Gestion de son serveur de courrier électronique

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 janvier 2024

https://www.bortzmeyer.org/mon-serveur-messagerie.html

Je gère depuis longtemps mon propre serveur de courrier électronique. Cet article va présenter quelques observations issues de cette expérience. Si vous êtes pressé·e, voici un résumé : 1) ça marche et je peux envoyer du courrier y compris aux grosses plateformes 2) c'est compliqué et ça fait du travail.

Je commence par des explications générales, si vous vous intéressez aux détails techniques, ils sont à la fin. Si vous n'êtes pas familier·ère avec le monde du courrier électronique, quelques notions. Un élément essentiel du cahier des charges du courrier est la possibilité d'envoyer des messages non sollicités, à quelqu'un avec qui on n'a jamais échangé. Les cas d'usage de cette fonction sont nombreux (candidature spontanée à une entreprise, demande d'un devis à une entreprise, remarques sur un article de blog, etc.). Cet élément est une des raisons du succès du courrier électronique, qui reste aujourd'hui le principal moyen de contact universel. Mais il y a un côté négatif, le spam, puisque les spammeurs, eux aussi, utilisent cette possibilité pour nous envoyer leurs messages sans intérêt. La lutte contre le spam est un sujet complexe <https://framablog.org/2020/11/13/i-dont-want-any-spam/> mais le point qui nous intéresse ici est que, comme pour toute question de sécurité, il y a forcément des faux négatifs (des coupables qui s'en tirent) et des faux positifs (des innocents frappés à tort). Ceux qui vous diraient le contraire et prétendraient qu'on peut avoir des solutions sans faux positifs ni faux négatifs sont des menteurs ou des commerciaux.

Des organisations qui gèrent des grandes plateformes de courrier, comme Google avec gmail.com ou Microsoft avec outlook.com et hotmail.com, déploient diverses techniques pour lutter contre le spam. Un effet de bord de ces techniques, dit-on souvent, est de bloquer les petits hébergeurs ou les auto-hébergeurs, les petites structures ou les particuliers qui, comme moi, gèrent leur propre serveur. Une accusation courante est qu'il ne s'agit pas de difficultés techniques, mais d'une politique délibérée, que ces grandes entreprises essaient volontairement de tuer cet auto-hébergement. Il n'y a pourtant aucune raison technique, ni dans les normes techniques du courrier électronique (RFC 5321 [1] et RFC 5322), ni dans des règles légales, qui impose que le courrier ne passe que par un oligopole de grandes entreprises ; une personne ou une petite organisation peut parfaitement gérer son propre serveur. Sans

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc5321.txt

le spam, ce serait même plutôt simple techniquement. Mais, avec le spam et ses conséquences, les choses se compliquent.

(Point philosophico-politique au passage : la délinquance ou l'incivilité a des conséquences directes, si on vous vole votre vélo, vous n'avez plus de vélo mais aussi, et c'est trop souvent oublié, des conséquences indirectes et qui sont souvent plus coûteuses : déploiement de mesures de sécurité chères et gênantes, perte de confiance qui délite la société, etc.)

Voyons maintenant la légitimité des plateformes de courrier électronique à prendre des mesures anti-spam qui m'empêcheront parfois de joindre mon correspondant. Le gestionnaire d'un service de messagerie est maître chez lui. Il ou elle peut déployer les techniques qu'il veut, même si cela bloque certains émetteurs, de même que vous n'êtes pas obligés de prendre le tract qu'on vous tend dans une manifestation. Google n'est pas obligé d'accepter vos messages, rien ne l'y force. Toutefois, la situation n'est pas la même que celle de la personne qui ne veut pas prendre un tract. Ici, il y a un intermédiaire, qui va décider pour ses utilisateurs. Ceux-ci et celles-ci ne sont jamais informé·es de la politique de lutte anti-spam de leur hébergeur. Mieux, la propagande des grandes plateformes affirme en général que, si le message n'arrive pas, c'est de la faute de l'émetteur. Beaucoup d'utilisateurs ou d'utilisatrices croient sur parole ce discours.

