Sécurité : les cyberattaquants ciblent tous les échelons d'une entreprise

Les médias sociaux constituent un centre névralgique d'engagement entre les entreprises, les marques et les clients. Mais ils sont également un « Far West » du risque numérique. C'est l'un des enseignements du rapport de Proofpoint sur les menaces cyber.

Le rapport (*Quaterly Threat Report Q2 2018*) s'appuie sur la base mondiale de clients de l'éditeur américain de logiciels de sécurité. Premier constat : les manipulations psychologiques et les techniques d'ingénierie sociale qui trompent la vigilance d'employés et exposent des données sensibles ont le vent en poupe.

Résultat, au deuxième trimestre 2018, la fraude ciblant les utilisateurs des réseaux sociaux (*angler phishing*) a continué d'augmenter. Elle a bondi de 38% par rapport au trimestre précédent et s'est même épaissie de 400% par rapport au second trimestre 2017 !

Par ailleurs, après plusieurs mois de repli, les liens d'hameçonnage (*phishing*) transmis via les réseaux sociaux sont repartis à la hausse au deuxième trimestre (+30%). Ces liens visent à rediriger la cible vers un site illicite pour obtenir des données sensibles.

Tous ciblés, des opérations au comex

Quelles sont les cibles privilégiées par les cyberattaquants ? Proofpoint tente d'y répondre dans un rapport annexe (*Protection des personnes – été 2018*). L'éditeur constate que les cyberattaquants ciblent des individus présents à tous les échelons d'une entreprise.

Mais ce sont les employés et le management intermédiaire qui font l'objet de 60% des attaques extêmement ciblées par malwares et phishing d'identifiants de connexion. (Ici, des cyberattaques contre des organisations du Fortune Global 500 ont été étudiées).

Les employés impliqués dans la production ou des fonctions opérationnelles sont les plus exposés (23% des attaques extêmement ciblées). Les membres de la direction arrivent en seconde position (19%), suivis par les équipes de R&D et d'ingénierie (16% environ).

Le top management, une minorité influente, est donc lui aussi une cible de choix.

Dans ce contexte, Proofpoint réaffirme l'importance de former les équipes au risque que l'ingénierie sociale peut représenter pour l'activité de leur groupe.

Enfin, l'éditeur, qui prêche pour sa paroisse, recommande aux entreprises de ne pas limiter leur approche de la sécurité à l'infrastructure et aux terminaux.

Il s'agit de se doter et de maintenir à jour un système de protection contre les menaces ciblant les personnes par l'intermédiaire des médias sociaux, des e-mails et/ou du web.

(crédit photo © GlebStock – Shutterstock)

———————————————————————————————————————

La 18ème édition des Assises de la Sécurité à Monaco *aura lieu du 10 au 13 octobre.*
Rendez-vous incontournable de la cybersécurité en France, les Assises vous proposent un programme dense et varié avec, notamment, 170 conférences, ateliers et tables-rondes, des espaces de networking et des milliers de OneToOne