La fraude par email: Plus de contre-mesure
Internet
PostÃ© par : JerryG
PubliÃ©e le : 26/7/2023 13:00:00

Proofpoint, leader en matiÃ¨re de cybersÃ©curitÃ© et conformitÃ©, a publiÃ© sa nouvelle analyse des enregistrements DMARC (Domain-based Message Authentication, Reporting and Conformance) de lâ□□ensemble des entreprises du CAC 40.

Lâ□□Ã©tude rÃ©vÃ¨le notamment que plus de la moitiÃ© dâ□□entre elles (57 %) nâ□□auraient pas un niveau de protection assez important contre le risque de fraude par email. En novembre 2022, ce chiffre Ã©tait de 65%, ce qui montre une lÃ©gÃ¨re amÃ©lioration de la cybersÃ©curitÃ© des entreprises franÃ§aises.

Le rapport State of the Phish 2023 de Proofpoint montrait en effet que les attaques par courriel sont restÃ©es la principale menace pour les entreprises. En France, huit entreprises interrogÃ©es sur dix auraient ainsi subi au moins une attaque par hameÃ§onnage (Â«â□□phishingâ□□Â») rÃ©ussie lâ□□an dernier.

Pour parer Ã ce type dâ□□attaque, les entreprises peuvent donc appliquer le standard DMARC, un protocole dâ□□authentification des messages Ã©lectroniques conÃ§u pour protÃ©ger les noms de domaine contre une utilisation abusive par les cybercriminels.

Les principales conclusions sont les suivantes :

â□¢ Lâ□□adoption du DMARC par les entreprises du CAC 40 est en hausse. Cette annÃ©e, 36 des 40 entreprises du CAC (90 %) ont publiÃ© un enregistrement DMARC, contre 78 % en 2022 et 77 % en 2021.

â□¢ Si lâ□□amÃ©lioration est notable dâ□□annÃ©e en annÃ©e, 4 entreprises (10 %) du CAC 40 (contre 9 â□□ 22 % â□□ en 2022) nâ□□ont Ã ce jour toujours pas dâ□□enregistrement DMARC, exposant donc, sans aucune surveillance minimale, lâ□□ensemble de leur Ã©cosystÃ¨me partenaires, clients et fournisseurs Ã la fraude par email. Ã□ noter quâ□□en 2021, 23 % des entreprises du CAC 40 nâ□□avaient pas dâ□□enregistrement DMARC.

â□¢ 19 entreprises (48 %) du CAC 40 (contre 17 â□□ soit 43 % â□□ en 2022) ont pris les mesures initiales en publiant un enregistrement DMARC, mais nâ□□assurent aucun rÃ´le actif de protection, uniquement un niveau de surveillance et de mise en quarantaine minimale.

â□¢ Enfin, parmi les 36 entreprises du CAC ayant publiÃ© un enregistrement DMARC, 17 (43 %) dâ□□entre elles (contre 14 â□□ soit 35 % â□□ en 2022) ont mis en Å□uvre le niveau de protection recommandÃ© et le plus strict (rejet), qui empÃªche activement les courriers Ã©lectroniques frauduleux dâ□□atteindre leurs cibles.

Il sâ□□agit dâ□□une amÃ©lioration significative par rapport Ã 2021, oÃ¹ seulement 15 % Ã©taient au niveau Â«â□□rejetâ□□Â». La protection sâ□□amÃ©liore donc, mais plus de la moitiÃ© des entreprises du CAC 40 (57 %) laisse encore leurs clients exposÃ©s Ã un risque possible dâ□□hameÃ§onnage par courriel prÃ©tendant provenir de leurs domaines.

Le rapport State of the Phish 2023 de Proofpoint montre en effet que les attaques par courriel sont restÃ©es la principale menace pour les entreprises, et en France, huit sur dix auraient subi au

moins une attaque par hameÃ§onnage (Â«â□□phishingâ□□Â») rÃ©ussie lâ□□an dernier.

 Â«â□□Pour les grandes entreprises, câ□□est la protection de leur chaÃ®ne de valeur qui en dÃ©pend.

Appliquer les bonnes pratiques au sommet peut encourager tout un Ã©cosystÃ¨me Ã adopter des principes fondamentaux pour la cybersÃ©curitÃ©, incluant le protocole dâ□□authentification DMARC et les mesures supplÃ©mentaires de certification dâ□□origine des courriels telles que le sceau Â«â□□BIMIâ□□Â» (Brand Indicators for Message Identification)Â

â□□ uniquement ouvert aux noms de domaines protÃ©gÃ©s par DMARC â□□ et qui permet aux entreprises dâ□□afficher leurs logos directement au niveau de la boÃ®te de messagerie de leurs destinataires, Ã cÃ´tÃ© du nom de lâ□□Ã©metteur. Â» prÃ©cise LoÃ¯c GuÃ©zo, directeur de la stratÃ©gie cyber pour la rÃ©gion SEMA chez Proofpoint.

Vous pourrez retrouver lâ□□ensemble de cette analyse sur ce blog.Â