Quel plan d'actions pour la diffusion, l'explication et la mise en application de la nouvelle PSSI de l'Etat ?

Le 17 juillet 2014, le Gouvernement français publiait la circulaire N° 5725/SG imposant aux différents ministères ou autorités administratives de s'organiser afin de mettre en œuvre la Politique Sécurité Système d'Information de l'Etat (PSSI E), élaborée par l'Agence Nationale pour la Sécurité des Systèmes d'Information, (ANSSI). La PSSI de l'Etat doit s'appliquer aux systèmes d'information traitant les informations non classifiées de défense : Elle doit être mise en œuvre sur tous les systèmes d'information des administrations de l'Etat : ministères, établissements publics sous tutelle d'un ministère, services déconcentrés de l'Etat et autorités administratives indépendantes.

De la sécurité informatique à la sécurité système d'information.

L'analyse de cette PSSI de quarante et une pages montre très clairement la volonté de sortir d'une approche « sécurité informatique » au profit d'une approche orientée « protection de l'information et sécurité des systèmes d'information associés ». Elle prend en compte non seulement l'ensemble des informations métiers (numériques, papier et vocales) et les ressources informatiques classiques, la téléphonie, les copieurs multifonctions, mais aussi la composante humaine.

Dès le préambule, la PSSI de l'Etat formalise que ce référentiel SSI doit « assurer la continuité des activités régaliennes, renforcer la confiance des citoyens et des entreprises dans les télé-procédures, mais aussi prévenir la fuite d'informations sensibles ».

Il s'agit de protéger, non seulement, les ressources du système d'information, mais aussi l'ensemble des informations supportées par les différentes ressources du système d'information et manipulées par les différents acteurs utilisateurs du SI dans le cadre de leurs missions.

Ainsi la PSSI de l'Etat s'adresse « **à l'ensemble des agents de l'Etat, et tout particulièrement aux autorités hiérarchiques qui sont responsables de la sécurité des informations traitées au sein de leurs services**, aux agents chargés des fonctions de directeurs des systèmes d'information et aux personnes chargées de la sécurité et de l'exploitation des systèmes d'information ».

Cette approche est fondamentalement différente avec d'autres textes de références sécurité comme par exemple le PCI DSS, (Payment Card Industry Data Security Standard). Ce standard ne constitue pas une politique de sécurité à approche globale mais bien un standard de références orienté maîtrise d'œuvre devant s'appliquer sur les systèmes informatiques manipulant des données facilement identifiées comme sensibles : les données liées aux porteurs de cartes bancaires. L'objectif de ce standard est de sécuriser une partie du système d'information et non d'avoir une approche globale intégrant le facteur humain pour la protection des informations et la sécurisation de l'ensemble des systèmes qui les supportent.

La PSSI E s'appuie sur 10 principes stratégiques :

- P1 : Lorsque la maîtrise des SI l'exige, l'administration fait appel à des opérateurs de confiance. La qualification d'un prestataire de services de confiance (PSCO) est prévue par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives. Elle atteste de sa conformité à un niveau de sécurité du référentiel général de sécurité (RGS) destiné aux autorités administratives. Elle est délivrée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI)).

- **P2 : Tout système d'information de l'Etat doit faire l'objet d'une analyse de risques adaptée aux enjeux, dans une démarche d'amélioration continue** ;
- P3 : Les moyens financiers et humains consacrés à la SSI doivent être planifiés, quantifiés et identifiés ;
- P4 : Des moyens d'authentification forte des agents doivent être mis en place. L'usage de la carte à puce doit être privilégié ;
- P5 : Les opérations de gestion et d'administration des SI de l'état doivent être tracées et contrôlées ;
- P6 : La protection des SI doit être assurée par l'application de règles précises. Ces règles font l'objet de la PSSIE ;
- **P7 : Chaque agent de l'Etat doit être informé de ses droits et devoirs et formé et sensibilisé à la cyber sécurité. Les mesures doivent être connues de tous.**
- P8 : Les administrateurs de SI doivent appliquer après formation les règles élémentaires d'hygiène informatique[i] ;
- **P9 : Les produits et services acquis par les administrations doivent faire l'objet d'une évaluation et d'une attestation préalable de leur niveau de sécurité ;**
- P10 : Les informations considérées comme sensibles en raison de leurs besoins en confidentialité, intégrité ou disponibilité sont hébergées sur le territoire national.

