La sensibilisation des collaborateurs d'une organisation aux risques informatiques : élément incontournable ?

Élise Vernier

Rapport SI

La sensibilisation des collaborateurs d'une organisation aux risques informatiques : élément incontournable ?

Présenté par : VERNIER Elise

Tuteur universitaire : PEREA Céline

Master 1 pro. FI
Master Management des Systèmes d'Information
2019 - 2020

Rapport SI

La sensibilisation des collaborateurs d'une organisation aux risques informatiques : élément incontournable ?

Présenté par : VERNIER Elise

Tuteur universitaire : PEREA Céline

Master 1 pro. FI
Master Management des Systèmes d'Information
2019 - 2020

Avertissement :

Grenoble IAE, au sein de l'Université Grenoble Alpes, n'entend donner aucune approbation ni improbation aux opinions émises dans les mémoires des candidats aux masters en alternance : ces opinions doivent être considérées comme propres à leur auteur.

Tenant compte de la confidentialité des informations ayant trait à telle ou telle entreprise, une éventuelle diffusion relève de la seule responsabilité de l'auteur et ne peut être faite sans son accord.

RÉSUMÉ

Est-ce que la sensibilisation des utilisateurs d'une organisation aux risques informatiques est-elle un facteur important de la sécurité des systèmes d'information ? C'est à cette question que nous allons essayer de répondre tout au long de ce document. A travers de nombreux articles et exemples, nous parviendrons à établir la place de l'Homme dans la Politique de Sécurité des Systèmes d'Information ou PSSI et nous donnerons des solutions aux entreprises pour rendre l'utilisateur des outils informatiques acteur et responsable de la cyber-sécurité et non « l'angle mort » de celle-ci.

SUMMARY

We want to know if the awareness of users about the IT risks is an important factor in the security of organization's information systems. We will try to find the answer throughout this document. After reading articles and examples, we will establish the place of human in the Information Systems Security Policy or ISSP and give solutions to companies to make the user of IT tools actor and responsible of cyber-security and not the "blind spot" of it.

MOTS CLÉS : Politique de Sécurité des Systèmes d'Information ou PSSI, cyber-sécurité, utilisateur, entreprise, sensibilisation, risques informatique, crise, télétravail, nomadisme numérique, ISSP, Cyber-Security, user, Company, Awareness, IT risks, crisis, home-working, digital nomadism

SOMMAIRE

AVANT-PROPOS

Ayant été obligée de travailler à distance comme de nombreux étudiants ou salariés pendant ce confinement, je me suis demandée si ce mode de travail n'aura pas un impact sur la sécurité des données d'une organisation, qu'elle soit publique ou privée. En effet, nous avons dû nous adapter subitement au travail à distance, alors que la plupart des organismes n'y étaient pas, ou peu, préparés que ce soit en terme de management des personnes, techniquement ou même technologiquement, alors concernant les risques informatiques qu'ont-ils fait ? Et comment ?

Afin de répondre à cela, j'ai mené de nombreuses recherches sur les cyber-menaces et sur leur évolution durant cette crise sanitaire que nous traversons. J'ai fini par faire un état des lieux de la cyber-sécurité dans les entreprises pour me rendre compte que malgré la diversité des solutions techniques, des types et tailles d'entreprises et de nombreux autres facteurs tous différents, il existait un seul point commun entre tous : la sensibilisation de l'utilisateur. Ce dernier est un maillon faible de la sécurité informatique, que nous oublions souvent, tout en étant le dernier rempart contre les cybercriminels. Comment faire comprendre aux entreprises son importance ?

Ce ne fut pas simple de trouver la réponse à cette ultime question sans aborder de manière générale la Politique de Sécurité des SI et de ses composantes à mettre en place dans une entreprise. En prenant en compte tous ces paramètres, j'ai réalisé que la sécurité informatique d'une organisation n'avait pas un seul facteur important, l'utilisateur, mais aussi différentes autres caractéristiques, aussi bien techniques que technologiques et même également méthodologiques, qui font que celle-ci dispose d'un ensemble de moyens de protection qui peuvent lui faire éviter beaucoup de cyber-attaques. J'espère que la lecture de ce document permettra d'apporter des éclaircissement sur la place de l'Homme dans les enjeux de cyber-sécurité, tout en apportant des solutions sur une sensibilisation aux risques efficace.

INTRODUCTION

En ce printemps 2020, nous vivons une situation que nous ne pensions jamais vivre : un confinement mondial et un arrêt brutal de toute Economie. Cette crise sanitaire, causée par le virus nommé Covid-19, que nous pensions vaincre comme toutes les autres, nous a complètement prise de cours et a paralysé des pays entiers. A l'ère où les flux humains, alimentaires, industriels ou même d'informations n'ont jamais été aussi intenses, nous nous retrouvons bloqués et nous devons, pour notre sécurité et celle des autres, rester confinés.

Dans ce cadre justement, les différentes organisations publiques ou privées ont été obligées de s'organiser pour maintenir un approvisionnement de la population en ressources nécessaires et d'imposer, pour celles qui n'étaient pas vitales, une pause dans leurs activités ou tout du moins à distance. Cela a donc entrainé une mise en place du télétravail pour beaucoup d'entre elles et surtout pour celles qui le pouvaient.

Pour des entreprises qui avaient l'habitude du travail à distance, ce ne fût pas un problème mais pour celles qui n'avaient jamais mis cela en place, ceci s'est avéré être un nouveau challenge et pas qu'en matière de flexibilité mais aussi en terme de sécurité des données sensibles : financières, commerciales, administratives… On peut alors se demander si le télétravail ou nomadisme numérique présente un risque informatique important et si le fait de l'imposer sans pouvoir sensibiliser les employés ne va pas créer des failles de sécurité ?

L'étude de différents articles professionnels à ce sujet a démontré ce mode de travail présentait effectivement des risques pour la cyber-sécurité et que les utilisateurs, qu'ils soient en internes ou externes (prestataires, partenaires ou clients), étaient des cibles de choix pour les cybercriminels. Mais alors quelle est leur place dans la sécurité des systèmes d'information d'une société ? Quel est l'impact sur celle-ci de leur manque de sensibilisation aux risques informatiques ? Quels sont les moyens à mettre en place dans les entreprises pour éviter ou prévenir les cyber-attaques ? Ce sont à ces différentes questions que nous allons tenter de répondre dans ce document.

PARTIE 1 :
-
PRESENTATION DU PROBLEME

CHAPITRE 1 – PROBLEMATIQUE & ENJEUX

Dans ce premier chapitre, nous présenterons le sujet de ce rapport, ses enjeux pour les organisations publiques ou privées et plus précisément pour les services métiers concernés.

I. INTRODUCTION

Nous voulons aborder dans ce document un mode de travail en plein évolution et qui s'est imposé ces derniers mois à cause de la crise sanitaire : le télétravail ou nomadisme numérique.

Figure 1 : Illustration du télétravail (image libre de droit)

Beaucoup d'entreprises qui le pouvaient ont été obligées de continuer leur activité à distance et, après l'étude de nombreux articles (qui seront présentés plus tard dans le document), nous pouvons voir que ce mode, bien qu'il présente de nombreux avantages, surtout en matière de flexibilité et d'adaptation, présente des failles de cyber-sécurité. Surtout s'il a été instauré dans la précipitation.

Nous serons amenés ainsi à présenter la thématique suivante : la sécurité des données d'une organisation lors d'un nomadisme numérique imposé. Après une recherche approfondie dans la presse quotidienne et professionnelle, un facteur important de la cyber-sécurité s'est distingué : l'utilisateur et son degré de sensibilité aux risques de cyber-malveillance.

Cela nous fait poser la problématique suivante :

Est-ce que la sensibilisation des utilisateurs aux risques informatiques est l'élément le plus important dans la Politique de Sécurité du SI[1] ?

II. ENJEUX

La réponse à la problématique ci-dessus permettra de mettre en lumière l'importance d'une tactique de réponse aux risques informatiques ou plus couramment appelée la politique de sécurité des systèmes d'information (PSSI). Elle aura pour but de préparer les services informatiques à se poser les questions essentielles en matière de cyber-sécurité en terme de technicité et d'un point de vue assez inattendu celui du management des personnes. En effet aborder la cyber-sécurité d'un regard seulement technique recouvre une partie du problème et ne prend pas en compte les utilisateurs. Ce seront ces autres personnes qui sont visées à travers ce document.

La sécurité des données d'une entreprises n'est pas seulement du ressort de son service informatique et des moyens qu'ils ont mis en place, mais aussi de toute la direction générale, de la sécurité classique et d'un acteur souvent sous-estimé : l'utilisateur.

Le déroulement de ces recherches et la mise en place du plan pour répondre à cette problématique sera décrite dans le prochain chapitre.

[1] SI : Abréviation de Système d'Information

CHAPITRE 2 – ORGANISATION DE LA RECHERCHE

Dans ce chapitre, nous expliquerons quel chemin prendre pour répondre au mieux à la problématique introduite précédemment.

Une première réflexion sur le plan de recherches et d'organisation de travail sera réalisée et celui-ci sera décrit et expliqué. Dans la deuxième partie de ce rapport, nous reviendrons sur ce plan et sur l'élaboration du document et nous pourrons faire un bilan de tout ceci.

I. REFLEXION SUR LE PLAN

A travers la problématique suivante : « Est-ce que la sensibilisation des utilisateurs aux risques informatiques est l'élément le plus important dans la Politique de Sécurité du SI ? », nous voulons mettre en avant ce qu'est la PSSI, ses composantes et l'impact des utilisateurs sur celle-ci.

Mais avant d'en venir directement au problème il est nécessaire de rappeler comment nous en sommes venus à la thématique principale qui est le nomadisme numérique imposé et pourquoi c'est un sujet d'actualité très important en ce moment. Il sera important d'expliquer pourquoi, en partant de cette idée générale, nous en sommes venus à parler de la cyber-sécurité et surtout de la cyber-malveillance et des différentes attaques possibles contre les professionnels principalement (choisis par défaut dans ce rapport).

Une fois le contexte expliqué et détaillé à l'aide de recherches effectuées sur différentes sources médiatiques et professionnelles, nous pourrons faire le point sur les possibles failles des organisations publiques ou privées et aborder un facteur important : l'utilisateur et son impact sur la PSSI. Ceci introduira la problématique et apportera des précisions sur la PSSI, sur ses composantes et sur le niveau d'implication des utilisateurs dans celle-ci.

Enfin nous pourrons, après une étude plus approfondie d'articles professionnels et académiques, apporter des solutions diverses et adaptées à chaque société et des conseils d'organisation et de sensibilisations des utilisateurs pour essayer au maximum d'éviter ou prévenir les cyber-attaques.

