Petites entreprises et sécurité informatique : un mariage de raison ?

Yoann Bertrand [1]

Introduction

La sécurité informatique est devenue ces dernières années un enjeu de taille pour les entreprises. En effet, l'outil informatique, par ses nombreux avantages, s'est rapidement imposé comme le centre névralgique d'une entreprise, pouvant gérer à la fois les processus, les échanges et les données tout en améliorant la productivité et l'efficacité des affaires. Néanmoins, cette faculté de gestion globale a rendu l'outil informatique crucial et extrêmement sensible, le transformant *de facto* en une cible de prédilection pour un ensemble de belligérants. En effet, de plus en plus d'attaques ciblent les entreprises pour des raisons multiples et variées (e.g. guerre économique, espionnage industriel, vols d'informations, vengeance d'employés). Quel qu'en soit le motif, ces attaques peuvent être extrêmement rédhibitoires pour la rentabilité d'une société, pouvant induire des pertes financières et une perte de notoriété. Afin de réduire ces risques et se prémunir contre ces attaques, une entreprise dispose d'un arsenal de méthodes techniques, organisationnelles et juridiques. Si cet arsenal défensif a rapidement été pris en main, formalisé et amélioré par les grands groupes, des structures plus humbles, par manque de compétences, de temps et de connaissance des enjeux, restent en retard, devenant des cibles de choix pour des attaques.

Cet article propose d'étudier la sécurité informatique à travers ces petites structures. Pour cela, nous définissons dans un premier temps les principaux termes des structures morales étudiées (e.g. TPE/PME) ainsi que la terminologie inhérente à la

1. Consultant en Informatique, Villeneuve-Loubet (06). bertrand.yoann@gmail.com.

CC BY ND

sécurité informatique. Dans un second temps, nous présentons les principales menaces de sécurité ainsi que les contre-mesures permettant de réduire les risques de sécurité au sein de ces structures.

Contexte économique

L'article 51 de la loi n° 2008-776 du 4 août 2008 [36] définit comme « Petites et Moyennes Entreprises » (PME) l'ensemble des sociétés qui comptent moins de 250 salariés et présentent un chiffre d'affaires annuel inférieur à 50 millions d'euros ou un bilan annuel situé en dessous de 43 millions d'euros. Les « Très Petites Entreprises » (TPE) sont quant à elles les entreprises comptant moins de 10 salariés pour un chiffre d'affaires annuel et un bilan qui ne dépassent pas les 2 millions d'euros. Il est à noter que depuis 2008, le terme « microentreprise » (MIC) a remplacé le terme TPE. Néanmoins, cette terminologie peut prêter à confusion, car le terme microentreprise désigne également un régime fiscal spécifique des entreprises individuelles. Nous utiliserons donc, pour éviter les confusions, le terme TPE.

La France compte plus de 3.8 millions d'entreprises. Parmi elles, 140.000 sont des PME (soit environ 3.8 %) qui emploient 28 % des salariés. Le nombre de TPE est quant à lui beaucoup plus gros. En effet, 3.6 millions des entreprises françaises sont des TPE (soit 96 %) qui emploient au total environ 2.4 millions de salariés (soit 18 %) [9] [24]. Ainsi, ces statistiques montrent que plus de 99 % des sociétés sont des structures de taille relativement « modeste » qui emploient un peu moins de la moitié des salariés de France.

En partant de l'hypothèse qu'une grande partie des PME ont assez de compétences et de moyens pour répondre aux challenges de la sécurité informatique, il reste néanmoins une très grande quantité de petites structures issues de secteurs très divers (construction, santé humaine, hébergement et restauration, etc.) qui ont une connaissance limitée de l'outil informatique et de sa sécurité. En effet, plusieurs études soulignent des faits alarmants concernant la sécurité dans les PME du monde entier. Par exemple, une étude de Cisco [12], menée en 2018 sur plus de 1800 personnes de plus de 26 pays différents, montre que plus de la moitié des entreprises de taille moyenne ont connu une faille de sécurité qui a coûté, pour 20 % d'entre elles, entre 1.000.000 et 2.499.999 dollars. Une autre étude, menée par Kaspersky [26], montre qu'une TPE / PME sur trois confie la sécurité de son infrastructure à un employé inexpérimenté et qu'une sur deux reconnaît ne pas former ses salariés aux risques liés à la sécurité.

Principes de sécurité informatique

Historiquement, la sécurité informatique a commencé à être implémentée pour protéger les systèmes contre plusieurs attaques. Ces attaques étaient principalement

de la détérioration de matériel et du vol de données, perpétrées dans le but de perturber un service ou engendrer des pertes financières. Pour améliorer la robustesse des systèmes, plusieurs modèles, comme le modèle CIA-triad [21], ont été formalisés. Ce modèle propose de définir les trois grandes propriétés de sécurité suivantes : la Confidentialité, l'Intégrité et la Disponibilité (*Accessibility* en anglais).

Confidentialité

La confidentialité repose sur la prévention des accès non autorisés à une information. Cette propriété est définie par l'Organisation internationale de normalisation (ISO) comme « le fait de s'assurer que l'information est seulement accessible aux entités dont l'accès est autorisé ». Dans le milieu informatique, la nécessité de confidentialité est apparue suite à l'intégration des systèmes d'information critiques, tels que ceux des organisations gouvernementales ou de certaines industries issues de milieux sensibles (e.g. militaire, énergie). Néanmoins, la nécessité de rendre confidentielle une information est un principe beaucoup plus ancien, qui remonte à l'antiquité. Le principal mécanisme derrière la confidentialité est la cryptographie [31], processus mathématique permettant de transformer (i.e. chiffrer) une information de façon à la rendre non compréhensible par une personne ne possédant pas le mécanisme de déchiffrement (appelé « clé »). La cryptographie moderne se divise en deux grandes familles : la cryptographie symétrique, dans laquelle une seule clé est utilisée pour chiffrer et déchiffrer, et la cryptographie asymétrique, ou deux clés différentes sont utilisées (une pour chiffrer et une pour déchiffrer).

Intégrité

L'intégrité désigne l'état de données qui, lors de leur traitement, de leur stockage ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation. Dans le cas d'une ressource ou d'un service, l'intégrité signifie que ce dernier « fonctionne » correctement, c'est-à-dire qu'il respecte sa spécification. La propriété d'intégrité des données vise à prévenir toute modification non autorisée d'une information (qu'elle soit volontaire ou non). On discrimine en général deux grands types d'intégrité :

— La garantie de la fidélité des informations vis-à-vis de leur conteneur, que l'on nomme « intégrité des données ».
— La garantie des informations en rapport avec la création ou le propriétaire, que l'on nomme « intégrité de l'origine » ou « authenticité ».

Pour garantir l'intégrité d'une donnée, on utilise le principe de « *hash* cryptographique » (aussi appelé « fonction de hachage »), qui permet de représenter une information sous la forme d'une chaîne de caractères.

