Projet de communication pour le C&ESAR 2014

Réagir après l'attaque

Catégorie : générale

Auteur : Philippe Davadie, Gendarmerie Nationale, philippe.davadie@ensta.org
Proposition : 3 à 8 pages, v finale 8 à 16 pages.

Résumé

L'indispensable préparation des entreprises aux attaques informatiques pour sérieuse qu'elle soit, ne peut toutes les repousser. La réaction immédiate et à terme à une attaque doit donc être connue de l'entreprise, le simple retour en ordre de marche ne pouvant suffire.

L'entreprise doit d'abord différencier l'attaque de la négligence. Obtenir réparation, peut se faire par l'embryonnaire voie de l'assurance ou la voie judiciaire, qu'elle soit civile ou pénale. Chacune a ses partisans, l'intérêt de la voie pénale étant d'obtenir la condamnation du coupable.

La voie pénale n'est possible qu'en cas de faits prévus et réprimés par le Code pénal, la tentative étant parfois punissable. Le dépôt de plainte doit s'effectuer dans les meilleurs délais pour éviter la prescription. Enfin, une coopération étroite de l'entreprise avec les enquêteurs augmente les chances de réussite de l'enquête.

Mots-clés : attaque, négligence, infraction, tentative, Code pénal, plainte, prescription.

Malgré tous les efforts de protection informatique de l'entreprise, la probabilité d'attaque est importante. Comme les attaquants cherchent et exploitent les failles alors que de son côté, l'entreprise concentre ses ressources sur sa production et non sur la lutte informatique, ceux-là ont généralement un temps d'avance car celle-ci est davantage sur la défensive. La probabilité de succès d'une attaque est donc forte. Cela ne signifie pas que son anticipation est inutile. Elle demeure nécessaire en vue de réduire les dommages, mais n'empêchera pas tout passage à l'acte. L'entreprise doit donc envisager et anticiper le succès de l'attaque. Sa palette de réactions est large, sachant cependant que la légitime défense informatique ne tient pas juridiquement.

Une entreprise qui constate un dysfonctionnement de l'une de ses informatiques n'est pas pour autant victime d'une attaque. Ce peut être une négligence ou une erreur de manipulation de l'un de ses employés. Par commodité, le terme générique d'*incident* sera utilisé dans les lignes qui suivent pour englober tant l'attaque informatique que l'erreur ou la négligence.

Confrontée à un incident touchant l'une de ses informatiques, l'entreprise doit tout d'abord prendre des premières mesures, dites parfois d'urgence, qui doivent également lui permettre de trancher le dilemme attaque ou négligence. Du résultat de cette enquête dépendront les mesures à plus long terme qu'elle prendra, notamment le fait de porter plainte. Ces mesures doivent donc être prises en ayant le souci de préserver ses droits, car ce qui semblera une négligence peut être une attaque. Afin d'éviter la réitération de cet incident, elle devra aussi prendre les mesures nécessaires pour éviter la propagation de ce problème, tant à l'intérieur de l'entreprise qu'à l'extérieur.

Enfin, il lui sera utile d'obtenir réparation des dommages subis. Ceci peut s'effectuer en optant pour des assurances ou en choisissant la voie judiciaire civile ou pénale, cette dernière impliquant l'État, seul à disposer des pouvoirs d'enquête judiciaire et donc à identifier officiellement les coupables. De plus, impliqué dans la *guerre économique* aux côtés des entreprises, il est logique qu'il assume ses responsabilités en cas d'agression.

1 Réagir

Lorsqu'une entreprise a été victime d'un dysfonctionnement informatique, elle se demandera si elle a été victime d'une attaque ou si l'un de ses employés a commis une négligence ou une erreur. Ce distinguo peut être difficile à effectuer car, au premier abord, l'entreprise sera confrontée à une panne. Sa première réaction sera de vouloir remettre l'informatique en état de marche, ce qui peut nuire à la collecte des preuves.

Cette remise en marche a néanmoins des vertus, car elle permet d'avoir une première approche de la cause de la panne : informatique, mécanique (telle la défaillance d'un composant) voire inexpliquée. L'analyse de la panne et les mesures prises pour revenir à un état de marche normal sont des éléments importants pour connaître ce qui s'est vraiment passé.

