La gestion de crise cyber en état d'urgence

Face aux dramatiques évènements qui ont endeuillé le vendredi 13 novembre notre pays, la plupart des entreprises ont réagi en mettant en place, dès le week-end qui a suivi, des cellules de crise. Si la survenance d'attaques cyberterroristes n'a pas, à l'heure où nous écrivons ces lignes, été constatée, la vigilance, surtout dans le cadre de l'état d'urgence, demeure. Les services gouvernementaux et les RSSI sont sur le pont.

Vendredi 13 novembre, la France a été frappée par l'une des plus meurtrières attaques terroristes de son histoire, laquelle a fait 130 morts et 350 blessés en différents lieux de Paris et sa banlieue. En matière de gestion de crise, les entreprises dans leur ensemble ont fait front, et les réseaux sociaux ont permis une fluidité de circulation de l'information qui a sans nul doute

Etat d'urgence

Le projet de loi prolongeant jusqu'à février 2016 l'état d'urgence mis en place par la loi du 3 avril 1955 a été voté à la quasi-unanimité (551 voix pour, 6 voix contre, une abstention) le 19 novembre 2015 par l'Assemblée nationale.

Il prévoit notamment qu'*« il peut être accédé, par un système informatique ou un équipement terminal présent sur les lieux où se déroule la perquisition, à des données stockées dans ledit système ou équipement ou dans un autre système informatique ou équipement terminal, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial. Les données auxquelles il aura été possible d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. »* La perquisition donne lieu à l'établissement d'un compte-rendu communiqué sans délai au procureur de la République.

Le texte de loi précise que *« cette rédaction vise les données informatiques telles que celles qui sont présentes dans un ordinateur, celles qui sont accessibles depuis un ordinateur (*« nuage »*), celles qui sont contenues dans un téléphone… »*[1]. L'article 2 proroge également la possibilité *« d'ordonner des perquisitions de jour et de nuit »*. Le blocage administratif des sites a par ailleurs été aménagé[2].

Ces dispositions vont sans nul doute demander aux RSSI des fournisseurs d'accès, et, de manière générale, des grandes entreprises, de rester en veille, et de collaborer de manière plus étroite avec les forces de police.

[1] http://www.linformaticien.com/actualites/id/38575/etat-d-urgence-perquisition-dans-le-cloud-et-internet-coupe.aspx

[2] http://www.linformaticien.com/actualites/id/38601/etat-d-urgence-numerique-le-blocage-administratif-des-sites-evolue.aspx

permis de compenser la saturation des réseaux traditionnels de communication.

La plupart des entreprises ont mis en place une cellule de crise

Du côté des entreprises, la mobilisation ne s'est pas fait attendre : dès le samedi matin, voire le dimanche ou le lundi, des cellules de crise ont été montées dans la plupart des entreprises, pour évaluer les impacts psychologiques, mais aussi sociaux et économiques de ces attentats dans notre pays. Christian Sommade, délégué général du HCFDC, (Haut Comité Français pour la Défense Civile) a mis en place pour son organisation avec des outils adaptés (AMI Software, Vue Too) une Situation Room avec une veille médias dès le début du week-end pour permettre aux entreprises de répondre aux questions qu'elles se posaient, à savoir : quels sont les salariés qui auraient pu être victimes des attentats, et ce afin d'assister tout de suite la famille, qui apprendrait la nouvelle de la mort de l'un de leurs proches sur les réseaux sociaux.

Cécile Weber, *Présidente du Club de la Continuité d'Activité,*

"Les pertes créées par cette situation tragique ne doit pas faire baisser notre vigilance."

Canular « On est Tous Paris »

Le 17 novembre au matin, ce message est arrivé dans de nombreuses boîtes aux lettres :

> Objet : Message virus
> Vous risquez de recevoir un mail nommé *« on est tous Paris »* qui est diffusé à grande échelle depuis ce WEEK-END.
> Dans ce message une photo de bébé avec un bracelet de naissance où il est écrit *« on est tous PARIS »* vous invitant à cliquer sur la photo. NE CLIQUEZ PAS!!! ce message contient un malware (virus) qui permet de prendre le contrôle à distance de votre téléphone ou ordinateur et de récupérer toutes vos données et mots de passe.