J'ai ainsi été étonné de voir que des gens, ne recevant pas mes messages, ne voulaient pas se plaindre auprès de leurs fournisseurs, me demandant de le faire. Pourtant, n'étant pas client de `outlook.com`, j'avais certainement beaucoup moins de poids sur Microsoft que des utilisateurs de leur service.

(Si vous utilisez le fédivers comme réseau social, vous aurez noté que c'est pareil, et pour cause, le courrier électronique était un réseau social décentralisé bien avant le fédivers. C'est pareil car le gestionnaire d'une instance peut refuser qui il veut. En soi, ce n'est pas un problème, mais cela se complique quand le petit chef qui dirige une instance le fait pour le compte de ses utilisateurices.)

Donc, le petit hébergeur de courrier part avec un sérieux désavantage : Google ou Microsoft se fichent pas mal de lui, et leurs utilisateurs et utilisatrices font une confiance aveugle à ces GAFA, davantage qu'à leurs propres correspondant·es. Google, Microsoft, Orange, `laposte.net`, etc, se satisferaient certainement d'un oligopole où tout se passerait entre eux. Heureusement, le monde du courrier électronique n'en est pas là. On va voir qu'il n'est pas exact de dire que les gros hébergeurs bloquent délibérement les petits. D'une part, ils ne sont pas les seuls à poser problème, d'autre part, ils ne sont pas acharnés à bloquer les petits, c'est plutôt qu'ils s'en foutent.

(Au passage, les politiques anti-spam des grosses plateformes de courrier peuvent rejeter le message directement, ce qui donne à l'expéditeur un message d'erreur, ou bien escamoter le message sans avertissement, ou encore le mettre dans la boite Spam du destinataire. Je vais traiter tous ces cas ensemble.)

Parmi les problèmes que j'ai rencontrés, le fait d'être listé de temps en temps dans une liste de blocage de Spamhaus. Mon serveur n'a jamais envoyé de spam, il n'héberge même pas de liste de diffusion (héberger une liste est bien plus difficile, puisque, par construction, elles envoient en masse, ce que certains récepteurs considèrent comme du spam). La communication avec Spamhaus n'a jamais donné de résultat, notamment lorsque je leur ai demandé les spams que j'avais soi-disant envoyés, pour que je puisse les étudier et comprendre un éventuel problème (jamais de réponse). Le rejet du courrier via l'utilisation de cette liste est loin d'être spécifique aux gros méchants GAFA. Pas mal de libristes utilisent la liste de Spamhaus et se montrent assez agressifs quand on leur suggère que c'est peut-être une mauvaise idée (Spamhaus a beaucoup de "*fanboys*").

Autre problème, avec Microsoft, qui gère des services comme `outlook.com` et `hotmail.com`. Tous les services Microsoft rejetaient mon courrier par intermittence :

```
<DESTINATAIRE@outlook.com>: host
    outlook-com.olc.protection.outlook.com[52.101.73.31] said: 550 5.7.1
    Unfortunately, messages from [92.243.4.211] weren't sent. Please contact
    your Internet service provider since part of their network is on our block
    list (S3150). You can also refer your provider to
    http://mail.live.com/mail/troubleshooting.aspx#errors.
    [AMS0EPF000001AE.eurprd05.prod.outlook.com 2023-10-07T10:03:08.034Z
    08DBBB93AD81129F] (in reply to MAIL FROM command)
```

Résoudre le problème est très chronophage. Il faut essayer un des innombrables moyens de contact avec Microsoft comme , (le programme SNDS - "*Smart Network Data Services*" - ne fait qu'afficher, il ne modifie pas les listes de blocage) ou (le troisième a marché, pour moi, j'ai pu parler à un humain), ce qui nécessite parfois un compte Microsoft (et une adresse Gmail pour pouvoir leur écrire…). (Rappelez-vous que les clients de Microsoft n'osent jamais rien demander à Microsoft. Ce sont des gens comme moi, qui ne sont pas clients de cette entreprise, qui doivent la contacter, ce qui est évidemment moins efficace.) Bref, après des mois de discussions kafkaïennes (Microsoft prétendant même que mon adresse IP n'était pas bloquée alors que leur propre message d'erreur, cité plus haut, dit explicitement le contraire), Microsoft a fini par corriger le problème (« *"Thank you for contacting the Outlook.com Deliverability Support Team. We have implemented mitigation for your IP (92.243.4.211) and this process may take 24 - 48 hours to replicate completely throughout our system."* »). Je peux désormais envoyer du courrier à `outlook.com` et `hotmail.com` (pour l'instant, en tout cas). Mais on se doute bien que toustes les administrateurices de serveurs de messagerie n'ont pas envie de dépenser autant de temps et d'effort avec cette entreprise.

