Sans formation en cybersécurité le risque humain reste toujours le plus fort

Sans formation en cybersécurité le risque humain reste toujours le plus fort

Le risque humain figure toujours parmi les failles principales dans les affaires de cybersécurité. Les entreprises redoublent donc d'effort pour sensibiliser davantage leurs collaborateurs. La tâche est ardue.

Cela fait quelques années qu'au sein des entreprises, les principes de cybersécurité ne sont plus l'apanage des seuls experts (DSI, RSSI, responsables techniques). En effet, pour se prémunir contre les vulnérabilités d'origine humaine, les entreprises, avec plus ou moins de détermination, ont développé des processus de sensibilisation auprès de leurs collaborateurs, comité exécutif compris. « La mise en place de cette politique de sécurité doit être compréhensible par tous. Elle ne doit donc pas être écrite dans un jargon technique de spécialiste, explique Franck Greverie, Corporate Vice-president des activités cybersécurité chez Capgemini. Surtout les collaborateurs doivent apprendre à comprendre les risques qu'ils font courir à leur entreprise s'ils ne la respectent pas ». La sensibilisation passe donc pas une communication pédagogique sur des sujets tels que la gestion des mots de passe, le phishing, l'ingénierie sociale, l'utilisation d'applications qui ne sont pas à jour, etc. et les conséquences liées à ces attaques et au non respect des procédures.

Alterner des sessions de formations obligatoires avec des ateliers de mise en situation
De façon concrète, cette éducation peut prendre la forme de modules de formations obligatoires, de journées de démonstrations de piratage en comités restreints ou encore de mises en situation. En complément de ces événements de sensibilisation ponctuels, le niveau de maturité des collaborateurs doit être entretenu et mis à jour, par une communication interne régulière. « L'intranet, par exemple, représente un outil adapté pour aider les entreprises à planifier une campagne de sensibilisation à long terme », suggère Franck Greverie. Les pouvoirs publics ont également leur rôle à jouer. « En septembre 2015, certaines entités de l'Etat associées au CIGREF (une association rassemblant les patrons informatiques des grandes entreprises) annonceront conjointement une campagne de sensibilisation de grande ampleur », révèle l'expert.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://bfmbusiness.bfmtv.com/actualite/eduquer-tous-les-collaborateurs-a-la-cybersecurite-de-facon-simple-et-recurrente-891740.html
Par Eddye Dibar