Courriels validés de domaines authentifiés

Octobre 2017 : mois européen de la cybersécurité

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
ET DES FINANCES

MINISTÈRE DE L'ACTION
ET DES COMPTES PUBLICS

TABLE DES MATIERES

MENACES

En matière de sécurité, la messagerie électronique est généralement cataloguée comme une source de fuites d'information :

- C'est un des principaux flux à circuler en clair sur certains segments des réseaux inter-entreprises, y compris quand il contient des informations sensibles.
- Comme il est possible de cacher sa responsabilité derrière le constat précédent et que la traçabilité n'est généralement pas assurée, les utilisateurs eux-mêmes ne sont pas les derniers à participer aux fuites.

Pourtant le courriel est aussi utilisé comme une « preuve » d'identité, par exemple dans les procédures de récupération de mots de passe.

Enfin, et surtout, **le courriel est devenu le principal vecteur de compromissions / fraudes, par hameçonnage (« phishing »)** ou harponnage (dans le premier cas, il s'agit de campagnes sans cible individuelle spécifique, tandis que le second, il s'agit d'opérations parfaitement ciblées avec recherche d'information pour crédibiliser spécifiquement les messages), pour toutes sortes de compromissions de systèmes d'information.

Les problèmes de la messagerie électronique et particulièrement du protocole de relai entre serveurs (SMTP) proviennent de sa genèse, dans un environnement universitaire, avec de faibles enjeux de sécurité.

Spécifiquement, les défauts des systèmes primitifs étaient :

- à la réception, d'accepter tous les messages, sans discrimination ;
- à l'émission : ne pas donner suffisamment d'indication pour qu'un serveur en réception puisse vérifier la légitimité, l'authenticité du courriel

Dès le développement commercial d'Internet, la messagerie électronique a été un des premiers usages à rencontrer l'adhésion des utilisateurs, et à être abusé. En retour, toute une panoplie de mesures a été mise en œuvre, basée essentiellement sur l'idée d'identifier les mauvais germes :

- scan anti-virus des pièces jointes
- identification des adresses IP à mauvaise réputation

Mais ces systèmes de listes noires atteignent leurs limites, particulièrement face à un espace que l'attaquant peut agrandir à loisir et ils sont aujourd'hui incapables de juguler les campagnes d'hameçonnage par exemple. Et du fait de l'émergence d'IPv6, entre autres, les systèmes de réputation basés sur les adresses IP vont par nécessité s'effacer au profit de systèmes basés sur la réputation / l'authenticité des domaines, objet de ce document.

HISTORIQUE ET ETAT DE L'ART

DNS inverse et greylisting

Les efforts pour attribuer les courriels à une source fiable sont anciens. Dès les années 2000 et la lutte contre l'exploitation de PC compromis de particuliers, les administrateurs de systèmes de messagerie ont mis en place des vérifications de DNS inverse. Cela garantit que l'émetteur dispose d'une adresse IP fixe, généralement associée à un nom de serveur en bonne et due forme, rappelé également en début de l'échange SMTP.

Cette époque a également vu émerger les méthodes de *greylisting*. Elles ont pour but non pas de vérifier l'authenticité du serveur émetteur mais sa conformité aux comportements spécifiés par les standards, en ralentissant les campagnes de pourriels lancées par des logiciels malveillants qui n'ont souvent qu'une fenêtre d'exploitation réduite.

SPF

Plus fondamentalement, l'identification des serveurs émetteurs a commencé vers 2003 avec les premiers travaux sur SPF qui ont a abouti à un RFC en 2006. Il s'agit pour les administrateurs de domaines **d'identifier les adresses IP des serveurs légitimes** pour émettre des courriels en leur nom.

DKIM

En parallèle, d'autres travaux étaient initiés pour permettre d'apposer un cachet numérique à chaque courriel émis. Les premières ébauches de DKIM remontent à 2006 pour une normalisation rapide sous forme de RFC (2007). Concrètement, cette deuxième norme assure qu'**un courriel signé numériquement n'a pas été modifié** par les différents relais. Il assure l'authenticité complète d'un message et même son intégrité si l'administrateur de domaine assure lui-même capable la distribution sécurisée des droits à ses utilisateurs.

