Internet : L'authentification DMARC protÃ¨ge 60% des boÃ®tes mails dans le monde
Internet
PostÃ© par : JerryG
PubliÃ©e le : 13/3/2013 14:00:00

Return Path, leader mondial dans le domaine de l'Email Intelligence, ou veille appliquÃ©e Ã la messagerie Ã©lectronique, annonce, aux cÃ´tÃ©s de DMARC.org, que le protocole d'authentification DMARC offre aujourdâ□□hui **un niveau de contrÃ´le inÃ©galÃ©**, en empÃªchant la remise des messages potentiellement frauduleux dans une majoritÃ© de boÃ®tes de rÃ©ception Ã travers le monde.

DocuSign, leader de la sÃ©curisation par signature Ã©lectronique, s'associe Ã **DMARC** pour contrecarrer les attaques de phishing.

DMARC est en effet dÃ©ployÃ© par diffÃ©rents opÃ©rateurs de messagerie qui, ensemble, reprÃ©sentent 60 % des boÃ®tes de rÃ©ception de la planÃ¨te. Le protocole DMARC est Ã©galement mis en Å□uvre par 10 des 20 principaux domaines d'envoi, Ã l'origine d'une part importante du trafic journalier Ã destination des rÃ©seaux de rÃ©ception.

D'aprÃ¨s des donnÃ©es fournies par Return Path et d'autres membres de DMARC.org, le protocole a ainsi permis le blocage de plus de 325 millions d'emails avant qu'ils n'atteignent les boÃ®tes de rÃ©ception des usagers en novembre et dÃ©cembre 2012. Dernier exemple en date illustrant lâ□□engouement des annonceurs pour DMARC, DocuSign, qui a eu recours Ã ce protocole pour contrecarrer une attaque de phishing active.

DMARC (Domain-based Message Authentication, Reporting and Conformance) a Ã©tÃ© lancÃ© l'annÃ©e derniÃ¨re par un consortium regroupant des expÃ©diteurs et des opÃ©rateurs de messagerie de premier plan, dont Google, Microsoft, Yahoo!, Facebook et PayPal. DMARC fait appel Ã des protocoles d'authentification existants â□□ Sender Policy Framework (SPF) et DomainKeys Identified Mail (DKIM) â□□ pour permettre aux entreprises de publier des politiques de rejet des messages qui ne sont pas authentifiÃ©s de maniÃ¨re adÃ©quate. Autre avantage de DMARC : le protocole permet aux opÃ©rateurs de messagerie d'envoyer aux entreprises qui le mettent en Å□uvre des rapports leur indiquant si leurs domaines prÃ©sentent des problÃ¨mes d'authentification. Ces entreprises peuvent ainsi dÃ©tecter rapidement les attaques de phishing et maintenir leurs systÃ¨mes parfaitement opÃ©rationnels.

DocuSign en appelle Ã DMARC pour lutter contre la fraude

DocuSign, rÃ©fÃ©rence mondiale en matiÃ¨re de signatures Ã©lectroniques, a mis en place un rÃ©seau de confiance comptant plus de 27 millions de membres dans 188 pays, qui utilisent sa

plateforme de gestion des transactions au moyen de signatures Ã©lectroniques pour accÃ©lÃ©rer les opÃ©rations. La sociÃ©tÃ© aide les particuliers et les entreprises de toutes tailles et de tous secteurs Ã accÃ©lÃ©rer le processus transactionnel, de faÃ§on Ã obtenir des rÃ©sultats plus rapidement, Ã rÃ©duire leurs coÃ»ts et Ã satisfaire leurs clients.

