Formaliser une matrice de flux

Définition d'une matrice de flux

La matrice des flux est une liste des échanges de données entre une « source » (ex : application A) et une « destination » (ex : application B) à l'aide d'un protocole (ex : HTTPS) vers un port de destination (ex : port 443).

Objectif de la démarche

Réaliser une matrice de flux permet d'obtenir une liste exhaustive des échanges de données entre les différentes entités, applications, ou encore les différentes machines de l'infrastructure réseau. Elle est utile à la compréhension des interconnexions, notamment en cas d'incident de sécurité : celle-ci permet alors de réaliser un confinement précis du système impacté en évitant d'interrompre l'ensemble du système. L'intérêt est fort puisqu'il permet de maintenir un niveau de productivité et d'accès aux soins.

Etapes de réalisation de la matrice des flux

Formaliser une matrice des flux suppose d'avoir recensé au préalable les différents flux entre les entités, applications, systèmes et réseaux.
Certains outils (scans de découverte, outil de supervision, outil de surveillance de flux réseau type sFlow) peuvent s'avérer utiles dans ce cadre.
Une autre manière de faire consiste à analyser les flux entrants et sortants en se positionnant sur un équipement réseau (à l'aide d'un outil comme Wireshark/tcpdump par exemple) afin d'obtenir les informations nécessaires à la réalisation de la matrice. Cette démarche peut être répliquée application par application (en utilisant notamment l'inventaire des actifs réalisé au préalable).

Pour chaque flux il convient d'identifier les éléments suivants :

- **L'émetteur** de l'information (interne ou externe), appelé « source » ;
- **Le récepteur** de l'information (interne ou externe), appelé « destination » ;
- **La description du flux** (quelles données transitent) ;
- **Le protocole** utilisé ;
- **Le port** utilisé ;
- **Les mesures de sécurité mises en place :** authentification du flux, Access-List, chiffrement… ;
- Toute information utile permettant de mieux caractériser le flux (ex : par quel équipement réseau celui-ci transite-t-il, est-il monitoré…).

Les étapes à suivre afin de réaliser une matrice des flux peuvent être les suivantes :

1. Définir la portée de la matrice de flux (périmètre) ;
2. Recenser les flux sur le périmètre concerné ;
3. Compléter la matrice de flux avec les éléments récoltés ;
4. Faire valider la matrice par les différentes parties prenantes ;
5. Mettre à jour régulièrement cette matrice.

Points d'attention

La matrice de flux doit être validée par l'ensemble des parties prenantes (ex : architectes, équipe sécurité, etc.) afin que celle-ci soit la plus précise et la plus réaliste possible.

La difficulté réside dans le fait d'avoir le bon niveau d'exhaustivité, il faut non seulement représenter les flux externes (ex : ceux transitant par Internet) mais également les flux internes (ex : ceux entre applications internes). Construire une matrice globale peut s'avérer difficile, il est alors préférable d'en faire plusieurs (ex : une matrice par application Métier).

Pour chaque application, il peut être utile d'étudier la documentation éditeur afin de recenser les différentes recommandations en termes d'ouverture de flux minimum.

Pour bénéficier d'une matrice de flux réellement utile, il est indispensable de la mettre à jour régulièrement et à fréquence définie et lors de l'intégration de chaque nouveau « produit ».

Formaliser une matrice de flux

Exemple de matrice de flux

La matrice représentée ci-dessous est un exemple qui peut être repris et adapté.
En fonction des flux, certaines colonnes ne pourront pas être renseignées (indiquer alors « N/A »).

	Description		Source						Destination						Protocole	Port	Mesures de sécurité
#	Nom du flux	En quoi ce flux est-il nécessaire ?	Equipement	URL	IP	Masque sous-réseau	VLAN	Hébergement	Equipement	URL	IP	Masque sous-réseau	VLAN	Hébergement			
1	Accès web utilisateur	Permet à un utilisateur externe d'accéder à l'application depuis le web	Poste utilisateur	N/A	N/A	N/A	N/A	N/A	Serveur web application X	https://Applicationx.myweb.com	8.8.8.8	N/A	N/A	Azure	HTTPS	443	Authentification double facteur, chiffrement HTTPS
2	Accès admin serveur X	Permet d'administrer le serveur X à distance	Poste administrateur	N/A	192.168.10.X	N/A	12	N/A	Serveur X	https://serveurx.applicationy.local	2.12.32.17	N/A	18	Azure	RDP	3389	Filtrage IP (VPN), Authentification forte