Ces 10 principes stratégiques à la base de la PSSIE sont traduits en 13 familles d'objectifs à atteindre, par la mise en application des règles associées :

- O1 : Politique, organisation, gouvernance ;
- O2 : Ressources humaines ;
- O3 : Gestion des biens ;
- O4 : Intégration de la SSI dans le cycle de vie des systèmes d'information ;
- O5 : Sécurité physique ;
- O6 : Sécurité des réseaux ;
- O7 : Architecture des SI ;
- O8 : Exploitation des SI ;
- O9 : Sécurité du poste de travail ;
- O10 : Sécurité du développement des systèmes ;
- O11 : Traitement des incidents ;
- O12 : Conformité, audit, inspection, contrôle ;
- O13 : Continuité d'activité.

Nous nous intéresserons plus particulièrement aux aspects sécurité devant être adaptés aux enjeux (point stratégique 2) et à la problématique du facteur humain (point stratégique 7).

Ces points stratégiques sont plus particulièrement pris en compte dans les objectifs, O2 : Ressources humaines, O3 : Gestion des biens, O4 : Intégration de la SSI dans le cycle de vie des systèmes d'information.

Les missions et métiers des entités concernées par la PSSI de l'Etat sont très variées et très différentes. La PSSI de l'Etat insiste, très clairement dans le point stratégique 2 (P2), décliné par les objectifs O2, O3, O4, sur les enjeux et les sensibilités particulières à chaque métier ou contexte. L'idée est bien d'obtenir l'adhésion des métiers. Il ne s'agit plus de définir des bonnes pratiques techniques « d'hygiène informatique » dé-corrélées des besoins métiers. Il s'agit pour l'Etat de rappeler la méthodologie orientée enjeux et de remettre le facteur humain au centre de la problématique.

Par ailleurs, il est intéressant de noter que la nouvelle PSSI de l'Etat conformément à ce qui se fait aujourd'hui dans les grands groupes internationaux (notamment industriels) reprend globalement les chapitres de la norme ISO 27002, mais et c'est majeur de le souligner, oriente les directives sur un aspect fonctionnel. L'orientation fonctionnelle permet de garantir une réelle pérennité du texte de références ainsi qu'une liberté de choix pour l'intégrateur interne ou externe des solutions, du moment qu'elles sont validées conformes aux directives SSI et enfin homologuées. Le principe d'homologation est analysé plus loin dans l'article.

Il est vrai qu'une approche sécurité informatique constituée de règles techniques auto justifiées par les compétences techniques des directions informatiques a certes, permis, de faire monter le niveau de sécurité des systèmes informatiques mais a rencontré des difficultés majeures limitant très fortement son efficacité. Le constat est clair : la faible prise en compte du facteur humain et le peu d'engagement des responsables métiers dans la démarche de formalisation des enjeux, des besoins de sécurité et des risques associés représentent des vulnérabilités majeures.

La prise en compte du facteur humain : « faire des personnes les maillons forts des SI de l'Etat ».

L'approche réalisée par l'addition a posteriori, d'outils extérieurs (filtres réseau, filtres applicatifs, antivirus, pare-feu, réseaux privés virtuels, boitiers de chiffrement …) sur des systèmes non sécurisés nativement, comme l'essentiel des applications de l'Internet, n'a que très rarement pris en compte le facteur humain, surtout lorsque que l'on sait que l'essentiel des dommages est le plus souvent causé par l'ignorance des règles et des bonnes pratiques. Ce manque de connaissances engendre des erreurs et est toujours exploité par des personnes malveillantes quelles que soit leurs motivations (mafieuses, concurrentielles, ludiques, idéologiques ou stratégiques). Les pratiques d'incitation et manipulation de la personne cible utilisent toujours l'ignorance ou l'inconscience de la victime.