1.1 Négligence ou attaque

Aborder le distinguo négligence ou attaque, pose la question de l'acte délinquant et de sa qualification pénale.

Trois éléments sont constitutifs d'une infraction : l'élément *légal* (la loi qui prévoit et réprime l'infraction), l'élément *matériel* (les actes exécutés par l'auteur) et l'élément *moral* (l'intention coupable ou la faute d'un auteur conscient de ses actes). Cependant, l'absence de l'un de ces éléments ne signifie pas nécessairement qu'il s'agit d'une négligence. Ce peut être une attaque qui, par la défaillance d'un seul élément constitutif, ne pourra être réprimée pénalement. Si l'élément légal et l'élément matériel semblent assez faciles à établir, il est plus malaisé d'établir l'intention coupable. Précisons que l'intention ne peut se confondre avec le mobile de l'acte, quand bien même ces notions sont parfois proches l'une de l'autre. Elle doit être coupable, c'est-à-dire malveillante.

En première approche, on pourrait dire qu'une intention est malveillante dès lors que l'acte est commis *en pleine conscience et de propos délibéré*. En d'autres termes, le jugement de

l'auteur ne devait pas être altéré ni sa volonté contrainte. Le prouver demeure ardu.

Toutefois, certains éléments peuvent disculper un employé de l'entreprise d'une intention malveillante, tels que sa méconnaissance du système d'information ou de la politique de sécurité de l'entreprise. En outre, le personnel de l'entreprise peut être amené à en utiliser les ressources à des fins personnelles, la fragilisant ainsi par la connexion de ses ressources à des sites non sécurisés ou à des réseaux sociaux pour lesquels les alertes de sécurité abondent. Ces défauts de sécurité permettent d'effectuer aisément une ingénierie sociale, donc une intrusion dans le SI.

Le manque de formation à l'utilisation des différents outils peut aussi occasionner des actes involontairement malveillants, c'est-à-dire des actes dont les résultats sont préjudiciables à l'entreprise, sans pour autant que son auteur soit animé d'une intention coupable. Dans le cas de l'informatique périmétrique[1], on se rend compte que sa gestion quotidienne est souvent confiée non pas à des informaticiens, mais plutôt à des spécialistes de la sécurité. Autre situation rencontrée, la sous-traitance de l'exploitation de cette informatique par une société tierce. Dans ces deux cas de figure, compter sur les exploitants du système pour administrer correctement le réseau sur lequel se trouvent les capteurs (caméras, lecteurs de badge, etc.), détecter des *bugs* ou déceler des alertes est illusoire.

N'oublions pas que le manque de vigilance des employés de l'entreprise envers le matériel qui leur est confié (badges, ordinateurs et téléphones portables, etc.) est également responsable d'atteintes involontaires envers l'entreprise. Il se traduit concrètement par des pertes ou des vols qui sont de formidables opportunités pour les attaquants de toute sorte. Le savoir-faire et le professionnalisme de voleurs chevronnés peuvent inciter la victime à déclarer plutôt une perte inexplicable qu'un vol dont elle n'a pas la moindre preuve.

Deux autres cas de figure particuliers méritent également d'être mentionnés lorsqu'on évoque le dilemme attaque/négligence. Il s'agit du cas de l'AVAP (Apportez Votre Appareil Personnel ou BYOD en anglais) et celui du contrôle des licences logicielles.

Le développement de l'AVAP est paradoxal car il tend à confondre domaine privé et domaine professionnel, à une époque où les écoutes généralisées font crier au scandale. L'interrogation plus critique de la compatibilité des politiques de sécurité informatique de l'entreprise et de celles adoptées par chacun de ses employés (quand ils en ont une) ne peut manquer d'être posée. Ce problème est d'autant plus aiguë que le parc informatique personnel peut être très hétérogène et changer fréquemment, contrairement aux pratiques de l'entreprise. Aborder l'AVAP sous l'angle de la sécurité de l'entreprise, *via* sa sécurité informatique, amène à se poser la question de sa pertinence. Puisqu'il est un souci supplémentaire pour les personnes chargées de sécuriser le système d'information de l'entreprise, est-il vraiment utile ? Le directeur de l'ANSSI a pris clairement position dans son discours de Monaco en 2012 : « *Dans une entreprise : non on ne travaille pas avec son terminal privé, non on ne connecte pas un terminal contrôlé par un tiers, non on n'installe pas le dernier joujou à la mode.* » L'apport de l'informatique personnelle au sein de l'entreprise doit donc être sérieusement pris en compte, car il fait courir le risque que l'entreprise passe du *bring you own device* au *bring your own disease*.