L'ANSSI a vérifié la toxicité de ce message et affirmé dès le mardi 17 novembre que c'était un canular. Malheureusement, il n'est pas exclu que dans les semaines qui viennent, d'autres mauvais plaisantins ne prennent prétexte de la tension ambiante pour véhiculer d'autres messages de ce type. Face à cela, une seule attitude : la prudence. En cas de doute, suivez les publications de l'ANSSI, qui étudie en temps réel toutes les attaques, avérées ou non. (www.ssi.gouv.fr).

Comment gérer la situation avec une reprise d'activités ? Dès dimanche, par exemple, Cécile weber, Présidente du Club de la Continuité d'Activité, a mis en ligne des recommandations de bon sens pour les membres de son club, dont une vigilance sur une possible crise cyber. *« Comme la plupart des entreprises, nous avons mis en place une cellule de crise, composée de la direction générale, de la communication, des ressources humaines et des experts concernés »* explique Jean-Yves Oger, président de la commission gestion de crise au CDSE (Club des Directeurs Sécurité des Entreprises). Eric Wiatrowski, RSSI d'Orange Business Services, nous confie d'une voix tendue, lui d'habitude si jovial au téléphone : *« suite aux événements du Stade de France du 13 novembre, une cellule de crise a été activée durant le week-end. La cellule était composée de décideurs et de représentants de différentes fonctions : services généraux, ressources humaines, opérations, sécurité... Celle-ci a décidé de demander aux employés de ne pas se rendre à notre site de Saint-Denis le mercredi 18. Le télétravail et le redéploiement partiel sur d'autres sites ont permis d'assurer la continuité des activités. »*
Eric Wiatrowski indique, qu'en parallèle, une cellule de crise cyber a été activée et la vigilance a été renforcée sur les infrastructures IT et réseau.
Un haut responsable de l'administration précise, de son côté : *« nous avons mis en place des parades adaptées à la survenance d'une crise cyber. Mais ce n'est pas le même sujet, pas le même mode opératoire. Pour l'instant, cette crise n'a pas eu la même dimension d'attaques cyber que suite aux attentats de janvier dernier, qui avaient été suivis par des campagnes de défacements de sites, et, plus tard, par l'attaque de TV5 Monde. »*
C'est aussi l'avis d'Alain Bouillé, président du CESIN, qui nous appelle le 19 novembre : *« pour l'instant, nous n'avons pas eu de cas avéré d'attaques sur nos systèmes. Nous ne sommes, en tous cas pas pour l'instant, dans la même situation qu'au mois de janvier où il y avait une cible médiatique clairement identifiée. Mais, en interne, nous sommes restés vigilants et avons augmenté notre niveau de gestion de crise. »*
Même l'ANSSI, à part la mise en garde contre ce qui s'est avéré être le canular *« On est Tous Paris »* (lire encadré) n'a pas constaté, à l'heure où nous écrivons ces lignes, d'attaques sur les systèmes d'information des entreprises. Le seul commentaire fait est de maintenir un niveau de vigilance élevé sur les systèmes d'information, en respectant les bonnes pratiques

énoncées sur le site. Si on peut comprendre la discrétion et la réserve de l'ANSSI sur un tel sujet, cela ne doit surtout pas empêcher les entreprises de rester en veille. Car le fait qu'il n'y a pas eu, pour l'instant, de cyberattaques ne veut pas dire qu'il ne va pas y en avoir...

