

Retour d'expériences de 50 RSI Grands Comptes

Préambule

Réalisation d'une **étude exploratoire auprès de 50 RSI, des PME > à 200 personnes et Grandes Comptes de la région Rhône Alpes.**

✓ Une étude exploratoire qu'est ce que c'est ? :
C'est une approche permettant de mieux comprendre et connaître les motivations des acteurs étudiés et les mécanismes psychologiques de leur comportement.

Méthodologie :

- Entretiens par téléphone avec **un questionnaire semi-directif.**
- Un échantillon représentatif, tous secteurs d'activités représentés (Industrie, Transport, collectivités locales/ éducation, santé et services)
- Interviews auprès des acteurs Responsable Sécurité du Système d'Information

Objectif de cette étude :

- Mieux comprendre le métier de la sécurisation des données.
- Faire un retour concret sur les expériences des PME « sécurisées » afin d'en faire profiter des PME désireuses de développer un plan d'action.

Remerciements :

Nous remercions tous les interviewés qui nous ont permis de réaliser cette synthèse.

Certains RSSI, nous ont fait part, de **leur souhait d'interpeller les PME sur le sujet.** Aussi, nous avons notifié leurs remarques précises sur les différents points abordés.

PERCEPTION DE LA SSI EN PME PAR LES RSSI

Question 1 : « Quelle est votre perception en matière de sécurité au sein des PME ? (Situation ; Problématiques ; Etat d'esprit face à la sécurité; Prise de conscience du risque ; ...) »

3 points importants sont ressortis :

- **Manque de méthode formalisée, pas d'anticipation**

« Les PME n'ont pas réellement conscience des risques encourus, ce qui entraîne des écarts par rapport aux contre-mesures à appliquer », « La sécurité n'est pas un réflexe pour les entreprises », « Les entreprises attendent de voir et de subir les conséquences, c'est le : ça n'arrive qu'aux autres », « Les PME manquent de mise en place d'actions structurées, d'où les failles possibles de leur système », « Les entreprises françaises souffrent d'un retard par rapport aux entreprises étrangères comme le Royaume-Uni ».

- **Problématique Humaine**

« Il est courant qu'aucune équipe de sécurité ne soit établie au sein des PME », « Aucune sensibilisation faite aux usagers », « Les utilisateurs n'appliquent pas les recommandations faites par l'entreprise », « Pas de gestion des comptes »

- **Manque d'informations pour la prévention**

« Ils ont peu de communication et d'information sur les décisions et mesures à prendre en la matière »

PRECONISATIONS DES RSSI

Question 2 : « Si vous étiez amené à travailler au sein d'autres PME, avec votre expérience, que préconiserez-vous en matière de sécurité ? »

Plusieurs préconisations ont été relevées.

La plus citée a été :

- **L'importance de la protection de données :**

« Il est important d'avoir un niveau de confidentialité et ça c'est pour tout le monde », « Les informations étant centralisées, si le système plante, l'ensemble des données de l'entreprise sera perdu ! »

Suivent par ordre d'importance :

- **Le niveau de sécurisation à adapter selon l'entreprise et son métier.**

« Il ne faut pas oublier d'intégrer la sécurité dans tous les projets gérés par la société »

- **Impliquer sa Direction, faire adopter la politique sécurité**

« Faire adopter la politique de sécurité par la Direction Générale en exprimant les risques encourus », « C'est elle la responsable des outils informatiques », « Il faut un référent en interne en lien direct avec le dirigeant »

- **Utiliser des outils/ méthodologies nécessaires pour décliner une politique de sécurité**

« Se référer aux normes internationales : 27005 pour la gestion des risques, 27002 pour le référentiel SSI, 27001 pour le management au quotidien de la SSI », « Il existe des outils pour aider »

LES PREMIERES ACTIONS A FAIRE

Question 3 : « Avec du recul, quelles seraient pour vous, les premières actions à mettre en place au sein d'une PME ? »

Plusieurs actions en parallèle sont ressorties :

- **Réaliser un état des lieux de l'entreprise**

« Le premier pas, c'est l'analyse de ses risques et ses enjeux », « S'assurer des sauvegardes et des capacités de restauration des données, c'est le patrimoine de l'entreprise ! »

- **Etablir un Audit et mettre en place les actions nécessaires**

« En particulier au niveau de la sécurité périmétrique des postes de travail, protection interne et externe », « Décliner la sécurité en politique technique et mettre en place les outils répondant aux exigences exprimées », « Mettre en place une politique de traçabilité, sécuriser les accès critiques »

- **Ne pas oublier les utilisateurs**

« Il faut sensibiliser les utilisateurs sur l'importance des données de l'entreprise, communiquer ses données : c'est dangereux », « Etablir des fiches de « Bonnes pratiques » à destination des usagers », « Expliquer les risques Internet aux usagers »

UTILISATION D'UNE METHODE

Question 4 : « Au cours de votre parcours professionnel, quelles méthodes avez-vous eu l'occasion d'utiliser ? »

Les méthodes les plus utilisées au cours du parcours professionnel des RSSI sont :

- **Mehari (Marion)**
- **Méthodes internes**
- **Mélange des méthodes Ebios + Mehari**

Sachant que certains RSSI ont utilisé ses méthodes comme référentiel. Elles ont fait l'objet d'adaptation en rapport à leurs exigences métiers et au contexte auquel ils ont été confrontés.