Le contrôle de licences logicielles doit aussi être évoqué. En 2010, la société Oracle a été condamnée par le tribunal d'Amsterdam dans le cadre d'une action en contrefaçon qu'elle avait intentée contre son client (Philips). Le tribunal a en effet estimé que la demande formulée par Oracle envers son client était trop vague, trop large et que durant la phase de collecte de données,

1 Par informatique périmétrique nous entendons 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 s'était livrée à une *« fishing expedition »*. Ce dernier cas est emblématique de la difficulté à discriminer une négligence d'une attaque. L'employé d'Oracle a argué du fait que pour contrôler le nombre d'utilisateurs des logiciels Oracle il avait involontairement récupéré des informations, ce qui s'apparente à un acte involontaire, mais le tribunal en a décidé autrement.

1.2 Réactions pratiques

Une fois que l'entreprise a constaté l'incident, elle doit réagir au plus vite et de manière appropriée. Une première réaction est de procéder à la recherche des causes de l'incident et à leur analyse. Pour cela, il est possible de faire appel à des partenaires de confiance (SSII notamment) dans le cas où l'entreprise ne disposerait pas des compétences internes suffisantes. L'article 15 du décret 2010-112 du 02 février 2010 prévoit qu'un organisme habilité par l'ANSSI délivre à certains prestataires une *qualification qui atteste de la conformité des services à un niveau de sécurité défini par le référentiel général de sécurité*. Bien que ne visant que les échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, ce décret est intéressant car il permet de connaître les prestataires ainsi qualifiés. Cependant, si l'entreprise pense avoir été l'objet d'une attaque, il est conseillé que ces opérations techniques (mesures prises et résultats) soient authentifiées par un huissier, afin de ne pas être contestées lors de leur production devant un tribunal.

Les premières opérations ont pour but de circonscrire le périmètre de l'intervention. À ces opérations peuvent se superposer celles qui permettent de déterminer l'enchaînement des faits qui ont conduit à la *panne*. Celui-ci une fois identifié, il est souhaitable de réunir l'ensemble des protagonistes de l'incident pour procéder à son analyse à froid, afin de mieux comprendre le processus qui a mené à l'incident et l'incident lui-même pour y ajuster les réponses de l'entreprise. Il est souhaitable que cette réunion soit animée par un *bureau de la confiance*, sous forme de table ronde ou de rencontres séparées afin que chacun puisse livrer son ressenti et se livrer sans crainte de représailles. Elle peut aussi être confiée à un tiers de confiance. À chaque fois, un panel d'experts doit pouvoir déterminer si l'un ou de l'autre cherchant à se disculper ne tente pas de les égarer.

Ces entretiens terminés, il faudra rédiger des recommandations pertinentes car fondées sur les déclarations des protagonistes de l'affaire. Tout d'abord soumises aux responsables de la sécurité, elles pourront être diffusées à toutes les personnes concernées par la réitération d'un tel incident. En sachant ce qui s'est passé, les employés seront ainsi davantage impliqués dans la sécurité et donc la pérennité de leur outil de travail que si la direction leur diffusait de manière abrupte et sans aucune explication une liste de nouvelles mesures à prendre.

