CYBER THREAT INTELLIGENCE

Système de gestion de la sécurité de l'information apprenant

Valentin PRODHOMME

I. Introduction

Le management du système d'information est une discipline du management regroupant l'ensemble des connaissances, des techniques et des outils assurant la gestion de données et leur sécurité, et plus généralement l'organisation et la protection du système d'information.

Le SI est lui-même composé de matériels et logiciels ayant des conséquences dans le management des organisations. En effet, l'infrastructure technologique du système d'information est un ensemble de dispositifs pouvant provoquer des changements organisationnels dans une entreprise.

L'information est un principe fondamental de la stratégie. En conséquence, le SI est également un outil essentiel dans la stratégie d'entreprise. C'est pourquoi, la sécurité du système d'information représente un enjeu majeur pour l'entreprise.

II. Terminologie

Terme	Signification
CTI	Cyber Threat Intelligence
SI	Système d'Information
SSI	Sécurité des Systèmes d'Information
SMSI	Système de Management de la Sécurité de l'Information

Tableau 1 Terminologie

III. Gestion du SI

La gestion du système d'information contient plusieurs axes principaux tel que :

- La gestion du parc informatique
- La gestion des incidents
- La gestion de l'infrastructure informatique
- La gestion de la sécurité

C'est à ce dernier axe que nous allons nous intéresser plus particulièrement.

IV. Sécurité du SI

La sécurité du système d'information est une activité du management du système d'information. C'est l'ensemble des moyens techniques, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du système d'information.

> « Ainsi, une règle essentielle de la stratégie consiste à se préparer à déjouer une attaque, au lieu d'espérer qu'elle ne se produise pas. »
>
> *Sun Tzu - L'art de la guerre*

La sécurité du SI est assurée au travers d'un système de gestion de la sécurité de l'information ou SMSI.

Concrètement, le SMSI se traduit par la mise en œuvre d'un vrai processus d'analyse, d'élaboration, de contrôle et d'évolution d'une politique de sécurité. L'ISO/IEC 27001:2005 a notamment adopté l'approche de la Roue de Deming :

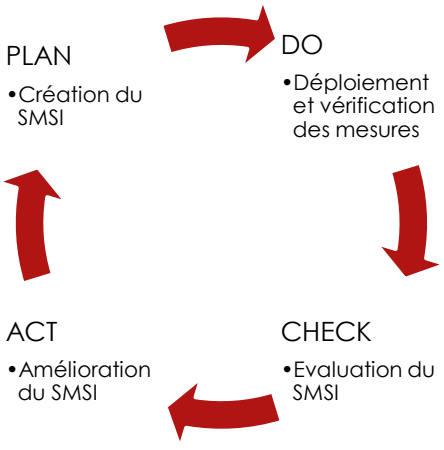


Figure 1 Roue de Deming – SMSI

Un SMSI doit être efficace et efficient sur le long terme, c'est-à-dire pouvoir s'adapter aux changements qui ont lieu dans l'environnement interne et externe.

Afin de conserver des performances optimales, un SMSI doit donc être constamment évalué et amélioré si nécessaire. Pour cela, on propose d'étudier la définition d'un système apprenant de gestion de la sécurité de l'information.

V. Système apprenant

Un système apprenant est un système ayant la capacité à améliorer ses propres connaissances. Dans l'ouvrage « Les systèmes apprenants et leur régulation », Alain BOUVIER présente les systèmes apprenants au travers de 12 hypothèses les caractérisant.

1. L'expert est l'acteur. Autrement dit, « celui qui sait fait ». Plusieurs savoir-d 'action sont évoqués : le savoir-faire, le savoir-comprendre, le savoir-combiner et le savoir-exprimer.

2. L'intelligence d'un système s'apprécie dans sa capacité à résoudre des problèmes nouveaux et de plus en plus complexes.

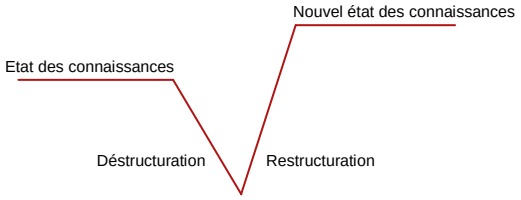
3. Pour un système, pas d'intelligence sans mémoire. Les systèmes souffrent, en effet, de leur absence de mémoire. Plusieurs types de mémoire sont à prendre en compte : à long, moyen et court terme notamment.

