Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialités Réseaux et Télécommunications
Parcours Cybersécurité

Étude du déploiement et de la mise en œuvre de la PSSI dans une organisation

Quentin DELCHIAPPO

CPAM des Bouches-du-Rhône

Responsable entreprise : Florence MOLAIRE

Responsable académique : Éric WURBEL

2023

Table des matières

1. Introduction

L'objectif du stage de deuxième année Réseaux et Télécommunications parcours Cybersécurité est de mettre en application toutes nos connaissances acquises lors du BUT (Bachelor Universitaire Technologique). Dont l'objectif est de se confronter à la réalité du terrain et de la pratique en mettant un pied dans le monde du travail. Ainsi, j'ai pu réaliser la manière de mettre en forme, au sein d'un environnement de travail professionnel et non scolaire, l'ensemble de mes connaissances et mes compétences qui m'a été enseigné et transmise durant les différents cours, les interventions ainsi que les travaux pratiques suivis lors de ces deux dernières années.

J'ai effectué mon stage au sein de la CPAM des Bouches-du-Rhône (Caisse Primaire de l'Assurance Maladie), dans le service SSI (Sécurité des Systèmes d'Informations). Cette entreprise est un exemple parfait quant à l'importance de la protection des données dans le milieu informatique. En effet, celle-ci utilise et traite des données sensibles comme les coordonnées bancaires, les numéros de sécurité sociales ou encore de nombreuses données personnelles. Par ce fait l'entreprise doit être en mesure de sécuriser ces dernières puisque qu'elles contiennent des données sensibles et confidentielles, et peuvent donc naturellement représenter une menace en cas de mauvaises utilisations ou d'attaques informatiques.

Pourquoi avoir choisi la Caisse Primaire de l'Assurance Maladie ?
Ce choix a été étudié par rapport à de grandes caractéristiques majeurs que la CPAM réunit. En tout premier point, il s'agit d'une entreprise qui représente une responsabilité majeure sur la multiplicité des informations qui transitent entre les différents services de l'organisme et ces partenaires. Enfin, mon intérêt et souhait principal était d'effectuer mon stage dans une structure importante pour voir le fonctionnement des systèmes de sécurité informatique au sein d'un réseau et d'une infrastructure complexe.

Tout au long de ce rapport, je présenterai l'environnement ainsi que le cadre du déroulement de mon stage. Par la suite, j'expliquerai en détail les différentes missions et tâches que j'ai pu accomplir qui ont eu pour but l'étude du déploiement et de la mise en place de la PSSI (Politique de Sécurité des Systèmes d'Information) rattachée à la Caisse Primaire d'Assurance Maladie, dont la finalité est de garantir la protection des données sensibles liées à la santé des assurés.

2. Présentation de l’entreprise

2.1 Qu’est-ce que la CPAM ?

La sécurité sociale en France est un système de protection social qui vise à assurer une couverture de base à tous les résidents. Elle englobe divers domaines tels que l'assurance maladie, l'assurance retraite, l'assurance chômage et les allocations familiales. La sécurité sociale repose sur le principe de solidarité, où les cotisations des travailleurs actifs contribuent à financer les prestations dont bénéficient les personnes dans le besoin, qu'il s'agisse de soins médicaux, de pensions de retraite ou d'autres formes d'aide sociale.

La CNAM (Caisse Nationale de l'Assurance Maladie) est l'organisme national qui supervise et coordonne l'ensemble du système d'assurance maladie en France. Elle joue un rôle essentiel dans la définition des politiques et des règles de remboursement des soins médicaux, ainsi que dans la régulation des dépenses de santé. La CNAM travaille en collaboration avec les CPAM pour garantir une gestion efficace et équitable de l'assurance maladie dans tout le pays.

La CPAM (Caisse Primaire d'Assurance Maladie) est l'organisme local français chargé de la gestion de l'assurance maladie obligatoire au niveau départemental. Elle joue un rôle essentiel dans la mise en œuvre des politiques et des règles de remboursement des soins médicaux. En collaboration avec la CNAM (Caisse Nationale de l'Assurance Maladie), elle veille à une gestion efficace et équitable de l'assurance maladie à travers tout le pays. La CPAM est responsable du remboursement des frais médicaux, de la prévention des risques professionnels, de la promotion de la santé et de l'assistance aux assurés et aux professionnels de santé. En tant qu'acteur de proximité, la CPAM est le point de contact direct entre les bénéficiaires et le système global de sécurité sociale représenté par la CNAM et la sécurité sociale en général.

Au sein de ces trois entités, la CPAM occupe une place centrale en tant qu'organisme de proximité chargé de la gestion quotidienne de l'assurance maladie obligatoire. Elle est responsable de l'immatriculation des assurés, du remboursement des soins médicaux, de la prévention des risques professionnels et de la promotion de la santé. La CPAM assure également le rôle de conseiller pour les assurés et les professionnels de santé, fournissant des informations sur les droits et les démarches administratives liées à l'assurance maladie. Ainsi, la CPAM est le lien direct entre les bénéficiaires et le système de sécurité sociale plus large représenté par la CNAM et la sécurité sociale en général.

La CPAM des Bouches-du-Rhône est la 1ère caisse de France par son volume d’activité, avec un effectif qui compte 2180 agents. Elle assure et accueille dans ses locaux différents publics :

- Des assurés sociaux
- Des professionnels de santé
- Des employeurs
- Des travailleurs indépendants

Si la CPAM devait être résumé en quelques chiffres :

- Nombre de bénéficiaires : 2,1 bénéficiaires
- 24 pôles de production
- 18 agences et 5 permanences
- Montant des prestations versées : 9,6 milliards d'€

Les missions principales de la caisse sont :

- Affilier les assurés sociaux et gérer leurs droits
- Prendre en charge les frais de santé
- Verser des revenus de remplacement en cas de maladie, maternité, AT/MP, invalidité
- Développer une politique de prévention et de promotion de la santé
- Assurer une politique d'action sanitaire et sociale

2.2 L'organigramme du service SSI

Figure 1 : Schéma de l'organigramme générale de la CPAM

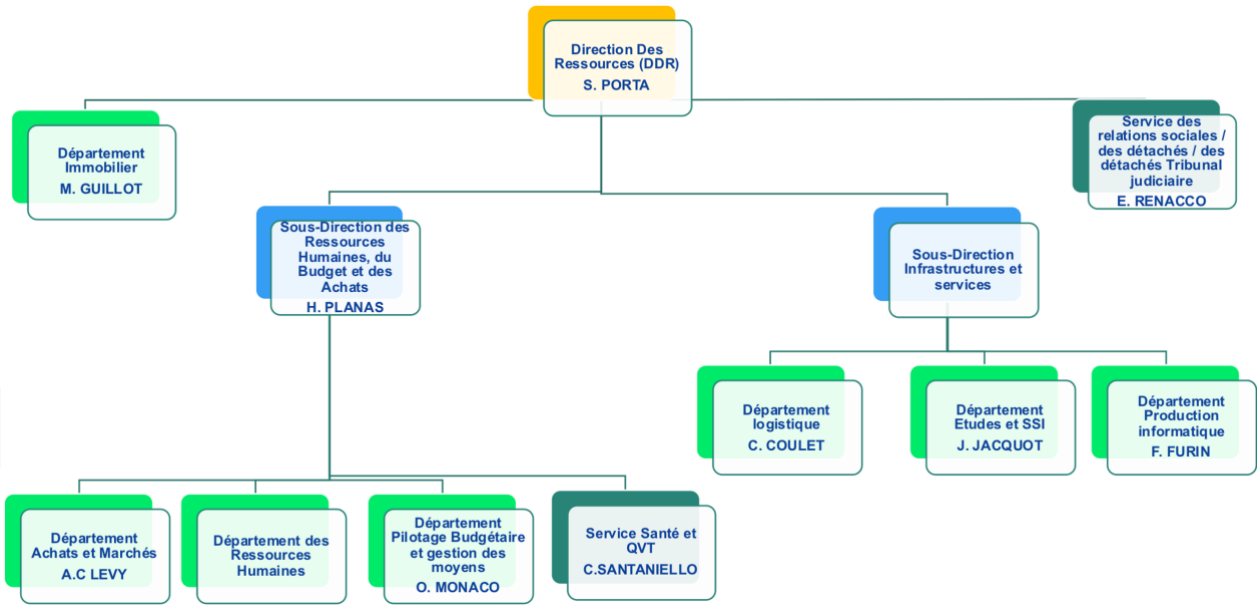


Figure 2 : Schéma de l'organigramme des services entourant le service SSI

2.3 La CPAM et son service SSI

Le service SSI, qui sont-ils et qu'est-ce qu'ils font ?