1.3 Éviter la propagation

Remettre l'informatique en ordre de marche et éviter la réitération de l'incident par la diffusion des éléments *supra* ne suffit pas. Ne pas diffuser ces éléments à l'extérieur de l'entreprise laisse l'avantage à l'attaquant. En maintenant ainsi le secret du mode opératoire on lui laisse l'initiative, car il conserve la possibilité de réitérer cette attaque sur une autre cible tout en sachant que diffuser largement le mode opératoire revient à prévenir l'attaquant qu'il a été en partie détecté. Partager ce mode opératoire avec des partenaires de confiance est judicieux. En agissant ainsi, l'entreprise met en garde les cibles potentielles des réitérations de ce type d'attaque, charge à elles de s'en prémunir. Cette alerte peut être diffusée aux partenaires de l'entreprise, aux chambres de commerce et d'industrie (CCI), aux CERT (Computer Emergency Response Team) ou CSIRT (Computer Security Incident Response Team) qui sont des centres d'alerte et de réaction aux attaques informatiques, destinés aux entreprises ou aux administrations mais dont les informations sont généralement accessibles à tous, ainsi qu'à l'ANSSI. En collectant les types d'attaques menées, celle-ci sera en mesure d'effectuer les rapprochements pertinents et de diffuser les alertes nécessaires. Notons qu'il est possible d'alerter l'ANSSI en passant par l'OZSSI (Observatoire Zonal

de la SSI) local, qui est le relais territorial de l'Agence mis en place en priorité pour tous ceux qui ne bénéficient pas du soutien d'une chaîne fonctionnelle SSI. Alerter également les forces de sécurité est utile car elles ont également un rôle de prévention et de conseil. Cela s'avère indispensable lorsque l'attaque est avérée et que l'entreprise décide de porter plainte.

Évoquer la plainte amène tout naturellement à se poser la question des modalités de réparation des dommages subis par l'entreprise.

2 Obtenir réparation

Une fois l'incident réglé, l'entreprise doit définir sa ligne de conduite. Estime-t-elle que cela fait partie des mauvais moments qui peuvent arriver ou qu'une réparation lui est due ? Dans ce dernier cas, deux possibilités s'offrent à elle : la voie de l'assurance et celle de l'action judiciaire.

2.1 La voie de l'assurance

Choisir la voie de l'indemnisation par l'assurance est une possibilité de plus en plus débattue. Champ nouveau pour la profession en France, l'assurance de l'informatique soulève plusieurs problèmes qui ne sont pas encore résolus. Si son rôle dans l'indemnisation est important, l'assureur n'est pas qu'un simple payeur. Il doit également évaluer les risques, prodiguer des conseils de sécurité, estimer le montant des dégâts envisageable afin de fixer la prime d'assurance. L'indemnisation ne vient qu'en fin de processus, une fois que le dommage a été constaté.

L'offre actuelle des assureurs ne couvre pas encore toutes les conséquences d'un cyber-incident. Actuellement, des compagnies d'assurance testent des contrats visant à rétablir la cyber-réputation (généralement d'une personne privée), mais aucune ne se risque sur le terrain de l'assurance contre les attaques informatiques visant une entreprise. C'est un terrain à explorer, mais il n'est pas certain que les offres que proposeront les assureurs correspondent vraiment à la demande des entreprises.

L'évaluation des risques

L'évaluation des risques est la première question à soulever. Comment un assureur, nouveau sur ce type de marché puisque la démarche vient à peine de débuter, peut-il sérieusement évaluer les risques d'attaque informatique contre une entreprise ? Les moyens nécessaires pour accomplir cette mission sont importants et ne peuvent être déployés par tous les cabinets d'assurance au profit de toutes les entreprises. Seules les grandes entreprises pourront s'offrir une telle évaluation, car les PME estimeront vraisemblablement que le coût de l'évaluation est supérieur au montant de la prime d'assurance.

Encore faut-il que les entreprises sachent elles-mêmes les risques auxquels elles s'exposent suite à une cyber attaque. Arrêt ou retard de la production, dégradation de sa qualité, accidents du travail causés par le dysfonctionnement d'un robot informatisé, la palette de risques est étendue. Il y a fort à parier qu'aucun assureur n'acceptera de couvrir tous ces risques. Il reviendra alors à l'entreprise de parier sur les plus probables et les plus handicapants ou destructeurs.

