Protection des infrastructures informatiques des entreprises face à la cybercriminalité

Vincent Lemoine[1], Charles Perez[2], Marc Lemercier[2], Pierre Vitard[3],
Virginie Bensoussan-Brulé[4], Alain Corpel[2], Rida Khatoun[2], Babiga Birregah[2]

[1]Gendarmerie Nationale et Université Paris-Sud - CERDI, 54 boulevard Desgranges, 92 331 Sceaux cedex

[2]ICD et UMR STMR, Université de Technologie de Troyes, 12 Rue Marie Curie, CS 42060, 10 004 Troyes Cedex

[3]ADIT (Agence pour la Diffusion de l'Information Technologique), 40 rue Buirette, 51 100 Reims

[4]Cabinet d'avocats Alain Bensoussan, 29 rue du Colonel Pierre Avia, 75 015 Paris

vincent_lemoine@orange.fr, charles.perez@utt.fr, marc.lemercier@utt.fr,
pv@adit.fr, virginie-bensoussan-brule@alain-bensoussan.com,
alain.corpel@utt.fr, rida.khatoun@utt.fr, babiga.birregah@utt.fr

Abstract – Les nouvelles technologies (Internet, terminaux nomades) révolutionnent jour après jour le fonctionnement des entreprises qu'ils s'agissent de la sphère commerciale, de la gestion de projets ou des mécanismes d'échanges d'information en général. Les entreprises doivent revoir leur stratégie digitale et leur système d'information pour intégrer ces nouveaux canaux de communication et de vente (logique crosscanal) symbole actuel de modernité et d'efficacité économique. Aujourd'hui, les nouvelles préoccupations stratégiques pour les entreprises sont maintenant leur référencement et leur réputation sur Internet, le Search Engine Marketing (SEM), le marketing viral et la relation client via Internet **(**eCRM / Electronic Consumer Relationship Management**)**. Les business models doivent désormais évoluer pour tenir compte non seulement des réseaux sociaux numériques (Facebook, LinkedIn, Twitter, etc.) mais aussi des dispositifs nomades interconnectés via le cloud (smartphones, tablettes). Cette mutation rapide a conduit les entreprises à s'exposer de plus en plus, rendant parfois accessibles aux plus grand nombre leurs infrastructures informatiques et permettant en même temps l'accès à des données stratégiques d'entreprises. Celles-ci sont de plus en plus la cible d'attaques informatiques (cybercriminalité) dont les principaux objectifs sont le vol de données à caractère personnel ou professionnel, les malveillances (dysfonctionnement de systèmes ou logiciels, atteinte à la réputation ou bris de carrière) et plus globalement la désorganisation de l'entreprise visée. Les entreprises doivent intégrer le concept de sécurité globale permettant d'assurer un niveau suffisant de prévention et de protection contre la cybercriminalité en prenant en compte leurs obligations règlementaires et juridiques. Nous présentons dans cet article les différentes approches étudiées dans le cadre du projet CyNIC[1] pour faire face à ces nouvelles menaces.

[1]CyNIC (*Cybercriminalité, Nomadisme et Intelligence éConomique*) est un projet CPER soutenu par la région Champagne-Ardenne, l'état français et le FEDER.

1. Introduction

Le monde actuel est de plus en plus complexe et difficile à appréhender, que ce soit au niveau des relations internationales, des relations entre individus ou des relations entre les acteurs économiques. La notion d'incertitude n'a jamais été aussi actuelle. Dans la sphère économique, les logiques partenariales disparaissent au profit de relations centrées sur l'intérêt unique d'une entreprise au détriment d'une autre. La mondialisation des échanges et des moyens de communication a permis aux entreprises d'entrer en relation les unes avec les autres quelle que soit leur implantation géographique.

Parallèlement à ce phénomène, l'accès à l'information numérique est de plus en plus aisé grâce à la multiplication des terminaux d'accès (ordinateurs, smartphones, tablettes) et la baisse continue des coûts de communication (forfait téléphone, forfait Internet). De cette manière, les recherches usuelles via les moteurs de recherche sont pratiquement gratuites et peuvent être automatisées. Les outils en ligne sont également de plus en plus nombreux : moteurs et méta moteurs de recherche génériques, moteurs de recherches spécifiques (de personne, de société, etc), bases de données, annuaires, etc. Le concept d'open data permet en plus un point d'accès pour la consultation de données publiques (http://www.data.gouv.fr/).

Les acteurs malveillants disposent de moyens de plus en plus importants pour identifier, sélectionner et traquer des citoyens ou des entreprises. Il n'existe pas de définition de la cybercriminalité dans le Code pénal, mais le ministère de l'Intérieur [1] définit la cybercriminalité comme « *l'ensemble des infractions pénales commises sur le réseau Internet* ». Nous pouvons citer à titre d'exemples certaines escroqueries (fraude à la carte bancaire, vente en ligne avec encaissement sans livraison de la marchandise), la contrefaçon, la vente de produits illicites, le recel de biens volés, l'usurpation d'identité, le vol de données, la diffusion d'images pédopornographiques, l'incitation au suicide ou à la haine raciale, les injures, etc. Cependant, il existe de nombreuses autres définitions de la cybercriminalité. La Convention de Budapest sur la cybercriminalité [2] l'a définie de la sorte « *ensemble des infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques* ». On peut synthétiser ces définitions par l'ensemble des infractions commises par l'intermédiaire ou dont la finalité sont les nouvelles technologies notamment les réseaux ou les équipements électroniques. La suite de l'article est organisée comme suit : la section 2 rappelle les risques juridiques, la section 3 présente la gestion des incidents, la section 4 se focalise sur l'anticipation et la prévention en présentant quelques solutions de protection des infrastructures informatiques des entreprises.

2. Risques juridiques

Les particuliers et les entreprises sont soumis à de nombreuses réglementations qu'il est important de rappeler dans le cadre de notre étude. Ce cadre juridique constitue un premier niveau de sécurité pour les entreprises mais aussi un recours en cas de dommage.

2.1 Responsabilité des particuliers

2.1.1 Abus de confiance

L'abus de confiance définit par l'article 314-1 du Code pénal est le fait par une personne de détourner, au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a accepté à charge de les rendre, de les représenter ou d'en faire un usage déterminé. L'abus de confiance est puni de trois ans d'emprisonnement et de 375.000 euros d'amende. Cet article est généralement utilisé dans le cas de détournements de l'usage des données dans une entreprise.

2.1.2 Violation du secret de fabrication

Le fait pour un directeur ou un salarié de révéler ou de tenter de révéler un secret de fabrication est puni d'un emprisonnement de deux ans et d'une amende de 30.000 euros (article 1227-1 du Code du travail). Le juge peut également prononcer, à titre de peine complémentaire, pour une durée de cinq ans au plus, l'interdiction des droits civiques, civils et de famille prévue par l'article 131-26 du Code pénal.

2.1.3 Compromission

L'article 434-10 du Code pénal précise qu'est puni de sept ans d'emprisonnement et de 100.000 euros d'amende le fait, par toute personne dépositaire d'un procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier qui a un caractère de secret de la défense nationale, soit de le détruire, détourner, soustraire ou de le reproduire, soit d'en donner l'accès à une personne non qualifiée ou de le porter à la connaissance du public ou d'une personne non qualifiée.