La PSSI de l'Etat formalise clairement la volonté de prise en compte du facteur humain notamment au travers de l'objectif 2: « **faire des personnes les maillons forts des SI de l'Etat ».**

Alors que la sécurité informatique réduit les vulnérabilités techniques, la PSSI de l'Etat a pour vocation de réduire l'ensemble des vulnérabilités, non seulement informatiques sur les ressources techniques support mais aussi sur les contenus et leurs utilisations par les différents acteurs. Elle se fixe notamment pour objectif de limiter les risques liés aux mauvaises utilisations. Elle définit donc des principes règlementaires structurants pour les trois composantes du système d'information :

- les contenus quels que soient leurs formes ;
- les ressources supports ;
- les acteurs qui les utilisent.

Ces principes peuvent être structurés de la manière suivante :

- le respect de la règlementation ;
- la classification des informations, des processus métiers qui les manipulent et des ressources qui les supportent ;
- l'utilisation des outils du système d'Information conformément aux règles gradées aux niveaux de classification ;
- les comportements généraux à l'intérieur et à l'extérieur des établissements.
-

De la gestion du risque informatique à la protection des enjeux métiers :

La deuxième grande difficulté est liée à la volonté d'avoir une approche orientée enjeux, en adéquation aux besoins relatifs aux missions et aux risques consécutifs aux contextes métiers.

Les métiers ne se satisfont plus de la sécurité informatique constituée de bonnes pratiques techniques « auto justifiées » et ressenties comme des contraintes inadaptées à leurs missions. Elles sont jugées parfois complexes et le plus souvent identifiées comme un facteur de ralentissement dans l'efficacité de la réalisation de leurs missions. Par exemple la restriction du téléchargement, l'authentification personnelle et incessible, l'interdiction des identifiants génériques, l'obligation du chiffrement pour les données sensibles, le filtrage de certains sites ou l'interdiction de certains transferts ou formats de pièces jointes par courrier électronique.

Si l'on veut obtenir l'adhésion des métiers, et c'est bien la difficulté, les règles doivent donc maintenant être absolument adaptées à leurs enjeux et leurs besoins. Il doit donc être clair que les directions des systèmes d'information et les équipes de sécurité système d'information n'ont pas la légitimité, voire la qualification et les compétences métier (à chacun son expertise) pour formaliser les besoins de sécurité. Seuls les responsables métiers ont cette légitimité et donc cette capacité d'assumer cette responsabilité. Ce n'est pas à la direction des systèmes d'information de définir, par exemples, la sensibilité des informations et des processus métier, les besoins de continuité d'activité ou les périmètres d'habilitation sur des données. Les équipes sécurité et équipes de la direction des systèmes d'information héritent de ces besoins sur les ressources. Le rôle de la DSI est protéger ces ressources en cohérence avec les besoins exprimés. Il est important de noter qu'une ressource peut avoir, en plus des besoins hérités des métiers, ses propres besoins intrinsèques de sécurité. Exemple un firewall protégeant un serveur web qui publie des informations publiques a ses propres besoins de protection en confidentialité des règles et informations qui lui sont intrinsèques et nécessaires à son bon fonctionnement. L'équipe SSI consolidera alors les besoins métiers avec les besoins intrinsèques.

Par le passé, l'engagement des directions métiers à formaliser leurs enjeux et leurs besoins de sécurité a rencontré de très nombreux écueils principalement causés par leurs ressentis de la sécurité comme étant une affaire d'informaticiens.