II. PLAN

Suite aux réflexions faites plus haut, nous pouvons ainsi répondre à la problématique en présentant le document suivant selon le plan suivant :

- Dans un premier temps, un état des lieux de la situation sera faite. La thématique du nomadisme numérique imposé ainsi que la problématique seront expliquées et contextualisés à travers des articles de presse professionnelle.
- Dans un deuxième temps, il y aura une présentation plus précise des recherches dans les presses professionnelles et académiques afin de faire le point sur les différentes composantes d'une PSSI et de voir au fur et à mesure de l'étude l'impact de l'utilisateur sur la sécurité des données d'une organisation.

  Nous verrons également quelles solutions ces différents auteurs apportent en terme de sensibilisation efficace.
- Une fois les résultats de ces recherches obtenus, nous pourrons essayer de répondre à la problématique et proposer différentes solutions à mettre en place aux organisations : techniques, technologiques, méthodologiques et surtout humaines.

CHAPITRE 3 – ÉLABORATION DU RAPPORT

Après avoir parlé de la recherche et du plan, qui sera mis en place pour répondre au mieux à la problématique, nous nous intéressons maintenant à l'élaboration du rapport.

Nous présentons, dans ce chapitre, l'organisation générale du travail à réaliser en vue de rendre un rapport complet et répondant à la problématique en temps et en heure en fonctions des livrables demandés par le tuteur enseignant (ici une tutrice enseignante).

Pour cela nous utilisons un outil important dans la gestion de projet : le diagramme de Gantt. Il permet en une vue d'avoir l'avancement du projet, de le suivre et de quantifier le temps à passer sur chaque tâche.

I. PRESENTATION DU GANTT ET IMPERATIFS

Avant de présenter le diagramme de Gantt voici une liste des livrables qui jalonne ce projet et dont il a fallu tenir compte dans l'élaboration du rapport :

Date	Échanges avec la tutrice IAE
Début avril	Démarrage du travail sur le rapport
9 Avril 2020	Validation Thématique du rapport
27 avril 2020	Validation Problématique et Gantt
18 mai 2020	Validation de Références clés parmi la documentation
30 juin 2020	Analyse sur le Gantt après fin écriture du rapport
	Envoi du rapport définitif

Tableau 1 : Livrables du Rapport SI

En page suivante voici le Gantt de l'élaboration du rapport.

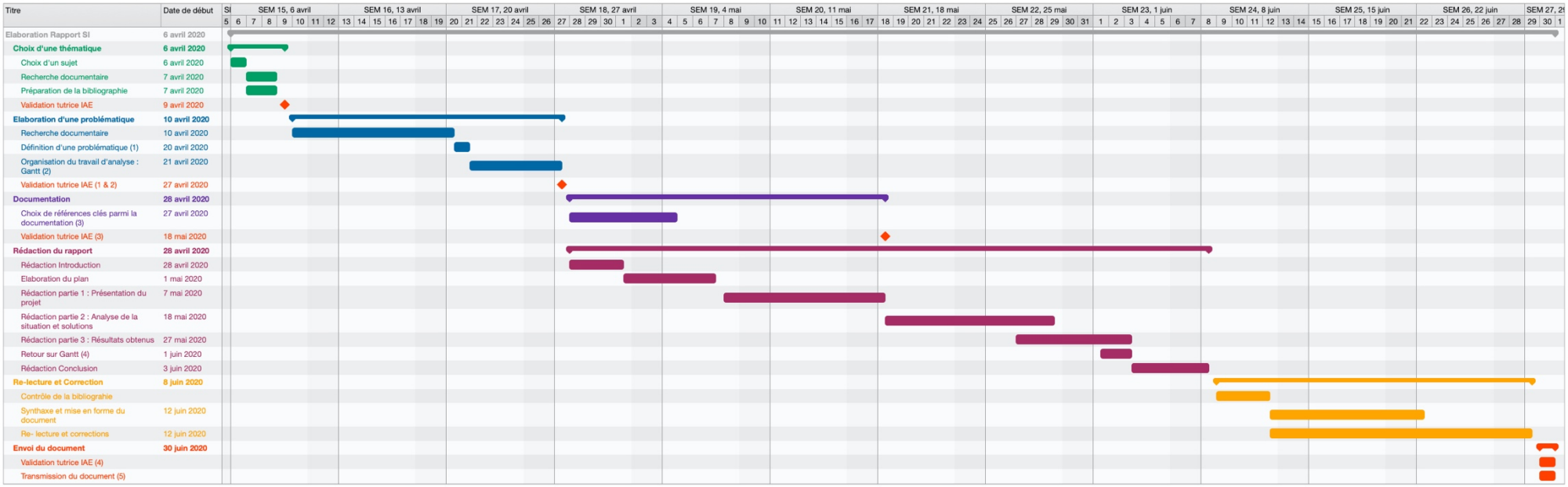


Figure 2 : Diagramme de Gantt du Rapport SI

II. ANALYSE DU GANTT : CHOIX ET OBJECTIFS

Choix faits sur la gestion de ce projet :

- Séparation de l'élaboration du rapport en 6 parties distinctes
- Jalon à chaque date clé
- Optimisation du temps rédactionnel : début de rédaction en parallèle de la recherche (parties 3 et 4).
- Temps important accordé à la correction et à la relecture du document
- Volonté de ne pas envoyer le document avant la fin pour éviter la précipitation.

PARTIE 2
-
ANALYSE DE LA SITUATION ET SOLUTIONS

CHAPITRE 4 – ANALYSE DE LA SITUATION

Dans ce chapitre, une approche détaillée de la thématique de ce mémoire et de ses limites, **la sécurité des données lors d'un nomadisme numérique imposé**, sera réalisée ainsi qu'une présentation des différentes recherches préliminaires (presse hebdomadaire, professionnelle et gouvernementale) menées dessus.

Ces études nous permettront d'avoir un état des lieux de la situation actuelle en terme de sécurité des données en temps de crise et de voir vers quel chemin se diriger pour répondre efficacement à notre problématique.

I. RECHERCHES PRELIMINAIRES

Comme précisé en introduction, nous nous intéressons tout d'abord à un grand sujet d'actualité : le nomadisme numérique.

Cette thématique est venue tout naturellement vu que nous nous sommes tous retrouvés, à cause de la crise sanitaire que nous traversons, dans une typologie de travail bien connue dans le domaine des Systèmes d'Information mais assez inattendue pour beaucoup d'autres secteurs d'activité ou petites structures : le télétravail ou nomadisme numérique.

Le nomadisme numérique, d'après l'Agence Nationale de la Sécurité des Systèmes d'Information, (ANSSI),

« désigne toute forme d'utilisation des technologies de l'information permettant à un utilisateur d'accéder au SI de son entité d'appartenance ou d'emploi, depuis des lieux distants, ces lieux n'étant pas maîtrisés par l'entité ».

Grâce à ce système de travail, les organisations ont pu mettre en place des mesures pour permettre aux services administratifs, commerciaux ou tout autre service informatisé de travailler à distance, pour la plupart, quand cela était possible ou nécessaire.

En effet, dans certains secteurs comme l'artisanat ou le BTP, par exemple, les employés ne pouvaient pas travailler à distance et n'utilisaient donc pas les outils numériques. Vu que cette situation n'était ni commune, ni volontaire, nous allons aborder ici les termes de « nomadisme numérique imposé ». Les organisations n'ayant pas eu le choix, pour continuer à pérenniser leur activité, de forcer tous les employés et services qui le pouvaient à travailler à distance.

Après une étude du sujet et la réalisation d'un *mind mapping* (voir ci-dessous) en vue de préciser le sujet de recherche, nous pouvons nous interroger sur de nombreux points :

- Cette solution du travail à domicile si vite adoptée ne présente-t-elle pas des failles pour une entreprise ?
- Les organisations dans la précipitation se sont-elles bien préparées à cette crise et à ce mode de travail et de management ?
- Quelles sont les garanties pour que les données sensibles d'une organisation, peu importe sa taille, soient en sécurité alors que les employés ne travaillent plus en présentiel, mais à distance ?
- Quelles sont les mesures prises et sont-elles vraiment efficaces ?

Afin de débuter les recherches , il a été nécessaire de décrire le sujet avec précision et d'en poser les limites. Pour cela, aidé du *mind mapping*, on a ciblé les différents mots clés à utiliser pour nos recherches dans la presse quotidienne puis professionnelle.

