Contrôler l'authentification (SPF, DKIM, voire DMARC)

Sécurité

Posté par : JerryG

Publié le : 15/1/2024 14:00:00

Alors que 2024 s'annonce déjà comme une année chargée en termes de législation cyber, notamment avec la mise en place de la réglementation NIS2, une autre annonce plus discrète aura un impact considérable sur les entreprises.

En effet, Google et Yahoo! ont annoncé leur intention de contrôler l'authentification (SPF, DKIM, voire DMARC) des courriels à destination de leurs plateformes.

Dès février 2024, les expéditeurs d'envois en nombre qui ne respectent pas ces exigences commenceront à recevoir des erreurs temporaires (avec des codes d'erreur) sur un petit pourcentage de leur trafic non conforme. Ces erreurs temporaires ont pour but d'aider les expéditeurs à identifier les messages électroniques qui ne respectent pas les nouvelles lignes directrices.

SPF et DKIM seront progressivement requis pour toutes les adresses email à partir d'avril, et seront obligatoires pour tous les emails en juin 2024. L'authentification DMARC, elle, sera obligatoire pour les entreprises envoyant plus de 5000 mails par jour.

Cette annonce est donc particulièrement importante pour toute organisation menant des campagnes d'information ou promotionnelles à grande échelle par email à ce soit une association, un acteur public, un parti ou une enseigne de la grande distribution.

Pour Loïc Guizo, Directeur de la stratégie cyber pour l'Europe chez Proofpoint, « cette annonce montre la volonté des acteurs de la messagerie électronique de protéger de plus en plus leurs utilisateurs ».

La généralisation du protocole DMARC sera une véritable épine dans le pied des cybercriminels, qui ne pourront plus se faire passer pour des entreprises et usurper leurs noms de domaines.

La mise en place de ce protocole sur de nombreux services administratifs en France, comme par exemple avec la Gendarmerie Française, montre déjà que des mesures fortes sont prises pour combattre activement l'usurpation d'identité en France ».

Les nouvelles exigences seront les suivantes :

☞ Pour envoyer des courriels aux destinataires Gmail et Yahoo!, la mise en place des protocoles SPF et DKIM : SPF (Sender Policy Framework) permet au serveur de messagerie destinataire de vérifier si l'email entrant provient d'une adresse IP autorisée par l'administrateur du domaine, tandis que DKIM (DomainKeys Identified Mail) permet à une entreprise de prendre la responsabilité de transmettre un message en le signant de sorte que les fournisseurs de messagerie puissent le vérifier.

☞ Pour les entreprises envoyant plus de 5000 courriels par jour, la mise en place du protocole DMARC : DMARC (Domain-based Message Authentication, Reporting and Conformance) authentifie l'identité de l'expéditeur d'un courrier électronique avant de permettre à un message d'atteindre sa destination.

Il constitue à ce jour l'une des armes les plus puissantes pour lutter contre une classe d'attaque par email très effective : le domain spoofing (ou usurpation de domaine) utilisée comme arme essentielle dans toute campagne de phishing. DMARC comporte trois niveaux de traitement des emails : surveillance, mise en quarantaine et rejet à ce dernier étant le niveau le plus sûr pour empêcher les messages suspects d'atteindre la boîte de réception du destinataire.

La mise en place des protocoles SPF et DKIM est un prérequis pour la mise en place de l'authentification DMARC, qui renforce encore le niveau de cybersécurité des entreprises en bloquant les emails qui essaient d'usurper un nom de domaine.

Proofpoint a mené plusieurs analyses sur la mise en place du protocole DMARC en France dont voici les conclusions les plus importantes :

• Seules 14 entreprises du CAC 40 (35%) ont adopté le niveau le plus strict et le plus recommandé de DMARC (Reject mode) qui bloque l'usurpation d'identité ;

• Seules 8 des 20 sites de vente en ligne les plus populaires (40%) ont adopté le niveau le plus strict et le plus recommandé de DMARC (Reject mode) ;

• Parmi les partis politiques candidats aux présidentielles de 2022, aucun n'avait protégé de façon proactive son nom de domaine.

Il reste donc peu de temps pour se mettre à niveau et déployer le protocole d'authentification DMARC exigé par les opérateurs de messagerie en ligne, notamment, par exemple, à l'approche des élections européennes de juin 2024.

Vous trouverez plus d'[information](#) sur ce sujet.