Les informaticiens ont mis en œuvre des règles génériques de sécurité. La priorité était de constituer un socle commun de sécurisation minimale indépendant des spécificités métiers, ce qui semblait pragmatique.

Il s'agissait pour les techniciens de la sécurité de gérer l'urgence. Ils ne pouvaient pas solliciter et impliquer les métiers sans avoir conçu ce socle de sécurité minimal.

En fait, le paradoxe est que les métiers n'adhèrent que très peu à cette approche. Ils ne ressentent pas que l'on ait pris en considération leurs spécificités. Ils vivent ces exigences de base comme des contraintes inadaptées. Cette difficulté s'est bien vue dans les grands groupes industriels et financiers où les métiers sont extraordinairement variés et différents au sein de la même entreprise.

Ainsi pour améliorer la qualité du dialogue entre les métiers et leurs maîtrises d'ouvrage d'une part et la direction des systèmes d'information d'autre part, les métiers devront être sensibilisés puis formés notamment à la classification des besoins de sécurité inhérents à leurs missions, à la gestion de risques informationnels et à la validation des risques résiduels.

Force, est de constater que malheureusement la démarche est aujourd'hui que très rarement intégrée par les responsables métiers.

Il sera donc fondamental d'expliquer que la formalisation des besoins de disponibilité, intégrité, confidentialité et preuve se fait par l'analyse de l'impact des dommages sur les missions et les valeurs essentielles de l'entité en cas d'incapacité de réponse à ces besoins.

La direction générale, (elle-même devant souvent être sensibilisée) ou l'AQSSI devra donc formaliser des valeurs essentielles de référence pour l'entité, afin de guider les responsable métiers dans l'analyse des enjeux.

Ces valeurs essentielles peuvent être par exemple pour une administration :

- la garantie de disponibilité et de qualité du service public ;
- la confiance des usagers dans leurs échanges avec l'administration ;
- la protection des investissements de l'Etat ;
- l'engagement de l'entité et de tous les acteurs concernés par la mission de l'entité à respecter les obligations légales ;
- la protection des personnes et des biens ;
- l'entretien de relations sociales de qualité ;
- le respect des intérêts légitimes et justifiés des partenaires et fournisseurs ;
- la préservation de l'environnement ;
- la protection et la valorisation de l'image de l'entité et du ou du ministère ;
- la protection du patrimoine historique et culturel de l'entité.

Les dommages sur les valeurs essentielles pourront ensuite être synthétisés par axes d'impact, par exemple :

- opérationnel : la capacité à remplir la mission ;
- financier ;
- juridique ;
- social/humain ;
- réputation/image.

Les métiers devant ensuite définir des échelles d'impact, permettant ensuite à la SSI de formaliser des règles « gradées en adéquation avec les besoins métiers exprimés.

Les difficultés de l'approche méthodologique orientée enjeux :

Les pièges sont nombreux : le premier est de classifier en fonction non pas de l'impact mais en fonction de la probabilité, le deuxième est de « sur classifier » par réflexe de « survalorisation » de sa mission, le troisième est de classifier en fonction de règles ou de solutions déjà mises en place, le quatrième est de classifier en fonction des règles jugées comme admissibles, le cinquième est de classifier en fonction des budgets jugés opportuns, enfin, le sixième piège est de ne pas adhérer à la démarche.

Il doit donc être bien clair que la stratégie de défense mise en avant dans la nouvelle politique de l'Etat nécessitera clairement d'obtenir l'implication des métiers.

L'expression de besoins de sécurité est le préambule à l'adhésion des métiers dans le respect des règles et des exigences naturellement liées à leurs missions. Les directives « Gestions des biens », « Intégration de la SSI dans le cycle de vie des SI » et les autres directives orientées plus mises en œuvre le montrent clairement, comme par exemple la stratégie de défense en profondeur déclinée par la constitution de zones logiques et physiques de protection adaptées et répondant aux enjeux et besoins classifiés. L'appartenance à une zone de protection devant être définie par la classification des besoins de sécurité des informations, des processus qui les manipulent et des ressources qui les supportent. Cette stratégie de défense en profondeur constituée de zones logiques de sécurité constitue un élément fondamental de l'architecture de sécurité des systèmes d'information ne pourra s'appliquer qu'avec la participation active des représentants métiers.