Les conseils, les dommages couverts et la fixation de la prime

De la même manière, quels experts prodigueront des conseils de sécurité auprès des entreprises cherchant à s'assurer ? Sur quels documents se baseront-ils ? Il est fort probable que, dans un premier temps, ils utiliseront les guides pratiques et techniques publiés par l'ANSSI ou le CERT-FR. Cependant, ces éléments purement techniques et essentiellement préventifs, s'ils sont indispensables à la sécurisation de l'entreprise, ne peuvent suffire à la mettre hors de portée de toute attaque. De plus, aucun expert ni cabinet de conseil en SSI ne s'engagera sur une efficacité totale de ses logiciels, produits ou recommandations. Il est donc fort probable que les assureurs proposeront des contrats basés sur des auto évaluations de risque, avec tous les risques de refus de paiement dus aux fausses déclarations que ce système comporte. Si l'on considère cette étape résolue, il reste alors

à fixer les dommages couverts et le montant de la prime d'assurance. La difficulté réside dans le fait qu'une attaque informatique se caractérise également par l'ambiguïté du dommage.

De plus, l'absence de définition par l'entreprise des risques qu'elle encourt (cf. *supra*) nuit à une fixation réaliste des dommages couverts et de la prime d'assurance.

L'évaluation des dommages et le paiement des indemnités

Une fois l'attaque ou la malveillance survenue, l'assureur devra estimer le montant des dommages. L'exercice peut s'avérer difficile, car sera-t-il certain que l'attaque est terminée ? Que se passera-t-il si l'attaquant a prévu une attaque en plusieurs phases avec un délai d'attente entre chacune d'elles ? Une autre question est celle du cas où une attaque vise plusieurs entreprises simultanément. Le risque systémique, à savoir qu'une attaque vise des SI du même type ou un *cloud* hébergeant des clients d'un même assureur est estimé important par plusieurs entreprises. Se pose alors la question de la solidité de l'assureur, à savoir sa capacité à dédommager ses clients. Cette difficulté peut donc amener les assureurs à ne pas démarcher tous leurs clients potentiels.

Les questions en suspens

Dans des domaines très techniques comme le transport ferroviaire (mais ce n'est pas le seul), les experts judiciaires sont d'anciens employés des sociétés de chemin de fer. Quelle que soit leur probité personnelle, un doute quant à leur partialité ne peut jamais être absent surtout lorsqu'un litige apparaît entre l'assuré et l'assureur. Comment les éventuels conflits d'intérêts seront évités dans le monde de l'assurance informatique ?

De plus, l'ambiguïté caractérise l'attaque informatique. Comment l'expert de l'assureur étaiera-t-il ses dires pour accorder ou refuser l'indemnisation ?

2.2 La voie judiciaire

Choisir la voie de l'assurance n'interdit pas de choisir la voie judiciaire pour obtenir réparation. Dans ce cas, deux possibilités s'ouvrent à l'entreprise : l'action au civil ou au pénal, étant entendu qu'elles ne sont pas exclusives l'une de l'autre. Cependant, la décision du juge civil ne peut être prononcée avant la décision pénale, sauf lorsqu'une action civile est engagée en réparation du préjudice direct résultant de l'infraction pour laquelle le juge pénal est saisi. Le choix reste libre, sachant que selon l'article 5 du Code civil, une fois la voie civile choisie, il n'est plus possible de porter l'affaire au pénal. La question de la voie à choisir est donc fondamentale pour l'entreprise, car si elle opte pour le civil, le retour en arrière n'est plus possible.

La voie civile peut être privilégiée lorsque la victime souhaite obtenir uniquement réparation d'un préjudice qu'elle a subi. Les contentieux civils ont pour objet des rapports d'obligation entre personnes, quelle que soit la nature de ces rapports : privés, commerciaux, contractuels, etc.

Initier la procédure civile

Pour initier une procédure civile, il faut que la partie s'estimant lésée ait un intérêt légitime à agir, donc qu'elle puisse arguer que la partie qu'elle attaque a lésé un de ses intérêts.

L'objet du litige

L'objet du litige est ce que revendiquent les parties en présence (dommages et intérêts, droit d'auteur, etc.) et ne peut être modifié arbitrairement en cours de procédure.

Prouver les faits

La partie lésée doit prouver l'existence du préjudice qu'elle avance. Pour cela, conformément à l'article 132 du Code de procédure civile, elle doit fournir des preuves, tant au tribunal qu'à la partie adverse, la fourniture de la preuve étant libre.

Solution du litige

Le litige peut être réglé de différentes manières. Par la voie amiable (transaction, conciliation, médiation) si les parties s'accordent ou par la voie contentieuse en cas de désaccord.

