Les attaquants profitent du comportement des utilisateurs pour porter atteinte à la cybersécurité – Global Security Mag Online | Le Net Expert Informatique

Proofpoint, Inc., dévoile les résultats obtenus suite à son étude annuelle portant sur la manière dont les attaquants tirent parti du comportement des utilisateurs pour porter atteinte à la sécurité informatique. L'édition 2015 du rapport « Le facteur humain », indique que les pirates ont, l'année dernière, décidé d'opérer dorénavant au niveau des entreprises, et non plus auprès du grand public.

Pour ce faire, ils se sont concentrés sur les processus de partage d'informations au niveau des cadres, tout en privilégiant la sophistication des attaques, et non plus leur volume. Les résultats obtenus par Proofpoint prouvent, à nouveau, que le comportement des utilisateurs, et pas uniquement les failles d'un système ou d'un logiciel donné, a une incidence significative sur la sécurité des entreprises. Le rapport indique également quelles mesures doivent être appliquées, alors que le nombre de clics ne cesse d'augmenter.

Comme le soulignent Nick Hayes, Christopher McClean et Claire O'Malley dans le rapport Reinvent Security Awareness To Engage The Human Firewall (consultation payante) de Forrester Research, publié le 17 décembre 2014, « Le facteur humain constitue l'un des éléments clés des programmes de sécurité, alors qu'il est souvent celui que l'on néglige le plus. C'est bien là le problème. En effet, les solutions de sécurité se révèlent fondamentales si vous souhaitez protéger votre environnement de travail, mais ne sont d'aucune utilité si des actions humaines viennent les affaiblir ». Malgré cela, de nombreuses organisations s'appuient uniquement sur des technologies avec passerelle. Elles n'optent pas pour des solutions de blocage, de protection contre les attaques ciblées, de détection et de gestion des menaces, qui sont toutes basées sur les utilisateurs plutôt que sur l'infrastructure.

Le rapport « Le facteur humain » de 2015 fait notamment état des points clés suivants :
Toutes les entreprises sont concernées. En moyenne, les utilisateurs cliquent sur un lien malveillant tous les 25 messages. Aucune entreprise à laquelle l'étude s'est intéressée n'a été en mesure d'éviter cela totalement.
Les cadres constituent une cible privilégiée. En 2014, les cadres ont été deux fois plus ciblés qu'en 2013, et leurs clics sur des liens dangereux ont doublé. En outre, ceux-ci, ainsi que les employés non cadres, ont effectué cette opération deux fois plus fréquemment que le personnel dirigeant.
Les services dédiés à la vente, aux finances et à l'approvisionnement (chaîne logistique) sont les plus ciblés. Ces services sont ceux qui ont le plus cliqué sur des liens contenus dans des messages malveillants, avec 50 à 80 % de clics en plus.
Un clic se produit très rapidement. Les organisations ne disposent plus de plusieurs semaines ou jours pour détecter et bloquer les courriers électroniques malveillants. En effet, les attaquants parviennent à faire cliquer deux utilisateurs sur trois dès le premier jour. À la fin de la première semaine, 96 % des clics se sont produits. En 2013, seuls 39 % des liens contenus dans les courriers électroniques ont été consultés lors des premières 24 heures. En 2014, cette estimation est passée à 66 %.
Les attaques se produisent surtout pendant les heures de travail. La plupart des messages malveillants sont envoyés lors des heures de travail, principalement le mardi et le jeudi matin. Le mardi constitue la journée la plus critique, avec 17 % de clics de plus que les autres jours.
Les utilisateurs sont plus vigilants, mais les attaquants s'adaptent rapidement. L'utilisation des réseaux sociaux dans les courriers électroniques malveillants s'est révélée être la stratégie la plus courante et efficace en 2013, mais a été réduite de 94 % en 2014. Le nombre des courriers électroniques comportant des pièces jointes douteuses, et non plus des URL (notifications, avertissements à caractère financier), s'est multiplié. En 2014, durant certains jours, Proofpoint a pu remarquer une augmentation de 1 000 % du volume des pièces jointes malveillantes. Cette même année, les fausses sollicitations par courrier électronique faisaient état de réception de fax ou de messages vocaux, voire d'alerte à caractère financier (facture, relevés de comptes, etc.).
« Le rapport « Le facteur humain » souligne à quel point il est fondamental de disposer d'informations précises sur les menaces. Il décrit également comment, quand et où les attaques se produisent », indique Kevin Epstein, Vice-Président en charge de la gouvernance et de la sécurité avancée chez Proofpoint. « Il existera toujours une personne qui cliquera sur un lien, et permettra ainsi aux menaces de se propager auprès des utilisateurs. L'approche de Proofpoint est efficace car nos systèmes sont capables d'identifier les individus concernés, de localiser ces derniers et de déterminer les actions en cours. Ainsi, nous permettons aux organisations de se protéger activement, ainsi que de prendre, en temps réel, les mesures adéquates. »

Le rapport Le facteur humain s'appuie sur des données obtenues auprès de clients utilisant notre suite de solutions dédiées à la protection avancée contre les menaces.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/Les-attaquants-profitent-du,20150422,52439.html