Les règles techniques et architecturales sont ensuite mises en œuvre en fonction des besoins formalisés par les responsables métiers, conformément aux directives fonctionnelles de la PSSI de l'Etat. L'outil méthodologique EBIOS, (Expression des Besoins Identifiés et Objectifs de Sécurité), conçu par l'ANSSI pour structurer l'approche et améliorer la qualité du dialogue sécurité entre les maîtrises d'ouvrage, les maitrises d'œuvre et la SSI est essentiellement ressenti encore comme une affaire de spécialiste.

Le référentiel général de sécurité (RGS) destiné aux autorités administratives devait permettre, dans son application, de rassurer la confiance des usagers dans l'administration électronique. Il exige lui aussi une approche orientée enjeux et gestion de risques informationnels est encore lui aussi, aujourd'hui clairement méconnu des métiers.

Aujourd'hui, il est donc fondamental de se poser, la question des moyens que se donneront les directions pour expliquer et respecter la démarche de la PSSI de l'Etat. Un grand nombre difficultés à surmonter sont bien de l'ordre de la pédagogie et de la communication.

A ce sujet, il est significatif et utile d'identifier les préjugés classiques rencontrés dans les métiers concernant la SSI et qu'il faudra absolument surmonter. Le premier est clairement la sous-évaluation des risques liés à l'ignorance des règles au profit de l'évaluation de la malveillance toujours plus médiatique. Le deuxième encore malheureusement très répandu est de croire que le but de la SSI est de garantir uniquement la confidentialité des données en oubliant la disponibilité, l'intégrité et la preuve. Ce préjugé est extrêmement grave car totalement démobilisateur pour les métiers qui ne manipuleraient pas d'informations confidentielles. Le troisième préjugé, et nous l'avons fortement souligné, est de croire que

c'est aux RSSI et aux DSI de formaliser les besoins de sécurité. Le quatrième préjugé est de croire que la technologie peut tout régler. Il doit être intégré par toutes les parties prenantes que la technologie ne peut interdire techniquement tout ce qu'une entité veut prohiber. Ce n'est par pas parce qu'une action sur le système d'information est possible qu'elle en est autorisée. Aussi la prise en compte du facteur humain prend tout son sens dans la formalisation, l'explication des règles et surtout le contrôle de leurs bonnes applications. Enfin le préjugé le plus grave est bien de croire que la sécurité est une science exacte et de donc de sous-estimer l'organisation de dispositifs d'arbitrage. C'est bien, sur ce piège que l'entité devra anticiper les difficultés. Les dispositifs organisationnels d'aide à arbitrage seront-ils mis en place pour :

- décider des seuils d'impact et de besoins ;
- identifier les menaces jugées pertinentes pouvant exploiter les vulnérabilités des processus métiers et des ressources qui les supportent ;
- décider des niveaux de gravité de risques ;
- définir les priorisations d'actions ;
- valider l'acceptabilité des risques résiduels ;
- décider de la mise à disposition des budgets nécessaires à la mise en application des règles relatives à ces contextes.

Les difficultés organisationnelles

Dès 1994, l'ANSSI (la DCSSI à l'époque) bien consciente de cette problématique avait poussé à l'Etat à formaliser la circulaire interministérielle N° 901/DISSI/SCSSI du 2 mars 1994 pour anticiper ces difficultés liées à l'arbitrage.

La solution mise en avant est la séparation des fonctions. Pour simplifier, il s'agit de mettre en place une voie fonctionnelle de sécurité complétée d'acteurs opérationnels de sécurité en complément de la voie hiérarchique.