Disponibilité

Comme son nom l'indique, la disponibilité est la propriété permettant de garantir le maintien de l'accès à une ressource ou un système. Bien que cette propriété semble moins importante que la confidentialité ou l'intégrité, la transformation digitale a rendu la disponibilité extrêmement importante, notamment via des services délocalisées et très rentables comme les services *cloud* et le e-commerce. En effet, une perturbation ou une interruption de services peut-être extrêmement néfaste en terme d'image et de rentabilité, pouvant forcer un client à changer de fournisseur de services.

Autres propriétés de sécurité

Les propriétés précédentes ont été enrichies et dérivées au fil du temps, faisant naître de nouvelles notions de sécurité, comme par exemple :

— Le contrôle d'accès, qui permet de définir qui peut accéder à quoi.
— La non-répudiation, qui permet de garantir qu'une transaction ne peut être niée.
— L'authentification, qui permet à un utilisateur ou une machine de prouver qui elle est (en utilisant par exemple un couple identifiant et mot de passe).
— La traçabilité, qui permet de garantir que les accès (et les tentatives d'accès) aux ressources sont horodatées, conservées et exploitables.

Dans cette section, nous avons vu les principales propriétés de sécurité utilisées pour améliorer la sécurité et la robustesse d'un système informatique. Dans la section suivante, nous présentons les principales menaces et attaques qu'une entreprise peut subir.

Tour d'horizon des attaques

Dans cette section, nous définissons dans un premier temps les principaux termes inhérents à la sécurité informatique. Dans un second temps, nous présentons les motivations et profils d'attaquants potentiels. Enfin, nous terminons cette section par une taxonomie des principales menaces qu'une entreprise peut subir.

Définitions

Rares sont les jours ou les médias ne parlent pas de menaces, d'attaques ou encore de vulnérabilités. Néanmoins, ces termes sont souvent mal utilisés par le grand public. Ainsi, commençons par définir rapidement ces termes afin d'éviter les ambiguïtés. Une menace est une attaque potentielle sur un bien de l'entreprise qui peut être causée par un individu, un groupe d'individus ou une cause naturelle. Une menace peut entraîner des conséquences potentiellement négatives pour l'entreprise (perte de crédibilité, image de marque altérée, pertes financières, etc.). Une attaque est quant à

elle une action qui vise à compromettre la sécurité d'un système d'information, pour un certain nombre de motifs. Une attaque peut être :

— Passive : l'individu écoute ou copie des informations de manière illicite.
— Active : l'individu altère l'information (modification, suppression) et/ou le fonctionnement d'un service.

Une vulnérabilité est une caractéristique d'une entité de l'entreprise (p. ex. logiciel, élément matériel, etc.) qui peut constituer une faiblesse au regard de la sécurité. Une vulnérabilité peut avoir plusieurs formes. En effet, elle peut être :

— Organisationnelle (p. ex. pas / peu de politiques de sauvegarde, pas de suivi des événements de sécurité, etc.).
— Logicielle ou matérielle (p. ex. bugs, codes non-testés, matériel défaillant, etc.).
— Humaine (p. ex. mauvaise formation du personnel, manque de compétences, volonté d'un employé de « vouloir bien faire », etc.).

Un attaquant est ainsi un individu représentant une menace et pouvant utiliser une vulnérabilité pour arriver à ses fins. Les motivations d'un attaquant peuvent être multiples et sont décrites plus en détail dans la sous-section suivante.

Motivations des attaquants

Argent : Pour beaucoup d'attaquants, l'argent est le moteur principal. Cet argent peut provenir d'une entreprise concurrente, d'une organisation de crime organisé ou encore d'un état. Pour d'autres, l'argent peut être obtenu à partir des informations récoltées (reventes des informations personnelles, prise en otage des données, etc.).

Challenge - Notoriété - Tests de compétences : Le challenge technique peut permettre à certains acteurs du milieu du *hacking* d'acquérir une certaine notoriété et/ou de tester ses compétences. Une grande partie des personnes motivées par le challenge sont techniquement très compétentes et avides de connaissances.

Rancune : Un ancien employé ayant quitté l'entreprise en mauvais termes peut devenir très néfaste pour l'entreprise. En effet, ce dernier peut encore posséder des droits d'accès ou simplement des connaissances pour mener à bien des attaques afin de satisfaire sa rancune. À noter que les attaques ne viennent pas exclusivement de l'extérieur. En effet, un employé en fonction dans une entreprise peut, par rancune ou volonté de vengeance, utiliser son savoir-faire, ses compétences ou ses accès à des fins néfastes.

Idéologie : Un attaquant ou un groupe d'attaquants peut mener des attaques pour des raisons politiques, religieuses, éthiques ou sociales. Ces attaques peuvent servir à faire passer un message ou une idéologie et sont considérées par ce type de personnes comme des actes militants.

Types d'attaquants

Les types d'attaquants sont nombreux et possèdent des compétences et des motivations différentes. Parmi les types d'attaquants, on peut citer les catégories suivantes.

Script Kiddies. *Script kiddies* est le terme péjoratif anglo-saxon qui désigne des utilisateurs possédant peu pas de compétences en sécurité informatique. Ces derniers se contentent d'utiliser le plus souvent des scripts et programmes développés par d'autres et récupérés sur Internet, sans connaissances particulières sur le fonctionnement des outils. Bien que peu compétents, les *scripts kiddies* peuvent s'avérer extrêmement néfastes pour un système informatique, à cause notamment de leur nombre et de leur pugnacité.
Principales motivations : Argent, Notoriété.
Niveau de compétences : Faible.

Hackers. Les hackers sont des attaquants possédant de solides compétences techniques. Il faut néanmoins distinguer plusieurs types :

— Les *blackhats*, dont les attaques et intrusions sont malintentionnées (par exemple, à des fins personnelles).
— Les *whitehats*, dont les attaques et intrusions sont intentionnelles (tests de sécurité) ou dirigées vers leurs propres infrastructures (expert sécurité).
— Les *greyhats*, dont les attaques et intrusions sont dirigées sur les infrastructures d'autrui sans autorisation (comme un *blackhat*), mais dans le but constructif d'améliorer la sécurité (comme les *whitehats*), en rapportant notamment les découvertes de failles aux administrateurs et experts sécurité.

Principales motivations : Idéologie.
Niveau de compétences : Moyen à Fort.

Hacktivistes. L'hacktivisme est un ensemble de pratiques consistant à promouvoir une idéologie religieuse, politique, éthique ou sociale en utilisant les technologies de l'information et de la communication. Un hacktiste est donc un militant pouvant utiliser des techniques peu scrupuleuses servant à la propagation de son message (insoumission à un système politique, combats idéologiques, militantisme écologique, etc.). L'hacktivisme étant plus un état d'esprit qu'une catégorie de personnes à part entière, ce dernier peut contenir en son sein à la fois des *script kiddies* et des hackers (par exemple, des *blackhats*).
Principales motivations : Idéologie, Notoriété.
Niveau de compétences : Faible à Fort.

Espions industriels - Concurrents. Une entreprise peut être espionnée par un concurrent peu scrupuleux. Cet espionnage peut avoir des répercussions sur l'économie de l'entreprise ciblée, notamment en cas de vol d'informations (e.g. propriété intellectuelle, fichiers clients, catalogue, mails). Dans ces cas de figure, l'entreprise attaquante utilise le plus souvent les services de *blackhats* pour mener à bien ses attaques. Il est aussi possible d'utiliser de manière directe ou indirecte un employé de la société ciblée.
Principales motivations : Argent.
Niveau de compétences : Moyen à Fort.

