Comment réagir face à une cyberattaque | Le Net Expert Informatique

	**Comment réagir face à une cyberattaque**

Choc, sidération, déni… Une attaque informatique paralyse souvent les entreprises qui en sont victimes. L'idéal est donc de s'y préparer pour avoir les bons réflexes le moment venu. « Au début, une cyberattaque ne fait pas de bruit. L'entreprise continue apparemment à fonctionner normalement. Les cellules de crise classiques ont donc du mal à se mobiliser. Il faut s'adapter en prenant en compte la dimension cyber de l'attaque », remarque Gérôme Billois, expert en cybersécurité chez Solucom.

1 MONTER UNE CELLULE DE CRISE CYBER

La cellule de crise décisionnelle (direction générale, service juridique, RH, informatique, communication…) doit être secondée par une cellule de crise cyber. Idéalement, cette équipe est pilotée par le responsable sécurité des systèmes d'information (RSSI). Elle regroupe des membres de la direction informatique et les responsables des applications informatiques liées aux métiers de l'entreprise. Tous ces protagonistes doivent être sensibilisés à travers des exercices spécifiques, organisés annuellement.

« Suivant le scénario d'attaque, cela peut prendre la forme d'un exercice sur table de quelques heures à la simulation d'un début de crise », explique Gérôme Billois. Tout le monde doit être sur le pont. Les managers pour identifier les ressources à protéger, les RH pour répondre aux interrogations des collaborateurs, le service juridique pour évaluer les suites judiciaires, la communication si l'information de l'attaque a fuité…

2 DÉCONNECTER LES MACHINES INFECTÉES

Dès les premiers soupçons d'attaque, il faut réagir. Un grand industriel européen s'est mordu les doigts de ne pas avoir pris au sérieux les alertes remontées en 2012 par les autorités nationales. Résultat : le pirate a eu tout le loisir de sonder en profondeur son réseau informatique. « La crainte est qu'il ait eu accès au code source de nos outils informatiques qui permettent de gérer les infrastructures de nos clients », confie cet industriel. Il ne faut toutefois pas confondre vitesse et précipitation, prévient Jean-Yves Latournerie, préfet chargé de la lutte contre les cybermenaces au ministère de l'Intérieur. Les entreprises sont entre deux feux. D'une part, elles doivent isoler leur système de l'extérieur pour éviter la propagation de l'attaque. D'autre part, il faut éviter d'en effacer les traces. « Si on coupe et on efface les disques durs, les enquêteurs perdent les preuves et la possibilité de remonter aux auteurs de l'attaque », souligne le préfet.

La déconnexion peut être utile. Victime, en avril dernier, d'une attaque sévère qui a interrompu ses programmes, la chaîne de télévision TV5 Monde a agi ainsi pour limiter la casse. « Par chance, les équipes informatiques étaient présentes le soir de l'attaque. Elles ont pu déconnecter les machines infectées. Cela été salutaire. Selon l'Agence nationale de la sécurité des systèmes d'information (Anssi), l'objectif était de détruire notre société », précise Yves Bigot, le directeur général de la chaîne.

L'urgence passée, il faut rapidement faire appel à des professionnels expérimentés dans la neutralisation des attaques informatiques. L'Anssi dispose sur son site internet d'une liste de prestataires disposant du label CERT-FR (centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques). Certains s'engagent à intervenir en moins de quatre heures.

3 PORTER PLAINTE ET ESTIMER LES PRÉJUDICES

« Les entreprises hésitent à porter plainte, car elles craignent que cela nuise à leur réputation. Or, sans cela, on ne peut traiter policièrement et judiciairement une affaire », déplore le « préfet cyber ». Il faut donc déposer plainte au commissariat ou à la brigade de gendarmerie locale. Certains disposent d'un investigateur en cybercriminalité qui fournira les conseils d'urgence. La seconde étape est de se rapprocher d'interlocuteurs techniques qui pourront apporter leur expertise.

Les entreprises en région parisienne doivent solliciter la Befti, la brigade d'enquête sur les fraudes aux technologies de l'information. Cette unité spécialisée conseille les entreprises victimes d'intrusion informatique ou de détournement de fonds… Les entreprises en province auront accès à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC).

Il faut venir avec le maximum d'éléments qui vont aider les enquêteurs : le journal des connexions, la configuration des machines, les disques durs des machines infectées… « Il faut aussi estimer les préjudices subis sur la base d'éléments concrets. Cela permettra de présenter un dossier solide auprès du procureur de la République. C'est sur ce dossier qu'il décidera des suites à donner à l'enquête », explique le colonel Freyssinet, spécialisé dans la lutte contre les cybermenaces au ministère de l'Intérieur.

4 RECONSTRUIRE LA SÉCURITÉ INFORMATIQUE

Il faut agir sur les conséquences de l'attaque. Le grand industriel européen qui craignait qu'un pirate ait eu accès au code source de son outil de gestion à distance des infrastructures de ses clients n'a pas tergiversé. « Le code du produit a été totalement revu afin d'éviter la création d'un backdoor [une porte dérobée, ndlr] exploitable par les pirates. Nous avons également informé nos clients de l'attaque subie », confie-t-il. Après son attaque, TV5 Monde a remis à plat sa sécurité informatique. Elle a remplacé le matériel technique compromis et déployé des nouveaux équipements de sécurité.

Les 400 salariés suivent une formation pour apprendre les gestes de base dans ce domaine. La chaîne a imposé des mesures drastiques : suppression du Wi-Fi, interdiction de connecter des équipements électroniques personnels (tablette, smartphone…) aux ordinateurs de bureau, passage des clés USB au sas de décontamination… Soit, au total, une facture de 5 millions d'euros.

Pour soigner les machines infectées, l'Anssi préconise de réinstaller entièrement le système d'exploitation et d'appliquer tous les correctifs de sécurité avant de la reconnecter. Elle recommande de modifier les mots de passe de tous les comptes de l'entreprise sous peine de revoir débarquer le pirate informatique. L'agence incite également les entreprises victimes à communiquer avec leurs pairs. « Généralement, les pirates s'attaquent à plusieurs entreprises d'un même secteur, en réutilisant les mêmes techniques. En partageant son expérience, on renforce la sécurité collective », explique Guillaume Poupard, le directeur général de l'Anssi.

La messagerie sous écoute

Dans la panique, les membres de la cellule de crise communiquent par e-mails et s'échangent des fichiers via le réseau de l'entreprise. Grave erreur. Il y a de grandes chances pour que ces systèmes soient compromis et sous écoute. Le conseil pour communiquer en toute discrétion : ouvrir temporairement des comptes de messagerie à partir de services web. Les échanges informatiques doivent également se faire par l'intermédiaire d'un réseau de secours indépendant de celui de l'entreprise afin de garantir leur confidentialité.

Denis JACOPINI est Expert en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.usine-digitale.fr/article/comment-reagir-a-une-cyberattaque.N354821
Par HASSAN MEDDAH