Concrètement, ma plateforme actuelle est composée d'un serveur de messagerie, qui est un VPS sous Debian. (Vous pouvez trouver son nom <https://dns.bortzmeyer.org/bortzmeyer.org/MX>, tout est forcément public, pour que ça fonctionne, ce qui peut avoir des conséquences en terme de vie privée.) Ce serveur est situé chez Gandi. J'aurais pu l'héberger à la maison (mon FAI bloque le port 25 - celui de SMTP - par défaut mais permet de l'ouvrir gratuitement simplement en un clic sur l'interface client) mais je n'avais pas envie de gérer l'alimentation électrique permanente, certains opérateurs qui refusent le courrier provenant d'adresses IP « résidentielles », etc. Sur cette machine tournent Postfix et les autres logiciels utiles (comme OpenDKIM <http://www.opendkim.org/>).

Bien sûr, j'utilise SPF (mon enregistrement <https://dns.bortzmeyer.org/bortzmeyer.org/TXT>), DKIM (la clé actuelle <https://dns.bortzmeyer.org/mail0._domainkey.bortzmeyer.org/TXT>) et même DMARC (avec une politique laxiste <https://dns.bortzmeyer.org/_dmarc.bortzmeyer.org/TXT> car DMARC casse les listes de diffusion, ce que je trouve inacceptable). Et j'ai un enregistrement inverse (de l'adresse IP vers le nom) dans le DNS. J'ai testé toutes ces configurations avec divers auto-répondeurs <https://www.bortzmeyer.org/repondeurs-courrier-test.html>. Et, pour me protéger moi-même contre le spam, je valide les assertions SPF, DKIM et DMARC, ce qui ajoute au courrier des informations (RFC 8601) comme :

```
Authentication-Results: mail.bortzmeyer.org;
        dkim=pass (2048-bit key; unprotected) header.d=mailchimpapp.net
        header.i=rayna=rs-strategy.consulting@mailchimpapp.net header.a=rsa-sha256 header.s=k2 header.b=Gr+4sGal
        dkim-atps=neutral
Authentication-Results: mail.bortzmeyer.org; spf=pass (sender SPF authorized) smtp.mailfrom=mail198.atl221.rsgsv
        (client-ip=198.2.139.198; helo=mail198.atl221.rsgsv.net;
        envelope-from=bounce-mc.us5_165546418.9420482-fccde11058@mail198.atl221.rsgsv.net)
```

Comme SPF et DKIM ne font que de l'authentification (et qu'un spammeur peut lui aussi s'authentifier), j'ajoute du "*greylisting*" (RFC 6647), avec Greyfix <https://www.kim-minh.com/pub/greyfix/>, SpamAssassin (comme tout le monde…) et surtout bogofilter, qui est particulièrement efficace, les faux positifs sont en nombre infime.

Quelques lectures :

---

https://www.bortzmeyer.org/mon-serveur-messagerie.html

— Vous ne devriez pas faire tourner votre serveur de mail parce que c'est dur <https://poolp.org/fr/posts/2019-08-30/vous-ne-devriez-pas-faire-tourner-votre-serveur-de-mail-> (le titre n'est pas à prendre au premier degré).
— Être un géant du mail, c[Caractère Unicode non montré [2]]est faire la loi…<https://framablog.org/2017/02/17/etre-un-geant-du-mail-cest-faire-la-loi/> (sans défendre les GAFA - qui n'ont pas besoin de moi pour ça, je trouve l'article trop unilatéral ; mes messages ont souvent été bloqués par des petits serveurs mal gérés).

En conclusion, si vous m'avez écrit et que vous n'avez pas eu de réponse, c'est peut-être que votre hébergeur de courrier fait n'importe quoi et bloque mes messages. Dirigez vos reproches vers eux, pas vers moi.

2. Car trop difficile à faire afficher par LaTeX