3 Est-ce punissable ?

Une fois que l'entreprise a déterminé, ou au moins obtenu un bon aperçu de ce qui peut être considéré comme l'élément moral de l'infraction, et dans le cas où la négligence est écartée, il est indispensable de savoir si cette attaque ou tentative d'attaque est pénalement répréhensible.

3.1 Le bruit de fond des attaques informatiques

L'augmentation des attaques a conduit à la création de ce qui peut être appelé *bruit de fond* des attaques informatiques : ce sont des attaques de faible intensité lancées régulièrement et sans cible précise, avec des moyens peu performants au vu de l'état de l'art, mais qui réussissent si les cibles visées s'avèrent négligentes dans la mise en œuvre de mesures de sécurité élémentaires. Distinguer les vraies attaques du bruit de fond peut s'avérer ardu. Le succès de ces tentatives est le plus souvent limité, voire inexistant, car pour être automatisées, elles utilisent des méthodes connues. Cependant, elles saturent les défenses de l'entreprise et dispersent l'attention des personnes chargées de la protéger. L'attaquant peut aussi tenter de dissimuler son attaque dans le bruit de fond de celles qui l'entourent afin de rester caché. Il est néanmoins possible de discriminer une véritable attaque du bruit de fond en définissant une activité moyenne de l'entreprise, voire d'un employé-type. Cette définition et sa caractérisation (volume moyen de données échangées, horaires d'activité, etc.) permet d'automatiser les recherches et d'être alerté selon des critères définis.

3.2 Quelles infractions sont punissables ?

La discrimination malveillance / attaque effectuée et l'attaque s'avérant distincte du bruit de fond, il convient de qualifier l'atteinte subie par l'entreprise afin de savoir si elle est prévue et réprimée par un article du Code pénal donc pénalement répréhensible.

Les attaques informatiques contre l'entreprise sont évoquées dans les livres II et III du Code pénal, à savoir les *crimes et délits contre les personnes* (livre II) et les *crimes et délits contre les biens* (livre III).

Les atteintes aux personnes

Le Code pénal prévoit la *protection de l'image individuelle* (article 226-1), réprime l'usage de l'identité d'un tiers *en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération (*article 226-4-1) et protège les correspondances par voie électronique (article 226-15).

L'entreprise a des obligations similaires, notamment lorsqu'elle met en œuvre des traitements de données à caractère personnel. Elle doit respecter les prescriptions de la loi informatique et liberté (226-16 et 17), ne peut collecter des données personnelles par des moyens frauduleux illicites ou déloyaux (226-18) ou lorsque la personne s'y oppose (226-19), ni les conserver au-delà du délai légal (226-20), ni les détourner des fins pour lesquelles elles ont été collectées (226-21) ni encore les divulguer (226-22).

Les atteintes aux biens

Les atteintes aux biens peuvent être lourdes de conséquences, certaines étant mentionnées dans le livre III du Code pénal. L'accès ou le maintien frauduleux dans un système de traitement automatisé de données, quand bien même celles-ci ne sont ni modifiées ni supprimées, l'entrave à son fonctionnement, l'introduction frauduleuse de données dans ce système, la suppression et la modification des données qu'il contient, sont réprimées par le Code pénal.

La protection du système d'information de l'entreprise et de ses composants est effective grâce à ces articles. Cependant, par l'article 323-3-1, le Code pénal la dissuade d'agir d'une manière que certains n'hésitent pas à qualifier, abusivement, de légitime défense.

3.3 La tentative est-elle également punissable ?

Il peut arriver que l'entreprise parvienne à déjouer l'attaque prévue. Mais dans certains

cas, la tentative est punissable, ce qui autorise l'entreprise à porter plainte.

La tentative, définie par l'article 121-5 du Code pénal, est une infraction manquée, contre la volonté de son auteur. Dès lors qu'il y a tentative, son auteur est considéré comme auteur de l'infraction et passible des mêmes sanctions que l'auteur d'une infraction commise. Encore faut-il que la tentative soit considérée comme punissable, ce qui n'est pas le cas par défaut. Pour les délits que nous venons d'évoquer, le Code pénal prévoit formellement la punition de leur tentative.

