Les entreprises attendraient-elles gentiment les attaques ? | Le Net Expert Informatique

Les entreprises attendraient-elles gentiment les attaques ?

Qu’on se le dise : n’importe qui peut se faire attaquer, qu’il s’agisse d’une petite comme d’une grande entreprise.

En 2013, le New York Times a subit une cyberattaque de l’armée électronique syrienne ; un groupe d’activistes soutenant Bachard El Assad. Les auteurs ont ciblé la partie la moins sécurisée du réseau, les serveurs DNS alors qu’ils sont devenus la pierre angulaire de toute applications internes ou externes.
En juin dernier, l’US Army s’est faite attaquée par les mêmes hackers. Et ce, alors même que l’Etat--Major américain avait fait de la cyberdéfense une priorité en investissant fortement. Pourtant, ces deux attaques démontrent qu’ils sont faiblement protégés et que, quelque soit leur taille, toutes les entreprises ou organismes sont des cibles potentielles. Les services informatiques n’ont donc pas su s’adapter à ces nouvelles menaces.
En France, le 1er semestre fut dense en matière de cyberattaques : TV5 Monde, Charlie Hebdo et Thales ont fait l’objet de sévères attaques de leur système informatique. On se souvient que des documents présentés comme des pièces d’identité et des CV de proches des militaires français impliqués dans les opérations contre l’EI avaient été postés sur le compte Facebook de TV5Monde par les pirates.
L’attaque avait été initialement revendiquée par des inconnus se réclamant de Daech (Etat Islamique). L’enquête s’oriente en juin vers des hackeurs russes. Le vol de données semble être le principal objectif des hackers.
Quelques semaines plus tôt, Manuel Valls annonçait que la défense française allait intégrer des community managers et hackers, plus à même de contrer les attaques. Une méthode innovante…. mais est--ce suffisant pour protéger une infrastructure réseau ?

Les entreprises françaises en mal d’inspiration ?
En général, les entreprises ne communiquent pas ou très peu sur leurs attaques. En effet, en regardant de plus près les cyberattaques subies en France, on s’aperçoit que les informaticiens n’ont pas su anticiper les nouvelles menaces. Ils ont préféré sécuriser leurs réseaux grâce à des méthodes utilisées depuis des décennies. Malheureusement, cela ne s’avère plus suffisant pour contrer les nouvelles menaces et les nouvelles techniques utilisées par les hackers.
En parallèle, cela met en exergue les problèmes d’investissement que les entreprises rencontrent et leurs manques de réactions.
Selon une étude menée par IDC [1], si la plupart des organisations sont conscientes des risques de sécurité liés aux serveurs DNS (82 % des répondants étaient conscients des menaces, qu’ils ont reconnues), l’essentiel des budgets en sécurité réseau est encore consacré à des solutions de sécurité plus traditionnelles telles que les pare--feu (68 %).
L’étude d’IDC a également révélé que même si 85 % des répondants disposent des fonctions de sécurité du DNS de base, les entreprises restent vulnérables, car ces fonctions sont généralement inefficaces en cas d’attaque.
Enfin, 73% des entreprises françaises ont subies des attaques sur leurs serveurs DNS mais elles ne sont que 7% à les considérer comme une très grande menace contre 27% aux Etats-- Unis, alors que les dégâts subies lors de ces attaques ont été très importants (vol de données, interruption de service, …).
Sans prise de conscience des responsables informatiques français, les cyberattaques ne cesseront de s’intensifier. Avec la multiplication des appareils connectés à internet, dans tous les domaines d’activités (hôpitaux, grandes administrations ou petites entreprises, dans la banque, l’énergie, la défense,), les données continueront d’avoir de la valeur aux yeux des pirates informatiques si les RSI ne changent pas leurs méthodes de protection.

[1] Enquête IDC sur la sécurité des serveurs DNS, avril 2014

Source : https://www.globalsecuritymag.fr/Les-entreprises-attendraient-elles,20150715,54386.html
par Hervé Dhelin, Directeur Marketing d’EfficientIP