, etc.) ne disposent pas d'une authentification multi-facteurs, facilitant l'accès en cas de vol de mot de passe.
- Impact : Accès non autorisé aux systèmes via des comptes compromis.

3. Mauvaise configuration des pare-feux

- Description : Une mauvaise configuration des pare-feux ou des règles trop permissives ouvrent des portes aux attaquants.
- Impact : Accès non autorisé aux systèmes internes depuis l'extérieur.

4. Utilisation de mots de passe faibles

- Description : Certains systèmes critiques ou comptes administratifs utilisent des mots de passe faibles ou par défaut.
- Impact : Accès non autorisé aux systèmes sensibles, compromission des comptes utilisateurs.

5. Endpoints non sécurisés (appareils des utilisateurs)

- Description : Les ordinateurs ou appareils mobiles utilisés par le personnel hospitalier ne disposent pas de protections suffisantes (antivirus, cryptage, etc.).
- Impact : Propagation de malwares, accès aux données sensibles.

6. Absence de segmentation du réseau

- Description : Le réseau n'est pas suffisamment segmenté, permettant à un attaquant d'accéder à plusieurs parties du réseau après avoir compromis un seul point d'accès.
- Impact : Accès transversal à plusieurs systèmes critiques, propagation rapide d'attaques.

7. Absence de surveillance continue (logs, IDS, etc.)

- Description : L'absence de systèmes de détection d'intrusion (IDS) ou de surveillance des logs réduit la capacité à détecter les activités suspectes en temps réel.
- Impact : Identification tardive des intrusions, laissant aux attaquants plus de temps pour causer des dommages.

8. Manque de sensibilisation du personnel

- Description : Les employés ne sont pas suffisamment formés pour identifier les attaques de phishing ou adopter des bonnes pratiques de cybersécurité.
- Impact : Failles humaines, tels que des clics sur des liens malveillants, augmentant les chances de compromission.

6) Inventaire des scénarios d'attaques

1. Ransomware ciblé sur les systèmes critiques

- **Description** : Les attaquants infiltrent le réseau de l'hôpital et déploient un ransomware pour chiffrer les dossiers médicaux électroniques, les images radiologiques, ou d'autres systèmes vitaux.
- **Impact** : Indisponibilité des données patients, impossibilité de fournir des soins adéquats, risques pour la santé des patients.
- **Vecteur d'attaque** : Email de phishing, vulnérabilité dans un logiciel non patché, compromission des droits d'administrateur.

2. Phishing ciblé (Spear Phishing)

- **Description** : Un email frauduleux est envoyé à des employés de l'hôpital pour collecter des identifiants ou injecter un malware.
- **Impact** : Vol d'informations d'identification, compromission des systèmes sensibles via les identifiants obtenus.
- **Vecteur d'attaque** : Email frauduleux semblant provenir d'une source de confiance (par exemple, une entité médicale ou un fournisseur de services).

3. Compromission des dispositifs IoT ou équipements médicaux connectés

- **Description** : Les dispositifs médicaux connectés, tels que les pompes à perfusion ou les moniteurs de patients, peuvent être compromis à cause de failles de sécurité.
- **Impact** : Manipulation des dispositifs médicaux, mise en danger des patients, défaillance des systèmes de surveillance.
- **Vecteur d'attaque** : Exploitation des failles non corrigées dans les dispositifs IoT ou appareils médicaux mal sécurisés.

4. Exploitation d'une vulnérabilité dans le logiciel de gestion hospitalière

- **Description** : Un attaquant exploite une vulnérabilité dans le logiciel de gestion hospitalière pour accéder aux données patientes ou désactiver certaines fonctionnalités.
- **Impact** : Vol de données sensibles, perturbation des processus hospitaliers.
- **Vecteur d'attaque** : Exploitation d'une faille logicielle non patchée.

5. Attaque DDoS (Distributed Denial of Service)

- **Description** : L'attaquant lance une attaque de déni de service distribué (DDoS) sur les systèmes de l'hôpital, rendant les services (site web, messagerie, etc.) inaccessibles.
- **Impact** : Interruption des services numériques essentiels, ralentissement des opérations administratives et médicales.
- **Vecteur d'attaque** : Inondation des serveurs ou des équipements réseau par des requêtes massives.

6. Compromission des accès à distance (VPN ou RDP)

- **Description** : Un attaquant utilise des failles dans l'accès VPN ou RDP pour pénétrer dans le réseau interne de l'hôpital.
- **Impact** : Prise de contrôle de systèmes critiques, vol ou manipulation de données.
- **Vecteur d'attaque** : Accès non sécurisé ou exploitation de failles dans les interfaces de gestion à distance.

7. Attaque interne ou usage malveillant d'un employé

- **Description** : Un employé malveillant ou négligent utilise ses accès pour exfiltrer des données ou compromettre des systèmes critiques.
- **Impact** : Vol de données, sabotage interne, interruptions des services.
- **Vecteur d'attaque** : Utilisation des privilèges d'accès ou manipulation des systèmes internes.