L'état d'urgence : maintenir les OIV en état d'alerte

L'ANSSI a été ainsi partie prenante de ca cellule de crise interministérielle qui a été constituée lors des attentats, et travaille, dans l'ombre, pour maintenir les Opérateurs d'Importance Vitale (OIV) en état d'alerte. Car une attaque cyber reste, plus que jamais, possible, et la mobilisation des entreprises sur ce risque doit rester intacte, surtout dans le cadre du vote à la quasi-unanimité le 19 novembre dernier du projet de loi sur la prolongation jusqu'à au moins février 2016 de l'état d'urgence sur le territoire national. Cécile Weber ne dit pas autre chose : *« la mise en évidence des pertes créées par cette situation tragique ne doit pas faire baisser notre vigilance face aux risques cyber »*. Christian Aghroum, commissaire divisionnaire, ancien patron de l'OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication) et maintenant directeur général de Socoa, basé en Suisse, qui conseille notamment des grandes entreprises pour la gestion de crise, estime, lui, qu'une attaque cyberterroriste n'est absolument pas à exclure. *« C'est une forme de réplique à laquelle on est en droit de s'attendre. Une attaque sur les infrastructures vitales n'est pas non plus à écarter. Par principe, il faut se prémunir contre le pire »*.

« Nous n'avons jamais abaissé notre seuil de surveillance depuis les attentats de janvier »

Se prémunir contre le pire, c'est ce que ce RSSI d'un OIV qui tient à son anonymat a fait. Il nous raconte : *« nous n'avons pas connu de réunion de crise avec les évènements du vendredi 13 novembre, mais j'ai eu carte blanche de ma direction générale pour prendre les mesures nécessaires. Nous n'avons jamais abaissé notre seuil de vigilance depuis les attentats de janvier dernier. Nous avons bien évidemment beaucoup travaillé sur la sécurité opérationnelle. Le travail effectué depuis le mois de janvier a facilité nos opérations de surveillance »*.

Christian Aghroum, commissaire divisionnaire, ancien patron de l'OCLCTIC

> " Cette attaque a eu un véritable impact car il s'agissait d'un média grand public. "

Concrètement, il nous en dit un peu plus sur la procédure. *« Nous vérifions que les systèmes sensibles sont bien cloisonnés. La priorité n°1 pour la direction des systèmes d'information, c'est de renforcer le filtrage périmétrique. Nous vérifions une à une les règles du pare-feu et, sans trop dévoiler nos opérations, nous avons renforcé les opérations de détection d'intrusion dans le domaine cyber. Nous faisons des tests de vulnérabilité pour vérifier que nos systèmes sont à jour. De manière préventive, nous appliquons des patchs sur nos systèmes les plus exposés. Enfin, en matière de gestion de crise cyber, nous avons documenté nos règles de réponse, et notre documentation est formalisée »*. De manière plus générale sur le risque d'une attaque cyberterroriste sur les infrastructures industrielles, le RSSI confie : *« nous sommes en contact*

La gestion de la communication de crise via les réseaux sociaux

Alors que les forcenés faisaient rage dans les rues de la capitale et au Stade de France, plusieurs personnes très inquiètes cherchaient à tout prix à savoir où étaient leurs proches, et s'ils étaient en sécurité. La fonction Safety Check de Facebook a été utilisée par 5,4 millions de personnes après les attentats de vendredi dernier[1]. Cette fonction n'avait auparavant été activée que lors des tremblements de terre au Népal. D'autre part, dans une interview accordée au Figaro (23 novembre 2015), Damien Viel, directeur général de Twitter France, a souligné que le hashtag #PorteOuverte a été retweeté un million de fois. Christian Aghroum, comme d'autres professionnels, souligne quant à lui le rôle primordial qu'ont eu les réseaux sociaux dans la gestion de crise. *« Le rôle de Facebook a été assez symptomatique de la manière dont on peut gérer une communication en gestion de crise, et dont on peut se passer des réseaux traditionnels. Et, face aux débordements de haine sur les réseaux sociaux, il y a eu aussi une certaine forme d'autogestion par les réseaux sociaux »*. Certains internautes ont ainsi spontanément appelé à la dénonciation de messages haineux sur Facebook, pendant que le réseau social Telegram, créé par un Russe et notoirement utilisé par daesh, purgeait les chaînes appartenant à daesh[2].

