L’entreprise: nouveaux défis cyber

Colonel Philippe Davadie
Centre d'Enseignement Supérieur de la Gendarmerie

Mai 2014 – Article n° IV.4

Cet article présente la synthèse de l’ouvrage publié par Philippe Davadie, L’entreprise: nouveaux défis cyber, Edition Economica, 192 pages, mai 2014.

L'informatisation de l'entreprise s'est effectuée de manière transparente pour le grand public qui, pendant longtemps, ne s'estimait pas concerné par ce phénomène. Sa prise de conscience de l'importance de cette informatisation date du passage à l'an 2000 : alors que ce changement d'année devait être particulièrement festif, les spécialistes auguraient qu'il s'accompagnerait d'un bug transformant cette date festive en catastrophe. Ce passage aurait pu correspondre à une prise de conscience générale des enjeux de sécurité informatiques, mais il n'en a rien été, car tout s'est finalement déroulé de manière purement festive.

Estimant que leurs efforts avaient été vains, les entreprises se sont moins focalisées sur la sécurité informatique, laissant des pans entiers de leur informatique se développer de manière quasi autonome. L'irruption de la cybercriminalité n'a pas non plus modifié leur comportement, les menaces annoncées se focalisant d'abord sur les particuliers.

Parallèlement à l'avènement de la cybercriminalité, plusieurs phénomènes ont engendré des contraintes pour l'entreprise : les progrès de l'informatique personnelle cadençaient son informatisation et ses employés ont exigé que les outils qu'elle mettait à leur disposition soient aussi performants que les leurs propres. Afin de suivre ce rythme, elle en est venue à faire appel à davantage de prestataires de service qui lui proposaient des « solutions » clé en mains, acceptant *de facto* qu'une part de son informatique lui échappe.

Ces informatiques qui se sont développées de manière quasi autonome peuvent, pour plusieurs raisons, être appelées orphelines. La DSI n'en ayant pas reçu la responsabilité, personne ne se sent réellement concerné par leur sort. De plus, leur habituel bon fonctionnement donne l'impression qu'elles sont infaillibles. Enfin, à l'instar des maladies du même nom, les attaques les visant sont diagnostiquées tardivement et les démarches curatives encore peu développées.

I Les informatiques de l'entreprise

La grande dépendance, voire l'addiction de l'entreprise à l'informatique fait souvent croire que l'informatique de l'entreprise est monolithique. Lorsqu'on évoque cette dernière, on pense presque exclusivement aux diverses fonctions dont l'informatisation a été amplement médiatisée. Cela recouvre les RH, la paye, la comptabilité des matériels, l'administration courante de l'entreprise ainsi que sa présence sur l'Internet.

Très connue et mettant en œuvre des matériels également à disposition du grand public, l'informatique de ces fonctions exerce un monopole médiatique : parler de l'informatique de l'entreprise c'est, bien souvent, parler de l'informatisation de ces fonctions. Ce qui a eu pour

conséquence que la sécurité informatique s'est presque exclusivement consacrée à leurs problèmes, négligeant la réflexion sur les autres informatiques.

Pourtant, plusieurs dirigeants estiment que la part occupée par ces fonctions au sein du système d'infromation de l'entreprise est loin d'être majoritaire.

Le préalable à la sécurisation de l'entreprise est alors d'en recenser les informatiques.

L'informatique de production, à savoir l'ensemble des composants informatiques (automates, capteurs, ordinateurs et logiciels les équipant) qui permettent à une entreprise de produire les biens qu'elle vend à ses clients et de contrôler le processus de leur fabrication est la première qui vient à l'esprit. Au sein de cette informatique de production, nous trouvons les systèmes SCADA (*Supervisory Control And Data Acquisition*, commande et acquisition de données de surveillance). Permettant à l'entreprise de fabriquer ce qu'elle vend, elle tient donc une place essentielle et il peut sembler paradoxal qu'elle puisse être qualifiée d'orpheline. Cependant, on ne peut que constater que la littérature traitant de sa sécurité est faible et qu'il a fallu attendre l'arrivée de *Stuxnet* pour qu'une prise de conscience commence à avoir lieu.

