Retour d'expérience autour de la réalisation de la PSSI de l'ISIR

Ludovic Billard
Institut des Systèmes Intelligents et de Robotique
Université Pierre et Marie Curie
4 place Jussieu
75005 PARIS

Sylvie Dupuy
Direction des Système d'Information
Pôle Sécurité des Systèmes d'Information
Université Pierre et Marie Curie
4 place Jussieu
75005 PARIS

Valérie Givaudan
LAL IN2P3/CNRS
Service Informatique
Université Paris-Sud
91898 Orsay Cedex

Résumé

Dans le cadre d'une coopération entre l'UPMC (Université Pierre et Marie Curie) et la DR2 du CNRS (Direction Régionale 2, Centre National de Recherche Scientifique), les directeurs d'unités ont été incités à mettre en place une PSSI (Politique de Sécurité des Systèmes d'Information). Grâce à la nomination d'un CSSI (Correspondant Sécurité du Système d'Information) ce projet, sous l'égide de la direction et avec le concours des RSSI des tutelles, a pu être mené dans plusieurs unités mixtes. Dans cet article, nous évaluerons, à travers un retour d'expérience, l'adéquation entre les outils proposés par un groupe de travail formé par l'UPMC et la DR2 CNRS et la réalité du terrain. Cette évaluation à l'appui, nous mettrons en évidence l'existence de nombreux aspects communs aux unités de recherche indépendamment de leurs domaines d'activités. En s'appuyant sur des objectifs de sécurité exprimés en termes de Confidentialité, Intégrité et Disponibilité, et en disposant d'une méthodologie de travail, nous partagerons ce retour d'expérience en montrant comment mettre en place cette démarche. Nous rappellerons, d'autre part, que l'implication des différents acteurs (groupe projet, direction, CSSI) aux différentes étapes du projet de PSSI – de l'ébauche à son application - est primordiale pour la bonne conduite de ce projet.

Mots clefs

PSSI, UPMC, CNRS, UMR, EBIOS, ISO27001, ISO27002

Introduction

En 2008 l'Université Pierre et Marie Curie et la Direction Régionale 2 du Centre National de la Recherche Scientifique ont fait le choix d'œuvrer ensemble à la mise en œuvre de politiques de sécurité dans les Unités Mixtes de Recherche en demandant conjointement aux directeurs d'unités de nommer officiellement un Chargé de Sécurité du Système d'Information. La mission principale du CSSI était, bien sûr, l'amélioration du niveau de sécurité de son unité, quel que soit son point de départ. A cette époque, le CNRS disposait d'une Politique de Sécurité du Système d'Information officiellement applicable depuis plusieurs années. L'UPMC, pour sa part, s'était engagée dans l'élaboration d'un document fortement inspiré des normes 27001 et 27002. Ces documents émanant des tutelles constituaient un cadre de référence et ils permettaient de comprendre ce qu'était une PSSI et le type de mesures de protection que l'on pouvait y trouver. Cependant,

en dehors d'un petit nombre de personnes habituées à utiliser le vocabulaire de la SSI, le côté formel de ces documents ne les rendait pas facilement utilisables par les CSSI. Un groupe de travail impliquant plusieurs CSSI et Responsables de la Sécurité du Système d'Information fut donc constitué afin de réfléchir à la façon dont pourrait être mené un projet de PSSI dans une unité. L'unité Sisyphe (UMR 7619) fut choisie comme unité pilote avec comme phase essentielle du projet, la réalisation d'une analyse des risques complète permettant d'élaborer un outil adapté au contexte des unités de recherche et réutilisable par d'autres. Des scénarios présentant des menaces et des vulnérabilités habituellement rencontrées dans notre environnement d'enseignement et de recherche ont été intégrés à cet outil afin d'illustrer une analyse de risques sur des actifs dits "génériques". La valorisation des risques sur ces actifs génériques résulte aussi bien des enjeux liés aux données scientifiques ou administratives détenues par l'unité que des enjeux liés à la continuité d'activité, c'est-à-dire à la disponibilité des services vitaux. Les représentants SSI de la délégation Paris B et de l'UPMC contribuent à diffuser ces outils auprès des CSSI. Cet article décrit, vu du terrain, l'intérêt des outils fournis par les tutelles sans oublier de mettre en exergue les écarts existant entre la méthode et la réalité.

Retour d'expérience sur la mise en place d'une PSSI à l'Institut des Systèmes Intelligents et de Robotique

Suite à la nomination du CSSI de l'ISIR, la direction a décidé de porter le projet de Politique de Sécurité du Système d'Information, avec le soutien des RSSI de ses tutelles: l'UPMC et le CNRS. Après la formation à l'analyse de risques, le premier travail du CSSI a été de réaliser l'inventaire des données et services concernés par la SSI à l'intérieur des différents périmètres constituant les principales missions du laboratoire : enseignement et recherche. Pour atteindre cet objectif, le comité de pilotage SSI de l'ISIR a été formé et composé de la direction de l'unité, des représentants de chaque équipe et du CSSI. La première mission du comité SSI a été la constitution de la liste des données utilisateurs dites "sensibles".