Membre du personnel ou ancien membre du personnel. Un employé ou un ancien employé peut être la cause directe ou indirecte d'une attaque. En effet, ce dernier peut avoir été manipulé par ingénierie sociale (attaque non-volontaire) ou être lui-même la cause d'une attaque volontaire sur le système d'information. En effet, un employé possède souvent des accréditations et des connaissances particulières sur l'entreprise et ses employés, augmentant *de facto* la sévérité des attaques. De plus, l'impact humain est souvent très élevé dans ce type d'attaque et peut conduire à des sanctions graves (blâme, licenciement, etc.).
Principales motivations : Rancune, Argent.
Niveau de compétences : Faible à fort.

Cyber-terroristes - Institution étatique. Les cyber-terroristes ciblent des infrastructures critiques et administratives pour générer du chaos et de la peur afin de propager des idéologies politiques ou religieuses. Certaines de ces activités peuvent être commanditées et/ou menées par des états avec des objectifs géostratégiques, économiques ou encore politiques.
Principales motivations : Argent, Idéologie.
Niveau de compétences : Fort.

Comme nous venons de le voir, les profils et motifs des principaux attaquants sont variés, rendant complexe la tâche consistant à sécuriser un système d'information. De plus, cette tâche est encore plus difficile lorsque l'on regarde les nombreuses attaques pouvant intervenir sur un système. Les paragraphes suivants proposent une taxonomie de ces principales attaques.

Taxonomie des principales attaques

Nous proposons dans cette partie une macro-catégorisation composée de sept grands groupes permettant de dresser un panel non exhaustif des principales attaques.

Ingénierie sociale (*Social Engineering*) (ATK_SE)

L'ingénierie sociale englobe l'ensemble des techniques consistant à récupérer de manière déloyale des informations clés d'une personne, d'une entité ou d'un service. Pour cela, l'attaquant peut user de stratagèmes comme la ruse, l'usurpation d'identité, d'émotions comme la peur, la compassion ou encore l'excès de zèle. Ces techniques sont considérées comme extrêmement dangereuses car elles ne nécessitent souvent que peu de compétences informatiques. De plus, le fait qu'elles fassent intervenir l'humain rend ces attaques difficilement parables d'un point de vue strictement technique.

Un exemple concret d'ingénierie sociale est le *spear phishing* [6], technique consistant à envoyer des emails ciblées à une victime (par exemple, un email de votre banque demandant de changer votre mot de passe).

Attaques réseaux (ATK_NET)

Bon nombre de protocoles réseaux ont été historiquement implémentés sans faire intervenir la notion de sécurité. De nos jours, les infrastructures étant de plus en plus hébergées de manière distribuée, les réseaux ont pris une place conséquente dans les systèmes d'information actuels. En effet, les communications entre les différents éléments d'un système d'information se font par un ensemble de canaux voulus et implémentés à cet effet. Un canal caché est un canal de communication possible mais qui n'était pas prévu, lors de la conception du système, comme canal de communication. Un canal caché permet donc de transmettre des informations sans l'autorisation ou la connaissance du propriétaire de l'information ou de l'administrateur du réseau.

Un exemple d'attaque réseau est le déni de service (distribué) (*(Distributed) Deny of Service* ou (D)DoS). Ces attaques consistent à surcharger en requêtes un serveur (ou la connexion réseau à ce serveur) afin de rendre son/ses services lents voire inopérants. Des cas célèbres d'attaques DDoS, comme celles subies par OVH en 2016 [39] ou GitHub en mars 2018 [34], peuvent être cités comme exemple.

Attaques sur les systèmes d'exploitation (ATK_OS)

Les services d'une infrastructure étant fournis au-dessus d'un système d'exploitation, plusieurs attaques consistent à exploiter ces derniers. Ainsi, un système d'exploitation non maintenu ou n'étant pas à jour est souvent la cause principale de ce type d'attaque. De plus, une vulnérabilité récemment découverte et pas encore corrigée est aussi un moyen très souvent utilisé par un attaquant [10].

Attaques basées sur une mauvaise configuration (ATK_CONF)

Pour des raisons de gain de temps ou par manque de compétences, les systèmes et applications sont souvent laissés dans leur configuration d'origine (i.e configuration par défaut). Ces configurations peuvent faciliter le travail des attaquants et avoir un impact sur la sécurité. Parmi les configurations par défaut, on peut citer les mots

de passe par défaut ou trop faibles, les chemins de fichiers de configuration par défaut, les droits et sécurité minimum, l'ouverture de ports par défaut, etc.). Pour un attaquant, une technique simple consiste à se procurer la liste de mots de passe par défaut d'un constructeur, en utilisant par exemple ce type de plateforme [11].

Attaques sur les applications et les logiciels (ATK_SOFT)

Les applications possèdent souvent des vulnérabilités pouvant être causées par une mauvaise implémentation (manque de contrôle des données d'entrée, laxisme au niveau des droits d'accès, etc.). Cette mauvaise implémentation peut avoir pour cause un laxisme lors des phases d'analyse et de conception en ce qui concerne la sécurité, un manque de compétences/sensibilité des développeurs, un problème de temps lors du développement ou encore un manque de tests de sécurité lors de l'implémentation. De nombreuses vulnérabilités logicielles sont découvertes par les experts sécurité ou les hackers. Par exemple, on peut citer Heartbleed[22], une vulnérabilité sur la bibliothèque OpenSSL découverte courant 2014.

Attaques basées sur le matériel (ATK_HARD)

Les infrastructures systèmes et réseaux étant basées sur du matériel, plusieurs vulnérabilités utilisent ce vecteur d'attaques. On peut par exemple citer la vulnérabilité Spectre[2], qui affecte les microprocesseurs modernes, ou Meltdown[8], spécifique aux microprocesseurs Intel x86. Nous englobons aussi dans cette catégorie les attaques visant à altérer physiquement le matériel et les infrastructures.

Attaques pour récupérer des informations (*Information gathering*) (ATK_INFO)

Cette catégorie englobe des attaques avec des cibles extrêmement variées (humains, équipement réseaux, logiciels, systèmes d'exploitation, etc.). Quelle que soit la cible, l'objectif de ces attaques passives est de récupérer un maximum d'informations le plus discrètement possible. Ces informations (date de naissance, ports ouverts, architecture du système d'exploitation, version de l'application, etc.) pourront ainsi permettre dans un second temps de mener des attaques actives sur les infrastructures du système d'information de l'entreprise. Plusieurs exemples de récupération d'informations, notamment via de l'ingénierie sociale, peuvent être trouvés, notamment à travers l'ouvrage du célèbre ex-hacker Kevin Mitnick [32].