4. Conception, structuration et fonctionnement des mémoires collectives.

5. Tout système peut apprendre.

6. Des liens dialectiques entre action et organisation.

7. Un système apprend par changement de l'état de ses connaissances collectives :



8. Pour devenir apprenant, un système doit se focaliser sur ses processus.

9. Pas d'apprentissage sans régulation de niveau 1 & 2. Le niveau 1 de régulation permet d'effectuer des réajustements dans le cadre des objectifs définis et de manière immédiate. Le niveau 2 de régulation implique la remise en question des objectifs définis ainsi que des processus.

10. Pour devenir apprenant, un système doit réguler son système de régulation. Il s'agit d'un niveau 3 de régulation qui vise à interroger la pertinence des actions de régulation de niveau 1 & 2. Il permet aussi une activité réflexive concernant les acteurs et systèmes afin de faire de toute action une occasion d'apprentissage.

11. Pour devenir apprenant, un système doit favoriser la conversion des connaissances en son sein. Cela fait référence à la spirale des connaissances, un phénomène exprimé par les auteurs Ikujiro Nonaka et Hirotaka Takeuchi.

12. Pour devenir apprenant, un système doit lutter contre les routines défensives. Il existe une multitude d'obstacles à l'évolution d'un système. On retrouve, par exemple, les idées reçues, les résistances, les conservatismes ou encore les corporatismes. Ainsi, pour devenir apprenant, un système doit lutter contre les routines défensives en son sein.

VI. La CTI au service de la SSI

Les systèmes apprenants requièrent la mise en place et l'exploitation d'une mémoire collective. Une telle mémoire implique d'expliciter des savoirs (des données par exemple) et de les partager avec des partenaires afin que chacun puisse apprendre de l'autre.

Nous pouvons donc exploiter la Cyber Threat Intelligence comme source de renseignement pour la Sécurité des Systèmes d'Information.

La CTI opérationnelle a pour objectif d'étudier les détails d'une attaque spécifique afin d'évaluer la capacité d'une organisation à se défendre face à des futures menaces.

Intégré au sein du processus de gestion des risques, la CTI opérationnelle fournit alors du renseignement précis et pertinent permettant l'amélioration continue de l'analyse des risques.

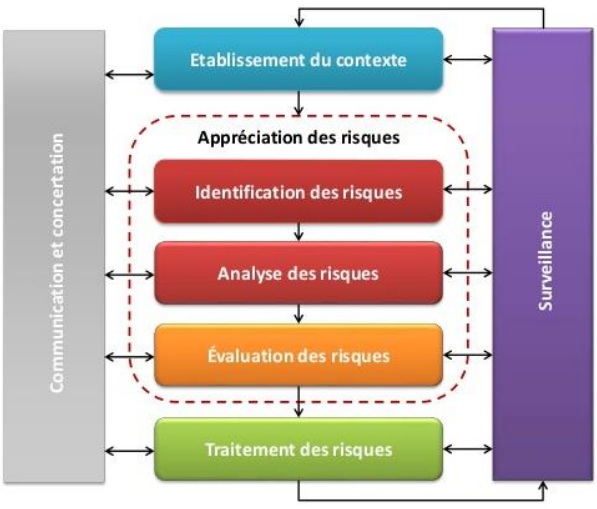


Figure 2 Le processus de management des risques selon l'ISO31000

VII. Système de gestion de la sécurité de l'information apprenant

La modélisation d'un SMSI apprenant implique la prise en compte des exigences relatives aux systèmes apprenants. Nous proposons le schéma suivant comme application du principe de système apprenant au système de gestion de la sécurité de l'information. La norme ISO 27001:2005 définissant le SMSI implique déjà l'évaluation et l'amélioration du système de gestion lui-même.

La roue de Deming définie dans la norme ISO 27001:2005 sert de référence pour la définition de ce système apprenant. Elle est enrichie du principe du renseignement, inspiré de la Cyber Threat Intelligence, afin d'implémenter des processus de création et de maintenance d'une mémoire collective entre plusieurs partenaires.