A la tÃªte de l'infrastructure de sÃ©curitÃ© le plus robuste du secteur, DocuSign recourt Ã des outils Ã la pointe de la technologie et innovants tels que le systÃ¨me d'authentification DMARC pour protÃ©ger sa marque et son rÃ©seau mondial d'utilisateurs. Ardent dÃ©fenseur de l'utilisation du protocole SPF pour l'authentification, DocuSign utilise DMARC pour surveiller les messages Ã©manant de ses domaines d'envoi. Il y a peu, lorsque DocuSign a commencÃ© Ã dÃ©tecter des emails frauduleux grÃ¢ce Ã DMARC, la sociÃ©tÃ© a rapidement compris que sa marque et ses utilisateurs Ã©taient la cible de tentatives de hameÃ§onnage et a immÃ©diatement pris des mesures correctives. Elle a publiÃ© une mise Ã jour de sa politique DMARC, invitant les opÃ©rateurs de messagerie partenaires Ã mettre en quarantaine tous les messages Ã©chouant Ã l'authentification, de faÃ§on Ã empÃªcher les emails suspects d'Ãªtre remis en boÃ®te de rÃ©ception.

Â« *DocuSign propose la plateforme de signature Ã©lectronique la plus fiable du secteur* Â», dÃ©clare **Joan Ross**, directeur de la sÃ©curitÃ© chez DocuSign. Â« *DMARC nous permet d'identifier rapidement toute attaque Ã l'encontre de la marque DocuSign et de protÃ©ger notre rÃ©seau mondial d'utilisateurs, afin que ceux-ci continuent Ã nous faire confiance pour la conclusion rapide et sÃ©curisÃ©e de leurs transactions.* Â»

Leader d'opinion dans le domaine de la sÃ©curitÃ©, DocuSign a rÃ©cemment publiÃ© un billet de blog consacrÃ© Ã **DMARC** et Ã d'autres meilleures pratiques dans le cadre d'une sÃ©rie de billets visant Ã aider ses utilisateurs Ã renforcer la protection de leurs donnÃ©es et informations.

DocuSign n'est pas le seul Ã adopter DMARC : face Ã la multiplication des attaques malveillantes de Spam ciblant des sociÃ©tÃ©s de renom, reconnues comme des marques de confiance, de nombreuses entreprises se tournent vers ce nouvel outil de sÃ©curitÃ©. A l'aide du protocole DMARC, ces entreprises peuvent demander aux opÃ©rateurs de messagerie de bloquer ou de mettre en quarantaine tout message non authentifiÃ© attribuÃ© Ã leurs domaines. Cela permet d'Ã©viter aux destinataires de recevoir des messages de phishing frauduleux provenant prÃ©tendument d'expÃ©diteurs familiers.

Return Path, pilier actif du mouvement DMARC.org

La suite de solutions anti-phishing Secure.EQ de Return Path comprend des outils qui aident les expÃ©diteurs Ã mettre en Å□uvre le protocole DMARC et ainsi Ã protÃ©ger leur marque contre les attaques de phishing. RÃ©cemment, la solution Domain Secure de Return Path a permis Ã Publishers Clearing House de bloquer 350 000 messages Ã©manant de faux services et d'infrastructures de transfert d'emails, qui n'appartenaient pas Ã la sociÃ©tÃ©. La non-remise en boÃ®te de rÃ©ception de ces messages permet de protÃ©ger des centaines de milliers d'usagers contre des emails nuisibles, ce qui Ã©tait impossible avant l'avÃ¨nement de DMARC.

Â« *Compte tenu du nombre croissant d'expÃ©diteurs reconnaissant l'efficacitÃ© de DMARC dans la lutte contre la fraude, la confiance des usagers dans la messagerie Ã©lectronique en tant que canal de communication devrait se renforcer.* Â», dÃ©clare **Didier Colombani**, Directeur de la rÃ©gion Europe du Sud et Benelux au sein de **Return Path**. Â« *Les principales marques montrent d'ores et dÃ©jÃ l'exemple, et les rÃ©sultats qu'elles obtiennent devraient inciter les expÃ©diteurs du monde entier Ã prendre ces mesures simples pour rendre l'ensemble de lâ□□Ã©cosystÃ¨me email plus sÃ»r.* Â»