La voie fonctionnelle de sécurité est chargée de cinq grands types de missions :

- Stratégique : Définir la stratégie SSI, élaborer et actualiser les directives, procédures et guides. Accompagner les métiers dans leur démarche de classification des informations et processus métiers. Assister les DSI dans la démarche de classification intrinsèque des ressources SI. Conseiller les parties dans la cartographie des risques.
- Le Pilotage : Organiser et contrôler le déploiement de la PSSI, s'assurer que les risques majeurs informationnels et SSI relatifs aux métiers sont sous contrôle, évaluer l'efficacité de l'action SSI, en vue d'une optimisation permanente.
- L'Opérationnel **:** Accompagner les parties prenantes à la mise en œuvre des mesures de sécurité préventives, dissuasives et réactives.
- Le Support **:** Permettre aux intervenants en charge, de la mise en œuvre de la PSSI, de réaliser les actions qui les incombent.
- Le Contrôle : S'assurer de la conformité à la PSSI, analyser son efficacité dans la protection des missions et sa contribution à la bonne efficacité des métiers.

Cette voie fonctionnelle dont le plus haut niveau pour le périmètre de l'entité est l'AQSSI doit être l'autorité responsable (au sens juridique) de la sécurité des systèmes d'information dans les administrations centrales et les services déconcentrés de l'Etat, ainsi que dans les établissements publics et dans les organismes et entreprises ayant conclu avec

l'administration des marchés ou des contrats visés par ce même article. Il est majeur de rappeler que cette responsabilité ne peut pas se déléguer.

Il est important de noter que le choix de l'AQSSI n'est pas sans difficultés. Certaines entités sont sous une double autorité de tutelle. C'est le cas de certain centre de recherches qui sont sous la double tutelle du Ministère de l'enseignement supérieur et de la recherche et du Ministère de la défense.

Cette voie fonctionnelle (HFDS - Haut Fonctionnaire de Défense et de Sécurité –, FSSI - Fonctionnaire de Sécurité des Systèmes d'Information, AQSSI, RSSI) doit permettre aux responsables métiers de solliciter du conseil interne pour arbitrage et aide à la décision. Elle doit faciliter l'obtention de dérogations éventuelles, si les demandes sont clairement argumentées et justifiées. Par ailleurs cette voie fonctionnelle doit faciliter la remontée d'incidents. En effet, même, s'il est clair que la notification d'incidents détectés doit être remontée aux responsables conformément au devoir de loyauté vis-à-vis de l'employeur, il ne faut pas sous-estimer le facteur psychologique. La remontée d'incidents est souvent identifiée comme culpabilisante voire parfois comme de la délation. Ainsi cette voie fonctionnelle est constituée d'acteurs, par exemple les RSSI sans autorité hiérarchique sur les agents ce qui permet d'anticiper cette difficulté, si bien sûr, elle est bien expliquée à l'ensemble des acteurs.

Or il faut bien constater dix ans après que l'essentiel des directions métiers dans les entités et en tout cas pas les utilisateurs ne connaissent pas ou peu l'existence de cette voie fonctionnelle, décrite dans l'ancienne directive interministérielle, et ne la sollicitent donc pas. Le RSSI est identifié le plus souvent comme un expert technique pour la direction informatique, il est rarement identifié comme un conseil pour les métiers ou les utilisateurs.

Il est intéressant de noter qu'un très grand nombre d'entreprises privées ou de codes règlementaires, notamment dans le monde industriel ou financier s'appuient sur le même principe de la séparation des devoirs et pouvoirs : Sarbanes Oxley, Solvency II, ….

Ainsi afin d'être plus efficace que par le passé, la mise en œuvre de la nouvelle PSSI de l'Etat devra fortement s'appuyer sur la capacité des cadres fonctionnels et du RSSI à se connaître et se comprendre.