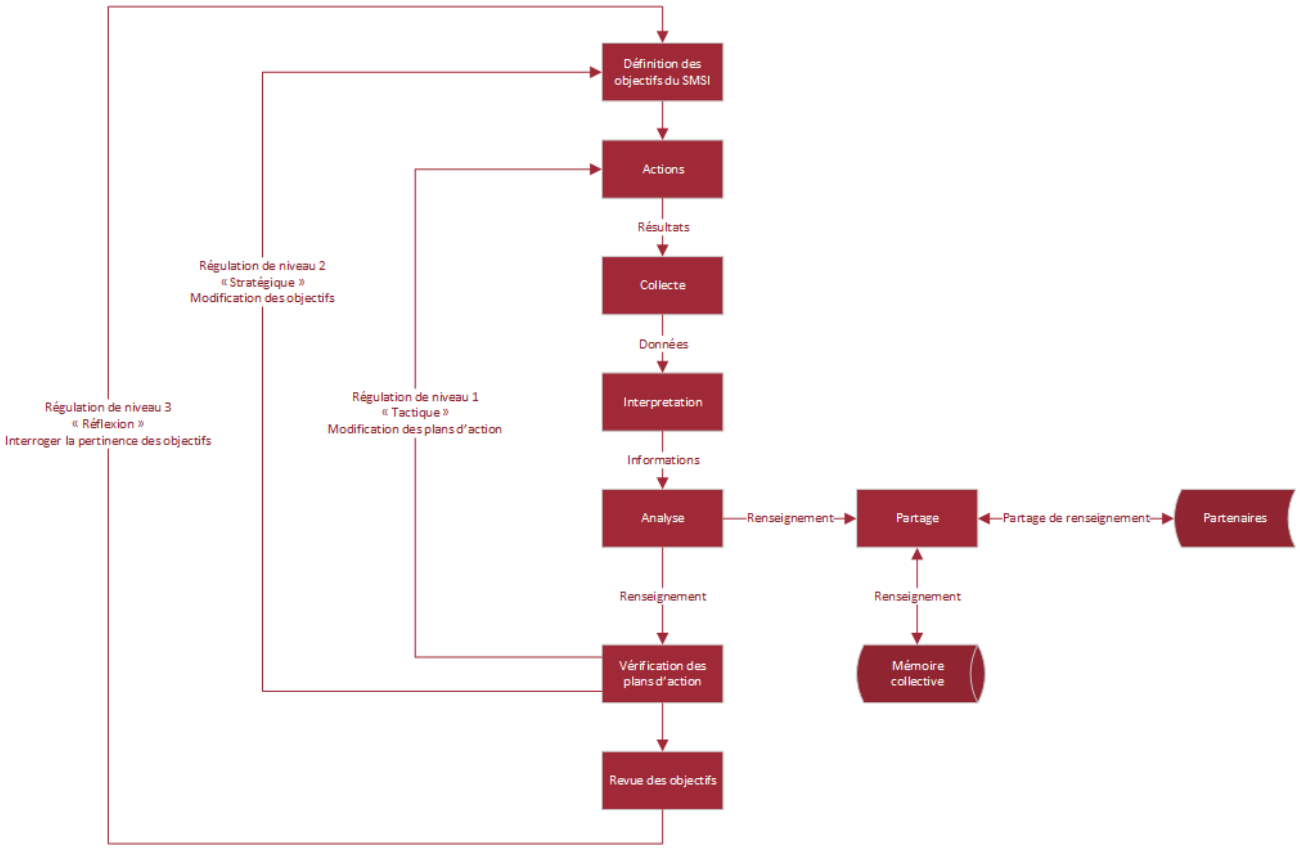


Figure 3 Système de gestion de la sécurité de l'information apprenant

Les principes des systèmes apprenants sont représentés au travers de cette modélisation du SMSI. Le système définit des processus permettant sa propre remise en question grâces à du renseignement en provenance du système d'information opéré et de systèmes d'information opérés par des partenaires.

VIII. Conclusion

Nous avons vu que face aux enjeux posés par la sécurité des systèmes d'information, les entreprises ont intérêt à maintenir des processus de gestion efficaces.

Un tel système de gestion de la sécurité de l'information doit alors être capable d'assurer, tout au long de son cycle de vie, l'efficacité et la pertinence de ses processus.

Nous avons proposé la combinaison des principes des systèmes apprenants et de la Cyber Threat Intelligence pour modéliser un SMSI apprenant.

La modélisation en résultant permet d'illustrer un système de gestion de la sécurité de l'information apprenant orienté sur le partage de renseignements entre partenaires, en exploitant la CTI.

IX. Références

- Management et sciences cognitives, Alain Bouvier
- Les systèmes apprenants et leur régulation, Alain Bouvier
- Cours CTI, Ronan Mouchoux
- Concept & principes pédagogiques – 5 : l'individu-plus, Marc Dennery
- Apprentissage artificiel Concepts et algorithmes, Antoine Cornuéjols Laurent Miclet
- Intelligence artificielle : les défis actuels et l'action d'Inria, Inria
- Pourquoi SMSI
- Système de gestion de la sécurité de l'information
- Sécurité des systèmes d'information
- Informatique décisionnelle
- Management du système d'information