Cybersécurité : l'essor du spear phishing en entreprise se confirme

La division sécurité d'IBM a publié deux nouveaux rapports sur la cybersécurité. L'édition 2015 du Cyber Security Intelligence index montre que 45% des **cyberattaques** perpétrées dans le monde en 2014 ont été menées par des pirates externes à l'entreprise ciblée. 31,5% l'ont été par des initiés malintentionnés et 24,5% par des acteurs involontaires, le plus souvent des collaborateurs trompés par des techniques d'ingénierie sociale. **55% des attaques** ont donc une **origine interne**.

L'an dernier, les États-Unis ont enregistré plus de 50% des cyberattaques étudiées (même pays d'origine et de destination dans la plupart des cas). La France fait elle aussi partie du top 5 des pays les plus touchés par des cyberattaques locales, selon ThreatMetrix.

La croissance des spams piégés

Les attaques par déni de service distribué (DDoS) ne sont pas les seules menaces qui inquiètent les entreprises. Avec le harponnage (au Québec) ou **spear phishing**, les cybercriminels cherchent à cibler spécifiquement des personnes dans l'entreprise pour obtenir un accès à des données sensibles ou les inciter à ouvrir une pièce jointe, au risque d'exécuter un programme malveillant. Or, le rapport X-Force d'IBM fait état d'une augmentation des spams intégrant malwares et liens malicieux. Jusqu'à l'été 2013, le pourcentage de spams piégés par des malwares ne dépassait pas 1% de l'ensemble des courriels non sollicités à caractère commercial. Mais il a atteint **4% début 2015**.

Lire aussi :
Les cyberattaques focalisées sur les PC, pas sur les mobiles pour Verizon
Cybercrime : un coût de 2100 milliards de dollars pour les entreprises d'ici 2019

crédit photo © Ivelin Radkov – Shutterstock