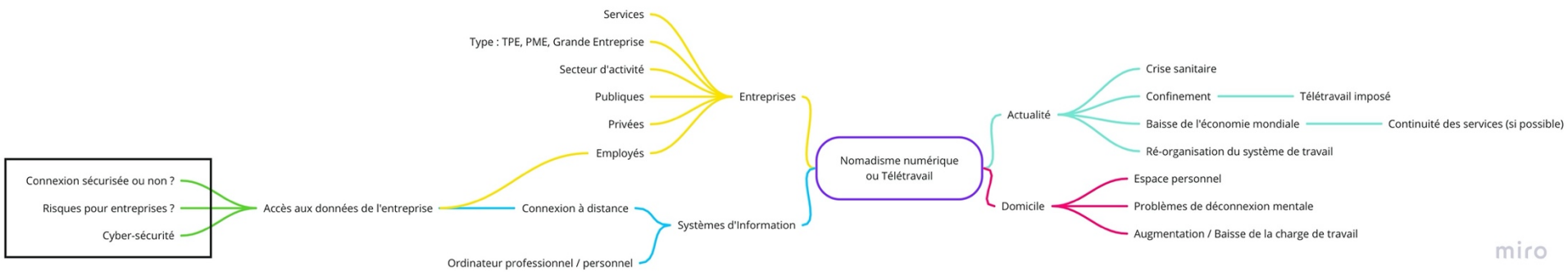


Figure 3 : Mind Mapping - Nomadisme numérique

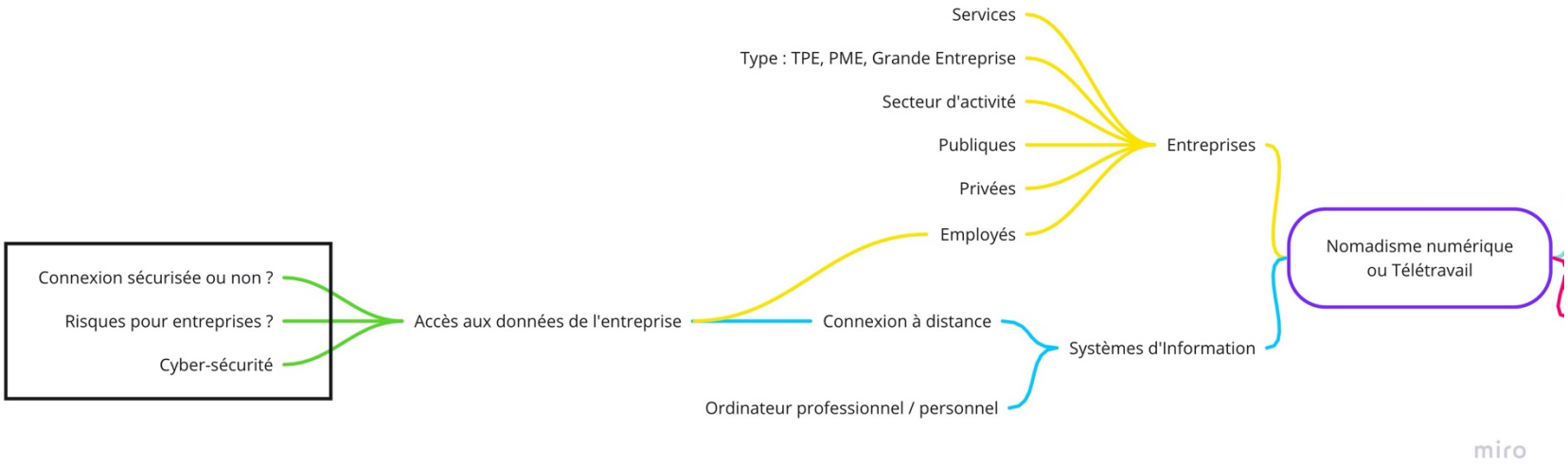


Figure 4 : Zoom du mind mapping sur la thématique

Grâce à cet outil ci-dessus nous avons pu cibler les mots clés importants pour débuter nos recherches sur la thématique suivante : la sécurité des données d'une organisation pendant un nomadisme numérique imposé.

Voici ceux que nous avons choisi :

Mots clés généraux :

- Télétravail,
- Sécurité des données,
- Cyber-malveillance ou Cybercriminalité ,
- Cyber-sécurité,
- Entreprise ou Organisation
- Travail

Mots clés liés à l'actualité :

- Crise,
- Covid-19,
- Coronavirus,
- Confinement

II. ÉTUDE DE LA THEMATIQUE

Nous abordons maintenant les différentes sources de documentation trouvées sur notre thématique et un résumé succinct des plus pertinentes sera fait pour chacune.

Les premières recherches effectuées ont été faites sur les sites de presse hebdomadaire, comme *France Info* ou *Le Monde*, des sites de presse professionnelle, comme *Le Big Data* ou *Le Monde Informatique*, ou encore des sites gouvernementaux comme l'*ANSSI* ou *Cyber-malveillance.gouv* .

- Les sites de presse hebdomadaire ont permis de voir l'évolution du taux de cyber-malveillance pendant la crise sanitaire et les attaques qu'ont subi certaines entreprises et autres organisations.
- Les sites de presse professionnelle ont permis de voir les risques de cyber-sécurité liés au télétravail et les moyens de les contrer mais sous forme de différents reportages.
- Et les sites officiels du gouvernement, quant à eux, fournissent de précieuses informations, conseils et contacts aux entreprises, comme aux particuliers, contre la cyber-malveillance et les cyber-attaques.

Les recherches ont débuté par des sites de presse quotidienne pour savoir s'il y a eu une augmentation de la cybercriminalité pendant le confinement et, d'après le média d'information *France Inter*, celle-ci a explosé depuis l'annonce de la crise sanitaire. En effet, dans un article écrit par Emmanuel LECLERE où il interroge deux experts français de sociétés privées de surveillance et de protection des données, l'un deux explique que depuis janvier 2020, les attaques ont augmenté de

30 000 %. Elles sont principalement de 3 types : hameçonnage[2] (phishing), logiciels malveillants (malwares) et nombreux sites malicieux qui ciblent les utilisateurs à distance.

« En janvier, on avait constaté 1200 attaques informatiques liées au Covid-19… et on était à 380 000 cyberattaques début avril ! ». Didier SCHREIBER – Directeur Marketing chez Zscaler

Ils informent également que les hackers se sont bien adaptés à cette crise et utilisent la crainte des personnes avec des attaques différentes :

- des sites promettant des remèdes contre le coronavirus,
- des faux sites de vente de masques,
- des mails venant de sites gouvernementaux, comme Pôle Emploi, et leur demandant des coordonnées bancaires entre autres,
- et pleins d'autres exemples…

Même les professionnels sont touchés : des mails, venant à première vue de l'entreprise via les VPN[3], mais qui en fait sont des faux et contiennent des liens viraux. Ou encore, des codes malveillants présents au moment de saisir les coordonnées bancaires de certains sites d'e-commerce, créés pour certains trop rapidement par de petites sociétés de proximité pour pallier la perte de chiffre d'affaires pendant le confinement.

Cet article nous fournit de très nombreux exemples de cyber-malveillance ainsi que leur augmentation avec la crise et le confinement. Toutes les failles sont exploitées et nous pouvons noter que les salariés qui travaillent à distance sont des cibles de choix pour les cybercriminels.

De manière plus précise, les sites de presse professionnelle nous expliquent que le nomadisme numérique ou télétravail (le second mot étant plus pertinent lors de la recherche) présente des risques de cybercriminalité plus accrue que lors d'un travail effectué en présentiel. Selon l'article du site *Le Big Data*, ce mode de travail présente une grave menace pour la cyber-sécurité des entreprises. Les cybercriminels peuvent piéger les employés travaillant hors des locaux de l'entreprise avec des faux logiciels ou contrefaçons habituellement utilisés pour la communication à distance, comme Zoom ou Microsoft Teams.

[2] Hameçonnage ou phishing : Principe consistant à récupérer des données personnelles sur internet afin d'usurper l'identité des organisations privées ou publiques, que ce soit financières ou administratives. Définition venant du Portail de l'Économie, des Finances, de l'Action et des Comptes Publics.

[3] VPN : Virtual Private Network ou Réseau Privé Virtuel, d'après Wikipedia, est un système permettant créer un lien direct entre ordinateurs distants de manière privée et sécurisée. Les flux d'information se font par un réseau privé et non public.

Ou encore, ils peuvent pirater directement l'appareil de l'utilisateur car celui-ci n'est pas assez protégé : logiciel de protection non mis à jour, mots de passe peu efficaces (ou réutilisés) ou utilisation d'un appareil personnel.

Il est spécifié également que, pendant cette période de crise, la protection informatique des entreprises n'a pas été une priorité et les employés n'ont pas du tout été sensibilisés ou formés aux risques qu'ils pouvaient encourir en terme de sécurité de données professionnelles. Plus précisément, dans l'article de *L'Usine Digitale*, qui date déjà de Mars 2017 et qui s'appuie sur une étude Symantec , 86 % salariés français déclarent accéder aux informations sensibles de leur société à travers d'outils nomades ou personnels et 42 % indiquent « ne pas mettre à jour constamment leurs paramètres de sécurité ». Ce sont des facteurs qui influencent dangereusement les risques de cyber-attaques.

En parallèle de nos recherches, nous avons remarqué aussi que de nombreux sites professionnels et gouvernementaux apportent des conseils sur les différentes manières de protéger efficacement les réseaux et SI des entreprises, mais sont d'accord sur un facteur important de la cyber-sécurité : **les utilisateurs**.

La web-conférence sur la cyber-sécurité présentée par le magazine professionnel *Le Monde Informatique* est aussi très enrichissante à ce sujet. De nombreux débats et interventions faits par des invités professionnels de l'informatique et de la cyber-sécurité présentent aux organisations différents types de cyber-attaques et les manières de s'en défendre.

Ils existent d'après eux deux types principales d'attaques :

- Les sophistiquées : utilisant des logiciels intelligents ou IA[4] capables de briser les défenses numériques des entreprises et récupérant les informations financières et administratrives clés.

  Comme pour le cas de la société Easy Jet, la compagnie aérienne anglaise, qui au 19 mai 2020 a subi une cyber-attaque visant les données de millions de voyageurs.

[4] IA : D'après Wikipedia, l'Intelligence Articificielle est « l'ensemble des théories et des techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence ». Elles sont ainsi utilisées dans tous les domaines y compris dans la cyber-sécurité et de manière inattendue depuis 2019 dans la cyber-malveillance, d'après Ondrej Vlcek, PDG d'Avast.

D'après le site de presse *Le Monde*, celle-ci fut très sophistiquée et pour 2208 passagers, la situation est plus inquiétante : leurs données bancaires ont été utilisées par les cybercriminels.

- Les standards (les plus utilisés) : phishing ou hameçonnage, ransomwares[5], fraude au faux fournisseur[6] ou effacement d'un site institutionnel entier, mais il existe de nombreux autres exemples.

  Comme pour le cas de la société Fnac-Darty qui, selon l'article de *Capital*, a informé très récemment (le 23/06/2020) ses clients de risques de phishing.

Il existent différentes solutions applicables suivant la taille des organisations :

- Utiliser d'un VPN sécurisé
- Mettre en place une redondance des sauvegardes,
- Cloisonner les différentes données,
- Utiliser un hébergement interne,
- Ou utiliser un cloud sécurisé ou Saas[7] avec les outils qu'il propose : antivirus nouvelle génération, contenir les attaques en ligne, analyse et installation plus rapide
- Méthode EBIOS[8]
- Avoir une protection complète et à jour
- Chiffrer les serveurs

Mais une seule est réellement commune à tous : **la sensibilisation des utilisateurs**.

Cette dernière revient très régulièrement tout au long de cette web conférence et les différents intervenants mettent l'accent sur le fait que, si les personnes ne sont pas sensibilisées, toutes les protections techniques ou technologiques deviennent inutiles.

[5] Ransomwares : Logiciels malveillants bloquants l'accès à l'ordinateur, à des fichiers ou autres données sensibles en les chiffrant et réclamant une rançon à la victime pour y avoir à nouveau l'accès.
Définition d'après le site gouvernemental Cyber-malveillance

[6] Fraude au faux fournisseurs : Le cybercriminel se fait passer pour le fournisseur d'une entreprise et demande les paiements de vraies factures émises par le vrai fournisseur.
Définition d'après le site Les Echos

[7] Saas : Logiciel en tant que service – Modèle de distribution de logiciel à travers le Cloud où les applications sont hébergées non pas par l'entreprise mais par un fournisseur de service et procure l'accès aux informations via internet.
Définition d'après les cours sur les Progiciels de Gestion Intégrés ou PGI de M. Olivier Lavastre – 2019-2020 IAE de Grenoble

[8] EBIOS : Expression des Besoins et Indentification des Objets de Sécurité – Outil complet de gestion des risques relatifs à la sécurité des systèmes d'information mis place par l'ANSSI. Elle permet d'évaluer les risques informatiques et aide à la construction d'une politique de sécurité des systèmes d'information (PSSI) adaptée aux risques identifiés. Voir Annexe 2

III. PROBLEMATIQUE

Suite à ces recherches préliminaires, nous pouvons ainsi voir qu'un des importants facteurs de risque en terme de cyber-malveillance est l'utilisateur. En effet, le projet principal des hackers est d'atteindre les données des entreprises afin de les utiliser à des fins criminels et le seul paramètre qui présente encore des incertitudes reste les utilisateurs des systèmes d'information.