Attaques par utilisation de code malveillant (ATK_MAL)

On range dans cette catégorie l'ensemble des attaques utilisant des logiciels malveillants qui sont, dans l'attirail des attaquants, les méthodes les plus connues du grand public. Néanmoins, le terme est souvent mal utilisé par les médias et les néophytes. Pour lever ces ambiguïtés, les prochaines lignes détaillent les principaux types de codes malveillants [20].

Parmi les exemples récents et innovants de code malveillant, nous pouvons citer Adylkuzz [13], logiciel malveillant découvert en 2017, qui permettait l'utilisation

des ressources matérielles de l'ordinateur infecté afin de miner des crypto-monnaies à l'insu de la victime.

Virus. C'est la dénomination la plus connue, le virus est un logiciel implémenté le plus souvent dans le but de nuire au bon fonctionnement d'un système. Comme son homologue biologique, le virus est capable de se répliquer lui-même et de modifier son code pour tenter de ne pas être détecté par des antivirus.

Ver. Les vers sont des variantes des virus qui se propagent par le réseau. Comme les virus, les vers peuvent se répliquer et sont utilisés comme porte d'entrée, permettant aux attaquants d'installer d'autres types de logiciels malveillants.

Cheval de Troie. Un cheval de Troie désignait initialement un programme se présentant comme un programme légitime destiné à remplir une tâche donnée, mais qui, une fois installé, exerçait une action nocive totalement différente de sa fonction « officielle ». Les chevaux de Troie font donc souvent appel à de l'ingénierie sociale, en usurpant un nom ou une icône connue pour piéger la victime.

Enregistreur de frappe (Keylogger). Les *keyloggers* permettent d'espionner et d'enregistrer les frappes d'un clavier. Ainsi, un *keylogger* permet de manière furtive de monitorer l'utilisation d'un système par un utilisateur ou de récupérer un ensemble d'informations confidentielles, comme des mots de passe, des conversations de messagerie, des informations bancaires, etc.

Maliciel furtif (Rootkit). Les *rootkits* sont des ensembles de programmes qui permettent de dissimuler la présence d'un attaquant ou d'un programme malveillant dans un système. De ce fait, les *rootkits* permettent une connexion entre la machine de l'attaquant et la cible, favorisant ainsi un point d'ancrage et une pérennité dans un système. Cette pérennité pourra par exemple servir à installer d'autres *malwares*, à mener diverses attaques ou à scanner une partie du réseau interne de la victime.

Porte dérobée (Backdoor). Conceptuellement proche des *rootkits*, les *backdoors* sont des morceaux de code laissés intentionnellement pour permettre un accès discret et distant à une machine. Une *backdoor* peut être laissée intentionnellement par le développeur d'une application, ou ajouté par un attaquant en utilisant différentes techniques (compromission d'une mise à jour, rétro-conception du code source original et ajout de la *backdoor* en se faisant passer pour le développeur légitime, etc.).

Rançongiciel (Ransomware) et logiciels destructeur de données (Wiper) : Les *ransomwares* sont sous les projecteurs depuis quelques années. Ces *malwares* chiffrent un disque (ou une portion d'un disque), empêchant les utilisateurs légitimes d'accéder à leur système ou leurs données. Pour pouvoir y accéder de nouveau, les utilisateurs doivent payer l'attaquant, le plus souvent en utilisant une cryptomonnaie comme Bitcoin [16] pour obtenir la clé de déchiffrement. Il est à noter qu'il n'est jamais garanti de recevoir la clé après paiement.

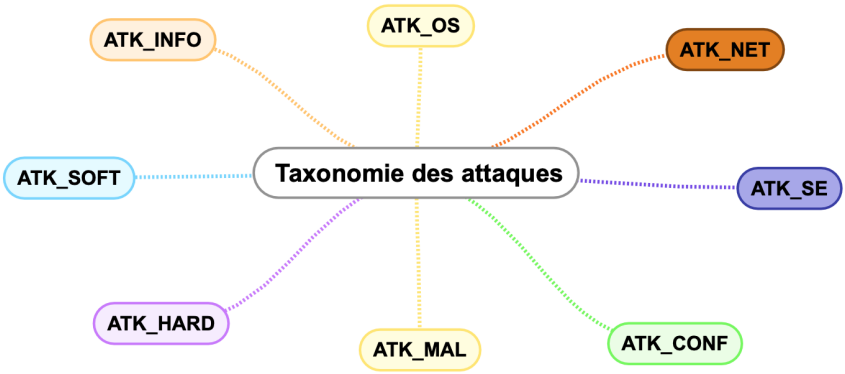

FIGURE 1. Carte heuristique des principales attaques.

Logiciel escroc (Rogueware). Ce type de logiciels malveillants utilise l'ingénierie sociale. En effet, ces applications se font passer pour des logiciels de sécurité (antivirus, parefeu, anti-malwares, etc.) mais permettent en réalité l'installation d'un ensemble de *malwares* (*rootkits*, *keyloggers*, etc.) pour rendre la machine cible infectée.

Logiciel publicitaire (Adware). Ces logiciels installent des publicités sur les systèmes. Rarement létal seul, un *adware* est néanmoins pénible pour le confort d'utilisation et peut permettre l'installation d'autres *malwares* plus néfastes. À noter que, comme les *ransomwares*, la principale utilité des *adwares* est leur lucrativité.

Logiciel espion (Spyware). Les *spywares* sont des logiciels permettant la récolte d'informations sur les utilisateurs (comportement, sites visités, etc.). Ces informations sont ensuite revendues à des agences de publicité permettant des campagnes de publicité ciblées. Rarement perçus par l'utilisateur, ces logiciels restent néanmoins liberticides car en violation avec les principes de vie privée.

Comme nous venons de le voir, un grand nombre d'attaques différentes peuvent être menées sur une infrastructure d'entreprise, en ciblant à la fois les services, les systèmes d'exploitation, les réseaux, le matériel ou encore les utilisateurs (voir Figure 1). Pour réduire le risque et l'impact de ces attaques, plusieurs contre-mesures ont été inventées. Ces contre-mesures sont présentées dans la section suivante.

Tour d'horizon des contre-mesures

Une contre-mesure est un ensemble d'actions mis en place pour réduire le risque d'une menace. Un risque peut être formalisé comme le produit d'un impact (mineur,

modéré, fort, etc.) et d'une probabilité d'occurrence / vraisemblance (peu probable, probable, très probable, etc.). Un risque peut être classé en fonction de ces deux métriques (p. ex. des risques critiques qui n'arrivent pratiquement jamais ou encore des risques avec un impact mineur qui peuvent arriver régulièrement). Ainsi, une menace est d'autant plus néfaste que son impact est fort et très probable. Il est à noter qu'une contre-mesure ne réduit jamais complètement un risque. En effet, le risque zéro n'existant pas, tout l'objectif de la sécurité informatique est d'évaluer ce risque et de le réduire au maximum en fonction de différentes contraintes. Dans cette section, nous présentons trois grandes catégories de contre-mesures visant à réduire ces risques : les contre-mesures techniques, les contre-mesures organisationnelles et les contre-mesures juridiques et légales.

