Gérard Beraud-Sudreau, Proofpoint : « L'humain doit être le point central de toute politique de sécurité »

Quelle approche de la sécurisation de la messagerie défendez-vous chez Proofpoint ?

Gérard Beraud-Sudreau – L'humain doit être le point central de toute politique de sécurité d'une entreprise. Pour se protéger contre les menaces, il faut d'abord comprendre qui est la cible, et ce, quelle que soit la qualité de la gestion de l'infrastructure informatique.

La spécificité de la fraude par email est qu'elle s'attaque à la nature humaine plutôt qu'à la technologie et reste encore aujourd'hui l'une des plus grandes cybermenaces.
Les cybercriminels cherchent à exploiter les faiblesses des collaborateurs avec des attaques très ciblées et tentent souvent de se faire passer pour des personnes d'autorité afin de voler de l'argent et des informations confidentielles aux employés, aux clients ou aux partenaires commerciaux de l'entreprise.

Aujourd'hui nous constatons de véritables lacunes en matière de culture liée à la cybersécurité (phishing, ransomware, malware, etc.) Pour faire preuve d'une grande efficacité dans la protection contre les menaces, il est important d'innover constamment avec des mesures concrètes comme la formation et les simulations de cyberattaques en entreprise.

Vous insistez sur le rôle déterminant du facteur humain dans une politique de cybersécurité. Que préconisez-vous comme action de prévention ?
Aujourd'hui, Proofpoint se distingue en effet sur le marché avec des solutions centrées sur l'humain. Nous avons notamment mis en place une solution de sécurisation de la messagerie contre les menaces telles que les logiciels malveillants, la fraude par email et le phishing, grâce à une classification détaillée des emails ainsi qu'une visibilité et un contrôle sur toutes les communications par courrier électronique.

Nous nous engageons en faveur de l'innovation dans la protection avancée des utilisateurs et des données informatiques pour les entreprises de toutes tailles. En association avec Wombat, nous sommes désormais investi dans la sensibilisation à la sécurité et à la simulation de phishing. La combinaison des fonctionnalités de Proofpoint contre les cyberattaques, associées à l'expertise de Wombat dans la simulation de phishing en temps réel, est une première dans l'industrie.

On a senti une plus grande sensibilisation aux problématiques de cybersécurité en 2018, comment l'analysez-vous ?

Aujourd'hui le paysage se dessine sous une complexification et diversification des menaces. Les cybercriminels redoublent d'inventivité pour dérober des informations personnelles ou financières. Loin des attaques par l'infrastructure, ce sont désormais les attaques pas l'ingénierie sociale qui priment.

La sensibilisation aux problématiques de cybersécurité s'était enclenchée grâce à WannaCry en 2017, et a continué en 2018 avec des cyberattaques de grande envergure qui ont fait couler de l'encre, comme Marriott, ou encore Pathé.

Pourtant le chemin reste encore long pour faire prendre conscience aux entreprises et collaborateur de l'importance d'assurer son environnement des cyberattaques. Il est nécessaire aujourd'hui de redoubler de vigilance, d'instaurer des solutions de protection et de mettre en place des bonnes pratiques. Les collaborateurs doivent être formés afin de pouvoir identifier et contrer les cyberattaques auxquelles ils seront confrontés tôt ou tard.