3.4 L'indispensable sécurisation préalable

Au vu des articles du Code pénal, l'entreprise peut s'estimer suffisamment protégée par la loi. Cependant, les récentes jurisprudences posent comme condition préalable à son indemnisation en cas d'attaque une indispensable sécurisation du système d'information de l'entreprise. Tel est le sens de la décision du TGI de Créteil en date du 23 avril 2013 qui a relaxé une personne accusée de s'être introduite frauduleusement dans un système de traitement automatisé de données, de s'y être maintenue et d'y avoir soustrait des données.

4 La plainte

Une fois que l'entreprise est persuadée que les faits (ou tentatives) dont elle a été victime sont prévus et réprimés par le Code pénal, elle peut décider de porter plainte pour que l'auteur des faits soit puni puis obtenir réparation des dommages subis.

4.1 L'intérêt de la plainte

Cependant, elle peut estimer qu'il est trop risqué de porter plainte, notamment au vu du contexte dans lequel elle évolue. La plainte révèle des faiblesses ou des défaillances dans la sécurité de l'entreprise, ce qui nuit à son image de marque surtout si les faits viennent à être rendus publics.

Il est donc logique que l'entreprise soit réticente à porter plainte. Les fuites d'information ne sont cependant pas systématiques, et se focaliser sur elles aurait pour conséquence de tétaniser les entreprises qui n'oseraient alors plus jamais porter plainte. Un tel comportement encouragerait *ipso facto* les attaquants, en leur donnant le sentiment qu'ils bénéficient d'une impunité quasiment permanente. L'intérêt de l'entreprise est donc de mener une véritable analyse de risque à long terme avant d'aller ou non porter plainte. Cette analyse de risque doit cependant être rapide pour des questions de délai que nous détaillerons *infra*.

4.2 Contre qui porter plainte ?

Une fois la décision de porter plainte prise, se pose la question de savoir qui viser dans la plainte. Elle peut viser soit une personne identifiée, soit ne viser personne. En tout état de cause, l'absence d'auteur identifié ne doit pas faire obstacle au dépôt de plainte.

La personne visée par la plainte n'est pas obligatoirement l'auteur de l'infraction. Si le cas idéal est de pouvoir l'identifier puis de la dénoncer formellement, cela ne correspond pas toujours à la réalité et l'entreprise peut n'avoir identifié que des « seconds couteaux. » Cette absence d'identification n'est pas grave, car c'est aux enquêteurs qu'il appartiendra d'établir formellement les faits et d'identifier les auteurs, puis aux magistrats de déterminer les responsabilités de chacun.

Il convient cependant d'agir avec prudence lorsqu'on vise une personne précise dans une plainte, car dans le cas où l'absence d'éléments viendrait infirmer les accusations portées, la personne visée pourrait alors s'estimer victime d'une dénonciation calomnieuse et porter plainte à son tour sur le fondement de l'article 226-10 du Code pénal.

4.3 Quels faits viser dans la plainte ?

Il est nécessaire que l'entreprise explique, au moins succinctement, dans quelle mesure un attaquant, identifié ou à identifier, lui a porté préjudice. Il faut aussi que les faits dénoncés soient

pénalement répréhensibles car, dans le cas contraire, la plainte sera sans effet. Elle peut donc viser une attaque délibérée pour laquelle elle dispose de preuves ou d'éléments de preuve mais aussi, si les conséquences de l'acte reproché ont eu pour conséquence le décès ou l'incapacité temporaire de travail d'un employé viser une faute *d'imprudence, de négligence ou de manquement à une obligation de sécurité* telle que le prévoit l'article 121-3 du Code pénal.

Nous l'avons vu précédemment, dans certaines conditions, la tentative est punissable. Tel est le cas pour les intrusions, altérations, modifications, etc. dans des systèmes de traitement automatisés de données que nous avons évoquées *supra*. L'entreprise est alors fondée à porter plainte pour ces tentatives de commission d'infractions.

Un autre point à prendre en compte est qu'il n'est nullement besoin d'estimer un préjudice, avéré ou potentiel, pour aller porter plainte. L'infraction peut être constituée sans même qu'il y ait préjudice comme c'est le cas des faits prévus et réprimés par l'article 323-1 du Code pénal.

