

## Retour d'expériences de 10 PME ayant mis en place la méthode ULYSSE

### Préambule

Réalisation d'une **étude exploratoire auprès de 10 PME** ayant utilisées au cours des derniers mois la Méthode ULYSSE.

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 « pilotes » de la politique de sécurité au sein de la PME.
- Typologie des fonctions : Responsable/ administrateur réseau, Informatique, Directeur administratif / financier, Responsable qualité et Chef de projet

### Objectif de cette étude :

- Mieux comprendre le processus de décisions des PME à agir et déployer une politique de sécurité.
- Faire un retour concret de l'expérience des PME « Sécurisées » afin d'en faire profiter des PME désireuses de développer un plan d'action. Marquer l'impact auprès des PME non sensibilisées.

### Remerciements :

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

### MESURE DE LA MOTIVATION DES PME

**Question 1** : « Comment avez-vous pris conscience de la nécessité d'une démarche d'Audit de sécurité ? »

Les deux motivations qui ont été le plus souvent remontées par les PME interviewées, concernant la prise de conscience de la nécessité de la démarche, ont été :

- **A la suite d'un problème survenu sur leur SI**
- **Une volonté de la Direction.**

### Les problèmes remontés par les PME ont été sur la perte de productivité :

« 2 jours où certaines personnes étaient dans l'impossibilité de travailler ! », « C'était la panique à bord, on a eu des difficultés à remettre le système en route ».

**Les Directions ont été sensibilisées en amont de la prise de décision de déployer cette démarche.** « Cela a été une réflexion à la suite de la visite de la DCRI », « C'est notre cabinet comptable qui nous a ouvert les yeux... ».

En parallèle, d'autres points forts ont été soulevés dans la prise de conscience :

- **L'augmentation du partage de données entre différents acteurs internes et externes** : « Nous sommes de plus en plus interconnectés entre nos clients et fournisseurs », « Nous avons ouverts de plus en plus notre système d'information avec, en conséquence, une perte de la maîtrise de l'ensemble ! »,
- **L'évolution des profils des utilisateurs** : « Nos collaborateurs sont de plus en plus jeunes, actifs sur le réseau », « Nos équipes ont évolué dans l'usage de l'informatique, les risques liés aux comportements aussi », « Nous sommes de plus en plus nombreux et donc plus vulnérables ! »
- **Pas de « formalisation » de la sécurité informatique** : « Pas d'intégration automatique de la sécurité dans les projets de la société », « L'aspect sécurité vient s'appliquer après le déploiement d'un projet, et si nécessaire ! »

### CHOIX DE LA METHODE

**Question 2** : « Qu'est ce qui vous a amené à utiliser la méthode ULYSSE ? »

La majorité des PME a orienté son choix vers la méthode ULYSSE car :

- **Conseillée par des acteurs externes :** « C'est une entreprise du même secteur d'activité que la nôtre qui nous l'a recommandée. », « Un prestataire avec qui nous avons déjà travaillé nous l'a conseillée, on lui a fait confiance ! », « Ca s'est fait par du bouche à oreille ».

Mais aussi,

- **Agrémentée d'outils** « on ne disposait pas des ressources nécessaires en interne »
- **Adaptée à la structure de l'entreprise** « C'est une personne du DCRI qui nous a dit que cette méthode était adaptée à la structure de notre entreprise »

## ORGANISATION

**Question 3 :** « Comment vous êtes-vous organisé pour déployer une politique de sécurité optimisée ? »

Par ordre d'importance :

- **La validation de la Direction avec des moyens à disposition :** « On avait besoin d'un appui financier et humain »
- **Mise en place d'un comité de pilotage:** « Il a fallu mobiliser des acteurs Internes et Externes », « une démarche longue et difficile »
- **Communication interne importante :** « Pour responsabiliser et sensibiliser nos collaborateurs, on a mis en place des réunions d'information », « les utilisateurs étaient réticents à ces changements, on a donc créé des supports de communication pour les accompagner au quotidien », « Il fallait montrer qu'il se passait quelque chose pour justifier de la nécessité de cette méthode »

Vient ensuite au même niveau,

- **La rédaction d'une politique de sécurité**
- **La « Priorisation » des actions à mener :** « on a hiérarchisé les actions et créé un planning »

