L’armée mène une bataille numérique au cœur des entreprises sensibles | Le Net Expert Informatique

	L’armée mène une bataille numérique au cœur des entreprises sensibles

3 mars 2015, les responsables d'une entreprise « sensible » sont inquiets. Il semble clair que la PME est l'une des nombreuses cibles d'une cyberattaque massive lancée contre les industriels français depuis plusieurs semaines maintenant. Face à cette attaque d'ampleur nationale et touchant des entreprises sensibles, le gouvernement fait appel à l'armée.

L'ordre est donc donné par le Premier Ministre d'agir rapidement et efficacement. La cellule de crise du commandement opérationnel de Cyberdéfense du ministère de la Défense va mobiliser dans les meilleurs délais ses équipes pour intervenir directement dans les entreprises touchées. Tous les relais militaires et civils spécialisés dans la cyberdefense sont en alerte.
Leur mission, atténuer la portée de l'attaque et reconstruire le réseau. Dépêchés le plus rapidement possible au cœur de l'entreprise, des équipes d'une quinzaine de spécialistes encadrés par un officier chargé de la logistique prennent place sur les postes informatiques de l'entreprise. Leurs outils ? Aucun, ils viennent dérouler le fil de l'attaque pour pouvoir mieux l'endiguer, colmater les brèches.
Leur difficulté c'est que pour limiter les dégâts, la PME est totalement coupée d'Internet. Les spécialistes s'acharnent à chercher les preuves, nettoyer en profondeur, détecter toutes les failles et verrouiller les portes. Des observateurs de l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) sont présents pour faire remonter les informations auprès de l'organisme et coordonner les actions éventuelles à mener avec les différents ministères du gouvernement.
Une équipe de spécialistes constituée d'étudiants en quatrième année de l'EPITA est déployée par le commandement opérationnel de Cyberdéfense de l'armée pour reconstruire un réseau d'entreprise ayant subi une cyberattaque d'envergure. Dans l'avenir, ces étudiants pourraient faire partie des milliers de réservistes spécialisés que compte recruter le Ministère de la Défense.

« C'est du vécu »
Rapidement, les experts comprennent que le cybermissile s'est introduit tout simplement via une vulnérabilité WordPress du blog de l'entreprise. L'attaquant a installé un relai de scripts sur le serveur du blog qui lui permet d'aller plus avant dans ses funestes objectifs. Il pouvait même prendre la main sur l'ERP de l'entreprise. L'organisation pirate en a profité pour absorber la base de données de la société.
Mais voilà, ce scénario catastrophe est ce que l'armée appelle un « jeu », avec des « joueurs ». En réalité, ce jeu fait partie d'un exercice en grandeur nature réalisé par 600 personnes et encadré par le Ministère de la Défense et l'ANSSI. Baptisé DEFNET, l'expérimentation consiste à mettre en place des équipes constituées de dix à 15 élèves provenant de grandes écoles spécialisées dans le domaine de l'informatique et des télécommunications (Epita, Insa, Télécom Paris Tech, Ensta Bretagne, CentraleSupélec,…).
Encadré par un enseignant et un militaire, l'idée consiste à former à partir de ces ressources, les réservistes dédiés à la cyberdéfense de demain. L'armée compte disposer de plusieurs milliers de réservistes dans les prochaines années.
Lors de l'exercice, auquel ZDNet.fr a pu assister, le contre-Amiral Riban, Directeur Général adjoint de l'ANSSI a tenu à préciser que cette expérimentation repose sur « du vécu », sans en dire beaucoup plus, secret défense oblige. Dans ce genre de situation de crise, l'ANSSI est le chef d'orchestre. En élaguant les vagues de cyberattaques et les défacements de sites web en janvier, qui, pour lui étaient d'un niveau faible, il souligne qu'une véritable cyberattaque ne se résumerait pas forcément uniquement à des conséquences tragiques en termes de vol de données.
Ainsi, si les réseaux informatiques des banques, des aéroports, des réseaux de transport (SNCF, Ratp,…), ou les opérateurs de téléphonie étaient victimes d'une cyberattaque, la France pourrait être paralysée en quelques heures, avec tous les dangers que cela peut représenter. Enfin, interrogé sur une riposte éventuelle suite à une cyberattaque, le contre-amiral a précisé que l'article 21 de la loi de programmation militaire oblige à faire cesser l'attaque, mais pas d'aller au-delà. Le sujet est donc bien la défense…

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.zdnet.fr/actualites/cyberdefense-quand-l-armee-mene-une-bataille-numerique-au-coeur-des-entreprises-sensibles-39817126.htm