4.4 Les délais pour porter plainte

Une fois l'attaque constatée, il est nécessaire de porter rapidement plainte pour deux raisons principales. La première est que la rapidité du dépôt de plainte permet de sauvegarder les traces et logs. Elle est aussi de mise pour éviter la prescription de l'action publique. Les infractions citées constituent des délits prescrits au bout de trois ans après leur date de commission, ce qui signifie que trois ans après la date de commission de l'infraction, la victime ne peut plus porter plainte. Cette situation peut paraître paradoxale, car une des caractéristiques maintes fois évoquée du cyber espace est son ambiguïté. Comment peut-on connaître avec certitude la date de commission d'une infraction dans un espace où l'ambiguïté règne ?

4.5 Les précautions

Pour que la plainte soit recevable et produise son effet, il faut que les faits ne soient pas prescrits et que l'affaire n'ait pas été déjà jugée. Il faut aussi que l'entreprise ne soit pas complice des faits qu'elle reproche à son agresseur. Elle ne doit pas non plus avoir incité l'un de ses employés à commettre la faute pénalement répréhensible visée par la plainte, et il lui est conseillé de s'abstenir de tenter de résoudre d'abord l'enquête par elle-même.

4.6 Les protagonistes de la plainte

Dans les cas où le préjudice vise l'entreprise en général, c'est à elle de porter plainte par le biais d'un de ses employés qu'elle aura dûment mandaté. Cependant, dans les cas où l'intimité de la vie d'autrui est l'objet d'une attaque, c'est à *« la victime, [...] son représentant légal ou [...] ses ayants droit »* de porter plainte en application de l'article 226-6 du même code.

La plainte peut être déposée de différentes manières, sans qu'il y ait de hiérarchie entre elles ou de gage de plus grande efficacité de l'une ou de l'autre. Elle peut tout d'abord être déposée dans toute brigade de gendarmerie ou commissariat de police. Il va de soi que l'entretien de bonnes relations entre les enquêteurs et l'entreprise est un gage de rapidité de la réception de la plainte et de sa qualité. Si l'entreprise choisit cette solution, il faut qu'elle garde en tête le fait que la personne à laquelle elle s'adressera sera très vraisemblablement un généraliste, qui plus est peu au fait de l'activité de l'entreprise. Le risque existe qu'en donnant moult détails techniques, l'enquêteur décroche et qu'un dialogue de sourds s'instaure.

Elle peut aussi être exposée dans une lettre adressée au procureur de la République. Le plaignant est tenu au courant des suites données à sa plainte, quelles qu'elles soient. L'éventuelle décision de classement sans suite peut être contestée par le plaignant qui peut former un recours devant le procureur général de la cour d'appel dont dépend le procureur de la République en question. Là aussi, le plaignant ne doit pas perdre de vue le fait que le magistrat qui ouvrira sa lettre ne sera pas nécessairement un spécialiste de l'informatique ni même de l'entreprise, et que si elle

doit décrire précisément les faits, il ne faut pas les surcharger de détails techniques, pertinents pour le rédacteur, mais obscurs ou déstabilisants pour le lecteur.

Enfin, il est également possible de porter plainte en se constituant partie civile par l'envoi d'une lettre au juge d'instruction. Les mêmes précautions que celles exposées ci-dessus sont à respecter en ce qui concerne l'aspect technique de la lettre.

Afin de faciliter ces démarches et d'éviter qu'un élément soit omis lors de la préparation de la plainte, un *guide pratique du dépôt de plainte* est disponible sur le site internet http://www.informatiques-orphelines.fr

Dans la mesure où nous avons parlé de l'analyse de risque à laquelle devait se livrer l'entreprise avant de porter plainte, il convient d'aborder de nouveau la question de la confidentialité de cette plainte.

Même si le Code de procédure pénale prévoit que l'instruction est secrète (article 11), aucun mode de dépôt de plainte ne garantit une confidentialité totale de l'affaire, l'actualité l'illustre abondamment. Par conséquent, cette question doit être exposée clairement aux enquêteurs ou aux magistrats, en leur expliquant en quoi la publicité de l'affaire serait nuisible à l'entreprise, afin que les mesures de préservation du secret soient les plus efficaces possible.

Bibliographie