DMARC

Malgré deux normes, il existait encore une faille dans l'authentification des courriels : SPF par exemple permet de vérifier le domaine de l'émetteur qui est sur l'enveloppe d'un message. Rien n'empêche un attaquant d'usurper le « papier à entête » à l'intérieur de l'enveloppe.
A partir de 2011, le consortium DMARC.org a repris des spécifications annexes de DKIM (ADSP) avec précisément pour objectif de créer un standard pour assurer « l'alignement » entre les identités *sur* et *dans* l'enveloppe.
Après inclusion dans le chemin des normes de l'IETF, DMARC a ainsi abouti à un RFC en 2015. Il s'appuie sur SPF et DKIM. Il permet d'indiquer la conduite à tenir si les courriels reçus montrent des discordances entre IP et domaines pour le SPF, et entre ses éléments et sa signature pour le DKIM.

Un point important de cette norme est que, **outre la publication de règle de gestion** (mise en quarantaine, rejet des courriels douteux), elle **définit un moyen et un format de retour d'information des plateformes de réception aux domaines émetteurs**. Les grands émetteurs gagnent ainsi une visibilité sur l'utilisation de leurs domaines (leurs marques), permettant d'être informés de campagnes de fraudes par usurpation d'identité, ou tout simplement de serveurs mal configurés qui ne permettent pas aux messages d'être correctement délivrés.

STARTTLS

Orthogonalement à ce travail sur l'authenticité des courriels, des travaux de standardisation **du chiffrement des transmissions** conduit en 2014 à un RFC dit de chiffrement opportuniste. Concrètement les relais de messagerie chiffrent la transmission des messages dès que les deux parties découvrent qu'elles ont des implémentations compatibles.
Le système n'est toutefois pas parfait puisqu'un intermédiaire peut modifier les échanges pour casser le processus de découverte et maintenir la transmission en clair. Concrètement ce constat est exploité par certains équipements de sécurité (Cisco) et par certains pays (Tunisie) selon une étude de Google.
Encore une fois, le DNS peut venir être appelé en renfort via des enregistrements DANE / DNSSEC permettant à l'émetteur de vérifier l'identité du serveur en réception.

Adoption à fin 2016

Les normes techniques étant anciennes, la question est plutôt de savoir quelles sont les dynamiques d'adoption. Sur ce point, il faut distinguer par catégories d'organisations.
Les fournisseurs internationaux de service grand public de messagerie (Gmail, Hotmail / Outlook.com, Apple, Yahoo, Amazon...) sont les premiers à adopter les normes qu'ils ont largement contribué à définir.
En France, les déploiements sont plus frileux, car les principaux acteurs sont des opérateurs télécoms qui n'ont pas d'audience internationale. On note toutefois la politique plus volontariste de La Poste (@laposte.net), sans doute en rapport avec les ambitions de ce Groupe comme fournisseur d'identité.

Du côté entreprises, un état des lieux démontre une situation disparate [1].
Pour que leurs courriels arrivent bien dans les boîtes aux lettres de leurs destinataires, les « petites » organisations (moins de 1.000p) ont été déjà « obligées » de répondre aux attentes des grands services de messagerie internationaux en adoptant au minimum SPF.
Les grandes organisations peuvent encore se prévaloir de leur poids pour ne pas voir leurs messages écartés. Très souvent aussi, elles délèguent à des prestataires le soin de distribuer leurs messages commerciaux ou transactionnels, et les prestataires utilisent des domaines « annexes » pour faire leurs envois.

[1] L'étude nationale sur la sécurité de l'espace numérique français publiée le 3 octobre 2017 apporte un éclairage statistique plus complet.

UNE DYNAMIQUE QUI S'ACCELERE

Néanmoins, la pression des fournisseurs de service de messagerie en ligne augmente via les interfaces web qu'ils proposent aux utilisateurs. Comme pour HTTPS, ils utilisent des alertes pour pointer du doigt les absences de signes techniques de confiance.

Par exemple, dans Gmail, en l'absence de chiffrement, les messages sont flanqués d'un cadenas rouge barré. L'aide en ligne stipule clairement : « N'envoyez aucun document confidentiel, tel qu'une déclaration d'impôt ou un contrat, à cette adresse e-mail. »
Plus récemment, le même portail de messagerie a commencé à afficher un symbole différent « ? » (à la place des initiales) quand le service n'a eu aucun moyen de s'assurer de l'authenticité de l'émetteur. Les différentes annonces de ces fournisseurs de messagerie Grand Public vont tous dans le même sens : mettez en place les normes permettant d'assurer l'authenticité ou vos messages finiront soit dans le dossier Courrier indésirable, soit seront marqués de diverses alertes toutes aussi peu encourageantes.