Le service SSI (Sécurité du Système d'Information) au sein d'une entreprise a pour mission de protéger les informations et les systèmes informatiques. Il gère les risques liés à la sécurité en identifiant les vulnérabilités et en mettant en place des mesures pour les réduire. Il élabore des politiques et des procédures de sécurité pour guider les employés dans les bonnes pratiques. Le service SSI surveille les activités du système pour détecter les incidents de sécurité et réagit rapidement en cas d'attaque. Il intervient pour enquêter, contenir et résoudre les incidents de sécurité.

Il sensibilise les employés à la sécurité informatique et fournit des formations sur les bonnes pratiques. Le service SSI veille à la conformité réglementaire en matière de sécurité des informations. En résumé, le service SSI assure la gestion des risques, met en place des politiques et des procédures, surveille et détecte les incidents, réagit aux incidents de sécurité, sensibilise les employés et garantit la conformité réglementaire.

3. Présentation du cadre technique général

3.1 Les missions du poste occupé

La mission qui m'a été proposée par ma tutrice est d'étudier le déploiement et la mise en place la PSSI au sein d'un organisme.

Cela signifie de comprendre ce qu'est la PSSI, pourquoi doit-elle être appliquée, comment sont mises en place les différentes règles.

Pour cela, l'objectif est de pouvoir faire un audit sur certaines règles réseau, comprendre comment faire le choix des preuves, et vérifier si les preuves apportées sont bien en adéquation avec la règle. De plus, des analyses de risques sur des solutions WIFI sont à mettre en place, c'est pourquoi je participerai à la réalisation de celles-ci afin de comprendre comment se construit une analyse de risque.

3.2 Fondamentaux

3.2.1 Qu'est-ce que la PSSI ?

La PSSI (Politique de Sécurité des Systèmes d'Information) est un ensemble de règles, procédures et mesures mises en place pour assurer la sécurité des systèmes d'information au sein d'une organisation. Elle est utilisée dans les services de Sécurité des Systèmes d'Information (SSI) de la CPAM, la Caisse Primaire d'Assurance Maladie, afin de garantir la protection des données sensibles liées à la santé des assurés.

La PSSI a pour objectif principal de prévenir les risques liés à la sécurité des systèmes d'informations et de mettre en place les moyens nécessaires pour y faire face. Elle vise à protéger les informations confidentielles, à assurer la disponibilité des services, à prévenir les intrusions ainsi qu'à détecter les éventuelles attaques. Elle définit les règles de sécurité à respecter, les responsabilités des différents acteurs, les procédures d'identification et d'authentification des utilisateurs, ainsi que les mesures techniques et organisationnelles à mettre en œuvre pour protéger les systèmes d'informations de la CPAM. Elle englobe des aspects tels que la gestion des accès, la protection des données, la sauvegarde et la restauration des informations, la sensibilisation des utilisateurs et la gestion des incidents de sécurité.

La PSSI peut donc s'appuyer sur les principes et les bonnes pratiques de l'ISO 27001 pour élaborer sa politique de sécurité, et pour mettre en place un système de gestion efficace de la sécurité des systèmes d'informations au sein de la CPAM. En intégrant les exigences de l'ISO 27001, la PSSI peut bénéficier d'un cadre reconnu internationalement pour renforcer la sécurité et la protection des données au sein de l'organisation. Actuellement, la CPAM se base sur la PSSI-MCAS, qui est la nouvelle version la PSSI.

3.2.2 Qu’est-ce que le RGPD ?

La RGPD (Règlement général sur la protection des données) est un règlement de l'Union européenne qui vise à renforcer la protection des données personnelles des individus au sein de l'UE et de l'EEE. Entrée en vigueur en 2018, la RGPD remplace la directive de protection des données de 1995 et impose des obligations aux organisations qui collectent, utilisent ou traitent des données personnelles.

Son rôle principal est de donner aux individus un plus grand contrôle sur leurs données personnelles et de responsabiliser les organisations. Elle exige un consentement clair et explicite pour la collecte et le traitement des données, ainsi que la transparence et la divulgation des pratiques de traitement des données. Les droits des individus sont renforcés, leur permettant d'accéder à leurs données, de les rectifier, de les supprimer, de restreindre leur traitement et de s'opposer à leur utilisation à des fins spécifiques.

La RGPD place la responsabilité sur les organisations en les obligeant à mettre en place des mesures de sécurité adéquates pour protéger les données personnelles et à tenir des registres détaillés de leurs activités de traitement des données. En cas de violation de données, les organisations doivent notifier les autorités compétentes et les individus concernés. La portée de la RGPD est mondiale, s'appliquant à toute organisation traitant des données personnelles d'individus de l'UE, qu'elle soit basée dans l'UE ou non. Son objectif est de garantir que les données personnelles sont traitées de manière éthique, sécurisée et que les individus ont un contrôle sur leur utilisation.

3.2.3 Qu’est-ce que la SSI ?

Le service SSI (Sécurité du Système d'Information) au sein d'une entreprise est responsable de la protection et de la sécurité des informations et des systèmes informatiques de l'organisation. Son rôle principal est de prévenir les incidents de sécurité, de détecter les potentielles menaces et d'y répondre de manière appropriée.

Le service SSI met en place des politiques, des procédures et des mesures de sécurité pour protéger les actifs informationnels de l'entreprise, y compris les données sensibles, les systèmes informatiques, les réseaux et les applications. Il s'assure de l'intégrité, de la confidentialité et de la disponibilité des informations, ainsi que de la continuité des opérations.

Les responsabilités du service SSI incluent la surveillance des activités de sécurité, l'identification des vulnérabilités, la gestion des incidents de sécurité, la sensibilisation et la formation des employés à la sécurité informatique, la mise en place de contrôles d'accès et de politiques de sécurité, ainsi que la conformité aux réglementations et aux normes en matière de sécurité.

Lorsqu’un site est considéré comme LAN, c’est qu’il suit un certain nombre de règle recommandé par la DR (Département Réseau), que l’on considère comme les bonnes pratiques à mettre en place dans l’organisme. À la suite de plusieurs décrets, articles de lois et arrêtés, ces organismes peuvent devenir des OSE (Opérateurs de Services Essentiels). Ces organismes, en plus de suivre les règles de bonnes pratiques, doivent en supplément, suivre des nouvelles règles, qui permettrons au site d’être encore plus sécurisé.

3.2.4 Qu'est-ce qu'un OSE ?

Les OSE jouent un rôle crucial dans le maintien des infrastructures et des services vitaux qui soutiennent le fonctionnement quotidien de nos sociétés modernes. Ils sont soumis à des réglementations spécifiques et doivent respecter des normes élevées de sécurité et de fiabilité pour garantir la continuité des services.