Nous pouvons alors nous demander si en expliquant et en sensibilisant les utilisateurs aux risques, ces derniers pouvaient être réduits, voire évités ?

C'est à ce que nous allons finalement essayer de répondre dans ce rapport :

Est-ce que la sensibilisation des utilisateurs aux risques informatiques est l'élément le plus important dans la Politique de Sécurité du SI ?

Avant de nous focaliser sur les recherches académiques et professionnelles, la problématique doit être expliquée afin de cibler les champs de recherche utiles à l'obtention de réponses et de solutions efficaces.

Premièrement, nous allons définir ce qu'on entend par sensibilisation des utilisateurs et quels sont les types d'utilisateurs qui sont visés ici. D'après le Larousse, la sensibilisation est l'acte par lequel nous rendons une personne ou un groupe réceptif à quelque chose auquel il ne manifestait pas ou peu d'intérêt. Le groupe que nous visons ici est celui des utilisateurs de SI d'une organisation, publique ou privée, qui ne font pas parti du service informatique et qui ne connaissent rien aux risques informatiques. Généralement ces personnes sont formées à l'utilisation des différents outils informatiques mis à leur disposition afin d'accomplir leur travail mais ne sont pas conscients de l'environnement qu'elles manipulent, surtout en travaillant à distance.

Nous pouvons ensuite faire un rappel des différents risques informatiques auxquels les entreprises sont soumis tous les jours. Comme il a été précisé plus tôt dans la partie « Étude de la thématique », il existe deux types de risques, sophistiqués et standards, dont une liste exhaustive a été présentée. Mais voici un rappel plus général, proposé par le site *Sécurité Info* :

- les virus et programmes malveillants ou malwares,
- les emails frauduleux,
- le piratage,
- l'espionnage industriel,
- la malversation,
- la perte d'information confidentielles,
- l'erreur de manipulation.

D'après le site gouvernemental ANSSI, ces risques ont trois buts principaux : **déstabiliser, saboter ou espionner** l'organisation qui est visée par le *hacker* (en) ou cybercriminel.

Enfin nous pouvons aborder un point important de notre problématique et de notre rapport : la PSSI ou Politique de Sécurité des Systèmes d'Information. Celle-ci reflète, toujours d'après le site de l'ANSSI, « la **vision stratégique** de la direction de l'organisme (PME, PMI, industrie, administration…) en matière de sécurité des systèmes d'information (SSI). ». Ce guide, élaboré par les responsables SSI, a pour but de réunir toutes les règles et procédures à suivre afin de garantir une bonne sécurité de l'information au sein d'une entreprise privée ou publique[9]. Il est établi suite à une analyse des risques informatiques et, après une validation du contenu par les responsables de la SSI et de la direction générale, diffusée à l'ensemble des acteurs du SI : utilisateurs, exploitants, sous-traitants et prestataires.

Nous verrons dans le chapitre suivant les composantes d'une PSSI et les conseils pour une mise en application efficace grâce à l'étude d'articles académiques et professionnels. Cela permettra également de mesurer l'impact des utilisateurs sur les risques informatiques et de voir si leur sensibilisation peut influer sur la cyber-sécurité d'une entreprise.

[9] Définitions et informations résumées sur le site Wikipedia, basé sur les informations de l'ANSSI.

CHAPITRE 5 – ANALYSE DES ARTICLES ACADEMIQUES

Comme précisé dans le chapitre précédent, nous allons maintenant essayer de répondre à notre problématique : « Est-ce que la sensibilisation des utilisateurs aux risques informatiques est l'élément le plus important dans la Politique de Sécurité du SI ? », grâce à de nombreuses sources professionnelles, gouvernementales et académiques.

Les sources suivantes ont été choisies et seront décrites ci-après :

- Documentation gouvernementale : ANSSI et à leurs documents *PSSI Méthodologie* qui « présente, de façon détaillée, la conduite de projet d'élaboration d'une PSSI, ainsi que des recommandations pour la construction des règles de sécurité » et *Méthode EBIOS* qui « ne protège pas des risques, mais fait prendre conscience aux décideurs ».

- Documentation académique :

- « En matière de sécurité des systèmes d'information, normalisation et standardisation sont-ils des facteurs d'efficacité ? » - de Etienne DE SEREVILLE
- « L'analyse du risque cyber, emblématique d'un dialogue nécessaire » - de Frédérick DOUZET et Sébastien HEON
- « La place de l'homme dans les enjeux de cyber-sécurité » - de Claude WEBER et Jean-Philippe
- « Espionnage, attaques subversives et cyber-sécurité : de l'impact des actions de « social engineering » et des vulnérabilités humaines sur la sécurité globale des entreprises » – de Franck DECLOQUEMENT

- Documentation professionnelle : l'article du site *Stormshield* « L'humain, clé de la cyber-sécurité des entreprises », écrit par Victor POITEVIN, qui explique que le maillon humain est très important dans une PSSI.

Ces articles seront présentés dans un ordre précis de réflexion sur l'impact de l'homme sur la PSSI d'une organisation : partant tout d'abord de la PSSI, de l'analyse des risques à son application en entreprise, en prenant en compte la méthodologie de mise en place, et allant ensuite aborder la place de l'homme dans la SSI.

Cela nous amènera à nous demander quelles sont les actions à mener, qu'elles soient méthodologiques, techniques ou humaines, pour que la SSI d'une organisation soit le plus efficace possible et adaptable à différentes tailles d'entreprise ?

I. DOCUMENTATION GOUVERNEMENTALE

La documentation gouvernementale provenant de l'ANSSI ou du site Cyber-malveillance donne aux entreprises les conseils et de nombreux moyens méthodologiques pour une mise en place d'une PSSI efficace.

Elle se construit suivant la méthodologie suivante :

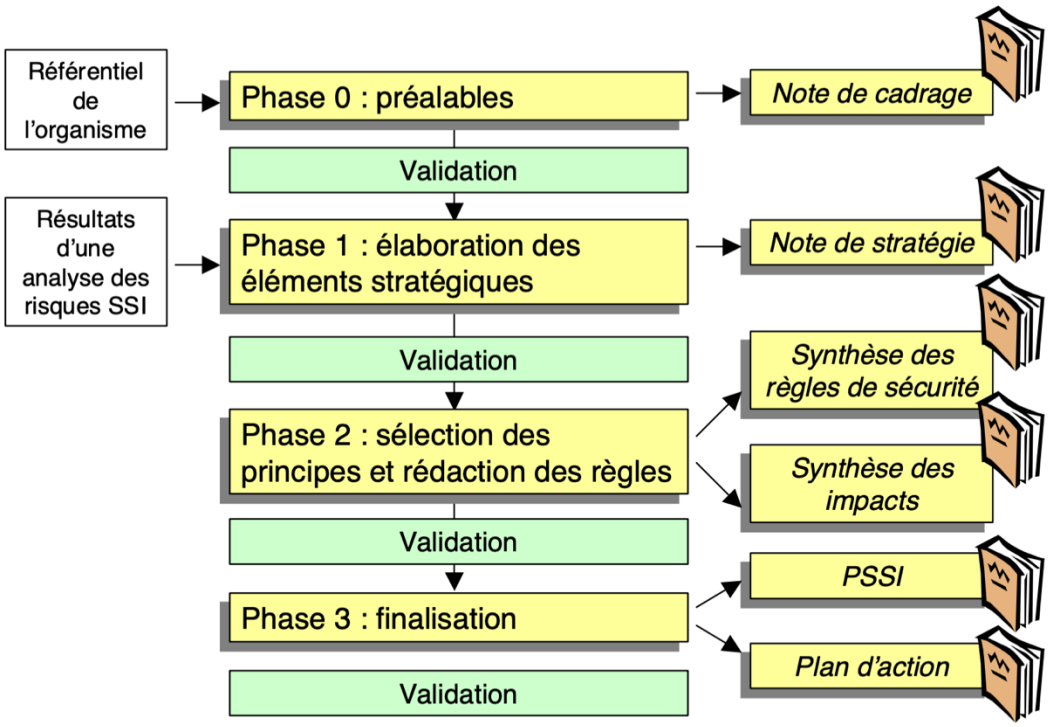


Figure 5 : Méthodologie d'élaboration d'une PSSI (source ANSSI)

Où chaque phase est expliquée ici :

- Phase 0 : Préalables
    - Organisation du projet : définir un cadre de mise en place du projet en choisissant un chef de projet, constituer un comité de pilotage et d'experts qui vont mener les tâches à développer, attribuer un budget, formaliser les objectifs et établir un planning d'actions à mener.

    - Constitution du référentiel : définir une base documentaire sur laquelle s'appuyer pour l'élaboration d'une PSSI (aspects légaux et réglementaires, grands principes d'éthique, obligation contractuelles envers clients, prestataires et autres partenaires, le référentiel de sécurité interne et du ou des SI)

- Phase 1 : Élaboration des éléments stratégiques
    - Définition du périmètre de la PSSI : formaliser une vision globale du SI concerné ou plus précisément décrire les domaines sur laquelle la PSSI va s'adapter.

    - Détermination des enjeux et orientations stratégiques : Cette tâche permet d'identifier les contraintes générales pesant sur l'organisation.

    - Prise en compte des aspects légaux et réglementaires, appliqués à la PSSI.

    - Élaboration d'une échelle de besoins : établir tout d'abord des critères de sécurité comme par exemple la fiabilité, la confidentialité, la disponibilité et leur attribuer une échelle d'importance et d'accessibilité (différentes entre un administrateur du SI et un utilisateur ou prestataire). Cela permet de mesurer les besoins de sécurité pour différents domaines d'activité.

    - Expression des besoins de sécurité

    - Identification des origines des menaces : avec, par exemple, la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) qui est très utilisée surtout dans les sociétés publiques ou la méthode MEHARI, plutôt utilisée par les société privées.