Contre-mesures techniques

Il existe un grand nombre de contre-mesures techniques pour réduire la sévérité ou la probabilité d'occurrence d'une attaque. Les contre-mesures les plus connues et les plus usitées ciblent les infrastructures réseaux et systèmes ainsi que la protection des données. D'un point de vue général, ces contre-mesures utilisent des mécanismes comme la cryptographie, le contrôle d'intégrité (via des mécanismes appelés fonction de hachage), le contrôle d'accès ou plus récemment l'intelligence artificielle. Les prochains paragraphes présentent succinctement les principales contre-mesures.

Contre-mesures réseaux

Une infrastructure d'entreprise est le plus souvent un conglomérat de services détachés sur plusieurs zones géographiques reliées par des interfaces réseaux. Plusieurs contre-mesures usitées par les entreprises visent à protéger et améliorer la sécurité de ces connexions, c'est le cas notamment des contre-mesures suivantes.

Pare-feux. Les pare-feux sont des mécanismes dont l'objectif est d'autoriser ou non l'accès à certaines parties du réseau, à autoriser certains services ou certains ports, voire à rediriger le trafic vers des zones spécifiques pour séparer les infrastructures critiques des infrastructures non critiques. Il existe plusieurs types de pare-feux qui fournissent des services variés (analyseur temps réels, filtrage de contenu, etc.) et qui sont le plus souvent décrits sous l'appellation NGFW (*Next Generation Firewall*) ou UTM (*Unified Thread Management*). Parmi les constructeurs et fournisseurs de pare-feux les plus plébiscités, on trouve notamment Stormshield, Fortinet, PfSense ou encore Sophos. Le site NSSLabs [27] propose des audits et des tests pour évaluer les performances de ces pare-feux. De plus, l'ANSSI propose aussi des guides pour choisir et configurer ce type de contre-mesures [4].

VPN (Virtual Private Network ou Réseau Virtuel Payant). Un VPN permet de sécuriser les échanges entre une source et une destination en utilisant la technique de « tunnel ». Ce tunnel peut être vu comme une extension des réseaux internes de l'entreprise, permettant ainsi de créer un lien direct entre des ordinateurs distants, en

isolant ce trafic de manière sécurisée. Pour cela, on utilise le chiffrement cryptographique pour appliquer le principe de confidentialité, d'intégrité et d'authenticité aux connexions. Il est à noter que beaucoup de pare-feux de nouvelle génération (NGFW) intègrent un VPN, notamment pour faciliter et sécuriser les connexions de ses collaborateurs et employés nomades [5].

Mécanismes de répartition de charge (load-balancing). Les *load-balancers* permettent, comme leur nom l'indique, de distribuer un travail entre plusieurs serveurs, afin d'éviter la surcharge, notamment en cas d'attaque par déni de service (DoS / DDoS). Les mécanismes de répartition de charge peuvent absorber une partie de cette charge et la répartir sur des serveurs redondants afin de réduire le risque de déni de service. Il est à noter qu'un mécanisme efficace contre ces attaques se doit aussi d'analyser rapidement les requêtes, afin de détecter les requêtes polluantes (i.e. celles issues de l'attaque), d'éventuelles requêtes légitimes (i.e. celles provenant de véritables utilisateurs). Pour cela, plusieurs techniques et algorithmes existent [1]. En ce qui concerne les principales solutions, on peut voir deux grandes tendances, les solutions matérielles (*Hardware Load Balancer* ou HLB) et les solutions logicielles (*Load Balancing as a Service* ou LBaaS)[23], chacune proposant des avantages et des inconvénients en terme de coûts, de passage à l'échelle et de flexibilité [35].

Contre-mesures systèmes

Cet ensemble regroupe les contre-mesures agissant directement sur les postes utilisateurs et les serveurs. Les objectifs de ces contre-mesures sont nombreux, mais l'on peut souligner la faculté d'analyser des services et des programmes dans le but de détecter des comportements étranges et des applications connues comme étant malveillantes.

Antivirus, anti-malwares et anti-spyware. Bien connues du grand public, ces contre-mesures permettent d'analyser un espace de stockage à la recherche de logiciels malveillants. Les mécanismes de recherche les moins complexes consistent à étudier les signatures (i.e. un numéro d'identification représenté par une chaîne de caractères). Néanmoins, l'évolution des logiciels malveillants en virus polymorphiques (i.e. qui peuvent changer de forme) et cryptomorphiques (i.e. qui peuvent chiffrer leur contenu) à rendu inefficace ce type de mécanisme. Pour pallier ce problème, des heuristiques plus complexes, comme l'étude du comportement d'une application en cours d'exécution, ont été implémentées. Le site AVTest [7] propose des tests et analyses des principaux antivirus du marché.

Contre-mesures de détection d'intrusion et de fuite de données

Pour réduire les risques liés à la sécurité informatique, un ensemble de contre-mesures vise à s'assurer que le périmètre de l'entreprise n'est pas compromis par un accès non-autorisé, ou qu'une donnée sensible ne sortent pas d'un périmètre préalablement défini.

Mécanismes de détection d'intrusions. L'objectif des mécanismes de détection/prévention d'intrusions (IDS pour *Intrusion Detection System* ou IPS [2] pour *Intrusion Prevention System*) est de prévenir les administrateurs et experts sécurité si une personne, un programme ou un service tente d'accéder à une partie de l'infrastructure qui ne lui était pas autorisé. Pour cela, les IDS et les IPS se divisent en plusieurs catégories :

— Les IDS / IPS réseaux, aussi appelés NIDS / NIPS pour *Network Intrusion Detection System*, dont l'objectif est de détecter les éventuelles intrusions par le réseau.

— Les IDS / IPS hôtes, aussi appelés HIDS / HIPS pour *Host Intrusion Detection Sytem*, dont l'objectif et de détecter les éventuelles intrusions sur différentes machines de l'infrastructure de l'entreprise.

— Les IDS hybrides, qui sont un mélange de NIDS et HIDS.

Pour analyser et détecter des intrusions, les IDS utilisent deux grands types de techniques, celles basées sur le comportement (*behavior-based*) et celles basées sur la connaissance (*knowledge-based*). Les techniques basées sur le comportement apprennent le comportement « traditionnel » de l'entreprise et lèvent des alertes quand un comportement suspect est détecté. Ces techniques sont utiles pour détecter des attaques originales ou inconnues mais nécessitent un temps d'apprentissage plus long. De plus, en fonction du contexte, il n'est pas toujours évident de mettre en exergue un comportement « traditionnel », créant de fait un grand nombre de faux positifs lorsque le comportement de l'entreprise varie légèrement.

Les techniques basées sur la connaissance analysent quant à elles la méthodologie d'attaques connues et existantes dans le but d'identifier des tentatives d'intrusions. Les IDS basés sur ces techniques sont moins soumis à la levée de faux positifs, mais nécessitent des bases de connaissances précises et souvent mises à jour. De plus, ces techniques sont moins efficaces pour les attaques nouvelles et/ou originales. Le marché des IDS est très complet, notamment en ce qui concerne les solutions libres et *open source* (e.g. Snort, Suricata, BroIDS, OSSEC [33]).