7) Protocole de réponse

Le protocole de réponse doit être le suivant :

Détection et Identification de l'incident

- **Action** : Le personnel ou les systèmes de surveillance (IDS, logs) détectent une activité suspecte (phishing, ransomware, attaque DDoS, etc.).
- **Ressources impliquées** : Service SOC, Service Support, Service Systèmes et Réseaux.
- **Outils** : Monitoring réseau, analyse des logs, détection IDS/IPS.
- **Objectif** : Identifier rapidement l'incident pour limiter son impact.

Analyse de l'étendue de l'attaque

- **Action** : Analyser et évaluer la portée de l'attaque. Déterminer quels systèmes, données ou utilisateurs sont compromis. Identifier le point d'entrée initial.
- **Ressources impliquées** : Service SOC, administrateurs systèmes, experts en sécurité.
- **Outils** : Analyse forensique, rapports de surveillance, outils de détection d'anomalies réseau.
- **Objectif** : Comprendre la gravité et l'étendue des dégâts causés par l'attaque.

Évaluation de l'incident

- **Action** : Classer l'incident en fonction de sa gravité (mineur, modéré, critique) et évaluer les conséquences potentielles sur les opérations hospitalières.
- **Ressources impliquées** : Équipe de gestion de crise, experts en cybersécurité.
- **Outils** : Tableaux de bord de sécurité, rapports d'incidents.
- **Objectif** : Prioriser les actions selon la criticité de l'incident et son impact sur les services hospitaliers.

Confinement de l'incident

- **Action** : Limiter la propagation de l'attaque en isolant les systèmes compromis et en restreignant les accès non nécessaires (ex : déconnexion des serveurs infectés, segmentation du réseau).
- **Ressources impliquées** : Service Systèmes et Réseaux, SOC.
- **Outils** : Segmentation réseau, filtrage via les pare-feux, blocage d'accès VPN ou RDP.
- **Objectif** : Empêcher l'attaque de se propager à d'autres systèmes ou utilisateurs.

Compréhension de l'attaque

- **Action** : Analyser les vecteurs de l'attaque pour comprendre comment le système a été compromis (exploitation d'une vulnérabilité, phishing, etc.).
- **Ressources impliquées** : Experts en cybersécurité, équipe forensique.
- **Outils** : Analyse des logs, reverse engineering des malwares.
- **Objectif** : Identifier la cause racine et documenter les étapes qui ont permis à l'attaquant de réussir.

Éradication de la menace

- **Action** : Utiliser des outils de suppression de malware, d'antivirus, ou de correctifs de sécurité pour éliminer toute trace de l'attaque et combler les failles exploitées.
- **Ressources impliquées** : Service SOC, Service Systèmes et Réseaux.
- **Outils** : Outils d'analyse forensique, antivirus, correctifs de sécurité.
- **Objectif** : Supprimer l'attaquant du système et s'assurer que l'attaque ne puisse pas recommencer.

Récupération des systèmes

- **Action** : Restaurer les systèmes affectés à partir de sauvegardes saines, vérifier l'intégrité des données, et remettre les systèmes critiques en ligne progressivement.
- **Ressources impliquées** : Service Systèmes et Réseaux, gestion des sauvegardes.
- **Outils** : Outils de sauvegarde (ex : Veeam), tests de restauration.
- **Objectif** : Assurer le rétablissement complet des services tout en garantissant la sécurité des systèmes restaurés.

Communication interne et externe

- **Communication interne** :
  - **Action** : Informer les parties prenantes internes (direction, services critiques) sur la situation, les mesures prises et l'évolution de l'incident.
  - **Ressources impliquées** : Service de communication, équipe de direction.
  - **Objectif** : Assurer une bonne coordination interne et éviter la panique.
- **Communication externe** :
  - **Action** : Informer les partenaires externes et les autorités compétentes, notamment :
    - **ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information, pour signaler un incident majeur.
    - **Tribunal** : Pour toute question juridique, notamment en cas d'infraction pénale.
  - **Ressources impliquées** : Service juridique, service de communication.
  - **Objectif** : Assurer une communication claire, conforme aux obligations légales et contractuelles.

Sensibilisation des employés

- **Action** : Lancer une campagne de sensibilisation suite à l'incident, avec des formations ou des rappels sur les bonnes pratiques de cybersécurité (ex : gestion des emails, MFA, etc.).
- **Ressources impliquées** : Service des ressources humaines, service informatique, service de communication.
- **Objectif** : Prévenir de futures attaques en renforçant la vigilance et la compréhension des risques chez les employés.

Rapport Post-Incident

- **Descriptif de l'incident** :
  - **Action** : Rédiger un rapport détaillé qui décrit l'incident, les étapes suivies pour sa résolution, les systèmes touchés et les mesures correctives prises.
  - **Ressources impliquées** : Service SOC, service juridique, service de direction.
  - **Objectif** : Documenter l'incident pour améliorer les processus de gestion des incidents à l'avenir.
- **Méthode mise en place pour la solution** :
  - **Action** : Décrire en détail comment l'incident a été résolu, quelles actions correctives ont été implémentées, et comment les vulnérabilités identifiées ont été comblées.
  - **Ressources impliquées** : Experts en sécurité, équipe de direction.
  - **Objectif** : S'assurer que l'incident est entièrement résolu et que les leçons tirées sont appliquées.