[1] http://www.linformaticien.com/actualites/id/38573/comment-reagissent-les-reseaux-sociaux-apres-les-attentats.aspx

[2] http://www.linformaticien.com/actualites/id/38581/telegram-reseau-social-apprecie-des-terroristes-leur-donne-la-chasse.aspx

permanent avec l'ANSSI et nos autres confrères RSSI d'OIV. Nous prenons très au sérieux une attaque logique sur les systèmes SCADA, mais, pour être franc, je redoute encore plus une attaque cyberterroriste de type physique sur les systèmes industriels. Dans tous les cas, la mobilisation est maximale», conclut ce RSSI. Une mobilisation qui prend tout son sens lorsque nous lisons - cela est passé relativement inaperçu et n'a pas été repris par beaucoup de médias - que Jürgen TodenHöfer, un journaliste, député allemand apparenté au parti chrétien-démocrate (CDU), et ancien juge, qui a passé dix jours en 2014 au sein de Daech, parlerait d'un «holocauste nucléaire»[1] que l'Etat Islamique serait prêt à lancer contre l'Occident. Face à la gravité d'une telle assertion que nous n'avons pas pu vérifier, la plus élémentaire prudence est de mise.

Si l'on repart sur le terrain moins visible d'une crise cyber, voire cyberterroriste, celle-ci doit être gérée avec les mêmes mécanismes que les autres crises, notamment par la constitution d'une cellule de crise, avec un rôle central dévolu à la communication de crise «interne et externe» souligne Christian Aghroum. *« Une bonne gestion de la communication implique d'accepter la crise, d'avertir les fournisseurs et les clients, et de remettre à niveau des systèmes et les organisations. La bonne communication et l'existence d'un PCA/PRA sont deux bons moyens de sortir d'une crise»* précise Christian Aghroum. Le réjouissant sketch joué en fin des Assises de cette année par la fine équipe d'Isabelle Tisserand, de la Poste, qui mettait en scène une équipe de bras cassés devant faire face au plantage d'un serveur informatique de gestion des rendez-vous en one-to-one deux jours avant les Assises et à l'enlèvement de Gérard Rio[2] soulignait un arsenal de bonnes pratiques, dont la gestion essentielle de la communication et de la répétition de scénarii de crises, avec formalisation de la conduite à tenir. Mais une crise cyber possède certaines caractéristiques intrinsèques. *« Ce type de crise arrive au hasard à un moment et à un endroit non prévisible. C'est un risque dont la source est inconnue, mais l'attaquant connaît les failles du SI. Cela demande une longue préparation»*, précise François Tête, président d'honneur du Club de la Continuité d'Activité. Christian Aghroum revient ainsi sur l'attaque de TV5 Monde : *« cette attaque a eu un véritable impact car il s'agissait d'un média grand public»*. Voire. Victor Rocaries, président de France Médias Monde, que nous avons essayé de joindre pour cette enquête à plusieurs reprises, a ainsi confié lors des Journées Interparlementaires de la Cybersécurité (lire en pages Tendances) s'être ému de l'attaque de TV5 Monde, et avoir pris depuis les mesures à ses yeux nécessaires, à savoir une plus grande sensibilisation des collaborateurs (les journalistes n'étant pas, pour des raisons culturelles, une population très encline à la protection de son outil de travail), *« une volonté de mutualisation entre chaînes publiques, sur des systèmes de supervision et de contrôle ; enfin, toujours entre chaînes publiques, nous réfléchissons à des PRA (Plan de Reprise d'Activités) et des PCA (Plan de*

François Tête, *président d'honneur du Club de la Continuité d'Activité*

> "Ce type de crise arrive au hasard à un moment et à un endroit non prévisible."