## POURQUOI EXTERNALISER ?

**Question 4 :** Qu'est ce qui vous a amené à faire appel à une société externe ?

- **Par manque de compétences internes en matière d'audit de sécurité**  
« On ne disposait d'aucune méthodologie et d'aucun outil pour faire cet audit » « On ne se sentait pas capable de mettre en place un projet adapté et ne négligeant aucune facette de l'entreprise », « On ne savait pas par où commencer », « c'était un projet trop conséquent », « On nous a contacté alors qu'on été en pleine réflexion sur ce projet, on a sauté sur l'occasion ! »
- **Accompagnement et suivi**  
« Le programme de formation était intéressant » « L'avantage, c'était d'avoir une solution clef en main », « Ils nous ont aidé à expliquer et communiquer auprès de nos utilisateurs », « On était bien encadrés », « Grâce à un suivi du prestataire, on a réussi à avancer aussi vite que prévu et à tenir le rythme »
- **Un avis objectif de la situation**  
« Il nous fallait faire un état des lieux de l'entreprise et pour ça, nous avons besoin d'un regard extérieur pour ne négliger aucun détail », « Faire appel à une société externe nous a donné plus de poids face à notre direction pour mettre en place des actions », « on a pris conscience de la vulnérabilité de nos systèmes »
- **Confiance dans le prestataire**  
« On avait déjà travaillé avec ce prestataire et on savait qu'il utilisait ces méthodes », « Il avait certes, la richesse des outils mis à disposition, mais aussi un dialogue humain »

## AVANTAGES ET INCONVENIENTS

**Question 5** « Pour vous, quels sont les avantages et inconvénients de la méthode ULYSSE ? »

Avantages, par ordre de fréquence de citation :

- **Formation inter-entreprise**  
« La formation permettait d'aborder des sujets très vaste (contrats ; réseaux ; rôle de chacun), « Le groupe de travail était composé d'une quinzaine de personnes d'entreprises différentes avec qui on pouvait confronter nos expériences », « Un groupe hétérogène ce qui favorisait l'échange ».

- **Formation interne**  
« Cette formation a enrichie mes connaissances professionnelles et m'a permis de prendre conscience des failles de la sécurité de notre système » « Ca a développé mon ouverture d'esprit »
- **Outils méthodologiques adaptés**  
« Les outils méthodologiques étaient adaptés à la structure de l'entreprise » « Les questions d'audit étaient restreintes à des structures petites et moyennes »
- **Organisation interne structurée**  
« Les dates d'échéance nous ont permis d'adopter un certain rythme quant aux actions à mettre en place »  
« On a avait une visibilité sur l'ensemble des actions et de leurs avancés »
- **Fiches de bonnes pratiques**  
« Des fiches dédiées aux utilisateurs nous permettent de mettre en place des réflexes quant au bon comportement à adopter »

Un seul principal inconvénient soulevé par la moitié de l'échantillon :

- **L'auto gérance de l'entreprise une fois le plan d'action mis en place**  
« Ce n'est pas vraiment un problème relatif à la méthode mais plus un problème interne pour débloquer du temps pour consacrer à la méthode », « Difficulté à tenir les échéances », « On a tendance à repousser les dates butoirs ! », « Pour être cohérent, il est nécessaire d'avancer au rythme de la méthode », « Si on n'avance pas, on passe à côté d'actions qui représentent un réel apport pour l'entreprise »

#### PLAN D'ACTION

Question 5 : « Quel a été le plan d'action mis en place ? »

La majorité des PME interviewées ont soulevé les 4 points suivants :

- **Politique de sauvegarde et de restauration** « On a mis en place un serveur test pour simuler la perte de donnée et de logiciels métier » « La perte de données serait critique pour notre entreprise, il fallait être capable de se prémunir contre ce problème »
- **PRA / PCA** « Grâce à un plan de secours informatique, nous sommes plus confiant, il n'est plus question de panne et d'arrêt de la production »
- **Sécurisation des PC portables**
- **Elaboration d'un cahier des charges et de la charte informatique**

Des cas particuliers ont été remontés selon les besoins propres aux situations :

- **Sécurité du réseau informatique**
- **Sécurité du système d'accès**  
« Avant tout le monde pouvait se connecter à notre réseau wifi en se garant sur notre parking ! », « On a instauré une politique de mot de passe au niveau des postes de travail »,
- **Mise en place d'un « destructeur de documents »**
- **Verrouillage des accès**  
« Pour éviter toute imprudence qui engendrerait une percée de notre système, nous avons bloqué l'accès à certains sites internet et messageries fréquentés par nos utilisateurs. »
- **Virtualisation/ Cloud privé**
- **Externalisation de la maintenance informatique**

#### ET APRES LA METHODE ?

Question 6 : « Aujourd'hui, existe-t-il un suivi ou une continuité relative à la méthode ULYSSE ? »

Les actions par ordre d'importance pour instaurer une politique de continuité :