Etude du périmètre de l'Administrateur Système et Réseau

Dans un premier temps, l'inventaire le plus rapide consiste à étudier les services et actifs gérés par l'ASR de l'unité. En effet, ayant une vision complète de ce périmètre, il peut facilement le réaliser rapidement et de manière de façon à peu près exhaustive tenant compte des critères de l'environnement des serveurs. Cet inventaire mentionne différentes informations : conditions d'accès aux actifs de soutiens (serveurs), contrats de maintenance, conditions d'accès logique et physique aux services...
Dans un second temps, le regroupement de services contribuant aux mêmes activités est effectué dans le but de faire émerger des fonctions qui pourront être plus facilement valorisées par le comité de pilotage SSI.

Exemple : fonction « communication », qui comprend les services supports suivants : la téléphonie, la messagerie internet, le site institutionnel etc.

Etude du périmètre métier : recherche et enseignement

En élargissant le périmètre de l'étude, nous avons inventorié les services supports de la « fonction recherche » et intégré les plates-formes expérimentales : conditions d'accès, sécurité particulière des informations, identification des architectures sensibles (SCADA). Ensuite, les flux de dépôts de brevets / publications ainsi que les processus de valorisation de la recherche auprès des différentes tutelles ont fait l'objet d'une analyse toute particulière.

Exemple : étude du processus de dépôt de brevet. Les échanges avec les différents services de valorisation de la recherche scientifique sont ils chiffrés ? Les échanges avec les co-auteurs sont ils aussi sécurisés ? Les usagers sont ils informés du risque d'échanges non chiffrés ?

Etude du périmètre administratif

Dernier périmètre inventorié, nous recensons les personnes manipulant des données administratives (nominatives), les actifs de soutiens (machines) et nous faisons un bilan sur les processus de traitements automatiques de données en vue de déclaration Commission Nationale de l'Informatique et des Libertés. Les logiciels utilisés par les tutelles, mais aussi les développements logiciels locaux, sont inventoriés.

Enquêtes utilisation des données

En parallèle, une enquête sur l'usage habituel des données sensibles est réalisée auprès des utilisateurs représentatifs de la population de l'ISIR et un questionnaire est rempli par les personnes auditionnées. Nous obtenons ainsi un bon aperçu des usages dans l'unité et des données et de leur environnement de stockage. Cette étape nécessite beaucoup de temps car les auditions sont à conduire de façon rigoureuse. Lors de ces entrevues, de nombreuses questions sont soulevées par les usagers, notamment sur le caractère "bon/mauvais" de leurs habitudes de gestion de leurs données.

Exemple : les publications en cours d'écritures sont elles copiées quelques part ? Si oui sur quel support ? Où ces données sont elles principalement stockées et/ou traitées ? Dans le cas d'ordinateurs portables, il conviendra d'appliquer la directive du CNRS sur le chiffrement systématique de portable.

L'analyse de risques

Présentation de l'outil de la DR2

Cet outil a pour but d'aider les CSSI à mener au sein de leur laboratoire une réflexion sur les différents "actifs" (données, serveurs et service sensibles) qui, du fait de leur degré de sensibilité (confidentialité, disponibilité, intégrité) et des enjeux spécifiques au laboratoire, font courir à ce dernier des risques dans l'accomplissement de ses missions. Ces risques, lorsqu'ils existent, doivent être mis en évidence, évalués et réduits autant que possible. Une analyse de risques consiste, pour chaque enjeu du laboratoire, à déterminer l'ensemble des menaces et vulnérabilités ayant effectivement un impact sur ces enjeux et qui sont les plus probables dans le contexte du laboratoire. Cette étude se fait en fonction des critères de sensibilité retenus par le laboratoire sur les enjeux et en tenant compte des mesures déjà en place. L'outil fournit des fichiers génériques, basés sur les normes ISO 27001 (*Technologies de l'information – Technique de sécurité – Système de sécurité de l'information – Exigences*) et ISO 27002 (*Code de bonnes pratiques pour la gestion de la sécurité de l'information*), dans lesquels certaines menaces improbables dans nos environnements ont déjà été éliminées. Pour chaque couple menace/vulnérabilité retenu l'outil propose des objectifs et des mesures de sécurité permettant de réduire les risques. Les objectifs retenus correspondent alors aux futurs chapitres du document de PSSI. L'expérience menée avec le laboratoire pilote a permis de mettre en évidence une factorisation possible du travail d'analyse de risques : en effet, on peut en général dérouler pour tous les services "système" critiques la même analyse de risque, de même pour des typologies de données (données administratives, d'enseignement, de valorisation, de terrain, etc…) qui présentent souvent à la fois les même exigences de sécurité et les même risques. C'est ce constat qui a orienté l'outil vers des fichiers dit "génériques" que le laboratoire doit adapter à ses spécificités : enjeux, niveau de sensibilité, mesures déjà en place. Par ailleurs l'outil, réalisé sur la base des normes ISO 27001 et 27002, a l'ambition de proposer une interprétation concrète de ces normes pour nos laboratoires.

Utilisation de l'outil de la DR2 à l'ISIR

L'outil réalisé par la DR2 du CNRS a permis de réaliser très rapidement une analyse de risques des différents périmètres de façon structurée en intégrant les normes ISO 27001 et 27002. En effet, grâce à une pré-analyse de certains périmètres, la démarche a été simplifiée. Par exemple, l'analyse de la sphère administrative est identique dans beaucoup d'unités de tutelles CNRS / université, notamment en ce qui concerne la gestion des ressources humaines ou financières. De même, l'analyse des services informatiques communs, caractérisés par leur fort besoin en disponibilité, est en partie déjà réalisée par l'outil. Nous l'avons approfondie à partir de scénarios propres au contexte de l'ISIR. La simplification de l'analyse proposée par l'outil, par rapport à la méthode **EBIOS** [1] dans sa version complète, permet de se focaliser sur les contraintes spécifiques aux établissements de recherche sans tenir compte des aspects qui n'ont souvent un sens que dans le monde des entreprises. A travers une démarche dans laquelle le dialogue avec les utilisateurs est essentiel, l'outil permet de couvrir l'ensemble des menaces / vulnérabilités en fonction du périmètre à analyser. Il propose un choix de mesures issues de la norme 27002 permettant de réduire les risques et fait le lien entre ces mesures et les chapitres du futur document de PSSI.

[1] *Expression des Besoins et Identification des Objectifs de Sécurité : http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html*

La synthèse

La synthèse de ces analyses, de quelques pages, a été présentée à la direction de l'unité Elle décrit l'utilisation des données et leur cycle de vie, l'analyse du périmètre administratif, et rappelle les engagements des administrateurs de machines fixes et la politique de sécurisation des portables. Elle établit les dispositions d'accès aux ressources de l'unité par les invités (chercheurs et stagiaires), les possibilités de connexion des appareils nomades et dresse un état des lieux des données nominatives.

Scenarios et choix des mesures

A partir de la synthèse, plusieurs scénarios sont réalisés et étudiés afin d'établir la vraisemblance des menaces. La direction et le comité SSI prennent position sur chacun d'entre eux afin de faire émerger des priorités entre les différents risques en tenant compte des objectifs de sécurité et des impacts sur le système d'information. Chaque mesure compensatoire est alors évaluée, en termes de coûts financiers et humains, et présentée à la direction qui s'engage alors sur la mise en œuvre de ces dernières.

Exemple sur les dépôts de brevets : les usagers ne chiffrent pas systématiquement les échanges avec les services de valorisation des tutelles. Le risque est ici qu'une personne mal intentionnée puisse intercepter le mail et en prendre connaissance, faisant perdre toute légitimité à son (ses) auteur(s). Il faut donc communiquer sur ce point, à travers une campagne d'information dont le coût sera essentiellement humain. La direction s'engage sur cette mesure compensatoire et des sessions d'informations et de formation au chiffrement des échanges sont mises en place sur divers media : information orale, courrier électronique, fichiers sur l'intranet.

Autre exemple sur le service support « Connexion à distance » de la fonction télétravail. Ce service a été répertorié comme vital par le comité SSI et fortement valorisé par sa disponibilité (4h ouvrable). La menace la plus critique et vraisemblable est le crash matériel de la machine. La mesure compensatoire envisagée est alors de faire une redondance de ce service, dans un autre local climatisé (local cluster ou local brassage). La solution technique apportée à la contrainte de disponibilité est alors de mettre en place un mécanisme de haute disponibilité entre deux machines qui implémenteront ce service. Le coût financier est alors estimé à l'acquisition d'une nouvelle machine (permettant la virtualisation afin d'amortir l'investissement) et le coût humain de 3 jours - ingénieur pour la mise en place, le test et la production de la documentation.

Production et validation du document : la PSSI

A l'aide du plan type d'une PSSI d'unité, le CSSI renseigne chaque chapitre du document avec les mesures issues de l'outil DR2. Ce document est ensuite présenté au conseil de laboratoire et voté pour application. Il doit être à disposition du personnel de l'unité.

Conclusion

L'outil proposé par la DR2 du CNRS intervient à toutes les étapes de la mise en place de la politique de sécurité du système d'information d'une unité de recherche. La simplification de la démarche d'analyse de risques, le choix des mesures et le classement en chapitres réduisent considérablement le temps de production du document et permet d'avoir une approche très organisée et linéaire: commencer par un périmètre connu puis élargir vers l'ensemble de l'unité. Ainsi il permet à toute unité d'entamer la réalisation d'une PSSI. Cependant, cette démarche ne peut pas être totalement linéaire car elle nécessite un grand investissement de temps sur une courte période.