D'autre part, un OIV est une entité qui exerce une activité critique pour la sécurité nationale ou le fonctionnement de l'État. Les OIV sont souvent liés à des secteurs tels que la défense, la sécurité intérieure, les télécommunications, les systèmes d'informations, la santé, les transports, l'énergie et les finances. Leur importance réside dans le fait qu'ils contribuent à la stabilité, à la continuité et à la souveraineté d'un pays.

La principale différence entre un OSE et un OIV est donc leur niveau de criticité. Les OIV sont considérés comme ayant un impact encore plus crucial sur la sécurité nationale et le fonctionnement de l'État par rapport aux OSE. En conséquence, les OIV sont soumis à des exigences plus strictes en matière de sécurité, de protection des informations sensibles et de continuité des activités, ainsi qu'à une surveillance et à une supervision plus étroite de la part des autorités gouvernementales.

4. Audit sur les règles réseau de la PSSI

4.1 Quelles sont les règles étudiées ?

La PSSI est un document qui est construit par chaque entreprise, avec plus d'une centaine de règles. Un audit interne est réalisé chaque année afin de voir, au sein de l'entreprise, si toutes les règles de la PSSI sont bien mises en place.

Afin de préparer l'audit de l'année 2022-2023, voici les règles qui m'ont été attribuées afin de réaliser la supervision du bon déroulement de la récupération des preuves :

RES-CLOIS : cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes. Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.
RES-RESS : cloisonnement des ressources en cas de partage de locaux. Dans le cas où une entité partage des locaux (bureaux ou locaux techniques) avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place. Si le cloisonnement n'est pas physique, les mesures prises doivent être validées par le HFDS.
RES-SECRET : modifier systématiquement les éléments d'authentification par défaut des équipements et services. Les mots de passe par défaut doivent être impérativement modifiés, de même en ce qui concerne les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.
RES-SSFIL : mise en place de réseaux sans fil. Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifique. Les protections intrinsèques étant insuffisantes, des mesures complémentaires, validées par le SHFDS, doivent être prises dans le cadre de la défense en profondeur. En particulier, une segmentation du réseau doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion depuis la voie radio. À défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil sur des SI manipulant des données sensibles est proscrit.

Figure 3 : Liste des quatre règles supervisées lors de l'audit

Les règles sont énoncées de manière succincte dans la PSSI. De façon locale, un tableur est mis en forme pour chaque règle, avec les attentes précises de ce qui doit être effectuées et vérifiées. En guise d'exemple, on peut voir que pour la règle RES-CLOIS, on retrouve l'énoncé de la règle contenue dans la PSSI, puis les actions à mener pour être conforme.

Règles	Libellé	Actions (intégration correction du 04/03/2022 et 2023)	Spécif & Mesures
RES-CLOIS	Cloisonnement du réseau selon les consignes nationales	[A1]-En cas de non labellisation à 100% d'un des sites de l'organisme, l'organisme doit réaliser un plan d'action et mettre en oeuvre les actions de correction adéquates	Vérification possible sur le site du DR - Infrastructure>LAN>Audits/Labellisation>Liste de vos audits Les organismes peuvent faire une demande de labellisation de leur site auprès du DR Si un des sites de l'organisme est labelisé depuis plus de 3 ans, il conviendra de faire une demande de nouvelle labelisation au DR
		[A1]-Les préconisations nationales sont déclinées localement et vérifiées périodiquement par le Département Réseau (labellisation)	

Figure 4 : Tableau pour la règle RES-CLOIS de sa mise en œuvre au sein de l'organisme

4.2 Attentes et preuves des règles

Pour donner suite à l'approche de l'audit sur l'année 2022-2023, j'ai été nommé pour superviser quelques règles réseau venant de la PSSI (celles-ci-dessus). J'ai donc dû m'organiser pour récolter les preuves auprès des différents services. Pour se faire, nous avons organisé deux réunions. Une pour expliquer les points d'améliorations et ce qui doit être changé, avec des preuves de changement. Et une autre, plus tard, pour analyser ensemble les preuves, pour constater les changements ou non, afin de voir si nous sommes en conformité après les modifications demandées.

4.2.1 Règle RES-CLOIS

La règle RES-CLOIS est de montrer que chaque site de la CPAM est labellisé à 100%. Le terme labellisé signifie que le site doit suivre un nombre de mesure de sécurité imposé par le DR, et chaque site doit être à labellisé à 100%. De plus, un site n'est plus labellisé si la date de sa dernière labellisation est ancienne de plus de trois ans.
Pour répondre aux exigences, nous avons consulté le site du CNGR (Centre National de Gestion du Réseau), qui propose un onglet qui liste tous les sites et leurs labellisations.

Pour la règle RES-CLOIS, la PSSI demande de mettre un place un cloisonnement physique, en fonction du besoin de sécurité de chaque zone. Pour cela, et avec l'aide du site du CNGR, nous avons la liste de ce qui est mis en place localement en termes de sécurité :

1 - Architecture LAN générale *(Design, stackage, agrégats/interco (design), modèles de switches, ...)*
2 - ACCES *(conformité au chapitre « Configuration des accès » dans les guides)*
3 - SNMP – HPNA *(SNMP conforme et intégration de la totalité des switches dans HPNA, NOMMAGE des switches)...*
4 - Spanning-tree *(mise en œuvre générale conforme)*
5 - Version des switches *HP A3600 : 5.20.R2112P05 HP A5500 : 5.20.R2222P08 HP A5120 EI : 5.20.R2222P09 HP A5120 SI...*
6 - Configuration des interfaces *(configuration et description, shut des interfaces Giga HP, agrégats, ESX...)*
7 - LLDP - NTP – DHCP *(snooping / relais) (mise en œuvre générale conforme)*
8 - VLAN et Adressage *(mise en œuvre des VLAN minimum, adressage respecté, ACL si VLAN 224)*
9 - Interconnexion RAMAGE *(configuration / connexion sur ports normalisés)*
10 - Routages *(RIP et routages statiques sur fédérateurs / route par défaut à l'extrémité)*

Figure 5 : Liste des mesures de sécurité mise en place pour respecter le cloisonnement

Par la suite, chaque site sont détaillés, et en fonction de ce qui n'est pas mis en place, nous aurons une annotation de ce qui doit être modifié au sein même du site en question. Après avoir trié dans un tableau Excel tous les sites qui ne sont pas conformes à la labellisation, je me suis penché plus en détail sur les points qu'il fallait changer. Le seul point se trouve sur le site du Patio, c'est un VLAN qui n'a pas les bonnes adresses IP de configurées.

10 - Routages *(RIP et routages statiques sur fédérateurs / route par défaut à l'extrémité)*		vlan 5 : adresse non normalisée [redacted]

Figure 6 : Retour d'audit sur les problèmes du site du Patio (CNGR > Audit)

Dans notre cas, pour que la labellisation soit à 100%, une demande PSN (Portail Support National) a été faite, la voici :

cas: Evolution ou création d'une liaison réseau
Nom du site: Plusieurs
Adresse postale du site: Plusieurs sites concernés
En cas d'absence:
Nom/référence de la liaison:
Type d'évolution souhaitée:
Justification argumentée du besoin:
Bonjour,

Dans le cadre de la labellisation LAN de plusieurs sites de notre organisme, nous devons mettre en conformité le plan d'adressage du VLAN d'interconnexion.

Nous avons établi une liste de correspondance pour les sites concernés (cf. pièce jointe).

Il est à noter que pour des raisons de rupture de service inhérentes à ces changements, les opérations de MOD-CONF devront avoir lieu à 12H.

Merci de transmettre cette demande au GIDOPE afin d'en assurer son traitement.

Cordialement.

Figure 7 : Capture d'écran de la demande PSN pour labelliser le site du Patio

Les points qui devaient être changés n'ont pas encore été modifiés lors de ma présence. Sachant que toutes les modifications d'équipements proviennent d'une validation du CNGR, donc du national, la demande a bien été prise en compte, mais un créneau pour intervenir sur les équipements est à venir. La procédure quant à elle, est bien en cours.

4.2.2 Règle RES-RESS

La règle RES-RESS, si on se fie à ce que la PSSI demande, est de vérifier que si la CPAM accueille un organisme dans ses locaux, des mesures de cloisonnement doivent être mis en place de manière physique. Si le cloisonnement doit être fait en réseau, c'est la mise en place de VLAN dédier qui permet de répondre à la règle. Cette règle est mise en place dans notre organise selon plusieurs règles :

- Baie informatique dédier pour l'organisme hébergé ou intégré avec les équipements déjà présent
- La gestion des risques se fait par le site qui héberge l'organisme
- Les logs doivent être conservés sur trois mois
- Les mises à jour et les configurations doivent être conforment aux recommandations du CNGR

Un tableur est mis en place, en local, pour vérifier quels sont les sites qui hébergent des organismes extérieurs :

Date MAJ : Fév 2023 / [redacted]		Organismes Hébergés			
Site	Hébergeur	ELSM / DRSM ?	CARSAT Sud Est ?	MSA ?	CEIR Sud ?
Aix Mansard	CPAM Bouches-du-Rhône	O	O	N	N
Arles Alyscamps	CPAM Bouches-du-Rhône	O	O	O	N
Aubagne Défensions	CPAM Bouches-du-Rhône	O	O	N	N
Cabot	CPAM Bouches-du-Rhône	O	O	N	N
Capelette	CPAM Bouches-du-Rhône	O	N	N	N
Chateauneuf	CPAM Bouches-du-Rhône	O	O	N	N
Chartreux	CPAM Bouches-du-Rhône	O	O	N	N
Gardanne	CPAM Bouches-du-Rhône	O	O	N	N
Marignane	CPAM Bouches-du-Rhône	O	N	N	N
Salengro	CPAM Bouches-du-Rhône	O	O	N	N
Salon Canourgues	CPAM Bouches-du-Rhône	O	O	N	N
Valmante	CPAM Bouches-du-Rhône	O	N	N	O

Figure 8 : Tableau des organises hébergés en fonction de l'hébergeur ici la CPAM

Pour vérifier cette règle, j'attends comme preuve que les recommandations nationales soient mises en place dans ces sites.

Cette règle a déjà été validée l'année dernière, et aucun changement n'a eu lieu. Il n'y a pas de preuve supplémentaire à ajouter.

4.2.3 Règle RES-SECRET

La règle RES-SECRET est très certainement la plus évidente. Il s'agit de vérifier que chaque mot de passe utilisé dans n'importe quelles circonstances est bien changé tous les ans, et qu'ils correspondent bien à la politique des mots de passe suivante : comprendre entre 12 et 18 caractères en fonction de l'importance du mot de passe, avec des lettres majuscules, minuscules, des chiffres, des caractères spéciaux.

Cette règle demande à ce que les mots de passe soient changés au moins une fois par an.
Nous n'avons pas besoin de preuve formelle, mais le MSSI doit s'assurer que la mise en œuvre de cette règle est bien appliquée. Cependant, elle n'est pas appliquée dans les services, ce qui pose plusieurs problématiques sur la sécurité. En effet, si un mot de passe n'est pas changé, cela implique que : en conservant le même mot de passe pendant une longue période, on augmente les chances d'une compromission potentielle de nos comptes. Les attaquants pourraient exploiter des failles de sécurité, des fuites de données ou des techniques de piratage pour obtenir les mots de passe et accéder ainsi à des comptes sensibles. Le changement régulier du mot de passe est une bonne pratique qui renforce la sécurité en limitant la période d'exposition potentielle et en réduisant les risques liés à une utilisation non autorisée de nos comptes.

4.2.4 Règle RES-SSFIL

La règle RES-SSFIL se décompose en deux parties :

- Le Bluetooth : je dois me renseigner auprès des services concernés si du matériel Bluetooth est positionné dans l'organisme. Pour l'instant, l'analyse est en cours, et en attente de réponses.

- Le WIFI : sur les sites de la CPAM, trois types de WIFI sont possibles : le WIFI Interne, le WIFI Assurés et le WIFI Invité. Je sais d'ores et déjà que le WIFI Invité va être décommissionné, et donc que ce type de WIFI ne rentre plus dans la règle. Étant donné que cette solution ne sera plus utilisée, le fait de laisser les équipements toujours en place peut favoriser les attaques puisque les composants ne seront plus à jour, et ils ne seront plus supervisés. Le service SSI attend donc la preuve que ces équipements soient bien enlevés de l'architecture, pour assurer que la règle est bien mise en place. En revanche un QERSIweb (Questionnaire d'Evaluation des Risques pour le Système d'Information), communément appelé analyse de risque doit être fait pour les deux autres types de WIFI. J'ai la charge d'aider à la réalisation de l'analyse de risque pour le WIFI Interne, que j'aborderai dans le point suivant. Le QERSI concernant le WIFI Assurés va être initialisé sous peu, puisque le changement de solution est récent, et doit être mené à l'étude.

5. Analyse de risque sur le WIFI Interne

5.1 Le QERSIweb qu'est-ce que c'est ?

Le QERSI est une méthodologie d'analyse de risques utilisée au sein de l'Assurance Maladie, pour évaluer et gérer les risques liés à la sécurité du système d'information.

L'objectif principal du QERSI est d'identifier les vulnérabilités potentielles, les menaces et les conséquences associées à la sécurité des systèmes d'informations de la CPAM. Il s'agit d'une approche systématique qui permet d'évaluer les risques et de prioriser les mesures de sécurité appropriées pour les atténuer.

La méthodologie du QERSI repose sur plusieurs étapes clés. Tout d'abord, il consiste à identifier les actifs informatiques importants de la CPAM, tels que les systèmes, les données et les infrastructures. Ensuite, il évalue les menaces potentielles auxquelles ces actifs sont exposés, en tenant compte des événements indésirables, des acteurs malveillants et des vulnérabilités connues.

À partir de là, le QERSI permet d'analyser les conséquences probables en cas de compromission de ces actifs. Cela inclut les impacts financiers, opérationnels, juridiques et réputationnels. Il reste tout de même en compte les risques résiduels, ceux pour qui les risques qui leurs sont affectés ne sont pas traités puisque l'on décide que le risque ne générera pas de perturbation importante. Une fois les risques évalués, des mesures de sécurité sont recommandées et priorisées en fonction de leur efficacité pour réduire les risques identifiés.

Le QERSI doit être utilisé dès le début d'un projet touchant le système d'information, que ce soit un projet informatique (mise en place d'une nouvelle application développée au sein de son organisme, par un organisme partenaire), stratégique (projet RH (Ressource Humaine), thématique),
Le QERSI doit être utilisé dès le début d'un projet touchant le système d'information, que ce soit un projet informatique (mise en place d'une nouvelle application développée au sein de son organisme, par un organisme partenaire), stratégique (projet RH (Ressource Humaine), thématique), ou encore organisationnel (déménagement, modification des locaux), traitant des informations sur support numérique ou physique. Dans notre cas, c'est le support numérique qui sera privilégié.
Parfois, le QERSI doit être complété avec une analyse de risque, en amont, si le besoin se ressent.

5.2 Mise en place du QERSI pour le WIFI Interne

Pourquoi avoir fait un QERSI sur une solution qui a déjà été mise en œuvre ?

