Impact Influence

Préconisations pour la sécurité informatique du réseau

Faivre Mickaël 10/12/2024

Firewall

Actuellement, aucun filtrage n'est appliqué sur l'ensemble des flux (entrants et sortants du réseau). Cela implique que n'importe quelle personne peut accéder au réseau, y compris aux services critiques.

1. **Flux entrants :** En limitant les connexions entrantes, nous limitons ainsi l'accès aux différents services de l'entreprise depuis l'extérieur et, de fait, nous réduirons la surface d'attaque.
2. **Flux sortants :** La surveillance et le filtrage des flux sortants devrait également nous permettre de limiter l'exfiltration d'informations sensibles (ex : blocage des IP des C&C (commande et contrôle) de malwares connus). Il est aussi possible de bloquer l'accès à des sites ou services non-professionnels.
3. **Administration des services :** Configurer le firewall pour restreindre l'accès aux ressources d'administration du réseau (routeur, switchs, etc.) réduirait considérablement la surface d'attaque. Seules les machines connectées sur un VLAN dédié à l'administration pourraient y avoir accès.

Le déploiement d'un firewall serait un élément crucial pour l'amélioration de la sécurité du réseau de l'entreprise. Limiter les flux entrainerait mécaniquement une réduction des surfaces d'attaque disponible. De plus, la journalisation des événements nous permettrait d'être plus réactif en cas d'intrusion.

Serveur RADIUS

L'accès aux différents équipements du réseau n'est, pour l'heure, pas limitée. C'est un problème de sécurité majeur contre lequel nous devons nous prémunir.

En complément du firewall, limiter l'accès aux switchs et routeurs aux personnes autorisées, via un couple login/password, nous permettrait d'accroitre la sécurité en empêchant les accès non désirés à ces éléments.

Cette centralisation des identifiants apporterait un avantage en termes de simplicité mais aussi en termes de sécurité : une surveillance accrue des accès au serveur RADIUS limitera d'emblée les risques d'accès non autorisé aux différents équipements du réseau.

La journalisation des événements apportés par RADIUS sera aussi un avantage. Une surveillance des logs nous donnera la possibilité de voir plus rapidement les comportements à risque.

RADIUS fonctionnant aussi avec des annuaires type LDAP cela apporte une centralisation supplémentaire tout en supprimant les comptes partagés (chaque administrateur aura son propre compte plutôt que d'un compte unique devant être utilisé par tous).

Bastion

L'installation d'un bastion (type Guacamole) serait un facteur déterminant dans la sécurisation et la simplification de l'administration de nos services et réseau.

Le bastion représenterait un point d'entrée unique sur le réseau de l'entreprise. Toute connexion, interne ou externe, devra passer par le bastion et toutes les connexions aux services de l'entreprise (SSH, RDP, etc.) ne pourront être autorisées que si elles viennent du bastion.

Il nous offre une centralisation et, par extension, une possibilité de mieux surveiller les agissements des personnes s'y connectant et de focaliser la sécurité sur ce point précis.

Il apporte également une facilité pour les clients car toutes les connexions se font via un simple navigateur et ne nécessite pas l'installation d'un client particulier.

Nous pouvons également limiter les accès aux services en fonction des identifiants utilisés. Par exemple, l'accès SSH au serveur web pourra être limité aux seuls membres du SI.

Conclusion

Les trois éléments proposés pourront déjà offrir une couche de sécurité robuste. Chacun des services ajoutant une protection supplémentaire.

Ainsi, avec un firewall, un serveur RADIUS et un bastion, nous serons en mesure de pouvoir contrôler beaucoup plus finement les flux transitant sur notre infrastructure. Nous pourrons aussi centraliser l'ensemble des accès tout en ayant la possibilité de journaliser les événements et ainsi pouvoir agir en conséquence le moment venu.