Les bonnes pratiques de management pour la sécurité :

Les cadres dans leurs directions métiers devront s'approprier la démarche organisationnelle et méthodologique afin d'assumer leurs engagements de responsabilité :

- faire classifier les informations créées par les agents dans leurs missions quotidiennes,
- participer à la diffusion des règles relatives aux niveaux classifiés,
- expliquer les exigences règlementaires, (devoir de réserve, devoir de confidentialité, devoir de de loyauté, devoir de notifications d'incidents, devoirs liés aux responsabilités civiles et pénales de l'entité et celles liée à l'agent ou au sous-traitant,
- valider les risques résiduels,
- formaliser les scénarios de crises pouvant affecter leurs missions,
- gérer les personnes ou fonctions identifiées comme stratégiques ou devant manipuler des informations sensibles dans leurs missions,

- gérer les sous-traitants, faire valider et homologuer les produits et les prestataires,
- participer au contrôle du respect des exigences SSI et à l'analyse de leurs efficacités.

Les produits et services acquis par les entités doivent être homologués :

La PSSI de l'Etat précise que les entités doivent acquérir des produits ayant fait l'objet d'une évaluation et d'une attestation préalable de leur niveau de sécurité (homologation). Il en est de même pour les prestations de sécurité conduites sur son système d'information. L'autorité administrative doit attacher le plus grand soin dans le choix du prestataire. En effet, la fourniture de produits ou de services (comme l'activité d'audit) est très critique eu égard aux vulnérabilités qu'elle est susceptible de générer ou de révéler. L'autorité administrative doit disposer de garanties sur la compétence du fournisseur, sur la qualité sécurité des produits ou du prestataire d'audit.

Cette véritable certification est un processus par lequel un organisme se voit attribuer une homologation attestant que ces produits ou acteurs sont conforme aux règles normées.

L'idée de base est la capacité de s'appuyer sur un tiers ici l'ANSSI, et de considérer que les produits mis en œuvres ou utilisés répondent à des exigences de sécurité à la convenance de l'ANSSI et de l'entité.

Les intérêts directs pour l'entité sont clairs, elle n'a plus à avoir à analyser elle-même la façon dont la sécurité est assurée au sein d'une des composantes, produits et prestataires, cette responsabilité incombe à l'ANSSI. Néanmoins cette approche n'est pas sans écueils. Outre le faible nombre de produits homologués, il n'y par exemple pas d'anti-virus ou d'OS dans les produits qualifiés, il doit être clair que les produits ou prestataires doivent répondre à des besoins et respecter des règles relatives à ces besoins. Nous retrouvons ici la difficulté liée à la faible implication des responsables métiers, aujourd'hui à formaliser leurs expressions de besoins de sécurité.

Quelle Organisation mettre en place ?

Quatre grands types de fonctions sécurité système d'information seront à mettre en place dans l'organisation de l'entité :

1. **Les fonctions en charge d'identifier les obligations légales spécifiques aux missions, de classifier la sensibilité des informations**, (l'expression de besoins de sécurité), l'identification des menaces spécifiques aux métiers, voire l'identification des vulnérabilités qui leurs sont propres et la validation des risques résiduels.

   Ces fonctions ne pourront qu'être occupées par des correspondants métiers sensibilisés et formés dans les métiers afin de formaliser les besoins.

2. **Les fonctions en charge d'élaborer et de faire appliquer la politique de sécurité**.

Ces fonctions sont bien identifiées et sont sous la responsabilité des acteurs de la voie fonctionnelle de sécurité, FSSI, HFDS, AQSSI et RSSI. L'axe d'amélioration est clairement de se faire mieux connaitre, notamment des métiers et des utilisateurs.

3. **Les fonctions en charge de mettre en œuvre la PSSI, c'est-à-dire d'intégrer techniquement les règles fonctionnelles** relatives aux besoins dans les solutions d'architecture.