Est puni des mêmes peines le fait, par la personne dépositaire, d'avoir laissé accéder à, détruire, détourner, soustraire, reproduire ou divulguer le procédé, objet, document, information, réseau informatique, donnée informatisée ou fichier visé à l'alinéa précédent.

Lorsque la personne dépositaire a agi par imprudence ou négligence, l'infraction est punie de trois ans d'emprisonnement et de 45.000 euros d'amende. Cet article concerne les documents classifiés.

2.1.4 Espionnage, intelligence avec une puissance étrangère

Le fait de livrer ou de rendre accessibles à une puissance étrangère, à une entreprise ou une organisation étrangère ou sous contrôle étranger ou à leurs agents des renseignements, procédés, objets, documents, données informatisées ou fichiers dont l'exploitation, la divulgation ou la réunion est de nature à porter atteinte aux intérêts

fondamentaux de la nation est puni de quinze ans de détention criminelle et de 225.000 euros d'amende.

2.2 Responsabilités des entreprises

2.2.1 Manquement à la sécurisation des données

Le manquement à la sécurisation des données est réprimé par l'article 226-17 du Code pénal. Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée est puni de cinq ans d'emprisonnement et de 300.000 euros d'amende. L'article 34 précise que le responsable de traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

2.2.2 Divulgation illicite de certaines données personnelles

La divulgation illicite de certaines données personnelles est réprimée par l'article 226-22 du Code pénal. Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir.

2.2.3 Violation du secret professionnel

La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15.000 euros d'amende par l'article 226-13 Code pénal.

2.2.4 Complicité par assistance ou fourniture de moyen

L'article 121-7 du Code pénal précise qu'est complice d'un crime ou d'un délit, la personne qui sciemment par aide ou assistance en a facilité la préparation et la consommation.

2.3 Textes et réglementations liées à la cybercriminalité

Les atteintes à un système de traitement automatisé de données, par quelque moyen que ce soit, sont sanctionnées par les articles 323-1 et suivants du Code pénal.

L'expression « *tout ou partie d'un système de traitement automatisé de données* », non définie par la loi du 5 janvier 1988 relative à la fraude informatique [3] désigne l'ensemble des éléments physiques et des programmes utilisés pour le traitement de données, ainsi que ceux qui permettent d'établir la communication entre les différents éléments d'un système et donc, non seulement les ordinateurs et les périphériques d'entrée-sortie, mais également les terminaux d'accès à distance et, d'une manière générale, tous vecteurs de transmission de données.

Le délit d'accès frauduleux dans un système de traitement automatisé de données est prévu et réprimé par l'article 323-1 du Code pénal aux termes duquel « *le fait d'accéder (...), frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30.000 euros d'amende* ».

La protection du système par un dispositif de sécurité n'est pas une condition de l'incrimination : il suffit que le maître du système ait manifesté son intention d'en restreindre l'accès aux seules personnes autorisées.

Le délit de maintien frauduleux dans un système de traitement automatisé de données est prévu et réprimé par l'article 323-1 du Code pénal aux termes duquel « *le fait (...) de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30.000 euros d'amende* ».

Le délit d'atteinte volontaire au fonctionnement d'un système de traitement automatisé de données est prévu et réprimé par l'article 323-2 du Code pénal aux termes duquel « *le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75.000 euros d'amende* ».

Le délit d'introduction frauduleuse de données est prévu et réprimé par l'article 323-3 du Code pénal aux termes duquel « *le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75.000 euros d'amende* ».

L'article 323-3-1 du Code pénal incrimine « *le fait, sans motif légitime, (...) de détenir (...) un programme informatique (...) conçu ou spécialement adapté pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 du Code pénal* ».

Le délit d'association de malfaiteurs informatiques est prévu et réprimé à l'article 323-4 du Code pénal selon lequel « *la participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3-1 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* ».

La présentation de ces textes prouve la solidité juridique de notre pays pour lutter contre les atteintes à un système de traitement automatisé de donnée, mais également contre l'ensemble des atteintes aux fichiers de part la Loi informatique et liberté (loi de 1978 modifiée en 2004). Les

obligations et incriminations s'appuyant sur cette loi sont de plus en plus présentes au sein des entreprises de part l'évolution des technologies. Ces dispositions vont être renforcées par l'obligation de déclarer les pertes et fuites de données en vertu d'une directive européenne.

Ces outils constituent des recours en cas d'atteinte mais ne constituent pas une barrière physique face aux attaques des cybercriminels qui trouvent des solutions de plus en plus innovantes pour cacher leur identité. Il est à déplorer que les services de sécurité intérieur ne dispose pas de tous les instruments pour mener à bien leur mission. En effet, si l'Union Européenne a consacré depuis des années la libre circulation des biens et des personnes, les données transitent entre pays sans possibilité d'être appréhendées facilement. De plus, tous les pays de l'Union n'ont pas encore ratifiés la convention cybercriminalité de Budapest. En outre, aucun pays de l'Afrique ne l'a ratifiée alors que nous constatons une expansion de certains types de faits (harcèlement, racket, etc) en provenance de ce continent. De plus, le caractère international intrinsèques aux systèmes informatiques sublimé par le Cloud, doit faire face au caractère national de la justice ce qui constitue une marge souple qui peut servir de rempart à un acteur malveillant.

Apres avoir évoqué les aspects juridiques, il convient d'évoquer les aspects de la gestion des incidents de sécurité qui permettront à une entreprise de réagir correctement face aux menaces liées a la cybercriminalité. En effet, si les entreprises maîtrisent parfaitement les aspects de PCA et PRA, elles doivent impérativement prendre en compte les aspects techniques pour pouvoir apporter une réponse judiciaire à ceux-ci.

3. Gestion d'un incident de sécurité

Les problématiques de cybercriminalité sont réelles aussi bien au niveau des attaques virales, de l'usurpation d'identité, de vols ou divulgations d'informations à caractère privé ou stratégique. L'actualité récente n'a cessé de démontrer les graves impacts des déficiences en matière de sécurité. Ainsi, en juin 2012, des centaines de dossiers médicaux ont été diffusés sur Internet et rendus accessible via le moteur de recherche Google. Ces dossiers comprenaient des comptes-rendus opératoires, des bilans, des conclusions de prélèvements et toutes les informations confidentielles généralement associées. La gestion de la crise par les responsables de la clinique a conduit à fermer l'accès aux données médicales et à intervenir auprès du moteur de recherche afin d'en effacer les données sensibles. La seconde décision a consisté à réutiliser les versions papier des dossiers jusqu'à la mise en place d'une solution de sécurité satisfaisante [4]. Cet exemple illustre bien la situation actuelle de nombreuses petites et moyennes entreprises ou administrations en France et leur sous-estimation des risques liés à la cybercriminalité.

3.1 Analyse numérique (forensique)

Il est important d'analyser les différentes traces laissées à la suite d'un incident de sécurité. L'analyse post incident est l'ensemble des techniques visant à analyser un système informatique dans le but de collecter des informations et de recréer une image des activités ayant eu lieu sur un système informatique [5]. Principalement utilisée dans le cas d'investigations liées à la cybercriminalité, cette analyse est employée dans le cas d'incidents qui peuvent être liés à l'exploitation du système informatique pour comprendre les dysfonctionnements. Les objectifs sont principalement la cessation de la compromission, le rétablissement du fonctionnement normal du système et l'amélioration de la sécurité afin d'éviter la réédition de l'incident.

Le DFRWS (*Digital Forensic Reseach Workshop*) qui regroupe une communauté d'experts en analyse forensique a édité un rapport permettant de définir une formalisation du processus d'analyse et de préciser les enjeux et verrous du domaine [6]. Cette formalisation définit les huit étapes de l'analyse des traces numériques : l'identification, la préservation, la collecte, l'examen, l'analyse, la présentation et la décision [7].

Dans le contexte d'un incident, la méthode consiste à lister, identifier et analyser les processus en cours, les applications suspectes, les ports TCP et UDP ouverts et les applications qui les utilisent et les traces (logs) pertinentes présentes sur le système informatique. La majeure partie de cette étude consiste à faire une analyse a posteriori des éléments saisis au cours de l'investigation (phase de collecte). Ces éléments peuvent être des supports de stockage informatique (disques durs, bandes, cartouches, cd/dvd, clés USB, cartes mémoire type SD, etc.) ou du matériel informatique (ordinateurs, PDA, téléphones, lecteurs MP3, appareils photos, disques de photocopieurs, GPS, cartes bancaires, etc.).

Les techniques d'analyse post incident sont bien maîtrisées lorsqu'elles sont au niveau des disques durs ou du réseau. Ce qui n'est pas le cas de l'analyse forensique en mémoire (live-forensic) qui est une technique jeune. Les problématiques nécessitant ce type d'analyse répondent la plupart du temps à un incident de sécurité, à la collecte de traces « *volatiles* » d'une intrusion. L'objectif est de comprendre la méthode d'intrusion de l'attaquant. Dans ce cas, il s'agit souvent d'intrusion ciblée discrète ne laissant aucune trace sur les disques durs.

Actuellement, de nombreux travaux de recherche sont réalisés sur les terminaux nomades (smartphones, tablettes). En effet, ces terminaux intelligents rendent compliqués les phases de préservation des données, de collecte et aussi d'analyse car les types et les volumes de données sont en croissance continue [8,9,10,11].

La contrainte principale est la non altération de la preuve car une contre-expertise doit pouvoir être effectuée. Les outils d'analyse utilisés ne doivent en aucun cas modifier les fichiers journaux (logs), les dates d'accès aux fichiers analysés, ne doivent pas utiliser le ou les fichiers

d'échanges (swap) et ne doivent laisser aucune trace de montage sur les supports analysés. Il est donc important de travailler, si c'est possible, sur des copies des données. L'utilisation de solutions de blocage en écriture et/ou la réalisation de copies parfaites (copie bit à bit d'un disque dur) permet de répondre à cette contrainte. Il est possible d'utiliser des outils commerciaux spécifiques de collecte et d'analyse comme Forensic Toolkit d'Access Data, Encase de Guidance Software, X-Ways, etc.

Il faut exprimer les limites de fiabilité de l'analyse : date et heures des évènements modifiées, créateur d'un document n'est pas nécessairement le propriétaire du support numérique, données et traces stockées chez un tiers éventuellement à l'étranger (cloud [12]), chiffrement des données, des traces ont pu être laissées par un malware, la machine a peut être été utilisée dans le cadre d'un botnet ou réseau de machines zombies. Nous pouvons citer la mise en ligne d'un Wiki sur ce domaine permettant les échanges d'information [13].

L'une des difficultés majeures de la phase d'analyse réside dans le fait qu'il n'est pas toujours facile de savoir ce que l'on cherche notamment dans le cas de piratage. Une autre difficulté réside sur la problématique d'exhaustivité de l'analyse car on se heurte aux contraintes de délai et de coût de l'analyse. Or, la masse d'information obtenue durant la phase de collecte peut être très importante. Notamment dans le cas d'analyse de système d'information d'entreprise où les volumes de données peuvent atteindre plusieurs Téra voire Péta octets avec des formats pas toujours faciles à manipuler (e.g. ERP avec une base de données associée sur des serveurs utilisant une technologie matérielle propriétaire). Il est donc nécessaire d'utiliser des méthodes de triage permettant de réduire le périmètre de la phase d'analyse.

Un support numérique peut contenir des fichiers connus car associés à des systèmes d'exploitation ou à des logiciels très utilisés. Il devient alors possible de détecter et d'écarter de nombreux fichiers de l'analyse numérique. Afin d'améliorer les performances de cette recherche, des bases de données de signatures de fichiers sont disponibles comme le *Reference Data Set* (RDS) de la *National Sofware Reference Library* (NSRL). [14] présente une étude sur les forces et faiblesse de cette approche.

Un outil forensique est généralement capable d'assurer la collecte des documents et de les classer par type. Cette classification n'est pas uniquement fondée sur l'extension d'un fichier et peut utiliser le data carving qui consiste à classifier les documents par rapport à une séquence d'octets présente au début de chaque fichier. Le résultat est donc un classement par type de documents : texte, images, vidéos et par application Word, Latex, etc. Dans le cas de documents textuels, il existe une solution capable de détecter le langage utilisé permettant ainsi d'affiner l'analyse [15].

Enfin, la dernière approche est une recherche par mots-clés. Certains logiciels de collecte construisent une indexation complète des données afin d'améliorer ensuite les performances des recherches. Dans ce cas, on procède à des traitements de masse. L'objectif est donc de comprendre rapidement l'architecture réseau, d'identifier les machines « *intéressantes* » et de faire des recherches brutes par critères (nom de fichier, mots-clés dans les courriers électroniques, etc).

3.2 Détection de malwares

Lors d'une analyse forensique, il peut être intéressant de vérifier que la machine, le terminal et/ou le disque n'a pas été infecté par un malware. Dans le cadre du projet CyNIC, nous avons étudié les approches concernant les terminaux nomades.

3.2.1 Cas de smartphones dans un environnement professionnel

Les smartphones sont très utilisés dans un cadre professionnel afin de permettre à certains collaborateurs d'être connectés en permanence à leurs courriers électroniques, calendriers, Intranets, réseaux sociaux, etc. Toutefois, si ces terminaux ne sont pas gérés et protégés correctement, ils peuvent présenter des risques pour les entreprises. A titre d'exemple, un smartphone peut subir des attaques et des intrusions comme :

- des attaques par déni de service qui consiste à empêcher le client d'accéder au service fourni par le smartphone en déchargeant le plus rapidement possible sa batterie par l'exécution de tâches consommatrice d'énergie;
- les vers (programme malveillant qui se reproduit d'ordinateur à ordinateur par l'intermédiaire d'un réseau) qui ciblent des smartphones peuvent aussi avoir un coût assez important, comme l'envoi des SMS ou MMS vers un numéro surtaxé ;
- les virus (programme malveillant, inclus dans un programme hôte légitime, qui se reproduit d'ordinateur à ordinateur) contaminent un ordinateur de bureau après une synchronisation avec le smartphone. Les virus et les vers peuvent aussi placer un cheval de Troie (programme apparemment légitime qui exécute des actions à l'insu de l'utilisateur) sur l'appareil, permettant le vol des données ou l'enregistrement d'appels téléphoniques en envoyant périodiquement un rapport vers un serveur.

Une autre étude réalisée par TrendMicro (leader mondial dans le domaine des logiciels antivirus) montre que Google Android serait menacé par plus de 5.000 nouvelles applications malveillantes. Nous citons à titre d'exemple les malwares Opfake.D [16] et RootSmart.A. Opfake.D est un Trojan (programme caché dans un autre, qui s'exécute à l'insu de l'utilisateur afin de voler des mots de passe et des données sensibles, ouvrir un port, etc) qui s'installe avec les applications gratuites de GooglePlay. Une fois installé sur le terminal mobile, il envoie des SMS vers des numéros surtaxés. Pour éviter d'être détecté par

les antivirus Opfake.D modifie ses paramètres internes à chaque téléchargement (par exemple changement du texte du SMS). RootSmart.A [17] peut contourner les analyses et les scans d'antivirus car il ne contient pas de code malveillant (programme dont le but est de nuire soit à un système informatique soit aux utilisateurs du système informatique). Dans une seconde phase, il télécharge un nouveau programme à partir d'un serveur distant lui permettant l'exécution de tâches malveillantes.

3.2.2 Approches de détection d'intrusions dans les smartphones

Les nouveaux malwares ne peuvent pas toujours être détectés par des antivirus avant la mise à jour de ceux-ci (vulnérabilité 0 day). Certains malwares nécessitent des analyses comportementales pour être enfin détectés. Dans ce contexte, les approches basées sur la détection d'anomalies sont plus adaptées à la détection d'intrusions car elles consomment moins de temps et d'énergie.

Dans le cadre général (ordinateur, stations de travail), deux approches pour la détection des malwares ont été proposées qui sont l'analyse statique [18,19] et l'analyse dynamique [20,21,22]. La première analyse le code source d'un programme pour chercher des signatures d'intrusions. La seconde étudie le comportement des programmes à l'aide des méthodes statistiques et probabilistes par une surveillance de certains paramètres du système comme les entrées/sorties, le taux d'utilisation de la mémoire, la consommation du CPU, le type de numéro utilisé par les SMS, etc.

Après la découverte du premier logiciel malveillant infectant les smartphones en 2004 [23], plusieurs approches ont été proposées pour détecter les malwares dans les téléphones intelligents. La plupart des solutions proposées a été basée sur un seul critère de détection qui est la consommation de l'énergie [24,25,26]. La surveillance continue de ce paramètre et sa comparaison avec une consommation normale permet la détection d'anomalies. Cependant, ces techniques ne sont utiles que pour des attaques qui ciblent la consommation d'énergie comme le déni de service pour mettre le terminal hors service par l'épuisement rapide de ses batteries.

En ce qui concerne l'analyse dynamique, plusieurs approches ont été proposées. Schmidt et al [27] ont proposé un système s'appuyant sur des événements survenus sur le noyau Linux généralement utilisé par les OS des terminaux nomades. Ils mettent l'accent sur des événements de contrôle au niveau du noyau : des fichiers des journaux, des fichiers du système et des évènements réseaux. Le modèle de sécurité du système Android, en particulier le modèle de sécurité basé sur l'autorisation a été étudié par plusieurs chercheurs [28,29,30]. Burguera et al. ont proposé Crowdroid [31], un système de détection de malwares pour Android basé sur le comportement des applications et non sur celui de l'utilisateur. Dans ce cadre, les données recueillies auprès des utilisateurs seront transférées vers un serveur distant pour être analysées.

4. Anticipation et prévention

4.1 Outils de surveillance et de détection

Les dispositifs tels que les antivirus et les pare-feux ont été les premières briques de sécurité implémentées dans les entreprises. Malheureusement même si elles sont nécessaires, elles restent insuffisantes. En effet, ces technologies agissent soient au niveau du poste de travail (pour les antivirus) donc sur le dernier maillon de la chaîne du système d'information donc trop tard, soit au niveau de la politique de filtrage (pour les pare-feux) aussi bien pour les flux provenant ou en direction de l'extérieur du réseau de l'entreprise que pour les flux internes (notamment au niveau des cœurs de réseau). Hors cette politique de filtrage ne peut être efficace à 100%, elle tend même à le devenir de moins en moins. L'avènement d'Internet et des applications orientées Web utilisant le protocole non sécurisé HTTP nous oblige à avoir une politique de filtrage très permissive. Ce que les attaquants ont bien compris en l'utilisant massivement comme vecteur d'attaques des systèmes d'information.

Une seconde ligne de défense devient donc nécessaire : la détection d'intrusion, que l'on retrouve dans la littérature anglo-saxonne sous l'acronyme IDS (*Intrusion Detection System*). On distingue trois types de sonde de détection d'intrusion : les sondes mises en place sur les systèmes hôtes, celles surveillant les applications et celles analysant les flux sur le réseau. La détection s'effectue soit à partir d'une base de signatures, soit par la constatation d'un comportement abusif. On distingue aussi deux méthodes d'analyse : l'analyse par signature et l'analyse comportementale.

4.1.1 Analyse par signature

Cette méthode d'analyse porte également le nom d'analyse par scenario et se retrouve dans la littérature anglo-saxonne sous l'expression « *misuse detection* ». En effet, elle repose sur la définition préalable de motifs caractérisant des attaques connues et insérées dans une base de données. Concrètement avec cette approche, *tout ce qui n'est pas interdit est autorisé*. La technique de comparaison la plus répandue est celle des algorithmes de recherche de motifs (*pattern matching*) dans les paquets d'informations transitant sur le réseau ou présents dans les fichiers de logs. Néanmoins, d'autres approches existent, comme celle proposée par Mé [32] basée sur des algorithmes génétiques pour l'analyse des audits systèmes, ou comme celle de Lunt et al. [33] s'appuyant sur l'utilisation de systèmes experts. L'outil le plus connu travaillant par analyse de signature est SNORT.

4.1.2 L'analyse comportementale

L'analyse comportementale repose sur la définition du comportement normal de l'élément surveillé (système, application ou réseau). Elle nécessite donc une phase d'apprentissage qui va permettre de définir le modèle de

comportement normal. Dans cette approche, toute déviation significative du comportement génère une alerte. A contrario de l'approche par signature, tout ce qui n'est pas explicitement autorisé est interdit [34]. On distingue deux approches dans les méthodes de détection comportementale : l'approche statistique comme dans le projet intitule NIDES [35] et l'approche probabiliste comme l'indique Zimmerman et Mé [36].

4.1.3 Système hybride

Contrairement à ce que l'on pourrait penser les approches par signature et comportementale ne s'opposent pas. De nombreux chercheurs font collaborer les deux méthodes de détection au sein des IDS comme c'est le cas dans les travaux de Jia et de Chen [37]. L'hybridation permet de tirer le meilleur parti des deux méthodes.

4.1.4 Une nécessaire corrélation

Pour assurer la sécurité d'un système d'information, il est évident que plusieurs équipements de détection d'intrusions vont être installés comme un HIDS (*Host-based Intrusion Detection System*) ou un NIDS (*Network Intrusion Detection System)*. Cependant, ces systèmes font remonter un flot important d'alertes à l'administrateur qui aura le plus grand mal à analyser ces données et à prendre les bonnes décisions durant la période de l'attaque. Aussi, comme l'indiquaient Mé et al. dès 2001 [38] les outils doivent coopérer. L'objectif est de limiter le volume global des alertes et en particulier de diminuer le nombre de faux positifs qui selon Julisch [39] représentent 99% des alertes.

4.2 Protection de l'infrastructure

A minima, deux types d'outils doivent être déployés pour sécuriser un réseau : les pare-feux et les sondes de détection/prévention d'intrusions. Mais, avant de mettre en place ces outils, il est nécessaire de bien connaître l'architecture de son réseau. En effet, un pare-feu ou une sonde mal positionné peut engendrer plus d'insécurité que l'absence de ces équipements car ils diminueraient la vigilance par une trop grande confiance.

Les pare-feux peuvent être de différentes sortes suivant la couche réseau sur lesquels ils agissent. Il est indispensable de déployer au moins un pare-feu d'infrastructure (couche 3 et 4 du modèle OSI) qui permet de filtrer tous les trafics provenant de l'internet, mais également de prévenir la fuite d'informations et la propagation de codes malveillants. Ce pare-feu sera placé en coupure juste derrière le routeur d'accès à Internet.

Il convient également de placer un pare-feu dit applicatif (couche 7 du modèle OSI) pour filtrer et analyser l'ensemble des flux applicatifs en particulier le protocole HTTP. Il devra être positionné au niveau des serveurs mandataires de l'infrastructure. L'état de l'art demanderait également de positionner au cœur du réseau un autre pare-feu d'infrastructure non seulement pour filtrer les flux inter-applications et inter-VLAN, mais également pour cloisonner le réseau et isoler les parties de celui-ci en cas de problème majeur.

Pour les sondes de détection/prévention d'intrusions dont l'objectif est soit de détecter et prévenir (en mode détection), soit de détecter et bloquer (en mode prévention) les attaques qui pourraient avoir lieu contre le réseau, une connaissance de l'architecture du réseau est indispensable pour pouvoir placer les sondes aux endroits stratégiques. Une connaissance fine des applications et des protocoles est également incontournable afin d'éviter de générer trop de faux positifs qui nuiraient à l'efficacité des sondes.

4.3 Réseaux sociaux et confiance numérique

Dans le cadre du projet CyNIC, nous menons des activités de recherche sur la sécurité et les réseaux sociaux numériques. La multiplicité des plates-formes sociales associée à la forte quantité de données personnelles et sensibles en fait des lieux où l'utilisateur est vulnérable. Depuis quelques années, les acteurs malveillants ont pris place sur les réseaux sociaux numériques afin d'attirer les utilisateurs non vigilants sur des pages web malveillantes. Ce moyen d'action souvent automatisé est effectué à grande échelle ce qui permet de toucher un public très large. A titre d'exemple, Koobface est un exemple de vers informatique ayant utilisé les réseaux sociaux comme vecteur de diffusion et de propagation [40]. Celui-ci avait la capacité de détecter, en analysant les cookies de la machine infectée, les réseaux sociaux sur lequel l'utilisateur se connecte afin de publier a son insu un message lui permettant ainsi de se rependre. Koobface avait la capacité de se propager sur dix réseaux sociaux numériques distincts (Facebook, Twitter, MySpace, etc).

Notons que la topologie des réseaux sociaux numériques suit pour la plupart d'entre eux le modèle du petit monde. Celui-ci est notamment caractérisé par une faible distance entre tout individu (nombre d'intermédiaire) et une forte tendance à former des groupes (les amis de mes amis sont mes amis). A titre d'exemple sur Facebook la distance entre toute personnes est approximée à 3.5. Cela induit une capacité de contagion très rapide et explique les phénomènes amplifiés de rumeurs et de buzz sur ces réseaux [41].

Nous menons conjointement deux pistes de recherche sur ces aspects dans le projet CyNIC. D'une part, la détection et la prédiction de comportements malveillants sur ces plates-formes. Il s'agit alors de mettre en place des indicateurs comportementaux suffisants pour identifier les entités malveillantes sur ces plates-formes. Les approches reposent alors sur les techniques de classification ou sur des modèles innovants [42,43]. Nous avons dans ce but conçu et expérimenté SPOT 1.0 (*Scoring Suspicious Profiles on Twitter*) qui est un outil de collecte et d'analyse en temps réel fonctionnant à partir de la plate-forme Twitter [44]. Cet outil propose une visualisation 3D permettant l'aide à la décision pour un utilisateur personnel ou professionnel. Il est ainsi possible de visualiser

rapidement les profils les plus virulents de la plate-forme. Cette analyse est en traitement pour être étendue et adaptée aux terminaux nomades.

D'autre part, nous investiguons l'utilisation des réseaux sociaux numériques pour sécuriser un utilisateur de ces plates-formes. Cet aspect de recherche est traité dans la littérature sous l'angle des systèmes de confiance numérique [45,46]. Notre approche originale repose sur une analyse fine des multiples profils d'un même utilisateur pour en déduire un indicateur de confiance. Cet indicateur peut être synthétisé à partir d'un Smartphone, appareil ubiquitaire qui est connecté en permanence à de nombreux services sociaux (appels, SMS, courriers électroniques, Facebook, Twitter). L'approche que nous proposons analyse les redondances entre les contacts d'un même utilisateur sur de multiples réseaux sociaux. Ces redondances sont illustrées par un indicateur d'imbrication. Un indicateur de confiance est alors calculé entre deux individus en fonction du nombre de contacts et du taux d'imbrication des amis communs. Nous avons montré [47] que dans le cas de Facebook notre approche obtenait un taux de détection de profils de confiance supérieur aux approches existantes (quantité de voisins commun, attachement préférentiel, etc.) [43]. La validation repose donc sur la capacité de notre approche à prédire les liens de confiance d'un utilisateur [48].

4.4 Intelligence économique et analyse des acteurs

Actuellement, l'accès à l'information de surface est relativement facile et rapide via une connexion internet et l'utilisation d'outils de recherche en ligne adéquats. La quantité d'informations disponible et reçue est également en très forte croissance voir en trop forte croissance d'où la naissance de différents termes tels que l'infobésité (État résultant d'une information jugée trop abondante par rapport aux besoins ou aux capacités d'assimilation des utilisateurs), ou le *Big Data*, voir même *d'infopollution* [49]. Nous assistons également au développement de collectifs comme l'IORG (*Information Overload Resource Center*).

Ceci signifie que tout le monde peut obtenir des informations sur une thématique ou un acteur, mais comme l'a évoqué Eric Sutter : « *l'abondance apparente d'informations masque, en réalité, la difficulté à accéder aux informations réellement utiles* » [50]. Pour Ludovic François, nous nous heurtons à la surinformation, germe de la *mésinformation* [51]. De même pour Éric Delbeque « *il importe surtout de hiérarchiser, de savoir ce qui relève de l'accessoire et de l'essentiel, du tactique et du stratégique* » [52].

Par ailleurs, toute information disponible n'est pas nécessairement fiable et pertinente. En effet, ces informations ne sont pas toujours correctes, à jour, validées, etc. Or, l'un des principaux problèmes pour l'utilisateur commun est de considérer toutes les sources comme étant au même niveau de fiabilité (sites institutionnelles, blog, sites personnels, profils de réseaux sociaux).

Pour évoquer un exemple parlant, lors d'une inscription sur les réseaux sociaux, aucun site ne demande une validation des informations saisies. Plusieurs profils peuvent ainsi être créés sur différents réseaux (comme par exemple Viadeo, LinkedIn & Xing) avec les mêmes fausses informations. Or plus une information est visible et présente sur des sources numériques différentes et plus elle semble valide pour l'utilisateur non averti. Nous avons tendance à confondre la visibilité et la validité des informations, or une information visible n'est pas forcément correcte.

Les exemples les plus parlant sont les différents "Hoax" (Canular informatique) ou "Fake" (qui signifie "Faux" et qui est repris sur le net pour désigner une personne ayant prit une fausse identité ou diffusant une fausse information disponible sur le web [53].

Ainsi, il est impératif de faire le tri dans les informations que nous recevons et que nous recherchons, c'est l'un des objectifs de l'intelligence Économique en général.

4.4.1 Qualification de l'information reçue

Il est impératif de qualifier l'information, qu'elle soit recherchée volontairement ou reçue sans démarche préalable, de la même manière qu'il est nécessaire de qualifier l'information qui circule au sein même de son entreprise.

Pour qualifier les informations reçues ou recherchées, plusieurs critères peuvent s'appliquer, tels que : la fiabilité de la source, la qualité du contenu, la confidentialité de l'information ou son importance. Pour chacun de ces critères, différents niveaux de qualification peuvent être appliquées : de fiable à peu sûre ou non évaluée pour la fiabilité de la source, de confirmé à improbable pour la qualité du contenu, etc.

La source peut également faire l'objet d'une attention particulière, en analysant le nom de domaine (dont certains sont attribués sur justificatifs comme les .gouv, .edu, …) en procédant à une analyse « *whois* » (protocole pour interroger une base de données afin de déterminer le propriétaire d'un nom de domaine ou d'une adresse IP) ou encore en vérifiant le « *pagerank* » (algorithme d'analyse des liens concourant au système de classement des pages Web utilisé par le moteur de recherche Google), afin de mesurer l'impact ou la dangerosité d'un site.

Cette méthodologie permettra de faire un premier tri dans les sources importantes et dans les informations pertinentes et celles de moindre intérêt.

4.4.2 Relations virtuelles entre acteurs

Dans ce contexte où tout type d'information non valide circule librement sur le web, il est également nécessaire de réduire les incertitudes existantes sur différents acteurs dans le cadre de relations commerciales ou contractuels.

L'objectif étant de réduire les risques lors d'un engagement avec un Tiers. De plus en plus de relations débutent via un contact ou une identification en ligne, ceci s'explique car l'entreprise est face à plusieurs défis :

- elle se doit d'être présente sur le Web, pour montrer qu'elle existe et exposer son savoir-faire, sur un marché mondial de plus en plus concurrentiel,
- elle doit piloter sa communication et vérifier ce qui est diffusé à son sujet : elle doit piloter sa e-réputation,
- mais elle doit également rester prudente sur les relations qui vont s'établir via ce canal de communication : contrat commercial, partenariat, …

Ces deux derniers points sont primordiaux car les conséquences d'une mauvaise image ou d'un mauvais partenariat, virtuel ou réel, peuvent être multiples et extrêmement graves, pouvant aller d'un déficit d'image, l'arrêt d'une production à la variation des cours de bourse, de l'arrêt de la production à des pertes de données et entrainer in fine des pertes financières.

Ainsi, une structure économique, avant toute relation, se doit de valider l'image qu'elle renvoie, et surtout de vérifier si les informations envoyées par d'éventuels partenaires ou partie prenantes sont exactes. Elle doit donc au minimum, et de manière non exhaustive :

- valider l'existence du partenaire : (1) par une étude du site Internet : qui sont les propriétaires, où est hébergé le site, le contact indiqué correspond t'il avec une personne en présence dans la structure, etc. (2) par la validation de l'existence même de la société : en se référant au registre du commerce du pays d'implantation par exemple
- valider de l'activité de la société : (1) en confrontant les éléments diffusés par la société à d'autres sources : institutionnelles, presses, etc. (2) en se rapprochant de clients (anciens ou actuels), de fournisseurs (présents ou passés), etc. (3) en se rapprochant d'éventuels syndicats ou organisations professionnelles d'attache, (4) en se rapprochant d'organismes certificateurs,
- valider des capacités financières (dans le cade d'un contrat de vente) en recherchant les dernières informations économiques disponibles auprès d'organismes d'autorité (registre du commerce) ou spécialisés (organisme d'assurance crédit), ...
- valider l'existence du contact au sein même de l'entreprise qu'il est censé représenter.

Malgré les informations intéressantes à obtenir via les sources électroniques, il est important de noter que tous les éléments utilisés ne peuvent pas être validés uniquement via Internet mais nécessitent le recours à d'autres sources, notamment humaines. Il devient donc de plus en plus important pour une organisation de disposer d'outils pour piloter sa communication en ligne et son e-réputation et de définir une politique afin d'identifier les informations à obtenir, à diffuser et à protéger.

4.5 Classifications des informations

La gestion de l'information revêt à l'heure actuelle une place primordiale dans les administrations mais également dans les sociétés et quelle que soit leur taille. Afin de la sauvegarder de manière optimale au sein des entreprises, il convient au préalable de définir les informations stratégiques (sensibles) des autres. Il existe plusieurs recommandations ou sources d'information dans ce domaine (ANSSI, AFNOR, Assises de la sécurité, Rapport Laborde, Clusif, etc.) mais elles ne sont pas toujours respectées par les PME. Nous proposons ici une démarche permettant d'initier un processus vertueux dans les entreprises.

4.5.1 Classification des informations

La classification des informations (documents, applications métier, messagerie, informations non formalisées) qui seront diffusées dans l'entreprise est nécessaire. Elle permet d'éviter que des informations sensibles, confidentielles soient diffusées volontairement ou non à l'extérieur de l'entreprise, ce qui pourrait porter préjudice à son activité. Un exemple très intéressant est celui mis en place au niveau interministériel par le SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale) s'agissant d'une classification d'un certain type d'informations afin de restreindre leur diffusion en raison de leur nature pour des questions de défense nationale ou de défense civile.

Une habilitation est requise pour posséder des documents classifiés ou accéder à des données classifiées. Il y a généralement plusieurs niveaux de sensibilité, classés par un système hiérarchique du secret utilisé. L'action d'assigner un niveau de sensibilité à une donnée est appelée « *classification des données* ».

L'intérêt de cet exemple c'est qu'il défini trois catégories importantes qui pourraient être reprises dans les sociétés privées, notamment pour les données sensibles,: les sources de programmes, les brevets, etc. Classifier les informations revient à affecter un degré de sensibilité aux informations. L'information est générale, c'est-à-dire ouverte à l'ensemble du personnel, restreinte car sa divulgation peut nuire de façon importante à l'entreprise ou strictement confidentielle car sa divulgation porterait lourdement préjudice à l'entreprise

4.5.2 Identification des personnes et habilitations

Le chef d'entreprise doit identifier les personnes qui peuvent avoir accès aux différentes informations afin de les valoriser au mieux. Cependant, pour éviter certaines dérives, l'accès aux différents types d'information doit être préalablement défini. Il faut veiller à éviter la surprotection des informations en les sur-qualifiant, ce qui pourrait en effet instaurer un climat de méfiance au sein de l'entreprise.

Ce type de restriction en matière d'information existe déjà dans nombre d'entreprises, notamment au niveau de la

gestion des systèmes d'information (Système RH à la société Générale, système AGHORA en Gendarmerie). En effet, en fonction de son poste ou de sa fonction, de ses attributions, la personne aura plus ou moins de droits sur le réseau ou pour accéder à des informations.

4.5.3 Définition des supports de diffusion

Les supports utilisés au sein d'une entreprise sont nombreux et offrent un niveau de partage et de circulation de l'information plus ou moins large, tels que :

- les réunions : il convient de définir précisément qui peut et doit y participer, préparer les documents qui y seront diffusés et en préciser le statut et le format (papier ou numérique) :
- les comptes-rendus de visites, rapports de mission : les destinataires, le degré de confidentialité les modalités de stockage (rapport de stage des étudiants) ;
- les lettres d'information régulières (newsletters) et les journaux internes (blogs) : la politique éditoriale doit être définie préalablement et préciser notamment ce que l'on peut écrire ;
- la messagerie électronique est un support de diffusion de l'information très utilisé ;
- l'intranet est un outil qui permet de diffuser et de partager de l'information au sein de l'entreprise, mais également Internet qui permet de cibler des informations nominatives.

4.5.4 Identifier l'information

Il est nécessaire pour les entreprises d'identifier la valeur et la sensibilité des informations via des marqueurs visuels sur les documents papiers et numériques tels que les en-têtes, pieds de page, filigranes, signatures numériques incrustées. Cela permettra d'informer les salariés du niveau de sensibilité de cette information et de prendre toutes les mesures adéquates pour les sécuriser, si cette information ne l'était pas, car oubliée sur un bureau, par exemple.

4.5.5 Contrôle de la diffusion de l'information

Pour faciliter la sécurisation des données, et notamment celles qui sont numériques, il est nécessaire de mettre en place certains dispositifs tels que les *Rights Management Services*, la mise en place de signature numérique pour certains type de documents également appelés "Hash" ou "Empreinte". Les documents numériques devant être agrémentés de métadonnées. Ce type d'information facilite ainsi les solutions d'archivage mais également de DLP (*Data Loss Prevention*).

En effet, il est nécessaire de mettre en place un filtre de contrôle de sortie des documents du système d'information de l'entreprise. La DLP est une solution basée sur des règles centralisées qui identifie, surveille et protège les données qu'elles soient stockées, en cours d'utilisation ou en mouvement, quel qu'en soit le support au moyen d'une sonde (CERT-IST).

4.6 Synthèse

Aujourd'hui, les risques auxquels sont confrontées les entreprises ne résultent pas uniquement de hackers aguerris, qui vont pénétrer les systèmes informatiques en raison de leur compétence, mais surtout du facteur humain au sein de l'entreprise. Celui-ci peut se traduire par une mauvaise sécurisation des systèmes d'information, mais également de certaines informations détenues par l'entreprise. L'un des exemples les plus frappants est l'exemple des Google Dork. Un Google Dork est une signature typique d'une technologie Web parmi tout ce qui est indexé par Google. A l'aide d'une requête spécifique via ce moteur de recherche, il est possible de trouver certaines informations, certaines failles : (1) l'accès à la configuration des imprimantes non sécurisée en réseau (intitle:"hp laserjet" inurl:info_configuration.htm), (2) l'accès à des données ne devant pas être diffusées (filetype:pdf inurl:gouv.fr "ne pas diffuser) ou (3) l'accès des informations sur des serveurs (inurl:finger.cgi).

En s'appuyant sur ces simples requêtes, un internaute mal intentionné aura accès à des informations.

5. Conclusion

Cet article nous a permis de voir les différentes formes que peux prendre la cybercriminalité. Les citoyens, les collaborateurs d'une entreprise tout comme les systèmes ou équipements informatiques (des smartphones aux systèmes industriels de type Scada) sont concernés. De très nombreuses solutions de sécurité existent. Celles-ci interviennent à différents niveaux : utilisateurs avec leurs équipements personnels et terminaux mobiles, entreprises publiques et privées avec leur système d'information complexe et mouvant et l'obligation de respecter des contraintes juridiques et enfin au niveau des organismes de l'état (police et gendarmerie) qui dispose des méthodes et les moyens pour mener à bien les enquêtes.

Une défense intégrant une stratégie de cyber-défense est une révolution relativement récente dans de nombreux pays et les cyber-attaques contre l'Estonie en 2007 et l'Iran en 2010 ont certainement facilité cette prise de conscience. Le Japon a annoncé début septembre 2012 la création d'une unité militaire de cyber-défense chargées de contrer les cyber-attaques et que Tokyo se réserve le droit de répondre à des cyber-attaques par tous les moyens d'auto-défense à sa disposition.

Attention cependant à ne pas être trop confiant sur les problématiques techniques et technologiques. Un empilement de matériels et de logiciels aussi sophistiqué et performant qu'il soit ne sera jamais une réponse adéquate aux problèmes de l'insécurité électronique. La ligne Maginot en est le parfait exemple. La mise en place de solutions de sécurité reposent avant tout sur le bon sens, le pragmatisme, une politique, une organisation et des personnes sensibilisées et bien formées.

Références

[1] Ministère de l'intérieur. http://www.interieur.gouv.fr/A-votre-service/Ma-securite/Conseils-pratiques/Sur-internet/Qu-est-ce-que-la-cybercriminalite).

[2] Convention de Budapest (http://conventions.coe.int/treaty/fr/Treaties/Html/185.htm)

[3] J. Godfrain. *Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique* dite loi Godfrain.

[4] Article de du journal l'Est l'éclair. http://www.lest-eclair.fr/article/a-la-une/clinique-de-champagne-des-centaines-de-dossiers-medicaux-sur-le-net

[5] C. Altheide, H. Carvey. *Digital Forensics with open source Tools*. Syngress / Elsevier. 2011. ISBN : 978-1-59749-586-8.

[6] G. Palmer. *A road map for digital forensic reseach*. Technical report. DFRWS. November 6, 2001. http://www.dfrws.org/dfrws-rm-final.pdf.

[7] T. Duval. *Analyse informatique post-mortem : mise en œuvre et évaluation d'une approche bayésienne*. Thèse de doctorat en informatique de l'université de Rennes. 16 décembre 2005.

[8] J. Polewczyk, P. Testuz, M. Lemercier, A. Corpel. *Cybercriminalité : stratégies d'investigation numérique appliquées à l'iPhone*. Workshop Interdisciplinaire sur la Sécurité Globale (WISG 2010), janvier 2010.

[9] S. Morrissey. *IOS Forensic Analysis for iPhone, iPad and iPod touch*. Apress. 23 décembre 2010.

[10] A. Hoog. *Android Forensics – investigation, Analysis and Mobile Security for Google Android*. Syngress / Elsevier. 2011. ISBN : 978-1-59749-651-3.

[11] T. Vidas, C. Chengye and N. Christin. *Toward a general collection methodology for Android devices*. DFRWS 2011.

[12] J. Dykstra and A. Sherman. *Acquiring forensic évidence from infrastructure-as-a-service cloud computing ; Exploiring and evaluationg tools, trust, and techniques*. DFRWS 2012.

[13] E. Freyssinet. *Wiki de discussion et de recherche sur la lutte contre les bootnets*. bootnet.fr.

[14] N. C. Rowe. *Testing the National Software Reference Library*. DFRWS 2012.

[15] R. D. Brown. *Finding and identifying text in 900+ languages.* DFRWS 2012.

[16] M. Suenaga. *Android.opfake in-depth*. Technical report, Symantec Corporation, 2012.

[17] F-Secure Labs. *Mobile threat report Q1 2012*. Technical report, 2012.

[18] M. Christodorescu and S. Jha. *Static analysis of executables to detect malicious patterns*. In Proceedings of the 12th conference on USENIX Security Symposium - Volume 12, SSYM'03, pages 12–12, Berkeley, CA, USA, 2003. USENIX Association.

[19] A. Shabtai, R. Moskovitch, Y. Elovici, and C. Glezer. *Detection of malicious code by applying machine learning classifiers on static features: A state-of-the-art survey*. Inf. Secur. Tech. Rep., 14(1):16– 29, February 2009.

[20] M. Christodorescu, S. Jha, and C. Kruegel. *Mining specifications of malicious behavior*. In Proceedings of the 6th joint meeting of the European software engineering conference and the ACM SIGSOFT symposium on The foundations of software engineering, ESEC-FSE '07, pages 5–14, New York, NY, USA, 2007. ACM.

[21] T. J Lee and J.J. Mody. *Behavioral classification*. In In Proceedings of EICAR 2006, April 2006.

[22] K. Rieck, T. Holz, C. Willems, P. Dussel, and P. Laskov. *Learning and classification of malware behavior*. In Proceedings of the 5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA '08, pages 108–125, Berlin, Heidelberg, 2008. Springer-Verlag

[23] Cabir malware variants, http://www.fsecure.com/weblog/archives/00000414.html. December 2004.

[24] T. K. Buennemeyer, T. M. Nelson, L. M. Clagett, J. P. Dunning, R. C. Marchany, and J. G. Tront. *Mobile device profiling and intrusion detection using smart batteries*. In Proceedings of the Proceedings of the 41st Annual Hawaii International Conference on System Sciences, HICSS '08, pages 296–, Washington, DC, USA, 2008. IEEE Computer Society.

[25] H. Kim, J. Smith, and K. G. Shin. *Detecting energygreedy anomalies and mobile malware variants*. In Proceedings of the 6th international conference on Mobile systems, applications, and services, MobiSys '08, pages 239–252, New York, NY, USA, 2008. ACM.

[26] G. A. Jacoby and N. J. Davis IV. *Battery-based intrusion detection*. In GLOBECOM, pages 2250–2255, 2004.

[27] A-D Schmidt, H-G Schmidt, J. Clausen, K. Ali Yuksel, O. Kiraz, A. Camtepe, and S. Albayrak. *Enhancing security of linux-based android devices*. In Proceedings of 15th International Linux Kongress. Lehmann, October 2008.

[28] A. Porter Felt, E. Chin, S. Hanna, D. Song, and D. Wagner. *Android permissions demystified*. In Proceedings of the 18th ACM conference on Computer and communications security, CCS '11, pages 627–638, New York, NY, USA, 2011. ACM.

[29] M. Ongtang, S. McLaughlin, W. Enck, and P. McDaniel. *Semantically rich application-centric security in android*. In Proceedings of the 2009 Annual Computer Security Applications Conference, ACSAC '09, pages 340–349, Washington, DC, USA, 2009. IEEE Computer Society.

[30] W. Shin, S. Kiyomoto, K. Fukushima, and T. Tanaka. *Towards formal analysis of the permission-based security model for android*. In Proceedings of the 2009 Fifth International Conference on Wireless and Mobile Communications, ICWMC '09, pages 87–92, Washington, DC, USA, 2009. IEEE Computer Society.

[31] I. Burguera, U. Zurutuza, and S. N. Tehrani. *Crowdroid: behavior-based malware detection system for Android*. In Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, SPSM '11, pages 15–26, New York, NY, USA, October 2011. ACM.

[32] L. Mé. *Audit de sécurité par algorithmes génétiques*. Université de Rennes 1, RENNES, Thèse 1994.

[33] T.F. Lunt and R. Jagannathan. *A prototype real-time intrusion-detection expert system*," in Security and Privacy, 1988 IEEE Symposium, 1988, pp. 59 - 66.

[34] B. Morin. *Corrélation d'alertes issues d'outils de détection d'intrusions avec prise en compte d'informations sur le système surveillé*. INSA, Rennes, Thèse 2004.

[35] A. Debra, T. F. Lunt, H. Javitz, A. Tamaru, and A. Valdes. *Detecting Unusual Program Behavior Using the Statistical Components of NIDES*. Computer Science Laboratory, SRI International, 1995.

[36] J. Zimmermann and L. Mé. *Les systèmes de détection d'intrusions : principes algorithmiques*. http://www.rennes.supelec.fr/ren/rd/ssir/publis/misc02_zimmermann_me.pdf.

[37] C. Jia and D. Chen. *Performance Evaluation of a Collaborative Intrusion Detection System*. In 2009 Fifth International Conference on Natural Computation, Tianjin, 2009, pp. 409 - 413.

[38] L. Mé, Z. Marrakchi, C. Michel, H. Debar, and F. CUPPENS. *La détection d'intrusions : les outils doivent coopérer*. Revue de l'électricité et de l'électronique, no. 5, pp. 50 - 55, mai 2001.

[39] K. Julisch. *Clustering Intrusion Detection Alarms to Support Root Cause Analysis*. ACM Transactions on Information and System Security, vol. 6, pp. 443-471,

[40] J. Baltazar, J. Costoya, and R. Flores. *The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained*. pp. 1–18, Jul. 2009.

[41] J. Kleinberg. *The small-world phenomenon: an algorithm perspective*. Proceedings of the thirty-second annual ACM symposium on Theory of computing, New York, NY, USA, 2000, pp. 163–170.

[42] S. Abu-Nimeh, T. M. Chen, and O. Alzubi. *Malicious and Spam Posts in Online Social Networks*. Computer, vol. 44, no. 9, pp. 23–28, 2011.

[43] C. Patsakis, A. Asthenidis, and A. Chatzidimitriou. *Social Networks as an Attack Platform: Facebook Case Study*. Networks, 2009. ICN '09. Eighth International Conference on, 2009, pp. 245–247.

[44] C. Perez, M. Lemercier, B. Birregah, and A. Corpel. *SPOT 1.0: Scoring Suspicious Profiles on Twitter*. presented at the Advances in Social Networks Analysis and Mining (ASONAM), 2011 International Conference on, 2011, pp. 377–381.

[45] J. Sabater and C. Sierra. *Review on Computational Trust and Reputation Models.* Artificial Intelligence Review, vol. 24, no. 1, Sep. 2005.

[46] S. Hamdi, A. L. Gancarski, A. Bouzeghoub, and S. B. Yahia. *IRIS: A Novel Method of Direct Trust Computation for Generating Trusted Social Networks*. presented at the Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, 2012, pp. 616–623.

[47] C. Perez, B. Birregah, and M. Lemercier. *The Multi-layer imbrication for dataleakage prevention from mobile devices*. TrustCom'12, pp. 1–7, Jun. 2012.

[48] D. Liben-Nowell and J. Kleinberg. *The link-prediction problem for social networks*. J. Am. Soc. Inf. Sci. Technol., vol. 58, pp. 1019–1031, May 2007.

[49] E. Sutter. *Pour une écologie de l'information*. Documentaliste - Sciences de l'information, vol. 35, n°2, 1998, p. 83-86

[50] E. Sutter. *Intelligence Economique et management de l'information*. Paris, Editions Tec & Doc

[51] L. François, 2004. *Business sous influence*. Paris, Editions d'Organisation

[52] E. Delbeque. *L'intelligence Economique* , Paris, 2006. Editions PUF

[53] Site web sur les Hoax. http://www.hoaxbuster.com