Fin 2016, le National Cyber Security Centre britanique a lancé un programme intitulé « Making email mean something again » dont les concrétisations techniques seront l'implémentation dans les services gouvernementaux britanniques de DMARC / DKIM / SPF [7]. Les ministères économiques et financiers ont adopté un standard analogue à la même période (document non public, avec des jalons sur 24 mois en raison de l'étendue et la diversité des directions concernées).

RECOMMANDATIONS PRATIQUES

Pour revenir à une situation où un destinataire peut avoir confiance dans l'authenticité de l'émetteur et la confidentialité des échanges (et cesser les appels à ne pas cliquer sur les liens dans les courriels qui sont soit irréalistes [2] soit contraire à une analyse économique coût / avantage [3]), il faut effectivement en 2018 implémenter la panoplie complète SPF / DKIM / STARTTLS / DMARC.
Les services qui font du relai de messages (en gardant l'adresse de l'émetteur d'origine, ce qui n'est qu'un cas particulier) peuvent maintenant s'appuyer sur le standard émergent ARC, ce qui permettra de clore les combats d'arrière-garde.

Pour faciliter la prise en compte de cet objectif général et limiter les tâtonnements de chacun, les ministères économiques et financiers rendent ici publics ses choix d'implémentation. Les notes du M[3]AAWG (Messaging Malware Mobile Anit-Abuse Working Group [9]) sont aussi une source de documentations plus pointues.

Empêcher l'emploi de domaines non utilisés pour l'émission de courriel

Les organisations de taille respectable disposent d'un portefeuille de domaines. Il n'est pas rare que leur portail soit connu et accessible à une adresse www.marque.com mais que les courriels légitimes des collaborateurs soient émis selon le schéma prenom.nom@legroupe.fr
Les usurpateurs de courriel ne manqueront pas d'émettre des courriels du type prenom.nom@marque.com comptant sur les faits que les consommateurs, les entreprises connaissent le groupe sous ses noms de marques.

Dès lors il faut contrecarrer leur projet en publiant des politiques qui rendent clairs l'absence d'utilisation du domaine (et éventuellement des sous-domaines) pour l'envoi de courriel.

SPF : `v=spf1 -all`
DMARC : `v=DMARC1;p=reject;sp=reject`

Effectuer les signatures DKIM au plus près de l'émetteur

Quand un message transite par plusieurs relais internes, il peut être tentant de signer au niveau du dernier relai, exposé à Internet et d'utiliser une seule clé de signature.
Les organisations s'exposent alors à l'insertion de messages illégitimes dans leurs relais internes ; en cas de compromission de clés, l'impact est global. On constate également une difficulté croissante à procéder aux rotations de clés.
Les pratiques recommandées par les organisations qui utilisent DKIM à grande échelle consistent à :

- **Signer au plus près de l'émetteur**
  DKIM a la notion de « sélecteurs » qui peuvent être utilisés en parallèle à un même moment. Chaque relai (ou cluster quand un groupe de serveurs forme un bloc homogène) dispose de sa propre clé de signature. Comme le cachet

[2] comment faire une réinitialisation de mot de passe ?
[3] voir l'article Principes économiques et cybersécurité dans le dossier de la conférence du 3 octobre 2017

de la poste, cela permet de retrouver le « bureau de poste » et de changer de tampon des bureaux de manière désynchronisée.

- **Utiliser un sélecteur incluant un numéro d'ordre ou de série**
  Comme on ne peut pas synchroniser à la seconde près le changement dans le DNS et dans le relai SMTP signataire, on change de sélecteur pour faire une rotation de clés.
  1. On signe avec le « selecteur1 » (mis en place à la conception du système).
  2. On publie « selecteur2 » et la clé associée dans le DNS ; on laisse « selecteur1 » dans le DNS pour que les messages qui ne sont pas encore arrivés à destination soient authentifiables à leur arrivée.
  3. On modifie le relai pour signer avec « selecteur2 »

  NB : les étapes 2 et 3 peuvent maintenant être séparées de plusieurs jours.