   Il s'agit bien de la responsabilité de la DSI qui doit donc :

- intégrer les aspects sécurité dans les architectures ;
- spécifier, concevoir et maintenir les services et solutions de sécurité préventives et réactives ;
- formaliser et promouvoir la prise en compte de la sécurité dans les projets SI ;
- accompagner la mise en place des solutions de sécurité ayant un impact sur le fonctionnement des directions métiers ;
- mettre en place et maintenir les dispositifs de détection d'intrusion, de surveillance et de réaction à incident de sécurité ;
- alimenter le dispositif de pilotage de la SSI.

4. **Les fonctions de pilotage et arbitrage.**

- suivre l'application des règles de la PSSI ;
- éclairer les éléments d'arbitrage relatifs à la sécurité ;
  Sur ce point il est impératif d'identifier les grands types de « conflit » extrêmement tôt, afin d'éviter la pression sur l'arbitre. Ces divergences de vue s'opèrent classiquement entre d'une part le métier et sa maitrise d'ouvrage et d'autre part la direction des systèmes d'information ou entre la direction des systèmes d 'information et la sécurité système d'information, voire entre les directions métiers. Il est significatif que ces comités de pilotage soient rarement organisés et quand ils le sont, les responsables métiers sont très rarement sollicités. Ils sont le plus souvent des comités de pilotage de projet à vocation uniquement technique.
- rechercher les mutualisations ou optimisations possibles au sein de l'entité ou du ministère et promouvoir les meilleures pratiques ;
- définir un socle commun de contrôles et d'indicateurs permettant de suivre le déploiement de la PSSI et d'en apprécier son efficacité ;

La bonne réalisation de cette fonction de contrôle par l'entité nécessitera :

- la définition judicieuse de données brutes donnant une idée fiable de la sécurité, facilitant la prise de décision et la remontée d'information ;
- la définition des modalités de recueil et d'exploitation de la valeur de ces données brutes (procédures et outils) ;
- la protection de ces données et des dispositifs impliqués dans leur recueil et exploitation ;
- la conception de tableaux de bords agrégeant ces données en indicateurs.

Dans ce cadre, un indicateur est une information, brute ou présentant un certain degré de synthèse, dont la valeur, relevée à une fréquence donnée, reflète un aspect du niveau de sécurité alors qu'un tableau de bord est un document qui, pour un périmètre et un

niveau de pilotage donné, restitue la vision de la sécurité déterminée à partir de la valeur des indicateurs.

Les indicateurs relèvent pour l'essentiel des maîtrises d'œuvre. Les tableaux de bord, quant à eux, devront refléter les différents points considérés comme importants dans la PSSI : maturité, sensibilisation, analyse d'enjeux et de risques dans les projets, respect des règles, enjeux, etc.

Concrètement, très peu de tableaux de bords effectifs sont en place aujourd'hui dans les entités concernées par la PSSI E. Le seul tableau de bord, en complément du rapport annuel demandé par le HFDS, communément envisagé ou employé est la rosace de couverture « des best practices » qui permet une vision de l'évolution de l'application des règles « auto justifiées » de sécurité informatique.

Il est donc particulièrement clair que la bonne réalisation des ambitions formalisées dans la PSSI de l'Etat nécessitera de manière incontournable un plan d'actions de communication, sensibilisation, formation et surtout de responsabilisation plus efficace que par le passé, afin d'améliorer la qualité du dialogue entre les acteurs :

- les acteurs métiers et leurs maîtrises d 'ouvrage ;
- les acteurs directions système d'Information et leurs maîtrises d'œuvre ;
- les Responsables Sécurité Système d'Information ;
- et surtout bien sûr, sans oublier les utilisateurs du système d'information.

Le niveau de maturité en sécurité système d'information d'une entité ne peut se résumer à la compétence technique des informaticiens experts en sécurité informatique mais bien à l'engagement des acteurs métiers (responsables hiérarchiques et utilisateurs) à suivre la démarche d'expressions de besoins et à respecter les règles relatives à ces besoins.

Denis VIROLE

VIROLE CONSEIL FORMATION

[i] http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf