PARIS : Les hackers et les vacances… de parfaits étrangers les uns pour les autres

PARIS : Quelques astuces simples de FireEye pour finir ses vacances en paix.

Les vacances, une période attendue et appréciée par des millions de français, des vacances qui toutefois ne veulent pas dire déconnexion.
Le phénomène BYOD – Bring Your Own Device – a changé, en fait, à la fois la façon de travailler et de profiter de ses vacances. L'intelligence, l'agilité et la souplesse apportées

par les terminaux dont nous sommes tous équipés sont d'une aide considérable pour tous les employés en entreprise qui doivent jongler chaque jour entre les activités domestiques et la famille. Ce concept nous a permis d'être toujours disponibles même en vacances, avec la possibilité d'être toujours connecté au réseau d'entreprise à la plage et de lire nos emails dans notre transat. Le danger, cependant, nous attend au tournant.

« Durant la période d'été, les dangers s'accroissent pour les réseaux d'entreprise. Les employés, bien sûr, font moins attention à ce qu'ils voient, ce qu'ils lui lisent et où ils cliquent, » déclare Gabriele Zanoni, Consulting Systems Engineer chez FireEye. « Si cette baisse d'attention est compréhensible, pour les attaquants le mois d'août est identique au mois de mars. Les vacances n'existent pas et les périodes de grande chaleur restent les favorites pour les 'hackers' qui peuvent toujours compter sur des alliés précieux: relaxation et distraction des collaborateurs. «

FireEye, en tant que spécialiste de la sécurité informatique, propose cinq mesures simples pour finir l'été en paix.

1) Protection totale: assurez-vous que le téléphone et les ordinateurs (d'entreprise ou non) à partir desquels vous vous connectez pendant les vacances sont configurés correctement et possèdent tous les logiciels de sécurité indispensables. Des antivirus rigoureusement mis à jour et l'installation des 'patches' de sécurité les plus récents sont les bases d'un été en paix.

2) Naviguer dans des eaux sûres: méfiez-vous particulièrement lors de la lecture de vos emails d'une possible « fraude d'usurpation d'identité », l'une des attaques les plus courantes ces temps-ci. Si vous avez reçu un email de votre supérieur le 15 août vous informant de la perte de sa carte de crédit et vous demandant de procéder à un paiement ou, par exemple, si vous travaillez au service paie, de changer son IBAN pour le règlement de son salaire, une alarme devrait sonner dans votre tête. N'obéissez jamais immédiatement et vérifiez d'abord auprès de l'intéressé. Garder son calme est

une vertu des forts.
3) Faire attention aux réseaux empruntés: les connexions Wi-Fi dans les hôtels, bars et restaurants sont l'un des vecteurs d'attaque préférés des pirates, car elles ne sont quasiment jamais correctement sécurisées. Les PC, smartphones et tablettes connectés à ces réseaux font donc face à de grands dangers. Un attaquant peut avoir pris le contrôle du réseau lui-même, ce qui lui permet de diffuser des malwares ou d'intercepter les identifiants des sites sur lesquels vous vous connectez. Pour éviter ces risques, mieux vaut utiliser une liaison VPN et en dernier recours un partage de connexion via votre smartphone qui le transformera en routeur wi-fi mobile.
4) Eviter la sauvegarde de comptes/mots de passe et le pré-remplissage des champs : la sauvegarde automatique des données d'accès sur les navigateurs Internet, les VPNs et les applications d'entreprise, spécialement sur des terminaux personnels ou partagés (par exemple un PC en libre-service dans le lobby d'un hôtel) est à proscrire. Si vos terminaux tombent en de mauvaises mains, les attaquants auront un accès immédiat à tous ces outils, et pourront les utiliser pour accéder à un réseau d'entreprise et voler des données sensibles.
5) Mieux vaut être seul que mal accompagné: faites attention aux endroits où vous laissez vos terminaux, et assurez-vous que vous êtes le seul à pouvoir y accéder. Activer une authentification à deux facteurs pour vos comptes utilisateur vous permet aussi de recevoir une notification immédiate si quelqu'un essaie d'accéder à votre compte et ainsi de bloquer rapidement ces authentifications non autorisées. Activer les fonctions permettant de retrouver votre téléphone en cas de perte peut également être utile lorsque vous voyagez.
Bien évidemment les vacances d'été sont un moment important pour tous les professionnels. Elles vous permettent de recharger vos batteries et de vous préparer pour une nouvelle année de travail, mais rappelez-vous une chose: les cybercriminels, eux, ne prennent jamais de vacances !