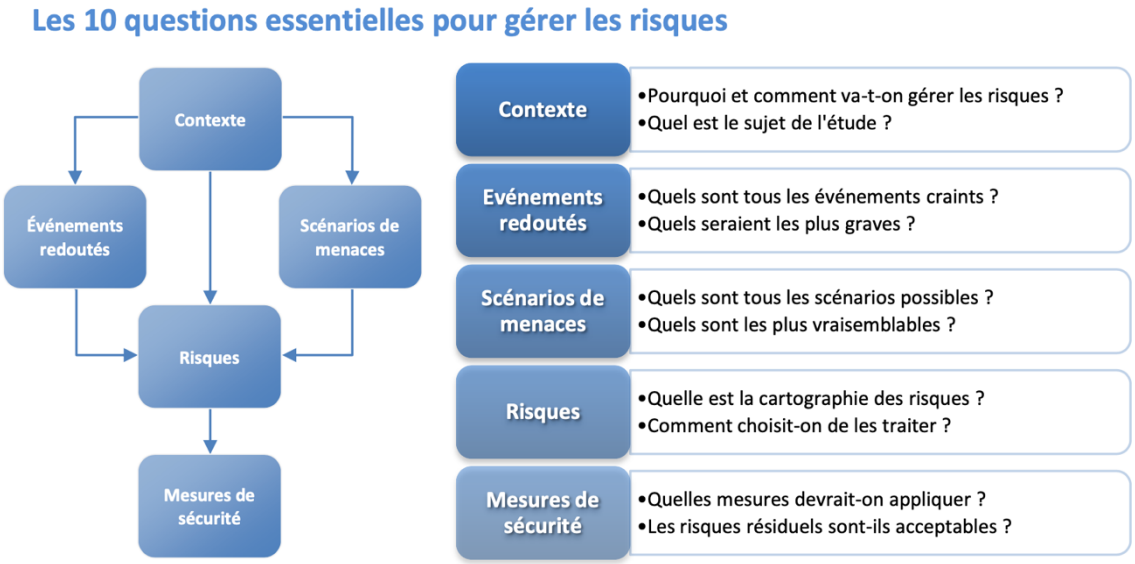


Figure 6 : Méthode EBIOS (source ANSSI)

- Phase 2 : Sélection des principes et rédaction des règles
    - Choix des principes de sécurité : Principes à développer et choisis en fonction du périmètre de la PSSI, de la stratégie de sécurité et des risques identifiés.

    - Élaboration des règles de sécurité

    - Élaboration des notes de synthèse : Synthèse des choix et des règles à mettre en place pour la PSSI.

- Phase 3 : Finalisation
    - Finalisation et validation de la PSSI : Production du document officiel qui sera validé par la hiérarchie et mis à jour en fonction des évolutions présentes dans l'entreprise.

    - Élaboration et validation du plan d'action : Dernière étape importante qui consiste à organiser la diffusion de la PSSI à tous les acteurs du SI de l'entreprise, qu'ils soient internes ou externes, et à mettre en place les premiers plans d'actions.

La méthode de mise en place de la PSSI a été décrite selon les indications de l'ANSSI mais l'utilisateur final n'apparaît que très rarement (juste à la fin) alors qu'il est un facteur important dans la SSI.

Nous allons voir par la suite une remise en question de la PSSI décrite ici et amener petit à petit l'impact de l'utilisateur dans la SSI.

II. DOCUMENTATION ACADEMIQUE

Nous allons poursuivre notre réflexion avec le premier article sélectionné : « En matière de sécurité des systèmes d'information, normalisation et standardisation sont-ils des facteurs d'efficacité ? » - de Etienne DE SEREVILLE

Cet article remet en question la standardisation et la normalisation mises en place et utilisées lors de l'établissement de la PSSI. Voici quelques exemples :

- Normes organisationnelles : ISO / CEI 27001
- Méthodologie : EBIOS ou MEHARI
- Standard technologiques : utilisation du système d'exploitation Windows

- Normes techniques : appliquées lors de la fabrication des composants par exemple, ITSEC pour la sécurité des composants

L'article met en avant le fait qu'utiliser des normes et standards sans discernement dans la sécurité des SI peut finalement créer des failles dans celle-ci. En effet, à cause d'eux, les SI deviennent prévisibles et ainsi accessibles aux cybercriminels.

Il faut que la sécurité des SI s'inspire des normes et standards mais ne les copie pas : une SSI à la carte doit être créée et doit s'adapter à l'entreprise et à son fonctionnement.

L'article suivant, « L'analyse du risque cyber, emblématique d'un dialogue nécessaire » - de Frédérick DOUZET et Sébastien HEON, se focalise quant à lui sur les acteurs de la SSI au sein d'une entreprise. Nous commençons avec celui-ci à entrapercevoir l'utilisateur comme acteur du SI.

Il précise l'impact des cyber-menaces sur toutes les dimensions de l'organisation : son activité, sa réputation, ses capacités de production, la protection de son patrimoine et même sur la sécurité de son personnel, et met en avant une mauvaise approche des risques cyber. Les experts en sécurité classique (de l'entreprise) ou Risk Manager (RM) considèrent que la SSI ne concerne que les informaticiens, et autres responsables du SI (RSSI), et inversement, ces derniers ne pouvant sensibiliser correctement les autres acteurs du SI s'en occupent seuls et sans concertation avec les RM et la direction.

Ce manque de communication entre ces deux entités fragilise grandement la SSI car elle n'est pas prise en compte dans la stratégie de sécurité globale d'une entreprise alors qu'une attaque peut avoir de graves conséquences directes ou indirects :

Impacts directs d'une cyber-attaque : nettoyage de l'attaque, remise en état du SI, perte de l'exploitation et des données, vols de données financières, stratégiques, commerciales et administratives, baisse de la production, coûts de remise en fonctionnement, perte de temps, etc.

Impacts indirects d'une cyber-attaque : liés surtout à l'image de la société, perte de la confiance en l'entreprise, que ce soit avec les clients ou les partenaires externes et même internes.

Il est important alors que les deux entités responsables de la sécurité, classique ou SSI, communiquent énormément, considèrent ensemble l'importance des risques cyber et mettent en place des mesures sensibilisant l'ensemble de l'entreprise, et pas seulement le service IT (Information Technology).

Une fois mis en avant l'importance de la communication dans un établissement en terme de sécurité, nous abordons enfin l'impact de l'homme dans les enjeux de cyber-sécurité à travers l'article suivant : « La place de l'homme dans les enjeux de cyber-sécurité » - de Claude WEBER et Jean-Philippe.

Celui-ci illustre clairement l'impact de l'homme sur les risques cyber en utilisant comme cadre d'étude le Ministère des Armées. Les auteurs ont choisi ce milieu car le cyberespace est officiellement désigné, d'après l'article, comme le cinquième milieu avec l'air, la mer, la terre et l'espace et est considéré comme « un champ de confrontation à part entière », ce qui place la cyberdéfense comme un des enjeux de l'institution militaire.

Ils commencent leur études par quelques chiffres marquants sur la sécurité des SI de manière générale et pas seulement dans le cadre militaire :

- Alors qu'en 2015, les attaques via la messagerie électronique (hameçonnage ou phishing) n'étaient que de 1%, elles sont passées à 42% fin 2016 !
- 90% des clics sur les URL[10] malveillants dans les mails reçus ont lieu dans les 24h après réception et pour 25,5 % des cas dans les 10 minutes !

Ensuite, ils démontrent que la sensibilisation des militaires à ces risques informatiques n'a pas été faite ou prise peu sérieusement, ce qui peut paraître étrange dans une structure où la discipline, l'obéissance aux ordres, le respect du règlement font partie des fondamentaux de l'institution militaire.

Cela peut s'expliquer tout d'abord par le fait que la sécurité des données n'est pas considérée par les militaires comme étant aussi importante que la sécurité d'une nation alors que les attaques subies par un état peuvent être, aujourd'hui à l'ère de l'informatique, autant physique que numérique. De plus, au sein d'une armée les Hommes s'entraident et sont organisés pour arriver au même but fixé mais devant un ordinateur, le militaire est seul et n'est pas conscient de ce qu'il a entre les mains et des risques qu'il encourt. Enfin le risque cyber n'est pas pris au sérieux car il est vu comme une activité technique « trop éloignée des représentation guerrières et combattantes » et jugé « trop peu valorisant » par des cadres.

Ces points mettent en avant qu'une sensibilisation efficace, marquante et orale aux risques numériques est importante même si des règles écrites ont été imposées et transmises à tout le monde, ici l'armée.

[10] URL : Uniform Resource Locator ou adresse web plus couramment – d'après les cours de Mme CASTELLANOS, Conception et réalisation de sites web - IAE de Grenoble

Claude WEBER et Jean-Philippe apportent ainsi quelques solutions pour améliorer cela et contrer le fait que « les séances de sensibilisation sont trop peu nombreuses et mal ciblées » :

- Coupler un entrainement pratique à la diffusion d'information théorique
- Mettre en place des exercices de simulations d'attaque cyber
- Développer des comportements réactifs et non se baser sur la prévention
- A travers des outils techniques, analyser les comportements des utilisateurs dans un milieu numérique et adapter une réponse en fonction de leurs actions et erreurs (cours, ajustements de la sensibilisation)

Dans le dernier article académique que nous allons voir, « Espionnage, attaques subversives et cyber-sécurité : de l'impact des actions de « social engineering » et des vulnérabilités humaines sur la sécurité globale des entreprises » – de Franck DECLOQUEMENT, nous allons compléter l'article de Claude WEBER et Jean-Philippe et démontrer la faiblesse de l'Homme face à aux risques numériques.

L'auteur met tout d'abord l'accent sur la centralité de la dimension humaine dans les risques informatiques où les cybercriminels favorisent la manipulation humaine dans leurs attaques : « toutes ces actions criminelles sophistiquées entretiennent un point commun : elles sont en effet basées pour l'essentiel sur un art consommé de la persuasion et de la supercherie, déployé très habilement par un opérateur malveillant pour parvenir à ses fins ». La cyber-malveillance vise principalement à corrompre et influencer l'humain pour parvenir à des informations sensibles comme les mots de passe, les codes d'accès, les données financières et administratives.

Il qualifie ensuite l'Homme de « point faible », de « parent pauvre des dispositifs de protection des architectures réseaux » et « d'angle mort des politiques de sécurité » car il est un animal très intelligent mais extrêmement manipulable et influençable qui a tendance à mélanger domaines privé et professionnel dans l'utilisation d'outil numérique.

Il justifie ses dires grâce aux rapports du CESIN de 2016 qui démontrent que :

- 41 % les salariés sont jugés trop peu sensibilisés aux risques cyber
- 52 % sont trop peu enclins à suivre les recommandations de leur RSSI
- 58 % des moyens techniques mis en place sont jugés insuffisants
- 69 % des moyens humains le sont également

Il parle également des sous-traitants comme « porte arrière dérobée » et démontre qu'ils peuvent être aussi des accès aux informations sensibles d'une entreprise. Aucune organisation n'est à l'abris des cyber-attaques car elles peuvent venir autant de l'intérieur que de l'extérieur.