Certains RSSI, n'appliquent pas ses méthodes :

- **Le 1 er frein vient de la Direction Générale:**

« Aucune prise de conscience du risque, pas nécessaire », « Ce n'est pas la priorité », « Investir pour gagner plus et à court terme », « Manque de temps, de personnel ou de moyens (financier / matériel) pour mettre en place ces audits ». « On répond aux demandes urgentes des utilisateurs »

PRISE DE CONSCIENCE/ MOTIVATION

Question 5 : « Comment avez-vous pris conscience de la nécessité de cette démarche ? »

Par ordre d'importance :

- **Se prémunir contre tout incident.**

« Analyser les risques liés à l'infrastructure de l'entreprise et à certaines applications critiques a été une nécessité », « la prise de conscience est survenue après avoir subi un incident »

- **Une prise de conscience de la direction**

« La politique de sécurité doit être dérivée de la stratégie et non par l'opérationnel », « les normes internationales et certifications ont évolué et il a fallu faire quelque chose », « Le besoin de structurer la politique de sécurité dans l'entreprise, il était indispensable de regrouper ces politiques pour être plus efficace et éviter certaines failles »

ORGANISATION POUR DEPLOYER UNE METHODE

Question 6 : « Comment vous êtes-vous organisé pour déployer une politique de sécurité optimisée ? »

2 points ont été prédominants :

- **Impliquer tous les usagers en interne**

« Nous avons mis en place une politique d'information et de sensibilisation des usagers, avec une charte, un intranet », « Le dialogue doit se faire en amont pour prévenir des problèmes! », « On organise des réunions de sensibilisation », « Souvent les utilisateurs n'appliquent pas les préconisations faites et c'est notre point de vigilance »

- **Mise en place d'un plan d'action précis**

« Mise en place d'un Système de Management de la Sécurité de l'Information, un SMSI », « Des réunions régulières avec le groupe de travail, une fois par mois », « Il est convenu de faire un point annuel et si besoin bi annuel avec la Direction Générale », « Les audits sont prévus de manière réguliers »

AVANTAGES ET INCONVENIENTS DES METHODES

Question 7 « Quels sont les avantages et inconvénients des méthodes que vous avez utilisés ? »

La bonne nouvelle est qu'il a beaucoup d'avantages et peu d'inconvénients.

- **Les méthodes globalement sont jugées comme « facile et rapide » à mettre en œuvre**
- **Répondent aux problématiques de l'entreprise :**
« Analyse pragmatique, concrète », « Fiches Réflexes », « Bonnes pratiques », « en accord aux enjeux »
- **Permet d'extraire les sujets sensibles de l'organisation afin de mettre en place les actions adéquates.**
- **Coût de la méthode respectant le budget attribué par l'entreprise**

Les 2 inconvénients relevés ont été :

- **Difficulté pour faire adhérer le projet d'Audit à l'ensemble des acteurs internes**
« Pas de prise de conscience de l'intérêt de cet audit »
- **Réussir à maintenir une politique de continuité de la méthode**

PLAN d'ACTION DEPLOYE

Question 8 « Quel a été le plan d'action mis en place ? »

La première action citée par l'ensemble des interviewés a été de

- **Réaliser un Audit de sécurité pour mesurer les risques encourus**

Puis au même niveau,

- **La Rédaction d'une politique de sécurité par domaines informatiques :**
 - **Système d'exploitation**
 - **Base de données**
 - **Internet (site internet ; email...)**
 - **Sécurité physique (Contrôle d'accès ; traçabilité...)**
 - **Focus sur la sécurisation des accès virtuels**

- **La mise en place d'un cahier des charges avec des objectifs annuels**
- **La Création d'une charte informatique à destination des utilisateurs**
« Informer sur leur responsabilité individuelle du quotidien », « Focus sur les Echanges d'informations avec des acteurs externes (partenaire ; client ; fournisseur) »

CONTINUITÉ RELATIVE A LA METHODE

Question 9 : « Aujourd'hui, existe-t-il un suivi ou une continuité relative à la méthode utilisée ? »

Tous ont répondu affirmativement, il est intéressant de notifier comment a été instaurer une politique de continuité.

Cette politique de continuité s'applique avec :

- **Des audits réguliers**
- **La mise en place d'un processus de Qualité**
- **Des réunions régulières**
« Réadapter les actions et définir les points sur lesquels axer les efforts », « Rassembler les responsables de chaque service afin de relayer l'information à l'ensemble des utilisateurs ».

L'externalisation

Question 10 : « Avez-vous fait appel à une société externe pour mettre en place cette méthode ? »

1/ 3 des réponses ont été affirmatives, et touchent le domaine du Conseil.

« Plus experts dans le domaine du référentiel », « Au départ pour bien prendre la mesure du métier de RSSI », « Meilleure compréhension des enjeux du responsable de la sécurité mais aussi des enjeux et risques liés à l'activité de l'entreprise », « Nécessite l'intervention d'experts ».

Les raisons négatives :

« Des moyens financiers insuffisants », « Des compétences internes existantes en particulier avec l'aide du service qualité », « Je souhaitais d'abord réaliser un test interne pour voir l'intérêt de cette méthode avant de faire externaliser »