- **Réunions régulières des pilotes du projet**

« On essaye de se rassembler pour continuer à mettre en place des audits internes plus ciblés » « On continue à s'imposer des délais pour chaque action, ça nous permet d'avancer ! »

- **Mettre en place de nouveaux plans d'actions**  
« Aujourd'hui, j'avance selon les nécessités » « Les besoins et les enjeux de l'entreprise évoluent, on doit sans cesse se réadapter »
- **S'informer**  
« Je me tiens régulièrement informé des nouveaux moyens de sécurisation et des nouvelles normes mises en place »
- **Réunions ponctuelles avec les utilisateurs**  
« On les réunit essentiellement pour les gros projets, pour le reste, on a mis en place un système de relais avec les responsables de chaque service »

La principale difficulté étant

- **Le manque de temps** « On a de réelles difficultés internes pour débloquer le temps nécessaire à ces actions » « On a du mal à s'imposer des réunions et à respecter les délais »

### PERCEPTION CAPITALISEE

**Question 7** « A ce jour, 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 ; ...)

- **Les PME ne se sentent toujours pas concernées :**  
« On attend les problèmes ! », « Les sinistres feront avancer la prise de conscience ! », Les entreprises sont loin de se douter de « l'épée de Damoclès au dessus de leur tête ! », « Du jour au lendemain, elles peuvent se retrouver sans rien ! »
- **Un sujet non abordé par manque d'information ou de sensibilisation**  
« Si les entreprises étaient sensibilisées à la sécurité, ce serait plus facile ! », « Certaines entreprises connaissent les problèmes de virus mais elles ignorent le plus souvent l'importance de la perte ou de la confidentialité de leurs données », « Depuis peu de temps, on commence à sensibiliser sur les bancs de l'école, c'est une bonne chose ! »
- **Problème de vulgarisation du vocabulaire** « Le jargon utilisé dans la sécurité n'est pas adapté à l'ensemble personnes qui y sont confrontées » « Les acteurs de la sécurité veulent connaître l'impact des améliorations mises en place, pas l'aspect technique ! »
- **Le manque de temps** « Les entreprises ont la tête dans le guidon », « Leur priorité, c'est produire et régler les problèmes qui freinent la production », « La sécurité vient s'ajouter au fur et à mesure des besoins dans l'entreprise et non pendant la mise en place d'un projet »

### EXPERIENCES CAPITALISEES

**Question 8** : « Grâce à votre expérience et si vous étiez amené à travailler au sein d'autres PME : Que préconiserez-vous en matière de sécurité ? »

- **Faire un audit de diagnostic de l'entreprise pour mettre en place des actions concrètes** « Avant toute chose, il faut faire un état des lieux ! », « on doit être conscient des enjeux et des risques métiers dont est sujet l'entreprise », « Il est important de connaître les faiblesses, les besoins de l'entreprise pour ensuite dédier des actions aux problématiques soulevées »
- **S'informer sur les législations et sur les nouveaux systèmes de sécurisation** « Je travaille avec le service qualité pour être informé des nouveautés dans le domaine »
- **Etre capable de continuer la production si un sinistre survient** « Pour toute entreprise, perdre une journée de production est inenvisageable surtout quand ça peut être évité ! », « il faut être sûr que s'il survient un sinistre majeur au sein de l'entreprise, la production en sera inchangée »

### PREMIERES ACTIONS A FAIRE

**Question 9** : « Avec du recul, quelles seraient pour vous, les premières actions à mettre en place au sein d'une PME ? »  
Le premier point qui ressort concerne les données :

- **Les Sauvegardes de données**  
*« Sauvegarder ses données, c'est sauvegarder le patrimoine de l'entreprise », « Il faut évidemment conserver les sauvegardes dans des endroits différents ! »*
- **Tester les sauvegardes**  
*« Il faut tester régulièrement les sauvegardes »,*
- **Identifier les données critiques et confidentielles**  
*« Il faut être capable de protéger et/ou crypter les données sensibles », « Il ne faut pas être crédule, on se doit d'identifier les destinataires représentant un risque pour l'entreprise »*
- **Sécuriser les accès aux données de l'entreprise**  
*« Il faut limiter les accès à la salle serveur et instaurer une traçabilité »*

Puis suivent,

- **La sécurisation de la mobilité***« Le wifi peut être un réel danger pour l'entreprise »*
- **Les utilisateurs avec :**
  - **L'élaboration d'une charte informatique**
  - **Former et sensibiliser** *« il est important de simuler le crash d'un serveur auprès des usagers »*

**Avec un focus, Soyons vigilant sur le métier de chacun**

*« Difficile de donner des conseils, chaque entreprise est un cas particulier avec des enjeux et des risques qui lui sont propres, cela demande une étude approfondie »*