Ces faits nous font prendre conscience qu'une sensibilisation humaine des risques cyber est aussi indispensable qu'une prévention technique dans la SSI d'une organisation.

III. DOCUMENTATION PROFESSIONNELLE

Nous allons conclure l'étude des différentes documentations relatives à l'impact de l'homme sur la cyber-sécurité par l'article professionnel du site *Stormshield* « L'humain, clé de la cyber-sécurité des entreprises » de Victor POITEVIN.

Cet article met d'abord en avant quelques faits importants : 1/3 des entreprises françaises considèrent que les collaborateurs sont involontairement à l'origine de certaines cyber-attaques, d'après l'enquête The Global State of Information Security Survey 2017, et lorsqu'ils ne sont ni conscients des risques, ni formés aux bonnes pratiques, ils représentent le cheval de Troie idéal d'après Matthieu BONENFANT, le Directeur Marketing de *Stormshield*.

L'auteur précise ensuite qu'il est important d'inclure l'humain dans la stratégie de sécurité informatique et vis-à-vis d'une organisation tous les utilisateurs doivent être sensibilisés et pas seulement les cadres de direction, les managers, les informaticiens, les assistantes de direction et les responsables financiers qui sont généralement plus ciblés par les attaques. Il donne des solutions de sensibilisation qui rappellent celles présentées dans l'article de Claude WEBER et Jean-Philippe « La place de l'homme dans les enjeux de cyber-sécurité » :

Quelques outils : Charte informatique, sessions e-learning, formation de groupe, dispositifs ludiques et participatifs, sessions de live-hacking (simulation de cyber-attaque)

Quelques règles de base dans la sensibilisation :

- Encouragements et soutien de la direction générale,
- Contenus pratiques, accessibles et adaptés aux usages réels des utilisateurs,
- Se limiter à quelques sujets importants et les traiter en profondeur,
- Former des équipes complètes et pas seulement quelques élus (généralement les managers),
- Contrôler les acquis à la fin de la formation,
- Offrir des piqûres de rappel, du fait de l'évolution constante des SI et des menaces qui y sont liées.

L'homme doit être ainsi perçu comme un levier de sécurité et non un problème.

Nous pouvons compléter ces conseils managériaux par quelques actions suggérées par de nombreuses sociétés de conseils en SSI (ici le site *Novatim*) :

- La **sauvegarde** en interne ou externalisée car il y a toujours un risque de cyber-malveillance.

- La mise à jour des SI et des logiciels de sécurité de manière générale.
- Le **pare feu** qui gère les entrées/sorties du système.
- L'**antivirus** payant de préférence car les gratuits ne sont pas efficaces pour les entreprises.
- **Protéger la flotte mobile** des collaborateurs qui est souvent oubliée.
- Le **cryptage des données** sur tous les supports : clé USB, ordinateurs, disques durs externes.
- La **stratégie de mots de passe** en utilisant des mots de passe complexes et non notés sur un carnet ou un post-it (outils de gestion de mots de passe disponibles et sécurisés)
- Une **gestion des droits d'accès** qui consiste à vérifier quel collaborateur a accès à quelle donnée et à mettre en place un VPN si les collaborateurs sont à distance. Chaque entrée/sortie doit être contrôlée.
- Le **monitoring des serveurs** mis en place de manière régulière qui permet de repérer les tentatives d'intrusion ou attaques.
- La **formation des collaborateurs**

Comme nous pouvons en juger, la dernière action, et pas des moindres, est la sensibilisation des utilisateurs. Sans elle tout ce qui peut être mis en place techniquement, technologiquement ou méthodologiquement ne fonctionnerait pas.

IV. RESULTATS OBTENUS

Les différents articles nous confirment que la sensibilisation des utilisateurs aux risques informatiques est un élément très important dans l'établissement de la Politique de Sécurité du SI mais pas uniquement.

Les articles gouvernementaux nous rappellent qu'une bonne préparation et une bonne méthodologie d'étude des risques et de mise en place d'une PSSI est essentielle pour chaque organisation qu'elle soit petite ou grande, publique ou privée. Ce qui est confirmé par les deux premiers articles académiques étudiés, mais à faire **avec discernement** et en favorisant la communication entre les responsables de la Sécurité des SI et les Responsables de la sécurité classique ou Risk Manager.

L'article suivant nous informe sur la place importante de l'homme dans les enjeux de cyber-sécurité et donne de nombreux conseils et outils pour les sensibiliser. Ils sont également cités par l'article professionnel *Stormshield* : charte informatique, sessions e-learning, formation de groupe, dispositifs ludiques et participatifs, sessions de live-hacking (simulation de cyber-attaque). Ils indiquent également qu'il faut prendre en compte tous les utilisateurs : collaborateurs internes, comme les

employés qu'ils soient cadre ou non, ou externes, comme les entreprises partenaires, clientes ou sous-traitantes.

Le dernier article académique de Franck DECLOQUEMENT, quant à lui, nous démontre surtout l'impact de l'homme dans les cyber-attaques subies par les organisations et vise à sensibiliser, voire choquer, les lecteurs sur les risques encourus et sur la responsabilité des collaborateurs qualifiés ici de « points faibles », de « parent pauvre des dispositifs de protection des architectures réseaux » et « d'angle mort des politiques de sécurité ».

PARTIE 3
-
SOLUTIONS ET PRECONISATIONS

CHAPITRE 7 – PRECONISATIONS

Suite à l'étude de ces différents articles, nous pouvons enfin apporter une réponse complète à notre problématique : « Est-ce que la sensibilisation des utilisateurs aux risques informatiques est l'élément le plus important dans la Politique de Sécurité du SI ? ». Nous avons pu ainsi voir qu'elle tenait une place importante et incontournable dans la mise en place de la PSSI d'une organisation.

Suite à cela, nous avons pu avoir de nombreuses solutions pour une mise en place efficace qu'elles soient techniques, technologiques, méthodologiques et même humaines. Ce sont celles-ci que nous allons proposer dans ce chapitre en commençant tout d'abord par des préconisation techniques, technologiques et méthodologiques à adapter à chaque entreprise. Ensuite nous aborderons des préconisations d'actions plus humaines et centrées sur la sensibilisation des utilisateurs.

I. SOLUTIONS TECHNIQUES, TECHNOLOGIQUES ET METHODOLOGIQUES

Seront abordés ici les solutions techniques, technologiques et méthodologiques à mettre en place pour avoir une bonne Politique de Sécurité du Système d'Information applicables à toutes les entreprises avec discernement et en fonction de leur taille et de leur activité.

En suivant les méthodologies de l'ANSSI dans la mise en place d'une PSSI et EBIOS pour l'analyse des risques, les acteurs de la sécurité des SI et de la sécurité classique doivent se réunir et communiquer les plans d'actions à mettre place pour prévenir et contrer les cyber-menaces. Une fois décidés ils doivent rédiger une charte qui sera appliquée à toute l'entreprise et communiquée à tout le monde en interne et en externe avec les partenaires.

Si les entreprises sont plus petites, la responsabilité de rédaction de la charte est du ressort des informaticiens et de la direction.

Suite à cela, ils doivent mettre en action leurs plans décidés ensemble et prendre des mesures techniques et technologiques afin de garantir la sécurité des postes et des données. En voici les principales :

- La **sauvegarde** en interne ou externalisée car il y a toujours un risque de cyber-malveillance.
- Hébergement de la plateforme web en interne si possible ou utilisation de Saas ou Cloud sécurisé si ce n'est pas possible.
- La mise à jour des SI et des logiciels de sécurité de manière générale.
- Le **pare feu** qui gère les entrées/sorties du système.

- L'**antivirus** payant et récent de préférence car les gratuits ne sont pas efficaces pour les entreprises.
- **Protéger la flotte mobile** des collaborateurs qui est souvent oubliée.
- Le **cryptage des données ou chiffrage** sur tous les supports : clé USB, ordinateurs, disques durs externes.
- La **stratégie de mots de passe** en utilisant des mots de passe complexes et non notés sur un carnet ou un post-it (outils de gestion de mots de passe disponibles et sécurisés).
- Une **gestion des droits d'accès** qui consiste à vérifier la bonne concordance entre le collaborateur et les données auxquelles il a accès ou non et à mettre en place un VPN si les collaborateurs sont à distance. Chaque entrée/sortie doit être contrôlée.
- Le **monitoring des serveurs** mis en place de manière régulière qui permet de repérer les tentatives d'intrusion ou attaques.

Mais ces actions doivent être utilisées avec discernement et s'adapter à l'entreprise : chaque entreprise doit trouver « chaussure à son pied » en matière de sécurité.

II. SENSIBILISATIONS DES UTILISATEURS

Comme il est rappelé de nombreuses fois dans ce chapitre, l'utilisateur a une place importante dans les enjeux de cyber-sécurité de l'entreprise et sa sensibilisation n'est pas à prendre à la légère. Même si les responsables de la SSI ou des services de direction et de sécurité générale d'une organisation établissent les règles et les mesures à suivre pour une cyber-sécurité efficace, si les utilisateurs des SI ne sont pas informés, formés et sensibilisés, toute action sera voué à l'échec et les risques cyber seront des plus critiques.

Voici quelques conseils en terme de sensibilisations :

Quelques outils d'aide :

- Charte informatique,
- Sessions e-learning,
- Formation de groupe,
- Dispositifs ludiques et participatifs,
- Sessions de live-hacking (simulation de cyber-attaque)

Quelques règles de base dans la sensibilisation :

- Encouragements et soutien de la direction générale,
- Contenus pratiques, accessibles et adaptés aux usages réels des utilisateurs,

- Se limiter à quelques sujets importants et les traiter en profondeur,
- Former des équipes complètes et pas seulement quelques élus (généralement les managers),
- Contrôler les acquis à la fin de la formation,
- Offrir des piqûres de rappel, du fait de l'évolution constante des SI et des menaces qui y sont liées.

Ces outils et règles de base permettront à chaque utilisateur d'une organisation d'être un acteur de la cyber-sécurité et de contribuer au bon fonctionnement de celle-ci de manière numérique. Cela permet de le responsabiliser à chaque fois qu'il utilise un SI et de comprendre pourquoi toutes les mesures prises par la SSI et la sécurité générale ont été mises en place.

Il faut néanmoins faire attention à présenter la sécurité des SI de manière ludique et positive sans pour autant qu'elle ne soit trop distrayante, c'est-à-dire trouver un juste milieu pour que la sensibilisation ait un impact significatif sans pour autant contraindre les collaborateurs à une charge mentale trop lourde à porter en plus de leur travail. C'est pour cela que la mise en place de simulations peut être une bonne aide.

