Surveillance continue de la sécurité de l'information

Une promesse et un défi

Bill Hargenrader, CISM, CEH, CISSP, est le technologue en chef de Booz Allen Hamilton, entreprise au sein de laquelle il développe une solution logicielle de gestion des processus de cybersécurité nouvelle génération. Il travaille sur une thèse en technologies de l'information centrée sur les points de convergence entre cybersécurité et innovation.

Pour traiter la gestion des risques et la conformité de manière exhaustive, il convient d'associer un référentiel de gestion des risques exhaustif, un ensemble complet de contrôles et une méthodologie de surveillance continue de la sécurité de l'information (SCSI - en anglais ISCM, Information Security Continuous Monitoring). Ces trois éléments combinés fournissent des contrôles dans un large éventail de domaines, avec un niveau de détail élevé et des indications pour personnaliser le système.[1] Pour adopter cette approche de gestion des risques, les entreprises doivent évaluer leur organisation, intégrer le référentiel de gestion des risques et établir un modèle de sécurité basé sur les normes en vigueur en matière de sécurité. Les organisations qui surveillent, évaluent et adaptent leurs contrôles en permanence ont franchi une étape importante pour réduire les risques liés à la sécurité.

Aux États-Unis, au niveau fédéral, de plus en plus d'entreprises mettent en œuvre la SCSI, à l'instar du Département de la Défense (DoD, Department of Defense), pour se conformer aux exigences de la loi FISMA (Federal Information Security Management Act) sur la gestion de la sécurité de l'information. Les problèmes de conformité ont par nature une portée fédérale, mais il y a un certain nombre d'enseignements à tirer et d'améliorations à implémenter dans tous les secteurs, comme la finance, les services publics et la santé. En 2013, le Département de la Sécurité intérieure des États-Unis (DHS, Department of Homeland Security) a présenté à toutes les agences fédérales un accord global de près de 6 milliards de dollars pour l'achat de logiciels de surveillance continue.[2] Le Bureau de la gestion et du budget des États-Unis (OMB, Office of Management and Budget) a publié une directive pour remplacer les cycles d'accréditation trisannuels actuels par la surveillance continue.[3]

La SCSI semble être la meilleure solution de substitution pour gérer les risques et la cybersécurité, mais les méthodologies et les logiciels qu'elle fait intervenir présentent encore des imperfections à corriger et d'autres défis à relever. Ainsi, trois points sont à prendre en considération dans le cadre de la SCSI : la journalisation manuelle ou automatisée des données, la technologie actuellement disponible et la fréquence d'échantillonnage des contrôles.

INFORMATIONS GÉNÉRALES SUR LA SCSI

Cette étude s'appuie essentiellement sur les recherches de l'institut national des normes et de la technologie (NIST, National Institute of Standards and Technology). « Le NIST est chargé d'établir des normes et des directives concernant la sécurité de l'information, y compris les exigences minimales applicables aux systèmes d'information fédéraux. »[4] Le NIST fournit des consignes détaillées pour l'implémentation d'un référentiel de gestion des risques.[5] En outre, il établit une liste étendue et détaillée des contrôles à effectuer dans les agences fédérales, qui peut également servir de norme dans toute autre organisation. Pour être valable au niveau fédéral, un programme de surveillance continue doit inclure le référentiel de gestion des risques, un ensemble de contrôles et des consignes d'implémentation de la surveillance continue. La **Figure 1** décrit trois publications majeures du NIST à ce sujet.

Figure 1 : principales publications spéciales du NIST relatives à la SCSI

Titre de la publication spéciale	Sujet
Publication spéciale SP 800-37 du NIST : « *Guide for Applying the Risk Management Framework to Federal Information Systems* »	Guide de mise en œuvre de la gestion des risques dans une organisation.
Publication spéciale SP 800-53 du NIST : « *Security and Privacy Controls for Federal Information Systems and Organizations* »	Approche multiniveaux de la gestion des risques par la conformité des contrôles. Cette approche inclut la structure, les critères et la désignation des contrôles de sécurité.
Publication 800-137 du NIST : « *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* »	Approche holistique permettant d'élaborer une stratégie de surveillance continue au niveau de l'entreprise, d'implémenter un programme et de mettre en œuvre les activités associées à celui-ci.

La recherche dans le domaine de la surveillance continue est lacunaire à différents égards, notamment parce que la grande majorité des études réalisées à ce jour concernent les secteurs de l'audit, de l'énergie, de la médecine et des réseaux de capteurs. Cela offre toutefois la possibilité de transposer une technologie ou un algorithme d'un secteur à un autre. Par exemple, l'implémentation d'audits permanents et de processus décisionnels dans les premières phases de conception des processus de traitement d'urgence[6] est fortement corrélée à l'intégration de la surveillance continue dans les systèmes dès leur création. La modélisation des solutions de SCSI dans ces autres secteurs pourrait donc être exploitée et permettre un bon en avant de la SCSI.

ÉVALUATION DE LA SURVEILLANCE CONTINUE DU RÉFÉRENTIEL DE GESTION DES RISQUES ET DE CONFORMITÉ

La surveillance continue est l'une des six étapes du référentiel de gestion des risques.[7] Il est donc important de choisir un référentiel adapté à l'activité concernée et aux contrôles de conformité effectués par l'organisation.[8] Ce choix sera basé sur les quatre domaines que sont la sécurité, les services, les activités et la gouvernance. Le principe de sûreté de l'information s'applique également à l'ensemble de ces domaines, car ils jouent tous un rôle dans l'efficacité d'exécution de la mission, l'objectif étant de mener cette dernière à bien. Les publications relatives aux méthodes de gestion des risques sont nombreuses, mais la plus importante est sans doute la publication spéciale 800-37 du NIST, complétée par les publications spéciales 800-53 et 800-137. Ces trois publications répondent de manière exhaustive et durable à la question de la sûreté de l'information dans le cadre de la conformité et de la gestion des risques.