  Pour s'y retrouver dans les sélecteurs, il est donc conseillé d'utiliser un identifiant qui désigne :
  - **le relai signataire**
  - **la date (format AAMMJJ) de la mise en place de la clé**

  i.e. sélecteur « `exchange170307` **»**

(par exemple Gmail utilise actuellement un sélecteur `s=20161025;`)

- Canoniser et signer les champs habituels :
  `c=relaxed/relaxed;`
  `h=Date:From:To:Subject:MIME-Version:Content-Type:Message-ID;`

- Utiliser les alias DNS quand la gestion du nom de domaine est dissociée de l'exploitation des systèmes de courriels
  Office365 / Exchange Online Protection utilise le renvoi par CNAME pour assurer la gestion de leurs clés de manière centralisée tout en leur demandant une configuration initiale très simplifiée à leurs clients [1].
  Si un relai ministériel signe pour plusieurs domaines, il peut utiliser une seule clé (active à un instant) pour ce relai, plutôt qu'une clé dédiée par domaine en utilisant ce dispositif de redirection.
  i.e.

```
selecteur._domainkey.domainegere.fr 3600 IN CNAME selecteur._domainkey.domainegestionnaire.fr
selecteur._domainkey.domainegestionnaire.fr 3600 IN TXT "v=DKIM1…"
```

Employer un chiffrement opportuniste à l'état de l'art cryptographique

Le chiffrement initié par STARTTLS est opportuniste : il nécessite l'accord entre les deux relais. Cela ouvre la porte à de nombreux scénarios de menaces. Afin de limiter leur occurrence ou leur impact, il est recommandé de :

- Ajouter un entête MIME précisant le chiffrement utilisé lors de la transmission
  i.e. dans Postfix `smtpd_tls_received_header = yes`

- Configurer les relais avec uniquement des moyens cryptographiques réputés sûrs (TLS ≥ 1.1, pas de RC4, pas de MD5, pas de DES, pas de chiffrement

export, pas de chiffre NULL…)
Le niveau B sur l'échelle de test de Cryptosense ([2] ce service hébergé en France malgré le nom) est l'objectif minimum à atteindre.
SSLyze [3] est un outil Python pour tests internes ou locaux.

- Utiliser un certificat avec une identité alignant les noms fournis par MX (indication des serveurs gestionnaires de courriel en réception), EHLO (nom fourni par les serveurs aux connections SMTP entrantes) et PTR (résolution inverse de l'adresse IP)

- Résoudre les MX des domaines destinataires via DNSSEC

Véhiculer les métadonnées via les entêtes MIME

A partir du moment où des signatures DKIM sont utilisées pour authentifier les messages, toute modification risque d'invalider la signature. Pour éviter cet écueil, il convient de :

- Utiliser la politique DKIM proposée ci-dessus afin que les informations signées ne comprennent que l'objet, la date & heure, et le corps du message, à l'exclusion des autres entêtes MIME.
  A contrario, l'ajout de préfixe à l'objet ([SPAM] ou autre), de pied de courriel est à décourager.

- Utiliser les entêtes MIME pour véhiculer les métadonnées associées à un message entre relais (et non des modifications de l'objet ou du message)
  Par exemple, les gestionnaires de liste ajoutent les entêtes List-Unsubscribe: et associés, les anti-virus et autres systèmes de filtrage leur note d'évaluation pour aiguiller un message vers le dossier Pourriel des clients de messagerie.

Assurer la validation des messages entrants

L'objectif de tous ses efforts de sécurisation est que les messages usurpant des domaines participants n'arrivent pas jusqu'aux boîtes aux lettres des utilisateurs.
Il convient donc de valider les messages entrants à partir de la politique DMARC publiée par le domaine.
Ensuite deux pratiques se distinguent : soit l'organisation rejette au plus tôt le message (mais elle doit gérer les faux positifs et les notifications automatiques), soit elle s'assure que la non-validation est bien propagée jusqu'au client de messagerie et le classement dans un répertoire Spam ou Courrier indésirable.

Faire reconnaître les identifications de suspicion par les clients de messagerie

Dans le cas où les messages suspicieux sont transmis vers les clients de messagerie, il faut s'assurer que l'identification des messages est bien prise en compte par l'aval. Comme toutes métadonnées, cela se fait par les entêtes MIME.

Thunderbird peut reconnaître X-Spam-Flag ajouté par un SpamAssassin au niveau de la configuration du client [4]

Exchange reconnaît par défaut l'entête `X-MS-Exchange-Organization-SCL` au niveau du serveur [5]. Les valeurs supérieures à 5 (en configuration par défaut) sont envoyées dans le dossier Courrier indésirable de l'utilisateur, où les liens sont désactivés, etc. Il est donc nécessaire de mettre en place une Transport Rules pour abouter un marquage amont (SpamAssassin ou autre) sur un entête reconnu par Exchange.