À côté de l'informatique de production, nous trouvons les télé-opérations, par lesquelles une personne extérieure à l'emprise physique de l'entreprise est autorisée, via un réseau qui peut être l'Internet, à prendre la main sur une autre machine informatisée, pour modifier sa configuration, diagnostiquer un problème ou le résoudre. Elles sont effectuées par des membres de l'entreprise ou des prestataires de service. Plusieurs points d'attention doivent être pris en compte lorsqu'on évoque ces opérations. Le nombre de partenaires, car en plus du prestataire et du bénéficiaire, l'opérateur télécom est partie prenante à ces opérations, ce qui augure de difficultés certaines dans la recherche du responsable d'un mauvais fonctionnement d'une telle opération. De plus, s'il est possible de décrire le périmètre de l'informatique de production, il est impossible de déterminer celui des télé-opérations, car le circuit de l'information transitant via l'Internet n'est pas prévisible.

L'informatique périmétrique entre dans la catégorie des informatiques orphelines. Elle comprend l'ensemble des capteurs et logiciels qui permettent la détection de toute transgression, par une personne ou une chose, d'un périmètre donné, quel qu'en soit le sens, entrée ou sortie, l'identification du transgresseur, et qui aident à déterminer si ce « bris de clôture » est une entrée ou une intrusion. La différence entre intrusion et entrée résidant dans le fait que celle-ci est autorisée, alors que celle-là n'est pas souhaitée. Elle comprend notamment les badges d'entrée, les puces RFID qui permettent de gérer les stocks, ainsi que les caméras vidéo. La portée des ondes émises par leurs composants bien souvent sans fil peut poser problème : la portée théorique peut laisser croire qu'il existe une sécurité au delà d'une certaine distance, alors que la portée pratique la dépasse parfois.

Enfin, le *cloud* présenté comme la solution aux besoins de mobilité et de disponibilité mérite également le qualificatif d'orpheline, car s'il permet à l'entreprise de ne pas s'occuper de questions très techniques pour lesquelles elle ne dispose pas toujours des compétences requises, il peut être vu comme une prise de contrôle des informations vitales de l'entreprise par un prestataire.

Il est alors cohérent de définir comme informatique orpheline une *informatique d'apparition peu récente qui, bien qu'indispensable à l'entreprise fait l'objet d'un désintérêt, tant en interne de la part de la DSI, qu'en externe de la part de la doctrine, mais continue pourtant à se développer à un rythme soutenu*.

Ce terme d'orpheline est, bien sûr, à rapprocher du terme médical qualifiant certaines maladies graves, rares, et ne faisant pas l'objet de recherches médicales suffisantes.

II Les raisons de l'existence des informatiques orphelines

Le caractère orphelin de ces informatiques est en partie le fruit de l'Histoire. Après sa mécanisation, l'entreprise s'est automatisée puis informatisée afin de produire mieux et plus vite. Ce faisant, les exigences de rapidité ont eu pour conséquence de ne pas prendre en compte toutes les questions de sécurité. Par la suite, l'apparition des DSI et les débats relatifs à la sécurité informatique, en se concentrant sur celle de gestion, ont accru l'isolement de ces informatiques. Enfin, le *cloud* en incitant les entreprises à se concentrer sur leur *cœur de métier*, a initié ou aggravé

le manque d'investissement de l'entreprise sur des sujets pourtant essentiels tels que le degré de sensibilité d'une information et ses règles d'accès.

D'autres facteurs moins rationnels expliquent également ce quasi-abandon. La croyance en un progrès quasi perpétuel et à la puissance de l'innovation peut conduire à penser que ce qui est bénéfique pour une informatique le sera à terme pour une autre. Les faibles taux de panne, le développement de la sécurité informatique et de l'*intelligence* embarquée devraient profiter à toutes les informatiques qui auraient débuté un mouvement de convergence les unes vers les autres.

Les fournisseurs de produits et logiciels informatiques ont également leur part de responsabilité. En proposant des « solutions » qui n'en sont pas, car leurs produits ne règlent pas tous les problèmes de sécurité, ils leurrent les DSI qui, confrontées à l'exigence de résultats de leur direction générale sont tentées de se laisser séduire.

Pourtant, la convergence des informatiques évoquée précédemment n'est pas encore à l'ordre du jour. Si certains points semblent l'annoncer (uniformisation des OS, des composants matériels et des protocoles réseau notamment), des divergences subsistent. Les exigences de disponibilité ne sont pas les mêmes : l'informatique de production doit fonctionner de manière continue, alors que celle de gestion peut être programmée. La production industrielle nécessite un fonctionnement en temps réel, ce qui n'est pas le cas de l'informatique de gestion. Enfin, les exigences de sécurité diffèrent, car si pour la gestion la confidentialité prime, c'est la disponibilité qui est cruciale pour la production, alors que l'intégrité l'est tant pour les télé-opérations que pour l'informatique périmétrique.

