Messaging, Malware and Mobile Anti-Abuse Working Group

Chiffrement TLS des e-mails : Recommandations Initiales du M³AAWG

www.m3aawg.org/TLSforMailBP-French

Résumé

Les révélations récentes faisant état de la surveillance de la messagerie électronique ont suscité un fort intérêt pour les moyens à la disposition des opérateurs pour protéger les boîtes mail de leurs utilisateurs de toute forme d'interception clandestine. Dans ce document, le M³AAWG recommande trois mesures concrètes que les fournisseurs de messagerie peuvent implémenter rapidement dans le but d'améliorer la sécurité et la confidentialité des e-mails de leurs utilisateurs.

Introduction

Ce document est volontairement succinct, ciblant les mesures les plus simples et les plus efficaces à mettre en œuvre. Le M³AAWG part du principe qu'un tel document ne saurait être exhaustif compte tenu de la complexité du sujet dont il est question, mais estime qu'il existe un intérêt indéniable à fournir une recommandation initiale, en parallèle de la littérature technique régulièrement tenue à jour sur cette thématique.

Ce document se concentre sur les mesures applicables par les fournisseurs de messagerie électronique. Il n'a pas vocation à aborder le sujet des fonctionnalités de chiffrement contrôlées par l'utilisateur final comme PGP/GPG ou S/MIME, assurant la confidentialité du contenu d'un message tout au long de son acheminement et de son stockage.

1) Protéger les échanges d'e-mail entre fournisseur avec « TLS opportuniste »

TLS, créé en 1999, est le successeur de SSL. En raison de nombreuses problématiques de sécurité avec SSLv2 et SSLv3, le M³AAWG recommande vivement de désactiver toutes les versions de SSL au profit exclusif de TLS. En revanche, les responsables informatiques doivent être conscients de l'impact possible de cette décision, en particulier pour les utilisateurs de versions anciennes de certains logiciels. Il est également à noter que certaines versions anciennes de TLS présentent elles aussi des problèmes de sécurité spécifiques.

Par défaut, les échanges d'e-mail entre fournisseurs de messagerie ne sont pas chiffrés. Dans les conditions normales, le chiffrement TLS nécessite l'utilisation de clés de chiffrement/déchiffrement, basées sur un certificat, ce qui a révélé être un véritable frein à son adoption et son utilisation. Néanmoins, la plupart des logiciels MTA (Mail Transfer Agents) peuvent être paramétrés pour établir

des sessions avec chiffrement TLS opportuniste*(1) en utilisant des clés temporaires pour protéger, dans la mesure du possible, les flux inter-MTAs de toute interception intempestive.

Le M³AAWG recommande fortement à tous les opérateurs d'activer l'option TLS opportuniste sur l'ensemble de leurs serveurs de messagerie.

Il est cependant important d'avoir conscience d'une limite : le SMTP est un protocole « point à point ». Etant donné que le TLS est une partie de la connexion TCP qui sert à l'établissement d'une session SMTP, le TLS opportuniste fonctionne également en mode point à point : si certains intermédiaires impliqués dans l'acheminement d'un message utilisent TLS alors que d'autres ne le font pas, la protection contre les interceptions sera incomplète. L'utilisation de TLS opportuniste n'offre donc pas une totale garantie de sécurité, mais il permet de protéger une partie importante des échanges de certaines attaques passives. En outre, la quête de la perfection ne doit pas vous empêcher de mettre en œuvre dès maintenant des mesures pouvant offrir des améliorations conséquentes.

Si vous avez déjà implémenté le chiffrement TLS opportuniste sur vos serveurs de messagerie, vous pouvez en vérifier le paramétrage et la disponibilité pour vos utilisateurs sur le site https://ssl-tools.net/mailservers (en anglais). [**Note:** lien mis à jour juillet 20.]

Le M³AAWG vous recommande spécifiquement de vous assurer que vos serveurs de messagerie utilisent TLS version 1.2[2] plutôt qu'une version inférieure, et que des suites cryptographiques permettant une confidentialité persistante[3] sont utilisées en priorité.

2) Protéger le trafic interne d'une entreprise de toute interception

Historiquement, le réseau interne d'un fournisseur, établi sur des liaisons physiques dédiées, était considéré comme sécurisé et n'ayant pas besoin d'être chiffré. Etant donné que des révélations récentes ont prouvé l'existence de programmes de surveillance réseau à grande échelle[4], ces considérations doivent être mises en doute. Le M³AAWG vous recommande de chiffrer l'intégralité du trafic interne de votre infrastructure, par l'utilisation de TLS ou d'autres méthodes de chiffrage, de la même façon que nous recommandons l'utilisation de TLS opportuniste pour chiffrer les échanges inter-MTAs au sein du réseau Internet.

3) Protéger les mots de passe de vos utilisateurs de toute interception (IMAPS/POPS/SMTP Submit/Webmail)

Quand des utilisateurs échangent leur identifiant et mot de passe pour accéder à leur messagerie ou envoyer un message, les opérateurs se doivent d'utiliser des méthodes de chiffrage pour protéger également ces paramètres d'une interception. Cela implique par exemple d'utiliser :

- IMAP (ou POP) avec TLS
- La soumission de messages par le port 465 avec TLS, ou par le port 587 avec STARTTLS
- Une interface Webmail protégée avec TLS

* Quelques exemples disponibles : https://bettercrypto.org/static/applied-crypto-hardening.pdf en section 2.3.

Conclusion

Le groupe de travail portant sur la messagerie, les logiciels malveillants et la lutte contre l'abus par voie mobile recommande que les fournisseurs de messagerie activent les technologies basiques de chiffrage décrites dans ce document en tant que premières lignes de défense contre d'éventuelles interceptions de communications de ses utilisateurs. Ces recommandations ne constituent qu'un premier lot de mesures à prendre et ne doivent pas être considérées comme une liste exhaustive d'actions à mener.
Le M[3]AAWG continue d'une manière générale à s'efforcer de fournir davantage de recommandations sur le thème de la protection de la confidentialité de la messagerie personnelle.

Références

1. Bettercypto.org, Applied Crypto Hardening, section 2.3 "Practical recommendations: Mail Servers" (en anglais), https://bettercrypto.org/static/applied-crypto-hardening.pdf.
2. TLS version 1.2 (en anglais), https://en.wikipedia.org/wiki/Transport_Layer_Security#TLS_1.2
3. Confidentialité persistante, https://fr.wikipedia.org/wiki/Confidentialit%C3%A9_persistante
4. MUSCULAR, https://fr.wikipedia.org/wiki/Muscular

RFCs concernées

- RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2," http://tools.ietf.org/html/rfc5246
- RFC 7258, "Pervasive Monitoring Is an Attack," http://tools.ietf.org/html/rfc7258

Mots-clé: Messaging, Malware and Mobile Anti-Abuse Working Group, M[3]AAWG, messagerie sécurisée, TLS, SMTP, sécurité réseau, sécurité des mots de passe, TLS opportuniste, surveillance, interception, écoute, transport layer security

M3AAWG087-French
As with all documents that we publish, please check the M[3]AAWG website (www.m3aawg.org) for updates to this document.