Les recommandations du Club de la Continuité d'Activité

Par la voix de sa présidente, Cécile Weber, le Club de la Continuité d'Activité a envoyé dès le dimanche 15 novembre les mesures suivantes pour ses membres : elles peuvent s'appliquer à n'importe quelle entreprise en situation d'état d'urgence.

- renforcer le suivi des consignes données par les pouvoirs publics dans le cadre de l'état d'urgence décrété sur l'ensemble de notre territoire, afin de pouvoir identifier les conséquences potentielles sur vos organisations (arrêt de transports publics, fermetures d'établissements scolaires..),
- assurer une veille renforcée des événements qui pourraient survenir sur notre territoire,
- envisager le renforcement de la surveillance et la mise en place de mesures de sécurité spécifiques sur certains de vos sites sensibles (avec communication auprès des collaborateurs concernés),
- maintenir un niveau de vigilance élevé sur le risque cyber,
- envisager l'opportunité d'annuler certains déplacements professionnels,
- envisager dès à présent les impacts métiers qui pourraient toucher vos organisations, à court ou moyen terme,
- effectuer une revue de votre PCA pour anticiper un risque d'indisponibilité de collaborateurs (incapacité à se rendre sur son lieu de travail).

---

[1] Voir http://www.midilibre.fr/2015/09/30jurgentodenhofer-l-ei-veut-lancer-un-holocauste-nucleaire-contre-l-occident,1220622.php et http://www.directmatin.fr/monde/2015-09-30/daesh-preparerait-une-attaque-nucleaire-pour-tuer-des-centaines-de-millions-de-0

[2] http://www.mag-securs.com/news/articletype/articleview/articleid/34716/quand-les-assises-jouent-a-guichets-fermes.aspx

[3] http://www.mag-securs.com/news/articletype/articleview/articleid/34720/france-medias-monde-un-temoignage-in-attendu.aspx

Continuité d'Activités) avec une redondance physique de nos moyens de diffusion »[3]. Pour en avoir avoir discuté avec lui lors des Assises, le directeur de production de la radio NRJ, Martin Cassagne, prenait lui aussi la menace de crise cyber et d'attaques sur son antenne très au sérieux, et, depuis TV5 Monde, sa direction aussi...

« Les entreprises sont incapables de travailler en mode dégradé »

« La principale caractéristique d'une crise cyber, c'est le fait d'être atteint et de ne pas s'en rendre compte tout de suite » observe Christian Aghroum. *« Ensuite, on ne sait pas forcément comment réagir »*. C'est ce qui s'est passé avec TV5 Monde, qui a révélé un total état d'impréparation face à une crise de ce type. *« Dans une organisation de crise, notamment cyber, il faut savoir revenir à un environnement dégradé, savoir travailler avec un papier et un crayon, sans les ordinateurs, qui peuvent être tous plantés si le réseau de l'entreprise est atteint »*, confirme Christian Aghroum. *« Je suis frappé de voir à quel point, dans les entreprises que je conseille, on est incapable de travailler en mode dégradé. Dans la plupart des cas, il n'existe même pas un document papier (classeur, fiches ou autres) dans lequel les procédures de gestion de crise sont répertoriées ! Comment fait-on si on n'a plus d'informatique ? »*.

Sur la gestion de la crise cyber proprement dite, peu de littérature existe, même si on commence à y réfléchir sérieusement. Selon François Tête, *« dans une cellule de gestion de crise cyber, il faut au moins la direction générale, la communication, le RSSI et/ou le DSI, le responsable du PCA/PRA, et quelques représentants des directions métiers impactées, sachant qu'il faut arbitrer entre les attentes des directions métiers, qui veulent redémarrer tout de suite, et les RSSI/DSI, qui veulent circonvenir la crise... »*. D'où la nécessaire présence de la direction générale. François Tête insiste aussi, dans la survenance d'une crise cyber, sur l'importance de ce qu'il appelle un *« point doré, ou point sain, ou point indemne : c'est une* « copie saine », *un point à partir duquel les composants de l'environnement informatique, les données ou les applications affectés peuvent être restaurés dans l'état où ils étaient avant la présence de l'attaquant »*. Il est d'autant plus difficile à identifier que, en général, on ne sait pas à quand remonte l'attaque. D'où la nécessité d'avoir fait des sauvegardes régulières de recours à ces « points dorés ».