III Répercussions des fragilités des informatiques orphelines sur l'entreprise

Bien qu'orphelines, ces informatiques ont des répercussions sur le système d'information général de l'entreprise. Les précédents de *Stuxnet* et *Shamoon* nous le rappellent.

Les attaques visant ces informatiques ont plusieurs caractéristiques. La récente multiplication des alertes et des rapports d'éditeurs de « solutions de sécurité » informatiques montrent leur permanence. Elles peuvent être *destructrices* si elles visent à altérer, paralyser ou modifier parfois de façon radicale - jusqu'à la destruction - un système informatique (supprimer des données, modifier le comportement d'un automate de production), ou *captatrices* si leur but est d'acquérir de manière frauduleuse des données ou savoir-faire d'une entreprise concurrente ou sur laquelle l'attaquant a des vues, d'influencer un décideur voire d'altérer son jugement (subversion). À l'instar des attaques visant l'informatique de gestion, leur motivation peut être ludique, cupide, terroriste ou stratégique, voire multiple ou croisée. L'augmentation du nombre d'utilisateurs de l'informatique, la facilité d'accès croissante à des maliciels éprouvés et le raccordement des informatiques à l'Internet font que la probabilité d'attaque d'une informatique orpheline croît avec le temps. Même si tous les succès ne sont pas médiatisés, certains incidents ont indubitablement une origine malicieuse.

Comme pour une attaque visant l'informatique de gestion, l'attaquant peut viser directement sa cible ou tenter de l'atteindre par rebonds successifs. La sophistication des attaques allant *crescendo*, elles sont de plus en plus soumises à la même succession de phases : renseignement, planification et conduite. Les cheminements demeurent variés et n'ont pour limites que l'imagination des attaquants.

Le temps de la sécurité par le secret est révolu, de même que celui de la sécurité par l'obsolescence. Les informatiques orphelines constituent donc des cibles potentielles et il convient de recenser leurs vulnérabilités afin de mieux protéger l'entreprise. Certaines leur sont d'ailleurs inhérentes comme l'obsolescence des OS, leur faible sécurisation, ainsi que celles générées par leurs contraintes d'utilisation (difficulté d'appliquer des correctifs, etc.). Enfin, leur raccordement à un même réseau les fragilise, car leurs vulnérabilités sont désormais accessibles à un plus grand nombre de personnes.

Les sécuriser constitue un vaste chantier, qui peut être rendu encore plus difficile par plusieurs ambiguïtés du cyberespace. À la difficulté d'identifier précisément l'attaquant, s'ajoutent

l'ambiguïté de la détermination du dommage réel (car il peut y avoir un dommage apparent), celle des moyens utilisés pour mener l'attaque, et celle de sa finalité. De ces ambiguïtés découlent la grande difficulté de prendre un attaquant sur le fait (flagrant délit) et l'impossibilité de répliquer en état de légitime défense.

Pour autant, les effets des attaques sont bien réels et certains peuvent être aisément imaginés. L'atteinte à la qualité ou aux cadences de production, aux personnes ou à l'environnement, la récupération de secrets industriels ou d'informations confidentielles de l'entreprise, l'utilisation de ses ressources à des fins illégales et l'atteinte à la réputation sont possibles en attaquant l'informatique de production. Viser les informatiques périmétriques permet de connaître le fonctionnement de l'entreprise et rend vulnérable tant ses infrastructures que ses employés. Cibler le *cloud* permet non seulement de récupérer des informations confidentielles mais peut aussi arrêter des fonctions essentielles à l'entreprise en la privant des données indispensables à leur réalisation. Enfin, viser les télé-opérations peut avoir sensiblement les mêmes conséquences que de viser l'informatique de production.

IV Anticiper l'attaque

Il est donc indispensable d'anticiper l'attaque. Pour cela, plusieurs opérations s'avèrent indispensables.

Tout d'abord, et même si cela peut paraître une évidence, il faut connaître le milieu dans lequel l'entreprise évolue. Cela signifie connaître son entreprise, les compétences dont elle dispose, l'état de son système de défense et ses mécanismes de réaction, mais également son environnement législatif et réglementaire, sans oublier l'environnement concurrentiel et hostile.