Un QERSI doit obligatoirement être initialisé dès qu'un projet voit le jour. Dans notre cas, le projet du WIFI n'a jamais été étudié, malgré le fait que la solution soit déjà mise en place au sein de l'organisme. Pour cela, le QERSIweb a été initié.
Voici, à l'étude, les différents points qui sont abordés dans le QERSI :

1 - Informations relatives aux données

Quelles sont les informations qui peuvent être dangereuses si elles sortent du système d'information, qu'est-ce qui est directement rattaché à une personne, y-a-t-il des données médicales ? Dans notre cas, les informations que l'on retrouve sont des données sur l'identité des personnes qui se connectent au WIFI, la version de l'OS (Operating System), ainsi que des données de géolocalisation, puisque dans les journaux de connexion, on retrouve le nom de la borne utilisée. Sachant que le nom est sous la forme du numéro de la salle et de l'étage, il est facile de géolocaliser la borne en question.

Une partie sert à comprendre qui fait quoi, c'est-à-dire qui agit sur l'édition, sur le transfert, sur les mises à jour, sur la consultation, soit qui y a accès. Dans notre cas, uniquement la consultation est prise en compte, et toutes les personnes qui sont habilitées peuvent alors utiliser la solution.

Il y a un aussi un focus sur l'administration de la solution, par qui et quoi ? C'est le service informatique qui s'occupe de l'administration des bornes WIFI. De plus, ils s'occupent de la gestion des bornes, des utilisateurs et des postes de travail.

Pour finir, la question se pose sur l'utilisation des données : d'où proviennent-elles, quel est le temps de conservation, y-a-t-il une destruction automatique, un archivage, où sont-elles stockées ?

2 - Mesures relatives à la sous-traitance et aux mutualisations

Ici, l'objectif est de comprendre si un sous-traitant intervient dans la manipulation des données, ou si tout est fait en interne. Pour donner suite aux différentes questions posées aux différents services, aucun sous-traitant n'intervient.

3 - Mesures relatives aux accès à l'application

On cherche à savoir qui a le droit d'accéder aux bornes WIFI. Seules les personnes qui sont authentifiées dans l'AD (Active Directory), et qui ont les droits d'accès pour se connecter pourront, peu importe le poste qu'ils utilisent. De plus, uniquement les postes de l'Assurance Maladie peuvent se connecter au WIFI.

5 - Mesures relatives aux cas de panne ou accès impossible

Cette partie nous permet de déterminer le temps d'action maximum d'indisponibilité de notre solution, et quels sont les impacts en cas d'indisponibilité de la solution. Etant donné que le WIFI est utilisé dans les salles de réunions, son indisponibilité n'aura pas un impact trop important pour ses utilisateurs. La connexion internet peut se faire en filaire. Mais la problématique du nombre d'utilisateurs pose alors un problème. Que faire si tout le monde doit travailler en réseau ? Il faut alors changer de salle de réunion. Le GTR (gestion de temps de réparabilité) est alors de huit heures, une intervention doit être investiguée.

6 - Modifications non désirées, disparition, vol ou accès illégitime à des données

Ici, on cherche à comprendre l'impact sur le SI, si l'intégrité n'est pas respectée. L'origine de ce problème peut être causé par l'erreur humaine, des personnes non-habilitées ou encore un piratage. Cela entraînerait des répercussions gênantes voir impactantes puisqu'il sera impossible de répondre à des requêtes judiciaires.

7 - Traces de connexions et traces applicatives

Le but est de comprendre s'il est important de garder les traces de connexion, et pendant combien de temps. Avec l'aide de toutes les documentations, la durée de conservation est définie à douze mois. En ce qui concerne les traces de connexions, elles doivent être conservées pour permettre de retracer les usages anormaux, qui se connecte, à quelle borne, qu'est ce qui est fait en aval.

5.3 Résultat du QERSI

Étant donné qu'une analyse de risque demande du temps et de nombreuses études avant d'être finalisée, je n'aurai pas le temps de voir la finalité. Cependant, j'ai pu tirer certaines conclusions. Il y a encore des points qui sont inconnus ou trop vagues, donc il faut pousser l'étude, et voir avec le national ce qui doit être mis en place. Par la suite, une demande PSN devra être faite, pour avoir un état des lieux de ce qui doit être rajouté pour augmenter la sécurité du WIFI au sein de la CPAM.

Le fait d'avoir travaillé sur cette analyse de risque m'a permis de découvrir tous les aspects à étudier avant qu'une solution soit mise en place, et j'ai pu aider le service SSI, puisqu'en parallèle, d'autre travaux ont pu être effectués.

6. Analyse de risque sur l'usage d'un service WIFI Public

6.1 La demande

Quelle est l'origine de la demande ?

Un service dit « métier » dont les missions se déroulent principalement au sein d'établissements hospitaliers s'est interrogé sur l'opportunité d'utiliser une connexion WIFI dont l'hôpital serait fournisseur d'accès.
Le service SSI a alors naturellement été saisi par rapport aux problématiques de sécurité que peuvent poser ce type de connexion « sans fils ».
Il m'a alors été demandé de mettre en avant l'ensemble des risques qui pourraient survenir.
Dans ce contexte, j'ai eu plusieurs options d'approche du sujet et sources d'informations à récupérer :

- Reprise de supports de cours du B.U.T. sur la question
- Suivi de l'actualité sur internet vis-à-vis des risques et menaces
- M'intéresser quant à la possibilité de faire une analyse de risques à partir de méthodes de référence

J'ai mis en œuvre les trois points ci-dessus, compilés sous forme d'une analyse de risques.

Le client souhaite pouvoir utiliser son réseau WIFI, interne à leurs locaux, pour que les CAM, qui sont des agents de l'AM, pour pouvoir utiliser les applicatifs qui sont dédiés l'Assurance Maladie. Cela implique que les CAM doivent pouvoir accéder au réseau RAMAGE de la CPAM et à tous les composants de protection. Il convient donc de vérifier que leur WIFI interne soit suffisamment sécurisé pour accueillir ces dispositifs.

C'est à ce moment que l'analyse de risque rentre en compte. Le but est de définir les différentes menaces et leur niveau de criticité, et de proposer des solutions en s'appuyant sur des méthodes spécifiques

6.2 Développement de l'analyse de risque

Pour faire une analyse de risque, j'ai eu deux solutions qui se sont offertes à moi. Utiliser la méthode EBIOS Risk Manager, ou utiliser la méthode Méhari. Mon choix s'est porté sur la méthode EBIOS. Cependant, le tableau de référence de Méhari vis-à-vis des risques relatifs au Wi-Fi me semblait plus actualisé et adapté. J'ai donc repris ce tableau pour notre projet d'étude de risques (EBIOS). Je me suis alors inspiré des deux méthodes pour étudier et évaluer les risques.

Dans un premier temps il a fallu que je définisse un couple « SR/OV », autrement dit, « Source de Risque » et « Objectif Visé (en termes de sécurité) » pour couvrir le risque. J'ai alors décidé de mettre en corrélation les règles de la PSSI qui, pour moi, sont primordiales quand on souhaite aborder un thème tel que le WIFI, avec le couple SR/OV. Mon objectif vise à répondre aux sources de risques, avec les règles de la PSSI, puisque des solutions de sécurités en découlent.