CHAPITRE 8 – RETOUR SUR L'ELABORATION DU RAPPORT

Maintenant qu'une réponse a été apportée à la problématique, nous pouvons faire un état des lieux de notre rapport et de son élaboration et le comparer à nos choix d'organisation initiaux (faits lors de la mise en place du Gantt).

Avant de débuter la critique de nos choix d'organisation dans la rédaction du rapport SI sur l'importance de la sensibilisation des utilisateurs aux risques informatiques, nous allons rappeler les axes de réflexion qui ont conditionné notre Gantt :

« Choix faits sur la gestion de ce projet :

- Séparation de l'élaboration du rapport en 6 parties distinctes
- Jalon à chaque date clé
- Optimisation du temps rédactionnel : début de rédaction en parallèle de la recherche (parties 3 et 4).
- Temps important accordé à la correction et à la relecture du document
- Volonté de ne pas envoyer le document avant la fin pour éviter la précipitation. »

Le premier point sera remis en question plus tard mais le deuxième a été très utile pour l'organisation et les échanges avec la tutrice enseignante, même s'il a été difficile à un moment de remplir les étapes à temps.

En effet le choix de la problématique, placé en deuxième partie, fut plus long que prévu car difficile à trouver malgré une documentation préliminaire efficace. Il a fallu faire appel à l'aide de la tutrice enseignante pour voir d'un œil différent l'ensemble des recherches effectuées. Cette étape a ainsi fait perdre du temps sur le planning initialement prévu (problématique finalement trouvée le 28 mai et non pas le 20 avril) et a grandement retardé la rédaction du rapport.

Ce dernier aurait pu d'ailleurs commencer plus tôt une fois la thématique trouvée et les recherches préliminaires approuvées par la tutrice enseignante. Cela aurait permis, au fil de la rédaction, de trouver peut-être la problématique plus facilement.

Du temps a donc été aussi perdu dans la recherche documentaire académique car celle-ci devait répondre à la problématique. On peut conclure que le temps de cette troisième partie a là aussi mal été évalué.

Concernant le temps accordé à la correction et à la relecture, cette étape reste très importante, mais ne doit pas être placé à la fin comme prévu mais au fur et à mesure de l'achèvement de chaque partie. Cela permet ainsi de ne pas s'écarter du contexte initial, de valider chaque partie sans avoir à revenir dessus et de mettre en forme petit à petit le rapport sans avoir à tout reprendre à la fin. Séparer ainsi l'élaboration en 6 parties comme établies initialement n'était peut-être pas judicieux.

Nous pouvons aborder aussi le cas de l'introduction placée initialement avant la rédaction de la partie 1, mais qui, au final, n'est pas simple à écrire car tout le contexte de recherche n'est pas encore abordé et ne peut donc être imaginé. Il est plus judicieux au final de finir par l'introduction une fois la problématique répondue et les solutions apportées.

Le dernier choix effectué concernant l'envoi du document proche de la date limite acceptée reste pour l'instant un choix logique qui permet vraiment de laisser du temps pour la relecture et la correction finale, malgré les retards pris lors de la rédaction du rapport.

CONCLUSION

Notre thématique de recherche, la sécurité des données pendant un nomadisme numérique imposé, fût un sujet d'actualité très enrichissant, mais malheureusement trop récent pour avoir une documentation officielle (publiée) et un réel retour d'expérience dessus. Dans les années à venir, nous pouvons nous attendre à ce que les chercheurs en science de gestion soient intéressés par une étude à mener sur les conditions de travail que nous avons eu pendant cette crise et leurs impacts sur la sécurité des données ou sur le bien-être des collaborateurs d'une entreprise. Nous aurons peut-être ainsi des conseils et actions à prodiguer aux organisations.

En fermant cette parenthèse sur l'avenir nous pouvons voir, suite aux recherches effectuées, que beaucoup d'informations ont été trouvées sur le nomadisme numérique et sur les risques que provoque ce mode de travail sur la sécurité des données. On aurait pu croire, qu'à distance, la sécurité d'une entreprise est plus facile à gérer vu qu'il y a moins de personne sur site mais en fait à distance un autre problème se créé : celui des cyber-attaques et des entreprises trop divisées physiquement pour y faire face correctement. Comme nous l'a précisé un des articles étudié, depuis le début de la crise les attaques ont augmenté de 30 000 % ce qui est incroyable et effrayant : pendant que toute l'économie était à l'arrêt forcé, ou fortement ralentie pour quelques chanceux, les cybercriminels ont augmenté leurs attaques et ont profité de cette période indécise pour s'attaquer à un des maillons faibles de la cyber-sécurité : l'Homme.

Après de multiples recherches, nous pouvons voir que les mesures pour les éviter, même à distance, sont différentes suivant la taille des entreprises, leur domaine d'activité et sont efficientes si et seulement si **l'utilisateur est sensibilisé**. Ce qui nous a mené à notre problématique : « Est-ce que la sensibilisation des utilisateurs aux risques informatiques est l'élément le plus important dans la Politique de Sécurité du SI ? ».

En y répondant nous avons pu se renseigner vraiment plus sur la Politique de Sécurité du SI et sur ses composantes et voir la place importante de la sensibilisation humaine dedans. Nous pouvons faire un parallèle à la sécurité classique observée en entreprise : si l'entreprise manipule des produits chimiques ou corrosifs, le service sécurité ou l'entreprise de manière générale (si c'est une plus petite structure) va proposer des formations, voire les imposer, pour prévenir les risques liés à la manipulation de ces produits. Ces formations sont généralement des séances mêlant activités théoriques et pratiques afin d'être sûr que les utilisateurs aient les bons gestes. C'est exactement pareil avec la sécurité des SI, les personnes doivent être sensibilisées si nous voulons éviter des risques d'intrusion, de vol dans les données sensibles d'une organisation, qu'elle soit publique ou

privée. Et la meilleure sensibilisation reste la mise en pratique à travers des simulations de risque, des exercices, des campagnes d'information.

Les utilisateurs ne doivent pas être vus comme des victimes ou même comme des problèmes, mais comme **des acteurs de la cyber-sécurité**.

La réponse à cette problématique m'a permis de réaliser à quel point une entreprise aujourd'hui pouvait être fragile en matière de sécurité des données, même de sécurité classique. Beaucoup pensent, et moi aussi avant, que la PSSI n'était réservé qu'au service informatique mais en voyant toutes ces attaques pendant la crise, les dégâts qu'elles pouvaient occasionner, et pas seulement techniques mais aussi en matière d'image et de confiance, cela fait penser qu'on sous-estime grandement notre époque numérique et que la cyber-malveillance devrait être considérée comme un risque général qui peut être subi comme tous les autres par une organisation.

Nous pouvons ainsi faire évoluer notre pensée en voyant que les SI sont utilisés comme des outils pratiques de stockage, de transmission, de centralisation d'information entre les différents collaborateurs, mais ne sont jamais perçus comme présentant un risque majeur pour une organisation. A cause de cela, les entreprises n'investissent jamais beaucoup dans ce domaine et nous pouvons ainsi nous demander comment protéger l'entreprise contre les risques informatiques et mettre en place une PSSI efficace si les SI sont peu considérés et donc vulnérables ?

BIBLIOGRAPHIE

ANSSI. (2004a, mars). *Guide pour l'élaboration d'une politique de sécurité de système d'information*. Consulté à l'adresse https://www.ssi.gouv.fr/uploads/IMG/pdf/pssi-section2-methodologie-2004-03-03.pdf

ANSSI. (2004b, mars 3). Publication : PSSI — Guide d'élaboration de politiques de sécurité des systèmes d'information. Consulté le 14 avril 2020, à l'adresse https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/

ANSSI. (2010, janvier). *EBIOS : la méthode de gestion des risques SSI*. Consulté à l'adresse https://www.ssi.gouv.fr/uploads/2011/10/EBIOS-PlaquetteMetho-2010-04-081.pdf

ANSSI. (2018, 17 octobre). Publication : Recommandations sur le nomadisme numérique. Consulté le 14 avril 2020, à l'adresse https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/

ANSSI. (2020). Principales menaces. Consulté le 14 avril 2020, à l'adresse https://www.ssi.gouv.fr/entreprise/principales-menaces/

Bastien L, & Le Big Data. (2020, 31 mars). Télétravail : une grande menace pour la cybersécurité et les données selon les experts. Consulté le 14 avril 2020, à l'adresse https://www.lebigdata.fr/teletravail-menace-cybersecurite

Berger, A. (2020, 23 juin). Des clients de Darty ciblés par une campagne de phishing. Consulté le 29 juin 2020, à l'adresse https://www.capital.fr/entreprises-marches/des-clients-de-darty-cibles-par-une-campagne-de-phishing-1373401

Bys, C. (2017, 27 mars). Le télétravail réduit la protection des données des entreprises, selon une étude Symantec. Consulté le 14 avril 2020, à l'adresse https://www.usine-digitale.fr/article/le-teletravail-reduit-la-protection-des-donnees-des-entreprises-selon-une-etude-symantec.N519379

Caruso, D. L. (2020, 15 janvier). « ; 2020 sera l&rsquo ; anné ; e des cyberattaques dopé ; es par l&rsquo ; intelligence artificielle» ; , pré ; vient Avast. Consulté le 17 juin 2020, à l'adresse https://www.leparisien.fr/high-tech/2020-sera-l-annee-des-cyberattaques-dopees-par-l-intelligence-artificielle-previent-avast-13-01-2020-8235087.php

Claude Weber, & Jean-Philippe. (2017). La place de l'homme dans les enjeux de cybersécurité. *Stratégique*, (117), 83-98. Consulté à l'adresse https://www.cairn.info/revue-strategique-2017-4-page-83.htm?contenu=resume

Cyber-malveillance - Site du Gouvernement pour l'Assistance et la Prévention du Risque Numérique. (2019, 20 novembre). Les rançongiciels (ransomwares) - Cybermalveillance.gouv.fr. Consulté le 17 juin 2020, à l'adresse https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

Echos, L. (2017, 15 décembre). La fraude au faux fournisseur. Consulté le 17 juin 2020, à l'adresse https://business.lesechos.fr/entrepreneurs/juridique/dossiers/11622811/tpepme-00011622811-3-la-fraude-au-faux-fournisseur-317042.php

Étienne de Séréville. (2009). En matière de sécurité des systèmes d'information, normalisation et standardisation sont-ils des facteurs d'efficacité ? *« Revue internationale d'intelligence économique »*, *1*, 271-287. Consulté à l'adresse https://www.cairn.info/revue-revue-internationale-d-intelligence-economique-2009-2-page-271.htm?contenu=article