Ensuite, dans les modes dégradés d'une crise, notamment cyber, il faut être capable de prévoir de constituer un site de secours où les employés peuvent travailler, pratiquement du jour au lendemain, soit d'un site distant, soit de chez eux. C'est notamment une des préoccupations du RSSI d'une ESN sur la place de Paris. Des offreurs de services de bureaux à la demande, comme Regus, seraient éventuellement à même d'offrir une réponse à ce type de préoccupation. Mais le fait de travailler à domicile de manière impromptue constitue aussi une réponse. *« C'est le TOAD (Travail Occasionnel à Distance) »* précise François Tête, qui prévient aussitôt : *« attention ! Ce n'est pas le télétravail ! Le TOAD doit lui aussi obéir à des règles négociées, avec la DRH, et prévoir des mécanismes de sécurité sur le domicile de l'employé pour que celui-ci puisse travailler en toute confidentialité »*. Ce qui implique des réseaux sécurisés... et une répétition avant la survenance de la crise, afin de ne pas se retrouver en état de panique totale le jour où l'événement survient. Mais tous les métiers ne sont pas éligibles au TOAD.

On le voit, la situation actuelle, très tendue, tension aggravée par la prolongation de l'état d'urgence jusqu'au mois de février au moins, va demander une capacité de résilience forte de la part des entreprises, ce que l'on pourrait appeler « éco-lience » (lire encadré). Malheureusement, comme l'ont déclaré nos gouvernants, nous devons vivre avec le terrorisme probablement à long terme, et une attaque cyberterroriste, même si elle n'a pour l'instant pas eu lieu, n'est pas à exclure, loin de là. Il faut cependant bien continuer à vivre, à travailler... dans un régime de vigilance et de surveillance accrue. Les systèmes d'information doivent faire partie intégrante de cette vigilance, et la relative absence de riposte des terroristes sur les réseaux informatiques ne doit pas faire oublier que la menace est bien réelle, probablement pour longtemps. A nous de ne pas baisser la garde. ■

Sylvaine Luckx

Ecolience : pour que l'économie nationale tienne en « état d'urgence »

Avant les évènements, les forces armées avaient fait discrètement passer le message que la nation doit disposer de moyens de cyberdéfense et s'en donne les moyens sans trop en parler.

Dans les entreprises, la même démarche prend place. La cybersécurité doit prendre forme. La manière est encore incertaine : technique ? Ou managériale ? Les entreprises sont à la recherche d'un modèle de gouvernance.

De quoi s'agit-il ? Tout d'abord de disposer d'une capacité de « tenir le choc » : une capacité de résilience. Attaquées de partout, les entreprises et la Nation doivent faire face et ne pas tomber.

Un système de résilience ne peut exister par lui-même, comme étant une unité cohérente et suffisante en elle-même. Elle doit trouver des éléments d'appui et de soutien : dans l'entreprise, et dans la société. Les forces de défense de nos armées font assurément partie intégrante de ce système. Elles doivent être complétées et s'appuyer sur les capacités de défense des entreprises et de notre société dans son ensemble.

C'est un écosystème de résilience qui doit être construit. Un système tellement complexe et tellement sûr qu'il pourrait être attaqué de multiples manières sans faillir. Des réponses peuvent provenir de différentes origines : gouvernementales, entrepreneuriales, sociétales.

Dans un langage « geek », le néologisme est d'usage. Comment nommer un tel écosystème de résilience : une écolience ? Qu'importe, il faut la mettre en œuvre.

Dominique Ciupa