Identification SR/OV (source de risque / objectif visé)		Règle à suivre	
Utilisation d'une interface non sécurisée pour accéder au wifi	Configurer les interfaces de connexion de réseau sans fil	PDT-NOMAD-CONNEX	Règle PSSI
Laisser des interfaces de connexions libres	Désactiver les interfaces de connexion de réseau sans fil	PDT-NOMAD-DESACTIV	
Avoir la visibilité sur ce que l'on fait	Filtre de confidentialité	PDT-NOMAD-FILT	
Libre accès aux informations	Stockage local d'informations sur les postes nomades	PDT-NOMAD-STOCK	
Accès non autorisé	Mettre en place un pare-feu local	PDT-NOMAD-PAREFEU	
Utiliser un pc étranger non reconnu	Déclaration des équipements nomades aptes à traiter des informations sensibles	EXP-NOMAD-SENS	

Figure 9 : Tableau sur le couple SR/OV avec les règles à suivre

Par la suite, il m'a fallu mettre en place une échelle de gravité en fonction des conséquences des potentiels risques, et qu'est-ce que cela engendrera. Cette échelle est propre à chacun, il n'y a pas d'échelle définie pour chaque type de projet. J'ai alors décidé que l'échelle serait représentée par :

Echelle	Conséquence
Critique	Le réseau devient indisponible, des donnnées sont dérobées et la sécurité du site est mise en péril
Grave	Arrêt temporaire de l'exploitation puis reprise sous une procédure particulière
Significatif	Ce type d'attaque doit être surveillé mais nécessite une sensibilisation pour que les risques soient moindres
Mineure	Attaque sans réelles conséquences, mais qui n'empêche pas le bon déroulement de son travail sur le poste

Figure 10 : Tableau pour définir une échelle de criticité et les conséquences qui en découlent

Grâce à la méthode Méhari, j'ai pu définir les différents évènements redoutés, puisque Méhari offre une base de données avec des explications des différents types d'attaques, de problèmes, qui peuvent être rencontrés. J'ai alors retenu une liste d'évènements qui serait susceptible d'arriver dans le cadre du projet à étudier. Il faut aussi comprendre en profondeur ces évènements, pour mieux appréhender les impacts qui pourrait en découler. Avec l'échelle de gravité définie précédemment, nous pouvons alors associer à chaque impact, sa gravité.

Afin de me simplifier la tâche pour la suite, nous allons nommer chaque évènement sous la forme « Rx », puisque nous allons devoir traiter huit évènements différents.

Intitulé	Evènement redouté	Impacts	Gravité
R1	Interception des données confidentielles lors d'une connexion	Récupération des mots de passes, d'adresses emails, de fichiers	C
R2	Installation de logiciel malveillant	Faire planter le système Paralyser le poste Prise de contrôle à distance du PC Perte de performance Installation de logiciel invisible	G
R3	Recevoir des mails / messages vous demandant de réinitialiser votre mot de passe	Ransomware Menace Pour les personnes non sensibilisées, possibilité de tomber dans le piège	S
R4	Repérer les activités d'un CAM sur Internet	Repérer les activités Préparation potentielle d'attaque	M
R5	Se faire attaquer son réseau	Indisponibilité du réseau Intrusion de personnes malveillantes Vol de données	C
R6	Avoir une mauvaise stabilité au niveau du réseau	Temps d'éxécution des tâches plus lente Perte de son travail (sans sauvegarde)	M
R7	Intrusion dans la pièce où se trouve le poste	Usurpation d'identité Vol de données	C
R8	Attaque sur le poste car mal sécurisé	Plus facile d'accéder à des données sur le poste Possibiliter d'installer des malwares Accès à tous les dossiers et information du poste	C

Figure 11 : Tableau pour définir les évènements redoutés et leurs impacts, avec leur niveau de gravité

Il faut comprendre que le risque zéro n'existe pas. Parfois, nous devons continuer d'utiliser notre solution, mais en essayant d'évaluer et de corriger pour la plupart, leur niveau de risque, son acceptabilité, et les décisions et actions à mener, si l'un de ces évènements venait à se produire.
Pour cela, j'ai mis en place une autre échelle sur le niveau de risque d'un évènement. En fonction de ce dernier, il sera possible d'envisager une solution différée, lorsque le service reste en exploitation, et dans d'autre cas, apporter une solution qui assurera la sécurité, le plus rapidement possible.

Niveau de risque	Acceptabilité du risque	Décisions et actions
Faible	Acceptable en l'état	Vigilance
Moyen	Tolérable sous contrôle	Suivi du risque et action à mener pour limiter et réduire l'impact de ces risques
Elevé	Inacceptable	Réaction rapide à mettre en place pour éviter de compromettre des informations, et perdre des données sensibles

Figure 12 : Tableau pour définir les décisions et actions à mener en fonction du niveau de risque

Après avoir défini toutes les échelles pour montrer la criticité, imaginé tous les évènements et impacts qui peuvent toucher notre solution, je dois maintenant classer ces évènements en fonction de cette échelle. Cela va me permettre d'éliminer les évènements mineurs, et me concentrer uniquement sur ceux qui sont les plus critiques pour la sécurité de l'entreprise. Pour commencer, nous devons classer chacun des évènements dans le tableau :

Gravité \ Probabilité	Improbable	Peu Probable	Probable	Très Probable	Certain
Critique			R7	R1 / R5 / R8	
Grave			R2		
Significative			R3		
Mineure		R4	R6		

Figure 13 : Classement des évènements en fonction de leur gravité et de leur probabilité

J'ai pu remarquer dans le tableau ci-dessus que certains évènements sont probables voir peu probable, et que leur impact, donc leur gravité est mineure. Au contraire, d'autres sont critiques, et en prime, il est très probable que ces évènements arrivent. Je dois être capable de proposer des solutions de sécurités suffisantes pour que, dans notre cas, les évènements R1/R5/R8 ne se trouvent plus dans la zone rouge du tableau. Lors d'une analyse de risque, tous les évènements qui ont été relevés doivent sortir de la zone rouge, puisque c'est la plus impactante et qui risque de paralyser tout le système informatique. J'ai alors décidé, avec mes recherches dans les documentations et ce qui est possible de faire, une ou plusieurs solutions pour les évènements restants :

Intitulé	Matériel mis en place pour :
R1	Utilisation d'un proxy pour limiter l'accès à des sites frauduleux Désactiver toutes les interfaces inutilisées
R2	Installer AdBlock / AdBlock+ Mise en activité d'un anti-virus McAfee ou MalwareBytes
R5	Bloquer les connexions non autorisées Surveiller les connexions entrantes et sortantes Utilisation d'un parefeu qui bloque tout
R7	Sécuriser la pièce avec un code, une carte accès unique Protéger l'ordinateur avec un code fort
R8	Service Cisco UMBRELLA Mise à jour régulière

Figure 14 : Liste des solutions proposées pour sécuriser les différents évènements

Je projette mon analyse, c'est-à-dire que j'image que ces solutions ont déjà été mises en place. Le tableau qui classe les évènements en fonction de leur gravité et de leur probabilité peut être mis à jour, puisque l'objectif de ces solutions est de réduire l'impact des évènements sur le poste de travail, dans le cadre de notre projet. Voici la version finale de ce tableau, lorsque les solutions ont été mises en œuvre.

Gravité \ Probabilité	Improbable	Peu Probable	Probable	Très Probable	Certain
Critique		R7	R1 / R5 / R8		
Grave		R2			
Significative		R3			
Mineure					

Figure 15 : Classement des évènements en fonction de leur gravité et de leur probabilité après la mise en place des solutions adéquates.

En conclusion, cette analyse de risque est à titre indicatif de ce qui doit être mis en œuvre ou non. Si j'étais dans les locaux où les solutions devraient être implémentées, j'aurais pu faire une analyse sur la durée, c'est-à-dire utiliser les mêmes évènements, mais étudiés sur plusieurs mois en termes de menaces, mais également les solutions à rajouter ou modifier.

6.3 Conclusion et réponse au client

Le MSSI de l'organisme a donc pris connaissance de mes travaux et s'est attaché à formaliser une réponse officielle à laquelle j'ai participé.