Il faut ensuite imaginer la crise en préparant son entreprise matériellement et humainement. Si pour le premier point des listes de contrôle peuvent être établies, il est indispensable de prêter une réelle attention à ses employés pour accomplir le deuxième. Le dialogue au sein de l'entreprise et l'établissement d'un climat de confiance sont des éléments indispensables à l'implication de tous les employés dans la sécurité de l'entreprise. Ces éléments sont nécessaires mais ne peuvent suffire, l'attaquant ayant toujours l'initiative au moment de l'attaque.

Élément indispensable, la préparation reste vaine si l'entreprise ne se met pas en ordre de bataille. Pour cela il lui faut, à l'instar des armées, raisonner sur le temps, l'ennemi et le terrain. Plus la détection sera précoce et mieux l'entreprise sera protégée. Elle le sera d'autant plus qu'elle aura aménagé son paysage informatique (VLAN, *honeypots*, etc.) et se sera tenue au courant des manières d'opérer des attaquants. Cependant, dans la mesure où elle n'a pas nécessairement les moyens pour réagir seule, il lui sera indispensable de se constituer un réseau qu'elle pourra mobiliser en cas de coup dur. Il comportera des acteurs institutionnels et privés qui pourront soit l'appuyer soit la soutenir dans sa réaction défensive.

V Après l'attaque

La préparation, pour sérieuse qu'elle aura été, peut cependant ne pas suffire à repousser toutes les attaques. L'entreprise doit donc savoir également réagir une fois les agressions terminées.

Le retour en ordre de marche, logique et indispensable, ne saurait suffire et doit s'accompagner de précautions. La première est de distinguer si l'entreprise a été victime d'une attaque ou d'une négligence. Phase délicate, elle n'est pourtant pas totalement impossible. Des partenaires de confiance peuvent l'aider dans cette opération. L'entreprise attaquée peut également aider à limiter la propagation de ces attaques en en diffusant les éléments caractéristiques.

Par la suite, il est tout aussi logique qu'elle cherche à obtenir réparation. La voie de l'assurance, bien qu'encore confrontée à plusieurs difficultés est envisageable. Cependant, l'évaluation des risques est encore embryonnaire, et les dommages couverts ainsi que la fixation de la prime d'assurance ne suivent pas des grilles d'évaluation incontestables, ce qui fragilise l'évaluation des dommages causés et le paiement des indemnités. Une autre solution est de choisir la

voie judiciaire, qu'elle soit civile ou pénale. Chacune de ces voies a ses partisans, l'intérêt de la voie pénale étant d'obtenir la condamnation du coupable.

Pour initier la voie pénale, encore faut-il que les faits ayant porté préjudice à l'entreprise soient punissables. Le code pénal prévoit et réprime dans ses articles 323-1 à 323-3 les atteintes aux systèmes de traitement automatisés de données, mais d'autres incriminations sont possibles, selon les dommages avérés. Dans certains cas précisés par le code pénal, la tentative est également punissable.

Si les faits sont pénalement répréhensibles, alors la plainte est justifiée et permettra l'ouverture d'une enquête qui pourra être préliminaire, de flagrant délit ou sur commission rogatoire, selon l'appréciation du magistrat la dirigeant. Si la qualification pénale par l'entreprise n'est pas indispensable pour porter plainte, il est de son intérêt d'effectuer cette opération dans les meilleurs délais afin d'éviter la prescription des faits, c'est-à-dire qu'ils ne puissent légalement plus être poursuivis. Si l'entreprise décide de porter plainte, il sera de son intérêt de coopérer le plus étroitement possible avec les enquêteurs pour que l'auteur soit démasqué et condamné.

Conclusion

En conclusion, comme tous les acteurs ayant choisi d'être présents dans le cyberespace, cette présence de l'entreprise s'accompagne d'un questionnement sur son fonctionnement. A-t-elle pris en compte la métamorphose des menaces auxquelles elle était déjà confrontée, s'est-elle organisée en conséquence, s'est-elle dotée des moyens indispensables pour que cette présence dans le cyberespace ne se traduise pas par un fiasco phénoménal ?

Une grande partie de la réponse lui appartient, même si des partenariats sont envisageables et si les travaux visant à faire converger la sécurité et la sûreté l'aideront à améliorer sa sécurité.