Franck DeCloquement. (2016). Espionnage, attaques subversives et cyber sécurité : de l'impact des actions de « social engineering » et des vulnérabilités humaines sur la sécurité globale des entreprises. *Sécurité et stratégie*, (22), 21-29. Consulté à l'adresse https://www.cairn.info/revue-securite-et-strategie-2016-2-page-21.htm

Frédérick Douzet, & Sébastien Héon. (2013). L'analyse du risque cyber, emblématique d'un dialogue nécessaire. *Sécurité et stratégie*, (14), 44-52. Consulté à l'adresse https://www.cairn.info/revue-securite-et-strategie-2013-3-page-44.htm

Jacques, A. (2018, 2 mai). Sé ; curité ; informatique : Quels enjeux pour votre entreprise ? Consulté le 14 avril 2020, à l'adresse https://www.securiteinfo.com/services/securite_informatique_quels_enjeux_pour_votre_entreprise.shtml

Jacques Cheminat, & Dominique Filippone. (2020, mars–juin). *Cyber-matinée Sécurité 2020 Auvergne Rhône-Alpes* . Web-conférence présenté à Cyber- matinée Sécurité - Web Conférence 2020, En ligne, France . Consulté à l'adresse https://www.cybermatinees.fr/

Leclère, E. (2020, 6 mai). Cybercriminalité : avec le confinement, les attaques ont augmenté de 30 000 %. Consulté le 16 juin 2020, à l'adresse https://www.franceinter.fr/justice/cybercriminalite-avec-le-confinement-les-attaques-ont-augmente-de-30-000

Novatim. (2019, 8 octobre). 10 bonnes pratiques pour la sécurité informatique de son entreprise. Consulté le 17 juin 2020, à l'adresse https://www.novatim.com/actualite/10-bonnes-pratiques-securite-informatique/

Pauline Raud, & Huffpost. (2020, 11 juin). *Illustration du télétravail* [Illustration]. Consulté à l'adresse https://www.huffingtonpost.fr/entry/non-vous-netiez-pas-en-teletravail-jusque-la-blog_fr_5ee0f6d6c5b6c65d796395fc

Pexels. (2020). *Illustration du télétravail* [Photographie]. Consulté à l'adresse https://www.pexels.com/fr-fr/photo/marketing-personne-individu-gens-3759080/

Poitevin, V. (2019, 21 août). Cybersécurité : former les salariés, une nécessité I. Consulté le 14 avril 2020, à l'adresse https://www.stormshield.com/fr/actus/lhumain-cle-de-la-cybersecurite-des-entreprises/

Politique de sécurité du système d'information. (s. d.). Dans *Wikipedia*. Consulté le 19 juin 2020, à l'adresse https://fr.wikipedia.org/wiki/Politique_de_s%C3%A9curit%C3%A9_du_syst%C3%A8me_d%27information

Portail de l'Économie, des Finances, de l'Action et des Comptes Publics. (2018, 1 septembre). Phishing (hameçonnage ou filoutage). Consulté le 17 juin 2020, à l'adresse https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/Phishing-hameconnage-ou-filoutage

Réseau privé virtuel. (s. d.). Dans *Wikipedia*. Consulté le 17 juin 2020, à l'adresse https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel

Reuters, L. M. A., & Le Monde. (2020, 19 mai). EasyJet victime d'une cyberattaque, les données de millions de clients dérobées. Consulté le 21 mai 2020, à l'adresse https://www.lemonde.fr/pixels/article/2020/05/19/easyjet-victime-d-une-cyberattaque-les-donnees-de-millions-de-clients-derobees_6040142_4408996.html

Sensibilisation. (2020). Dans *Le Larousse*. Consulté à l'adresse https://www.larousse.fr/dictionnaires/francais/sensibiliser/72106

TABLES DES FIGURES

TABLES DES ANNEXES

ANNEXE 1 : METHODE EBIOS

ANSSI Agence nationale de la sécurité des systèmes d'information

EBIOS : la méthode de gestion des risques SSI
Un outil simple et puissant

La gestion des risques est largement décrite et préconisée dans la presse, les normes, la réglementation… EBIOS® (Expression des Besoins et Identification des Objectifs de Sécurité) est la méthode de gestion des risques de l'ANSSI. Opérationnelle, modulaire et alignée avec les normes, c'est la boîte à outils indispensable pour toute réflexion de sécurité des systèmes d'information (SSI). Voici comment EBIOS peut vous être utile.

Le risque SSI dans EBIOS : un exemple éclairant

Définition du risque : c'est un scénario qui combine un événement redouté (sources de menaces, bien essentiel, critère de sécurité, besoin de sécurité, impacts) et un ou plusieurs scénarios de menaces (sources de menaces, bien support, critère de sécurité, menaces, vulnérabilités).

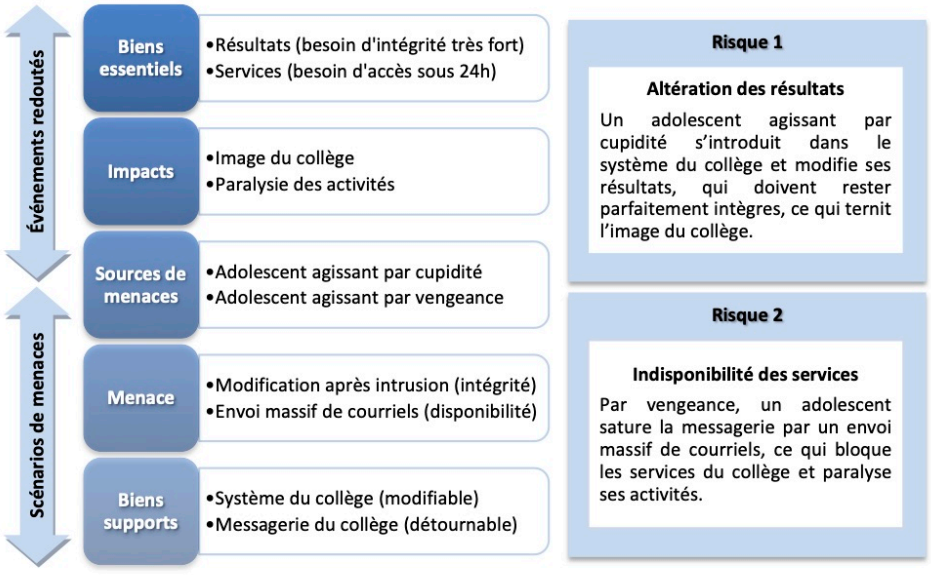
On estime son niveau par sa gravité (hauteur des impacts) et sa vraisemblance (possibilité qu'il se réalise).

Un adolescent de 15 ans « pirate » le système informatique de son collège pour améliorer ses notes.

Un adolescent de quinze ans a en effet été interpellé pour s'être introduit dans le système informatique de son collège dans le but de modifier ses résultats scolaires. Dépité de n'avoir pu atteindre ce but, le collégien a saturé le système informatique en expédiant plus de 40 000 courriels, manœuvre qui a provoqué une indisponibilité pendant quatre jours.

[Sources Internet : Le Point.fr et ZDNet]

À partir de ce fait divers et de la définition du risque d'EBIOS, nous pouvons mettre deux risques en évidence :

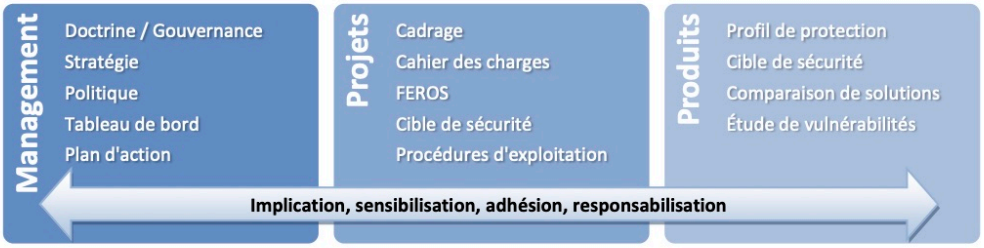


Une étude EBIOS appliquée au système du collège aurait permis, simplement et rapidement :

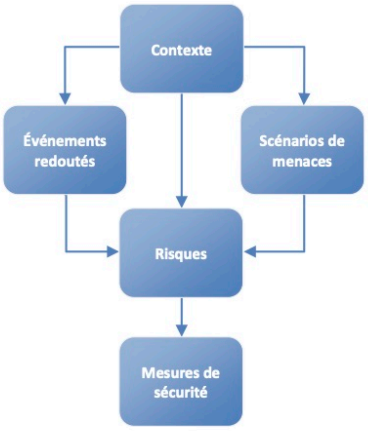
- d'identifier ces deux risques, ainsi que tous les autres qui pèsent sur le système d'information du collège ;
- d'estimer leur niveau (gravité, vraisemblance), les cartographier et prendre des décisions en conséquence ;
- de choisir les mesures nécessaires et suffisantes en termes de prévention, de protection et de récupération.

ANSSI Agence nationale de la sécurité des systèmes d'information

EBIOS est le "tout terrain" pour gérer les risques



Les 10 questions essentielles pour gérer les risques



Contexte	•Pourquoi et comment va-t-on gérer les risques ? •Quel est le sujet de l'étude ?
Evénements redoutés	•Quels sont tous les événements craints ? •Quels seraient les plus graves ?
Scénarios de menaces	•Quels sont tous les scénarios possibles ? •Quels sont les plus vraisemblables ?
Risques	•Quelle est la cartographie des risques ? •Comment choisit-on de les traiter ?
Mesures de sécurité	•Quelles mesures devrait-on appliquer ? •Les risques résiduels sont-ils acceptables ?

Grands principes à appliquer

Pour réussir une étude et son application, il convient de respecter 4 grands principes de mise en œuvre :

- employer EBIOS comme une boîte à outils pour une efficacité maximale ;
- utiliser la méthode avec souplesse pour adhérer au langage et aux pratiques de l'organisme ;
- améliorer progressivement l'étude, en temps réel, pour rester cohérent avec la réalité ;
- rechercher une adhésion des acteurs du système d'information pour élaborer des solutions de protection.

Une mise en œuvre facilitée

La méthode dispose de bases de connaissances riches et enrichissables, d'un logiciel libre et gratuit, de formations et d'une documentation variée.

La communauté des experts et utilisateurs de gestion des risques (industriels, administrations, prestataires, universitaires...) se réunit régulièrement au Club EBIOS pour échanger des expériences et enrichir le référentiel.

EBIOS ne vous protège pas des risques, elle vous permet d'en faire prendre conscience aux décideurs.

Informations : http://www.ssi.gouv.fr/ebios
Contact : ebios@ssi.gouv.fr

TABLES DES MATIERES