La formalisation de la réponse a pris en compte plusieurs critères :

- La présente analyse de risques
- La PSSI et les recommandations du CNGR
- Quatre points prépondérants de SSI : l'intégrité, la confidentialité, la disponibilité et les « traces et preuves » (critère de non-répudiation)

La synthèse est ainsi rédigée sous forme du mail ci-dessous, qui donne la conclusion à cette étude :

Avec l'aide du MSSI du service SSI, nous avons pu rédiger cette réponse :

Bonjour Guillaume,

Nous nous sommes penchés sur la question de la connexion Wi-Fi externe dans les conditions que tu décris, à savoir une connexion sur une borne d'accès dont nous ne maîtrisons pas la mise en place.

L'avis MSSI est le suivant :
Il n'est pas recommandé de se connecter à un réseau Wi-Fi de type « patient » qui n'est pas sécurisé. Seule une connexion sécurisée, à un réseau dit (si je reprends tes termes) : « du Personnel » ou « Direction » sera envisageable sous certaines conditions.

En terme de SSI, on raisonne sur 4 critères principaux : Disponibilité / Intégrité / Confidentialité / Traces & Preuves
Je vais donc m'efforcer de donner ici les premières recommandations/exigences à partir de ces critères.

Intégrité / Confidentialité :
Il faut s'assurer que le réseau Wi-Fi est sécurisé (comme toute entité publique, elle peut être attaquée).

- Il faut qu'il n'y ait aucune ambiguïté sur le nom du réseau sur lequel se connecter à partir du PMF portable. Un attaquant pourrait tromper un CAM avec un nom s'approchant du nom officiel, ex : WiFiHopital **vs** WiFiHopital (On ne voit pas ici la différence : mais dans le 2ème WiFiHopital, le dernier caractère est un « i » majuscule).
- L'établissement doit pouvoir fournir un *[nom d'utilisateur/mot de passe de connexion]* idéalement pour chaque CAM : si le RSSI local souhaite auditer les mouvements sur son Wi-Fi de manière individuelle. Mot de passe fort (au moins 12 c ; Maj/min/Chiffres…), que le CAM doit pouvoir changer (à la 1ère connexion par exemple).
- Quand on va se connecter : le système établi une liaison chiffrée associée à un protocole (certains de ces protocoles sont obsolètes, ne sont plus sécurisés aujourd'hui / crackables). Exigence : Le protocole de connexion Wi-Fi doit être WPA2 ou supérieur.
- Des dispositifs de type « PareFeu » et « Antivirus » sont surement installés au niveau de l'établissement. Seront-ils compatibles avec nos matériels ? Nous avons-nous-même déjà des outils de sécurité installés (StormShield / Tehtris / CISCO Umbrella si toujours actif – à vérifier).

Disponibilité :

- Le réseau Wi-Fi doit avoir une couverture suffisamment étendue afin de ne pas être dans la même problématique de déconnexions/reconnexions que celle actuelle qui touchent les téléphones portables : couverture locale (physique) et couverture horaire.
- Le réseau de l'établissement (Wi-Fi et LAN/routeurs) doit pouvoir laisser passer et supporter le flux VPN de l'Assurance Maladie. La bande passante reste à déterminer (on pourrait reprendre les mêmes métriques que pour une connexion nomade quand l'agent est en télétravail).
- Ce réseau sera réservé aux PMF portables de l'Assurance Maladie exclusivement, il serait mal vu que les agents s'y connectent avec leur téléphone perso.
- Un mot sur la rupture éventuelle de service : on ne pourrait biensûr pas exiger quoi que ce soit / on pourra repasser vers les téléphones portables.

Traces & Preuves :

- L'établissement en tant que "fournisseur d'accès" doit pouvoir consulter les journaux de connexions. Il faut donc que les CAM aient à l'esprit que cette possibilité est plausible. Par ailleurs, l'établissement devra s'engager à supprimer ces historiques au bout de 6 mois (glissants).

Dans l'idéal, une convention avec l'établissement serait indispensable, reprenant une bonne partie des items donnés ici :

- Le RSSI local pourrait demander par exemple des garanties sur la sécurisation de nos matériels : Il s'agit aussi pour l'établissement de s'assurer contractuellement que nous ne connecterons que des PMF de l'Assurance maladie.
- De notre côté, nous devons nous assurer que l'établissement décline aussi une PSSI locale, et nous pourrions demander à en connaitre les détails.

Voilà déjà les premières recommandations de SSI qui sont ressorties, suite à notre réflexion : réflexion qui pourrait être le point de départ à une analyse de risques peut-être plus complète.

A bientôt,
Cordialement,

A cette étape, il appartient au services métier de reprendre contact avec un premier établissement hospitalier pour convenir de la mise en place des recommandations formulées dans le mail. Selon les suites à donner, et afin d'officialiser l'analyse de risques en tant que telle, celle-ci sera transposée dans QERSIweb.

7. Sensibilisation des utilisateurs

7.1 Première approche sécurité des nouveaux employés

Lors de l'arrivée de nouveaux employés au sein de l'entreprise, peu importe le service dans lequel est affectée cette personne, il doit suivre une sensibilisation informatique sur les dangers et les précautions à adopter en cas de problème.
Cette sensibilisation est un point de vue général sur l'organisation et les risques liés aux systèmes d'informations de l'entreprise. Le but est alors de faire comprendre aux nouveaux arrivants les bases de la SSI.

Cette présentation se construit sous la forme :

- Une présentation générale
- Deux quizz pour vérifier s'ils ont retenu les informations importantes

Pour donner suite à une demande nationale, qui s'attarde beaucoup sur la sensibilisation de ses employés, une mise à jour des quizz a été mise en place.

Dans un second temps, lorsque vous êtes un nouvel employé, vous aurez accès à LIAM, un réseau social interne à l'Assurance Maladie, qui regroupe tous les services. Le service SSI parle de l'aspect sécurité des données, des bons gestes à avoir, de comment réagir en cas de problème. Cela montre qu'il y a une sensibilisation continue au cours de votre travail.

7.2 Création d'une partie ChatGPT dans les diapositives

Nous savons que les intelligences artificielles prennent de plus en plus de place dans notre société, elles deviennent des outils complémentaires pour nos travaux, mais elles présentent un risque très élevé concernant la sécurité des systèmes d'informations.
Étant donné que nous sommes dans le cadre d'une sensibilisation, l'objectif est de rendre accessible les problèmes liés aux intelligences artificielles et quelles conséquences peuvent-elles y avoir sur un système d'information.

Les quizz sont sous forme de diaporama, l'objectif est de faire quelque chose de clair, succinct et d'identifier les risques. Pour illustrer le plus de choses, nous avons mis en place trois diapositives différentes :

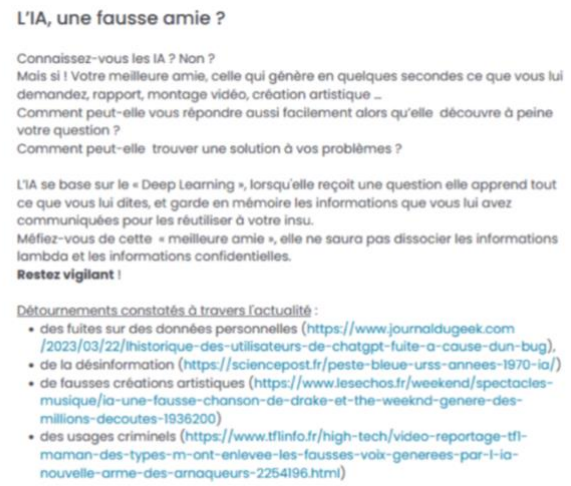
- Comprendre le risque des données sensibles qui sont utilisées sur ChatGPT, dans le cadre de la rédaction d'une lettre pour changer son compte bancaire

- Savoir quelles sont les informations que l'on donne à ChatGPT et qui peuvent corrompre la sécurité de vos informations (logo, documentation publique, numéro de sécurité social)

- Dans le cadre d'un informaticien, quelles sont les actions qui peuvent nous paraître sans conséquence, mais qui, si l'utilisation de l'IA (intelligence artificielle) est mal faite, celle-ci pourrait faire fuiter des données confidentielles.