Des règles Sieve peuvent être implémentés [8] sur les agents chargés de la livraison dans les boîtes aux lettres électroniques.

Implanter de manière progressive les politiques DMARC

Une politique DMARC est utile dès le début d'un projet de sécurisation du courriel.

Etape 1 : Supervision
Cette politique ne donne pas d'instruction de blocage des messages à leur réception mais avec une option type `rua` elle permet de recevoir des rapports des fournisseurs de courriel, notamment Gmail. Cela fournit le point de vue sur les émetteurs légitimes non référencés (campagnes de communication externalisées) comme illégitimes (usurpations d'email)

```
v=DMARC1;p=none;rua=mailto:courriel-rapport@domaine.fr
```

NB : dans le cas où une entité gère un nombre important de domaines, il peut être intéressant de centraliser les rapports via des renvois « externes » [6]

Etape 2 : Quarantaine ou rejet
Ces politiques constituent le cœur de DMARC, seuls les emails alignés (enveloppe envoyée par un serveur référencé par SPF, ou un message signé DKIM) doivent être délivrés sans réserve.

```
v=DMARC1;p=quarantine;rua=mailto:courriel-rapport@domaine.fr;pct=5
```

Le paramètre pct (pourcent) permet de définir progressivement de 0% à 100% pour éviter un phénomène d'avalanche d'incident au resserrement de la politique de sécurité.

Gérér les sous-domaines suivant les usages

Pour éviter des mélanges de politiques, entre des courriels envoyés manuellement avec des messages envoyés par des systèmes automatiques, il est recommandé de dédier aux seconds des sous-domaines, i.e.

```
@notifications.domaine.fr
@listes-diffusion.domaine.fr
@campagne-communication.domaine.fr
```

Ces sous-domaines doivent être protégés comme les autres (SPF, DKIM, DMARC).

Mais les hameçonneurs (et les spammeurs d'une manière générale) sont inventifs : quand ils s'aperçoivent qu'une cible domaine.fr est correctement protégée, ils essayent avec des variantes notamment `sous.domaine.fr`, y compris des sous-

domaines non définis (ils tenteront aussi `domain.fr` ou `d0maine.fr` mais c'est une autre problématique, le « cybersquatting »)

Etape 3 : Rejet sur sous-domaines

Le paramètre sp de la politique DMARC permet d'imposer l'alignement à tout sous-domaine, déclaré ou non.

```
v=DMARC1;p=quarantine;rua=mailto:courriel-rapport@domaine.fr;pct=100;sp=reject
```

EN RESUME

Les pourriels ont longtemps été traité comme une nuisance qui encombre les boîtes aux lettres électroniques comme certains dépliants commerciaux dans les boîtes aux lettres papier.
Mais les pourriels sont devenus les vecteurs d'hameçonnages et les techniques traditionnelles de lutte ont atteint leurs limites : pour l'analyse lexicographique, les faux courriels sont des copies quasi parfaites des authentiques ; pour la réputation des adresses IP, les émetteurs privilégient des botnets ou des serveurs temporaires dans les infrastructures « cloud ».

Comme pour le web, le principal levier de sécurisation consiste à introduire des preuves d'authenticité : SPF peut être considéré comme une authentification faible ; DKIM s'approche d'une authentification forte. DMARC apporte la cohérence globale à l'ensemble et des capacités de reporting.

Bien que des cassandres annonce sa mort depuis qu'il existe, le courriel est le premier vecteur de communication. Sa bonne santé est une tâche collective où chaque organisation attachée à la sécurité numérique doit apporter sa contribution.

RÉFÉRENCES

[1] https://blogs.msdn.microsoft.com/tzink/2015/10/30/how-office-365-does-automatic-dkim-key-rotation/
[2] https://discovery.cryptosense.com/
[3] https://github.com/nabla-c0d3/sslyze
[4] https://wiki.mozilla.org/Thunderbird:Help_Documentation:Dealing_with_Junk_E-mail
[5] https://technet.microsoft.com/fr-fr/library/aa996878%28v=exchg.160%29.aspx
[6] https://dmarc.org/2015/08/receiving-dmarc-reports-outside-your-domain/
[7] https://www.ncsc.gov.uk/blog-post/making-email-mean-something-again
[8] https://wiki1.dovecot.org/LDA/Sieve
[9] https://www.m3aawg.org/published-documents

Contact : dssi.shfds (at) finances.gouv.fr
Diffusion Internet : https://www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi

HFDS Bercy