Les campagnes de sensibilisation à la cybersécurité portent (petit à petit) leurs fruits

Les campagnes de sensibilisation à la cybersécurité portent (petit à petit) leurs fruits

Une étude souligne que les primo-adoptants de nouvelles technologies demandent l'autorisation avant d'amener de nouveaux équipements au travail.

Sachant que plus de 25 % des attaques identifiées en entreprise devraient associer l'Internet des objets d'ici à 2020 [1] et, pour nombre d'entre elles, s'inviter sur le lieu de travail, les conclusions de cette étude marquent une évolution significative dans la bonne direction et prouvent que les collaborateurs cernent mieux le rôle qui leur incombe dans le domaine de la cybersécurité.
Néanmoins, les résultats de cette enquête menée auprès de cadres en entreprise – les plus susceptibles, de par leur rémunération et leur état d'esprit, à être des primo-adoptants des nouvelles technologies – sont contrastés puisque 39 % d'entre eux auraient tendance à se soustraire au contrôle du service informatique. Ce qui laisse une énorme marge de risque.
Pire, parmi les collaborateurs qui se disent prêts à court-circuiter le service informatique, un sur huit « ne révélerait à personne » son intention d'introduire un nouvel appareil au sein de l'entreprise ou d'installer un outil professionnel, messagerie électronique par exemple, sur un équipement non sécurisé.

L'attitude a une incidence sur le respect des règles
L'étude révèle que le respect des règles de cybersécurité, telles que celles concernant l'introduction d'un nouvel équipement, est largement fonction des attitudes et opinions de chacun vis-à-vis de la technologie. Les professionnels ayant dérogé, dans le passé, aux règles de cybersécurité de leur entreprise justifient essentiellement leur geste par leur volonté de recourir à un outil ou un service plus efficace, ou considéré à l'époque comme le meilleur sur le marché. Les entreprises doivent élargir, et non restreindre, le choix de leurs collaborateurs, en s'appuyant sur la technologie et la formation pour gérer les risques.

Les intérimaires exigent une surveillance à temps complet
Les sous-traitants constituent le groupe contournant le plus souvent les règles de cybersécurité, 16 % des participants affirmant avoir vu un intérimaire se soustraire à celles-ci.
« Le concept BYOD a beau aujourd'hui avoir fait ses preuves, nombre d'individus continuent à éprouver des difficultés à dissocier clairement l'accès aux données personnelles de celui aux données professionnelles sur les appareils leur appartenant. Quantité d'entreprises ont déployé des solutions d'administration pour leur parc d'équipements, mais c'est la connectabilité de ces derniers qui pose véritablement problème, d'autant que la ligne de démarcation entre les services cloud orientés métier et les services personnels s'estompant, des passerelles méconnues sont jetées entre les réseaux d'entreprise et l'Internet en général. Une sécurité dernier cri doit être en mesure d'empêcher que toute communication à partir d'un équipement ne se transforme en faille et diminuer le plus possible les risques encourus par l'entreprise. » Greg Day, vice-président et responsable de la sécurité (CSO) pour la zone Europe, Moyen-Orient et Afrique (EMEA) chez Palo Alto Networks

Recommandations
Les entreprises doivent poursuivre leurs actions de sensibilisation auprès de leurs collaborateurs afin de faire en sorte que ceux positionnés en première ligne défensive possèdent les compétences nécessaires pour déceler les menaces.
Les professionnels de la sécurité doivent encadrer étroitement les activités des collaborateurs non permanents ou des sous-traitants, et veiller à ce que leur soient communiquées les mêmes informations que celles dispensées au personnel à temps complet.
Les entreprises doivent intégrer des solutions de sécurité modernes, en harmonie avec les nouvelles évolutions technologiques, afin d'écarter les fragilités inhérentes à un environnement informatique en constante évolution.
Les entreprises doivent réfléchir à la façon dont elles recensent et favorisent l'utilisation, dans de bonnes conditions de sécurité, d'applications et de services cloud dignes de confiance ou approuvés par leurs soins, et gèrent celle de ceux qu'elles ne jugent pas dignes de leur confiance ou n'avalisent pas.
Méthodologie de recherche
L'enquête a été menée en ligne, par Redshift Research en octobre 2015, auprès de 765 décideurs d'entreprises comptant plus d'un millier de salariés au Royaume-Uni, en Allemagne, en France, aux Pays-Bas et en Belgique.
Article original de edubourse.com

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Les campagnes de sensibilisation à la cybersécurité portent (petit à petit) leurs fruits