7.3 Création d'articles préventifs sur les intelligences artificielles

Sur LIAM, de nombreuses vidéos sont postées pour sensibiliser les employés. Parfois, dans des cas plus généraux, les équipes rédigent des articles sur un sujet particulier. Dans mon cas, l'objectif était de faire comprendre les risques de ChatGPT, premièrement d'une façon générale, puis deuxièmement, plus axé sur son utilisation dans le monde du travail.
La publication des articles ou de toutes informations se fait sur le réseau social propre à la CPAM, c'est-à-dire sur LIAM.
Après de multiples recherches, voici un des articles que j'ai pu rédiger et publié sur LIAM :



L'IA, une fausse amie ?

Connaissez-vous les IA ? Non ?
Mais si ! Votre meilleure amie, celle qui génère en quelques secondes ce que vous lui demandez, rapport, montage vidéo, création artistique ...
Comment peut-elle vous répondre aussi facilement alors qu'elle découvre à peine votre question ?
Comment peut-elle trouver une solution à vos problèmes ?

L'IA se base sur le « Deep Learning », lorsqu'elle reçoit une question elle apprend tout ce que vous lui dites, et garde en mémoire les informations que vous lui avez communiquées pour les réutiliser à votre insu.
Méfiez-vous de cette « meilleure amie », elle ne saura pas dissocier les informations lambda et les informations confidentielles.
Restez vigilant !

Détournements constatés à travers l'actualité :

- des fuites sur des données personnelles (https://www.journaldugeek.com/2023/03/22/lhistorique-des-utilisateurs-de-chatgpt-fuite-a-cause-dun-bug),
- de la désinformation (https://sciencepost.fr/peste-bleue-urss-annees-1970-ia/)
- de fausses créations artistiques (https://www.lesechos.fr/weekend/spectacles-musique/ia-une-fausse-chanson-de-drake-et-the-weeknd-genere-des-millions-decoutes-1936200)
- des usages criminels (https://www.tflinfo.fr/high-tech/video-reportage-tfl-maman-des-types-m-ont-enlevee-les-fausses-voix-generees-par-l-ia-nouvelle-arme-des-arnaqueurs-2254196.html)

Figure 16 : Article préventif sur l'utilisation de ChatGPT

8. Conclusion

Ce stage de dix semaines réalisées au sein du service SSI de la CPAM m'aura été grandement bénéfique tant sur le côté technique que sur le plan humain.

Cela m'a permis de découvrir un aspect de la cybersécurité qui est plus poussé et différent de ce que le public peut le voir et se l'imaginer. Quand on pense sécurité, on pense à tout ce qui est mis en place, mais pas forcément à la sécurisation des données et le rôle qu'elles peuvent y jouer.

De plus, le stage m'a permis de réellement découvrir le monde du travail, et mettre en application ce que j'ai pu apprendre et réalisé durant les travaux pratiques et l'année scolaire. Mais au sein d'un contexte professionnalisant, qui est adapté dans une équipe de travail avec ainsi le côté relationnel, et le travail en équipe.

Le fait de travailler sur plusieurs thématiques et sujets divers à la fois m'a permis de m'organiser pour ne pas me perdre dans mon travail, de voir plusieurs aspects de comment fonctionne un SI, et de réagir en fonction des besoins de l'entreprise.

Quant à ma mission, le fait de travailler dans un environnement inconnu et dans un domaine que je ne connais pas en profondeur, m'a permis de m'enrichir sur ma façon de m'organiser, j'ai su améliorer mes méthodes de travail individuelles et en équipe, et cela m'a conduit à mener un apprentissage en profondeur sur des domaines dont je n'ai pas l'habitude de travailler et traiter.

Pour finir, ce stage a renforcé mon intérêt de travailler et d'évoluer dans le domaine de l'informatique, et il a su enrichir mes connaissances au travers des diverses et multiples missions qui m'ont été données et pour lesquelles j'ai su m'investir et j'ai pu retranscrire mon savoir et mes différents bagages.

9. Remerciements

Tout d’abord, je tiens à remercier tout le personnel du service SSI (Sécurité des Système Informatique) de la CPAM pour leur accueil et l’accompagnement de qualité dont j’ai pu bénéficier tout au long de mon stage.

Je tiens à remercier particulièrement ma tutrice de stage Madame Florence MOLAIRE et Monsieur Jean Pascal BOIZIS, pour leur gentillesse, leur disponibilité à mon égard et pour leurs conseils qui ont orienté mon travail pendant la durée de mon stage.

Je remercie également Monsieur Benoit RICHARD, Monsieur Sylvain VIVANCO, Monsieur Swen FELICES, Monsieur Jean François JOUBERT et tout le service SASI informatique, pour leur temps, leurs réponses à mes questions, leur gentillesse, et leur aide lorsque j’ai pu avoir des questions concernant le réseau et ses infrastructures.

Et enfin je remercie toute l’équipe pédagogique Réseaux et Télécommunications de mon IUT de m’avoir guidé sur le plan professionnel et éducatif durant ces deux années qui m’ont été précieuses durant mon stage.

10. Glossaire

BUT : Bachelor Universitaire de Technologie

Labellisé : Ce terme permet de juger, à la suite des règles de sécurité qui doivent être appliquées sur chaque site de l'organisme, à combien de pour cent il applique ces règles.

CNGR : Le CNGR est le Centre National de Gestion du Réseau, c'est sur ce site que nous retrouvons toutes les documentations nécessaires pour configurer chaque équipement, les retours sur les audits des sites.

PSN : Portail Support National, c'est une demande qui est faite lorsque des problèmes sont rencontrés ou les réponses sont manquantes, et que nous avons besoin de l'aide ou de l'approbation du national.

CAM : Conseillé de l'Assurance Maladie, ce sont des agents de l'Assurance Maladie, qui travaillent dans des organismes extérieurs, dans notre cas dans les hôpitaux.

RAMAGE : Réseau de l'Assurance Maladie du Régime Général, c'est le réseau qui est utilisé par l'ensemble des sites de la CPAM.

Analyse de risque : Analyse d'un système ou d'une solution, pour comprendre les risques qui l'entourent et leurs gravités, afin de mettre en place des solutions de sécurités.

EBIOS Risk Manager : Méthode permettant de réaliser des analyses de risques.

Méhari : Méthode permettant de réaliser dans analyses de risques

Couple « SR/OV » : Autrement dit, « Source de Risque » et « Objectif Visé (en termes de sécurité) » dans une analyse de risque, ce couple permet de comprendre d'où provient le risque, et qu'est-ce que l'on cherche à mettre en place pour le sécuriser.

ChatGPT : Intelligence artificielle qui ne cesse d'évoluer, et qui représente une menace pour les systèmes d'information.

11. Bibliographie

- Toutes les documentations techniques pour rédiger mon rapport son des documents confidentiels, je ne peux donc pas les faire apparaitre.

- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031386468 (Journal Officiel, 1er Octobre, 2015).

  https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/
- EBIOS Risk Manager (Clusif)

- https://www.ssi.gouv.fr/guide/la-methode-ebios-risk-manager-le-guide/

- https://openai.com/blog/chatgpt (ChatGPT)

- https://www.ssi.gouv.fr