Rapport de sécurité de système d'information

Par Hugo LOURREIRO et
Alexandre BEROT-ARMAND
IUT Nord-Franche Comté - 2023

TABLE DES MATIERES

INTRODUCTION

Ce rapport de sécurité est lié à la SAE 503 qui a pour thème la sécurisation ainsi que la supervision avancée d'un système d'information.
Cette SAE nous situe dans le système d'information d'un hôpital fictif dont nous devons créer le réseau.

Ce rapport a pour but, dans un premier temps, d'expliquer quels sont les mécanismes à mettre en place pour fournir un certain niveau de sécurité a une infrastructure informatique en réseau. Ce niveau de sécurité doit prendre en compte l'importance de l'organisme (un hôpital dans notre cas)

La seconde partie de ce rapport fournis un avis sur les métriques de qualité ainsi que le type d'attaques à surveillé pour permettre de voir à l'avance lorsqu'un problème risque de se déclencher.

MECANISMES DE SECURITE

Dans le but de proposer un système d'information sécurisé, notre premier reflexe est de regarder quels sont les bonnes pratiques à suivre.
Le premier site à consulter se trouve être l'ANSSI qui propose un guide pratique pour mettre en place une infrastructure robuste. En suivant ce guide, nous avons donc décidé de créer une infrastructure comportant une DMZ multi-niveau.
Ce principe de multi-niveau permet d'avoir plusieurs zones entre le SI et Internet séparer par des pare-feux ce qui permet plusieurs points :

- Avoir les zones les moins critiques (notre serveur web accessible en externe) devant, puis les zones plus critiques en arrière (comme la base de données du serveur web)
- Avoir une zone d'administration externe au trafic avec son propre VLAN, et un accès à internet limité au strict minimum.
- Utiliser la rupture protocolaire pour ne montrer que le minimum possible derrière les pare-feux et ne pas permettre à une requête de traverser l'entièreté du réseau.

Pour notre projet, nous avons décidé de se limité a la séparation, via VLAN, du serveur web et de sa base de donnée, ainsi que de séparer les utilisateurs des serveurs.
Nous avons donc déjà des pistes d'améliorations structurelles avec l'ajout d'un nouveau Pare-feu qui menerais vers un Proxy et un Reverse-Proxy pour augmenter encore le degrée de sécurité.
Nous pourrions aussi utiliser un Pare-feu d'administration qui permettrais de séparer le flux et d'y mettre d'autres serveurs spécifique à la sécurité (comme un serveur SysLog, ou un serveur ELK).

A cette idée de DMZ multi-niveau, nous avons ajouter un serveur Snort.
Ce serveur se situe sur le pare-feu externe pour pouvoir capter l'ensemble du réseau entrant et sortant de l'infrastructure et pouvoir agir dessus via des règles.
En utilisant pfSense comme pare-feu, il existe une méthode rapide d'installation qui permet d'intégré rapidement la solution dans l'environnement avec la possibilité d'ajouter des règles pré-établies ainsi que d'ajouter ses propres règles customisées.

Pour finir, nous avons ajouter un serveur Kuma qui sert a vérifier le niveau d'uptime des serveurs avec la possibilité de recevoir un message via mail, sms ou différents réseau de contacte (telegram ou discord) si l'un d'eux venais à tomber.

L’infrastructure que nous proposons est donc assez légère mais reste robuste avec une conception évolutive en fonction de la nécessité qu’aurais l’hôpital à grandir en y ajoutant de nouveau Vlan et de nouveau pare-feux pour agrandir l’espace de sécurité entre le SI et Internet tout en permettant le trafic autorisé sans perte de performance globale notable pour les utilisateurs.

METRIQUES A SURVEILLER

Dans l'infrastructure que nous avons mis en place, nous avons plusieurs métriques que nous surveillons.
La première et la plus évidente est l'uptime des serveurs. En effet, si un des serveurs tombe, surtout un serveur de donnée ou de messagerie, alors une grande partie de l'hôpital ne pourrait plus travailler.
Ce type de métrique est facile à surveiller et surtout ne coute pas très cher en ressources. Il suffit de configurer un serveur Kuma, Zabbix ou une solution similaire pour pouvoir le vérifier et pouvoir agir rapidement.

Une deuxième métrique à surveillé est le flux réseau, sortant et entrant, du pare-feu externe. Cette métrique permet d'avoir un grand nombre d'information :

- Si le trafic qui entre est plus grand ou plus faible que d'habitude (Attaque DDoS en cours ou inaccessibilité au service ?)
- La quantité d'information qui sorte du SI (Exfiltration de données via internet ou Botnet ?)
- Surveiller le trafic web des utilisateurs pour ajuster les autorisations de sortie (oui pour Amazon, non à la pornographie ?)

Pour surveiller cette métrique, nous pouvons utiliser des services tel que Snort ou Suricata en version open source voir des solutions payantes comme IBM.
C'est aussi la métrique qui génère le plus de faux positif et la plus difficile à ajuster.

Pour finir, il y a une dernière métrique importante qui serais le trafic interne du SI. Cette dernière permet de voir si des machines tente d'avoir accès à des hôtes spécifiques (une machine utilisateur qui cherche à avoir accès a une caméra de sécurité ou a la configuration d'un pare-feu…) ou s'il y a une mauvaise configuration sur le réseau (tempête de broadcast ou tentative de DDOS interne.

ATTAQUES A SURVEILLER

Il y a énormément d'attaques différentes à surveiller sur un système d'information et ces attaques sont aussi complexes que diverses. Dans les différentes attaques à surveiller, nous pouvons proposer une liste non exhaustive :

- Le phishing, qui consiste à tromper un utilisateur pour obtenir ses logs et se connecter avec son compte. La meilleure façon de gérer ce problème reste de former le personnel sur les dangers du phishing et comment le reconnaitre.
- Les ransomwares, qui font beaucoup parler d'eux dans le secteur hospitalier. Même si la formation reste aussi ici la meilleure solution pour les éviter, il est aussi possible d'utiliser certains logiciel (tel que Snort ou Suricata) pour reconnaitre les signatures.
- Les attaques par déni de service (ou DDoS) qui porte atteinte à la disponibilité des services (autant interne qu'externe). La partie interne peut se gérer via des configurations de switch ou de routeur pour couper la connection d'une machine faisant trop de requêtes. La partie externe, elle, est plus complexe à contenir et cela se discute avec son fournisseur d'accès.
- L'accès non autorisé au réseau, autant via des points d'accès physiques non sécurisés que via un point WiFi mal configuré.
- Monitorer les versions logicielles et évaluer les CERT à leurs propos pour garantir la sécurité de l'infrastructure et éviter les failles dans des versions obsolètes.

La plupart de ces attaques sont assez basiques mais très courantes et si une partie peut se régler par des outils logiciels, une grande partie des menaces peut être évité avec une formation des agents sur ces menaces.
Pour finir, une veille constante sur les mises à jour des logiciels permet d'éviter des failles de sécurité nouvelles a l'issu des administrateurs systèmes, réseaux voir même des développeurs.