Antispam à l'Unil

Le filtre anti-virus et anti-spam de l'Unil

> Suite à un incident de sécurité (plus d'info ici: https://www.unil.ch/news/1766138859124), la quarantaine utilisateur est actuellement désactivée. Tous les mails qui auraient fini en quarantaine sont directement remis dans le dossier **Courrier indésirable** de votre boîte mail.

Nous utilisons Cisco Email Security pour scanner les emails arrivant et quittant le réseau de l'Unil. Ce service va analyser les mails et mettre les mails détectés comme spam ou phishing dans votre quarantaine, et bloquer les pièces jointes malveillantes.

En cas de résultat positif de cette analyse, le message subit des modifications dont le marquage du sujet qui permet alors à chacun de le classer ou de le détruire aisément (avec un filtre automatique par exemple). Les messages reconnus comme spam seront mis en quarantaine, ne polluant ainsi plus du tout la boîte aux lettres personnelle.

Cisco Email Security repose sur plusieurs couches de protection et de détection, parmi lesquels

- listes de blocage/sécurité
- de multiples filtres antispam
- un anti-virus
- un filtre analysant les pièces jointes pour des menaces connues
- un filtre "graymail" détectant les mails de marketing, de réseaux sociaux, etc
- des filtres manuels
- un filtre basé sur les menaces récentes détectées par Cisco
- etc.

Que fait le filtre anti-spam?

Dans le filtre anti-spam, le mail est soumis à une batterie de tests détectant des phrases ou des tournures souvent utilisées par les spammeurs, les URLs suspicieuses, ainsi qu'une analyse de la

réputation du serveur de messagerie de l’expéditeur.

Chaque test attribue une note au message. A la sortie, le message est considéré comme du spam si la somme des notes dépasse un certain seuil. Des lignes indiquant les résultats de ces tests sont ajoutées dans l'entête du message. Ces lignes sont reconnaissables par leur libellé "**IronPort-**" ou "**X-IronPort-**". Si le seuil est dépassé, il y deux options:

1. Le seuil est dépassé et Cisco Email Security suspecte que le message est un spam: le message {Suspected Spam?} est inséré dans le sujet et le message est distribué normalement.
2. Le seuil est largement dépassé, indiquant que Cisco est sûr que le message est un spam: le message {Spam?} est inséré dans le sujet et le message est mis dans la quarantaine de l'utilisateur.

> Suite à un incident de sécurité (plus d'info ici: https://www.unil.ch/news/1766138859124), la quarantaine utilisateur est actuellement désactivée. Tous les mails qui auraient fini en quarantaine sont directement remis dans le dossier **Courrier indésirable** de votre boîte mail.

Pour voir sa quarantaine, il faut se connecter sur https://spam.unil.ch avec ses identifiants Unil.

Que fait le filtre anti-virus?

Lorsqu'un message arrive dans Cisco Email Security, l'anti-virus Sophos effectue son analyse et, selon le résultat de l'analyse, va distribuer le courriel, ajouter un avertissement dans le sujet du message ([WARNING:), ou mettre le message en quarantaine.

La mise en quarantaine

> Suite à un incident de sécurité (plus d'info ici: https://www.unil.ch/news/1766138859124), la quarantaine utilisateur est actuellement désactivée. Tous les mails qui auraient fini en quarantaine sont directement remis dans le dossier **Courrier indésirable** de votre boîte mail.

~~Plutôt que recevoir dans sa boîte aux lettres les messages marqués comme spam, Cisco va conserver ces emails dans une quarantaine pendant 30 jours puis éliminés. Vous recevrez un email hebdomadaire si un ou plusieurs emails qui vous sont destinés ont fini dans votre quarantaine.~~

~~Il n'est pas possible de modifier la fréquence d'envoi du rapport de quarantaine, ni de configurer Cisco pour envoyer tous les messages, spam y compris, sur sa boîte plutôt que la quarantaine. Nous estimons que le filtrage amélioré offert par Cisco rend cela superflu.~~

~~Les messages mis en quarantaine peuvent être à tout moment consultés et éventuellement retirés de la quarantaine via l'interface web accessible à l'adresse https://spam.unil.ch Pour y accéder, il faut s'authentifier avec son nom d'utilisateur et mot de passe habituels (les mêmes que pour la messagerie). Dans la liste affichée des messages mis en quarantaine, vous pouvez libérer un message si besoin, c'est-à-dire de demander à Cisco Email Security de déposer tout de même le message dans sa boîte aux lettres. Il est également possible de gérer ses listes sécurisée et de blocage, qui sont des listes blanches et noires personnelles.~~

Le filtre anti-spam peut-il se tromper?

Si les tests qu'effectue le filtre anti-spam étaient systématiquement efficaces, le problème du spam serait définitivement réglé. Dans la réalité, bien que le taux de succès soit élevé, il faut prendre des dispositions pour traiter les erreurs possibles du système qui sont de deux types:

Les "faux positifs"

C'est le cas où un message légitime est marqué à tort comme spam. Il ne faut donc pas oublier de consulter régulièrement le rapport hebdomadaire envoyé par Cisco Email Security afin d'y déceler les éventuels faux positifs. Contactez le helpdesk en donnant les détails de l'email qui a été faussement bloqué avec ses entêtes en suivant la marche à suivre ici.

Les "faux négatifs"

C'est le cas où un spam déjoue les filtres de Cisco Email Security et parvient dans votre boîte aux lettres sans être marqué.

Afin d'améliorer l'efficacité de Cisco Email Security, il est utile de signaler ces erreurs en renvoyant ces messages au helpdesk avec ses entêtes en suivant la marche à suivre ici.

Créé 2019-10-15 12:53:23 UTC par Chr Gr
Mis à jour 2026-10-02 08:52:13 UTC par Chr Gr