Mécanismes contre les fuites de données. Ce type de contre-mesure englobe les mécanismes comme les *Data Leak Prevention/Protection* (DLP) [37] [38]. Comme leur nom l'indique, les DLP consistent à empêcher les fuites et les vols de données. Les DLP peuvent intervenir sur plusieurs parties d'une infrastructure d'entreprise :

— sur les bases de données et les espaces de stockage, afin de protéger les données stockées (DLP de type « *data at rest* »),

— sur des portions du réseau, afin de protéger les données transitantes (DLP de type « *data in motion* »),

— sur les postes clients et serveurs, afin de protéger les données en cours d'utilisation (DLP « *data in use* »).

2. Un IPS est un IDS actif qui permet de prendre des mesures en temps réel.

Quel que soit le type de DLP, ces derniers utilisent différents mécanismes, comme de la reconnaissance de chaînes de caractères (par exemple, pour détecter des numéros de carte de crédit), des techniques d'apprentissage automatique (*machine learning*), ainsi que des règles de contrôle de transmissions. Parmi les principaux acteurs sur le marché, on peut notamment citer Websense, Trend Micro, RSA, Symantec, Palisade Systems, NextLabs, McAfee, Code Green Networks ou encore Sophos.

Mécanismes de monitoring et centre de contrôle. Depuis quelques années, l'industrie se dote de mécanismes permettant la remontée centralisée d'informations. Parmi ces mécanismes, on retrouve le plus souvent les SIEM et les SOC. Une SIEM (*Security Information and Event Management*) est un outil, qui, comme son nom l'indique, est dédié au management d'événements. Pour cela, une SIEM est équipée le plus souvent d'agents s'occupant de charger, convertir, uniformiser, corréler, interpréter et afficher les journaux en provenance de sources hétéroclites, simplifiant *de facto* la tâche, souvent fastidieuse, de l'analyse de journaux d'événements et de la recherche de corrélation.

Néanmoins, les entreprises commencent depuis quelques années à comprendre qu'il est nécessaire de détecter rapidement les attaques, quelle que soit l'heure, et d'offrir des réponses graduées à ces menaces. Ainsi, les SOC (*Security Operation Center*) permettent de répondre à ces besoins, en proposant des centres de supervision dédiés à la sécurité, chargé de détecter des incidents 24 heures sur 24, 7 jours sur 7. Souvent gérées par des prestataires de services spécialisés, les SOC offrent plusieurs avantages. Premièrement, elles permettent une dimension industrielle à la surveillance des journaux. Deuxièmement, elles proposent une grande flexibilité et une grande évolutivité, permettant ainsi d'intégrer de nouveaux journaux et de nouvelles fonctionnalités à mesure que le SI grandit. Enfin, la grande réactivité des SOC en fait l'argument principal face aux méthodes présentées précédemment. Néanmoins, les SOC ont quelques inconvénients, comme le coût de prestation ou d'exploitation, et une perte de maîtrise quand la SOC est proposée par un prestataire externe.

Le choix d'une solution SIEM ou SOC dépend de nombreux paramètres (taille de l'entreprise, sensibilité des données, secteur d'activité, maturité vis-à-vis de la sécurité, etc.). Néanmoins, plusieurs guides existent pour mieux comprendre ces mécanismes et faire son choix [28] [30].

Contre-mesures organisationnelles

Outre les mesures purement techniques, une entreprise peut se doter d'un arsenal opérationnel pour améliorer la sécurité de son système d'information. Ces contre-mesures englobent plusieurs catégories, décrites dans les paragraphes suivants.

Certifications et normes. Comme nous l'avons vu précédemment, la sécurité est avant tout une question d'évaluation. Pour faire cette évaluation, de nombreuses recommandations, guides et normes existent. Parmi ces normes, on peut en premier

lieu citer la famille ISO 27000, qui aide les organisations à définir les processus organisationnels et la méthodologie à suivre pour assurer la sécurité de leurs systèmes d'information, notamment à travers sa norme d'exigence la plus connue, ISO 27001, qui permet la définition d'un « système de management de la sécurité de l'information » (SMSI) [25]. Cette définition du SMSI s'articule autour d'un processus itératif d'amélioration continue, appelé roue de Deming / cycle de Shewhart, dont l'objectif consiste à définir les politiques de sécurité (Plan), mettre en œuvre les outils et mécanismes nécessaires (Do), vérifier via des audits l'efficacité des mécanismes (Check) et d'effectuer des actions correctives en cas de manquement à la sécurité (Act).

Concernant la gestion du risque, plusieurs méthodes d'évaluation de ce dernier existent, comme MEHARI [14] (méthode du CLUSIF), EBIOS [3] (méthode de l'ANSSI), COBIT [18] ou encore ITIL [17]. À noter qu'il n'existe pas de modèle parfait, mais des modèles adaptés à des contextes spécifiques, dont les différences permettent d'orienter la sécurité dans une direction particulière. En effet, ITIL se positionne plus au niveau de la « production » informatique, ISO27001 s'adresse aux managers alors que l'objectif principal de COBIT est de s'inscrire dans la gouvernance d'entreprise. Quelle que soit la méthode choisie, cette dernière doit être scrupuleusement suivie pour pondérer efficacement le risque afin de bien définir les étapes visant à l'amélioration de la sécurité d'une infrastructure d'entreprise.

Planification de la reprise et de la continuité d'activités. De nombreuses entreprises mettent en place, par réelle connaissance des risques ou par effet de mode, des mécanismes de sécurité au sein de leur infrastructure. Néanmoins, il est pertinent de s'intéresser au bon fonctionnement des services pendant et après une crise (pannes, attaques, sinistres, etc.). Pour cela, une entreprise peut définir un Plan de continuité d'activité (PCA) ou un Plan de reprise d'activité (PRA) [19]. Le PCA consiste à définir la liste des moyens mis en place pour garantir le bon fonctionnement des services durant un problème ou une situation de crise. Le PRA, quant à lui, définit les moyens et procédures destinés à assurer une reprise rapide et ordonnée de la production après une situation de crise.

Formation et sensibilisation. Un système d'information est constitué à la fois d'une partie technique, mais aussi d'une partie sociale, qui englobe à la fois une structure organisationnelle et les personnes qui constituent les éléments de cette structure. Ainsi, la robustesse d'un système d'information passe aussi par la sécurisation de cette structure sociale. Pour cela, une entreprise peut décider de sensibiliser son personnel à la sécurité, en le formant notamment à des bonnes pratiques en ce qui concerne l'anonymat sur Internet (par exemple, en évitant qu'un développeur ne soit trop verbeux sur l'écosystème de l'entreprise sur son profil LinkedIn) ou encore le traitement des emails (par exemple, ne pas ouvrir les mails d'expéditeur inconnu). De plus, plusieurs politiques peuvent être mises en place par la direction du système d'information (DSI) et le responsable de la sécurité du système d'information

(RSSI). Ces politiques peuvent traiter des sauvegardes, des changements réguliers et de la complexité des mots de passe, des politiques de contrôle d'accès logiciels et physiques ainsi que du bon respect de principes de sécurité comme la séparation des privilèges, le fait d'utiliser ses machines personnelles dans un contexte professionnel (principe du *Bring Your Own Device*). L'utilisation de recommandations ou normes citées précédemment permet de soulever des questions et de mettre en place ce type de politiques.

Concernant l'écosystème technique, la sensibilisation et la formation des développeurs et des administrateurs est une très bonne chose, notamment en ce qui concerne le développement logiciel (audit de code, analyse en boîte noire ou boîte blanche). En ce qui concerne l'architecture système et réseaux, la mise en place d'outils de monitoring pour les administrateurs, devOps et experts sécurité, est de plus en plus sollicitée dans les entreprises, notamment à travers les SIEM et les SOC.

Contre-mesures juridiques et légales

Une entreprise peut utiliser des moyens juridiques et légaux pour réduire le risque lié à la sécurité. Les paragraphes suivants détaillent les deux principaux mécanismes juridico-légaux que sont le RGPD et les assurances en cybersécurité.

RGPD. Le Règlement général sur la protection des données (RGPD) est entré en application en Europe depuis le 25 mai 2018. Ce règlement est un texte de référence visant à mettre en conformité les entreprises manipulant des données à caractère personnel. Pour cela, le RGPD propose différentes étapes pour faire la cartographie des données manipulées, tenter de minimiser la récolte d'informations, tenir et suivre un registre de traitement et, dans certains cas, effectuer une analyse d'impact. En plus de recommandations, le RPGD exige une transparence de la part des fournisseurs de services qui doivent demander le consentement explicite pour la récolte des données utilisateurs et expliciter un certain nombre de choses, comme le but de la récolte (i.e. pourquoi ces données sont nécessaires), la durée de conservation de ces données, leur localisation ou encore qui peut y accéder. Enfin, le RGPD donne un ensemble de droits aux utilisateurs de services, comme le droit à l'oubli (i.e. permettre à un utilisateur de demander la suppression de ses données personnelles détenues par un tiers), le droit de retirer son consentement ou encore le principe de portabilité des données personnelles (i.e. permettre à un utilisateur de récupérer ses données dans un format ouvert et lisible). La CNIL fournit une bonne documentation pour aider les entreprises dans leur mise en conformité [15].

Cyber-assurances. Depuis quelques années, plusieurs sociétés spécialisées proposent des assurances contre les risques informatiques. On peut citer par exemple :

— la prise en charge des coûts liés à la reconstitution de données perdues,
— la prise en charge des coûts liés à du consulting suite à une attaque informatique (extorsion, rançons, etc.),
— la prise en charge de conséquences financières suite à la perte de données,

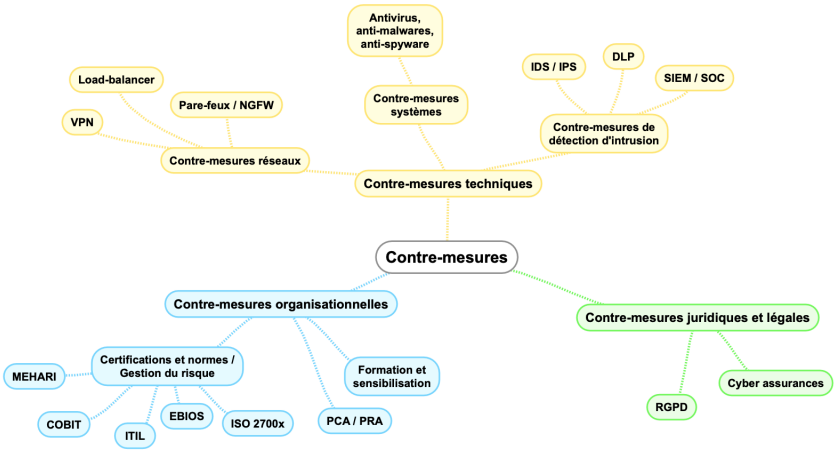

FIGURE 2. Carte heuristique des principales contre-mesures.

— la prise en charge des pertes suite à l'interruption d'un service,
— la prise en charge des coûts de conseils en relation publique en cas de perte d'image et de réputation à la suite d'un incident ou d'une crise.

Ces assurances sont encore très minoritaires en France, mais le marché commence à se développer petit à petit [29], notamment à travers l'élargissement des conditions d'assurances traditionnelles de type IARD (Incendie, accidents et risques divers).

Comme nous venons de le voir, une entreprise peut se doter d'un grand nombre de mécanismes pour réduire les risques et améliorer sa sécurité (voir Figure 2). Ces contre-mesures peuvent à la fois aider à réduire le risque d'attaques sur le réseau (ATK_NET, ATK_INFO) , comme c'est le cas des VPN et des pare-feux, mais aussi améliorer la sécurité des postes clients et des serveurs contre les programmes malveillants (ATK_MAL), notamment en utilisant des mécanismes comme les DLP, les IDS/IPS ou les antivirus. Enfin, des politiques de sécurité bien définies ainsi que la sensibilisation du personnel permettent de réduire les risques liés à l'ingénierie sociale (ATK_SE), aux problèmes de configuration (ATK_CONF), aux attaques sur les systèmes d'exploitation (ATK_OS) et, dans le cas de personnel technique comme des développeurs, à améliorer significativement la qualité de code, réduisant *de facto* le risque d'attaques logicielles (ATK_SOFT) et/ou matérielles (ATK_HARD).

Conclusion

Dans cet article, nous avons vu dans un premier temps les principales menaces inhérentes à la sécurité informatique d'une entreprise. Nous avons mis en lumière

que ces menaces représentaient un risque pour une entreprise, à la fois d'un point de vue économique, mais aussi d'un point de vue social (i.e. image de marque, litige suite à une faute, etc.). De plus, nous avons montré que ce risque pouvait avoir pour source des personnes aux motivations et aux compétences variées (script kiddies, hacktiviste, pirate, etc.) et cibler des parties différentes de l'infrastructure (réseaux, serveurs, logiciels, employés).

Dans un second temps, nous avons présenté les principales contre-mesures pour réduire ce risque. Ces contre-mesures sont nombreuses, mais peuvent être classées en trois grandes catégories, les contre-mesures techniques, les contre-mesures organisationnelles et les contre-mesures juridico-légales. Chacune de ces catégories offre des avantages et des inconvénients sur des critères financiers, logistiques ou encore d'efficacité. Néanmoins, malgré leurs différences, ces contre-mesures partagent un point commun : le fait de ne pas être parfaites ni suffisantes seules. En effet, le fait de se doter d'une solution technique performante et onéreuse ne remplacera pas la sensibilisation des employés, la mise en place de règles strictes et cohérentes ou encore le bon sens et la bonne utilisation des outils informatiques.

De manière analogue, la mise en place de politiques, que se soit dans un contexte organisationnel ou dans le cadre de la mise en conformité du RGPD, nécessite une mise en place technique, comme l'ajout de mécanismes de chiffrement ou encore des mécanismes de contrôle d'accès. Enfin, le choix d'une assurance et les coûts de cette dernière seront grandement déterminés par l'état de santé général de la sécurité de l'entreprise, tant d'un point de vue technique que du point de vue organisationnel.

Ainsi, nous ne pouvons qu'encourager les entreprises à conduire des audits réguliers auprès de professionnels et à diversifier leur arsenal défensif afin de mettre en place un ensemble de processus techniques, juridiques et organisationnels pour fournir une réponse adaptée, cohérente et pérenne.

Références

[1] K. Al Nuaimi, N. Mohamed, M. Al Nuaimi, and J. Al-Jaroodi. A survey of load balancing in cloud computing : Challenges and algorithms. In *Network Cloud Computing and Applications (NCCA), 2012 Second Symposium on*, pages 137–142. IEEE, 2012.

[2] ANSSI. Alerte : Multiples vulnérabilités dans des processeurs ? comprendre Meltdown et Spectre et leur impact. https://www.ssi.gouv.fr/actualite/alerte-multiples-vulnerabilites-dans-des-processeurs-comprendre-meltdown-et-spectre-et-leur-impact, 2018.

[3] ANSSI. Ebios - expression des besoins et identification des objectifs de sécurité. https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/, 2018.

[4] ANSSI. Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à internet. https://www.ssi.gouv.fr/guide/recommandations-pour-choisir-des-pare-feux-maitrises-dans-les-zones-exposees-a-internet/, 2018.

[5] ANSSI. Recommandations sur le nomadisme numerique. https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/, 2018.

[6] arobase.org. Le phishing : exemples d'e-mails piégés. https://www.arobase.org/phishing/exemples-phishing.htm, 2018.

[7] AV-TEST. Av-test | tests indépendants de logiciels antivirus. https://www.av-test.org/fr/, 2019.

[8] A. blog. Meltdown et Spectre, des vulnérabilités majeures touchant presque tous les ordinateurs du monde. https://blog.avast.com/fr/meltdown-et-spectre-des-vulnerabilites-majeures-touchant-presque-tous-les-ordinateurs-du-monde, 2018.

[9] CEDEF. Économie : que pèsent réellement les PME et TPE en france ? https://www.economie.gouv.fr/cedef/definition-petites-et-moyennes-entreprises, 2016.

[10] CERT-FR. Vulnérabilité dans Microsoft Windows. https://www.cert.ssi.gouv.fr/alerte/CERTFR-2018-ALE-009/, 2018.

[11] CERT-FR. Analogic s.r.o. https://default-password.info/, 2019.

[12] CISCO. Rapport sécurité pour les PME - 2018 : Petit mais puissant. https://www.cisco.com/c/dam/global/fr_fr/solutions/small-business/pdf/Cisco_2018_SMB_Security_FR.pdf, 2018.

[13] P. Citron. Malware : en étudiant Wannacry, des chercheurs découvrent Adylkuzz. https://www.presse-citron.net/malware-etudiant-wannacry-chercheurs-decouvrent-adylkuzz/, 2017.

[14] Clusif. Mehari - clusif. https://clusif.fr/mehari/, 2019.

[15] CNIL. RGPD : Par où commencer. https://www.cnil.fr/fr/rgpd-par-ou-commencer, 2018.

[16] J. P. Delahaye. Le Bitcoin, première crypto-monnaie. *Bulletin de la Société Informatique de France*, n° 4, pp. 67–104, octobre 2014.

[17] P. Delbrayelle. Itil france. https://www.itilfrance.com/, 2017.

[18] A. Fernandez. Qu'est-ce que Cobit ? https://www.piloter.org/gouvernance/COBIT_gouvernance_SI.htm, 2018.

[19] Foliateam. PRA / PCA : Comprendre les différences et les avantages. https://www.foliateam.com/pra-pca-comment-choisir-et-quels-avantages/, 2017.

[20] S. A. GERARD. 27 virus informatique ayant marqué l'histoire. https://www.supinfo.com/articles/single/3621-27-virus-informatique-ayant-marque-histoire, 2017.

[21] S. S. Greene. *Security policies and procedures*. New Jersey : Pearson Education, 2006.

[22] Heartbleed.fr. Faille Heartbleed. http://www.heartbleed.fr/, 2014.

[23] I. Incapsula. What is hardware load balancer (hld). https://www.incapsula.com/load-balancing/hardware-load-balancer-hld.html, 2018.

[24] INSEE. Les entreprises en France - INSEE. https://www.insee.fr/fr/statistiques/fichier/3152833/ENTFRA17.pdf, 2016.

[25] ISO. ISO/IEC 27001 management de la sécurité de l'information. https://www.iso.org/fr/isoiec-27001-information-security.html, 2019.

[26] ITSocial. Une TPE et PME sur trois confie la cybersécurité à des employés inexpérimentés. https://itsocial.fr/articles-decideurs/article-etude/1-tpe-pme-3-confie-cybersecurite-a-employes-inexperimentes/, 2018.

[27] N. LABS. Nss labs announces 2018 next generation firewall group test results. https://www.nsslabs.com/company/news/press-releases/nss-labs-announces-2018-next-generation-firewall-group-test-results/, 2018.

[28] L. N. Lacourte. SOC externalisé vs SOC interne : Comment choisir ? https://www.linkbynet.com/fr/comment-choisir-entre-un-soc-externalise-et-un-soc-interne%E2%80%AF/, 2018.

[29] ARGUS de l'assurance. La souscription de cyber-assurance en hausse ? https://www.argusdelassurance.com/acteurs/la-souscription-de-cyber-assurance-en-hausse.125743, 2018.

[30] L. V. Marchive. Choisir un SIEM commence par la définition de ses besoins. https://www.lemagit.fr/conseil/Choisir-un-SIEM-commence-par-la-definition-de-ses-besoins, 2017.

[31] B. Martin. *Codage, cryptologie et applications*. PPUR presses polytechniques, 2004.

[32] K. D. Mitnick and W. L. Simon. *The art of deception : Controlling the human element of security*. John Wiley & Sons, 2011.

[33] A. Nayyar. The best open source network intrusion detection tools. https://opensourceforu.com/2017/04/best-open-source-network-intrusion-detection-tools/, 2017.

[34] NextImpact. Github a survécu à une attaque DDOS de 1,3 tbps, OVH réagit. https://www.nextinpact.com/brief/github-a-survecu-a-une-attaque-ddos-de-1-3-tbps--ovh-reagit-2919.htm, 2018.

[35] PsychzNetworks. Software vs hadware load balancer. https://www.psychz.net/client/question/en/software-vs-hardware-load-balancer.html, 2017.

[36] re.sources. CEDEF - comment définit-on les petites et moyennes entreprises. http://resources.grouperandstad.fr/decryptages/economie-que-pesent-reellement-les-pme-et-tpe-en-france/, 2016.

[37] A. Shabtai, Y. Elovici, and L. Rokach. *A survey of data leakage detection and prevention solutions*. Springer Science & Business Media, 2012.

[38] B. L. Wavestone Thibault JOUBERT. DLP : Éviter les fuites, sans colmater les brèches. https://www.riskinsight-wavestone.com/2018/04/dlp-eviter-fuites-sans-colmater-breches/, 2018.

[39] ZDNet. OVH noyé par une attaque DDOS sans précédent. https://www.zdnet.fr/actualites/ovh-noye-par-une-attaque-ddos-sans-precedent-39842490.htm, 2016.