Streamail

Application de Mailing Réseau d'Entreprise (RSE)

Nom de l'application : Streamail

Streamail est une application de distribution des courriers électroniques en entreprise servant de filtre au contenu web pouvant corrompre le réseau.

Fonctionnement :

Installé sur l'ordinateur de l'Administrateur du réseau de l'infrastructure (Programmeur) et en relation directe avec le serveur il va faire office de pare-feu direct sur les réceptions de courriers. Toutes les adresses sont répertoriées sur Streamail et la redistribution se fait en 2 temps; les courriers sont tout d'abord traités pour en vérifier le contenu et envoyer une demande de l'adresse IP/Mac ainsi que celle de l'adresse du serveur avant même de les avoir ouverts. Ensuite les courriers sont renvoyés vers leurs adresses plébiscitées. Les publicités seront gérées de manière globale comme indésirables après leur 1er traitement au sein de l'entreprise et n'apparaitront plus par un renvoi au niveau du serveur du refus de la requête.

Au cas où Les courriers ayant étés mal filtrés contiennent toujours un code malveillant; caché dans un overlay, Streamail observe avant le chargement du code et envoie un message d'alerte sur son exécution. Il est toujours possible qu'une erreur technique survienne et il reste toujours l'option d'invalider le blocage de ce courriel.

En cas d'e-mail frauduleux demandant un accès au réseau ou la vérification de ses codes d'usage, la redistribution sur les contacts, une demande d'accès aux données ou à leur téléchargement; un accès internet afin de rediriger une attaque d'un autre endroit du web, le réseau internet et intranet est bloqué sur cet ordinateur afin de ne pas contaminer le reste de l'infrastructure. Les actions ne sont jamais mieux traitées qu'au cas par cas.

Descriptif :

Les boîtes courriels créées pour la communication en interne correspondant sur le serveur de la structure à l'amortissement des problématiques réseau avec accès internet Streamail permet de mettre en place un set (ensemble) d'adresses e-mail professionnelles.

Pour séparer les flux de données; le lien direct avec un établissement une cliente ou un client, il y-a un découplage réseau forçant l'accès par Streamail avant tout envoi ou réception afin de créer une zone tampon.

Le serveur de l'entreprise renvoie normalement tous les courriers et ne s'affiche pas sur le chemin d'accès car, il est nécessaire de pouvoir se délester de toute attaque en restreignant le réseau.

Pour ne plus avoir à traiter que 1 ordinateur et réduire l'impact tout en conservant la productivité Streamail réalise plusieurs actions :

- Création d'une adresse IP pour masquer la vraie adresse IP et empêcher de retracer le matériel.
- Redistribution des courriers par adresse e-mail créée.
- Découplage réseau interne/externe et cryptage IPv6.
- Détection des tentatives d'intrusion dans Streamail ou sur le serveur.
- Détection des codes joints aux courriers en texte ou en pièce jointe.
- Gestion globalisée du signalement d'un courrier comme indésirable.
- Mémorisation des requêtes à ne plus accepter dans la redistribution.
- Overlay inclus dans l'application à l'ouverture des courriers.
- Exclusion du poste pouvant être ou étant infecté sur le réseau.
- Alertes récursives ouverture d'un courrier frauduleux.

Avec la redistribution par adresse IP du matériel de l'entreprise et association pour le réseautage interne et externe ce système de pare-feu place directement ou indirectement les messages malveillants en quarantaine faisant de Streamail l'outil à joindre à une bonne protection antivirus.

Une entreprise sécurisée de bout en bout commence par séparer les mailings internes de la redistribution vers des utilisatrices/utilisateurs ou entreprises dont les responsabilités peuvent être mises en doute au niveau technique.