CADRE DU RÉFÉRENTIEL DE GESTION DES RISQUES

La publication spéciale 800-37 du NIST fournit des consignes pour la mise en œuvre d'un programme de gestion des risques au sein d'une organisation. Avec la sophistication et la préparation toujours plus élaborée des attaques, la sécurité nationale se trouve confrontée à des niveaux de dommages plus importants.[9] Pour avoir une idée de leur vulnérabilité et des dommages encourus en cas d'attaque, les organisations ont intérêt à adopter un système d'évaluation continue des vulnérabilités, de leur impact potentiel, des mesures prises pour réduire les risques et du niveau de risque résiduel acceptable. Les organisations qui ne disposent pas d'un système exhaustif s'en remettent essentiellement à la chance. La publication spéciale 800-37 fournit une description de ce système et précise les modalités de son implémentation, mais il revient aux organisations de l'adapter à leurs besoins et de l'appliquer efficacement.

Ce processus implique différentes étapes : catégoriser les systèmes d'information, choisir des contrôles de sécurité adaptés, les implémenter et les évaluer, autoriser les systèmes d'information et surveiller les contrôles de sécurité.
La publication spéciale 800-37 traite principalement de l'évaluation des contrôles pour déterminer le niveau de risque auquel l'organisation est exposée. Le niveau de conformité ou l'exhaustivité des contrôles de sécurité en place peut donner à la direction un aperçu du niveau de risque global de son organisation, ainsi que des indications sur les domaines à protéger davantage par le biais de politiques, de technologies ou de ressources humaines supplémentaires.

CADRE DES CONTRÔLES DE SÉCURITÉ

Dans le référentiel de gestion des risques, les contrôles de sécurité jouent un rôle essentiel. La publication spéciale 800-53 s'appuie sur une approche de gestion des risques à plusieurs niveaux, basée sur la conformité des contrôles. Cette approche inclut la structure, les critères et la désignation des contrôles de sécurité.[10]
Les publications spéciales 800-53 et 800-37 sont complémentaires, car elles superposent les contrôles au référentiel de gestion des risques pour une organisation. Les contrôles sont sélectionnés en fonction de la criticité et de la sensibilité des informations contenues dans le système et ils sont appliqués selon un ordre de priorité établi. Ces contrôles incluent, entre autres, l'identification et l'authentification, le plan de secours, la réaction aux incidents, la maintenance, l'appréciation du risque et la protection des supports.

CADRE DE SURVEILLANCE CONTINUE DE LA SÉCURITÉ DE L'INFORMATION

Le terme « surveillance continue » peut être ambigu, car il a différentes significations selon les secteurs d'activité. La publication spéciale 800-137 du NIST définit une norme à suivre pour appliquer ce principe au référentiel de gestion des risques en utilisant l'ensemble de contrôles établi par le NIST. L'implémentation de la SCSI consiste principalement à :[11]

- Définir une stratégie de SCSI
- Établir un programme de SCSI
- Implémenter un programme de SCSI
- Analyser les données et en tirer des conclusions
- Agir en fonction de ces conclusions

• Corriger et mettre à jour le programme et la stratégie de surveillance

Cela implique d'effectuer des vérifications manuelles et automatisées de manière à fournir en permanence des retours et des informations au système dans son ensemble.

Ces trois publications spéciales du NIST fournissent une base solide pour la surveillance continue de la sécurité, la gestion des risques et la conformité, mais il convient d'en revoir certains points pour être totalement efficace. La technologie automatisée est un élément moteur de la surveillance continue et elle est au centre des travaux effectués jusque-là concernant la SCSI.[12] Cependant, il n'est possible de suivre autant de contrôles qu'à l'aide d'un processus automatisé et ceci représente une différence certaine par rapport à un contrôle manuel des activités. Il faut en outre tenir compte de la disponibilité de la technologie. L'un des plus grands projets de SCSI réalisés au niveau fédéral a produit une suite d'outils automatisés pour y répondre. Reste à savoir combien de contrôles ces outils sont en mesure de traiter, et à quelle fréquence. La publication spéciale 800-137 du NIST fournit effectivement des directives, mais sans rentrer dans le détail.

AVANTAGES ET INCONVÉNIENTS DU MODÈLE : PROCESSUS AUTOMATISÉS OU MANUELS

Le modèle de la SCSI présente notamment l'avantage de recueillir de façon automatisée des données agrégées relatives aux systèmes existants. Ce processus automatique fournit en temps réel les informations à collecter qui seront examinées par la direction. En revanche, il ne permet pas de traiter les activités qui ne sont pas automatisées ou sont effectuées hors connexion, et c'est l'un de ses inconvénients. Il peut être difficile de saisir et de journaliser automatiquement la date de planification d'un achat ou de modification d'une politique, par exemple. De plus, il n'existe aucun rapport fédéral donnant des directives de journalisation manuelle. Selon la publication spéciale 800-137 du NIST, les contrôles et procédures manuels doivent répondre aux mêmes exigences que les contrôles automatisés.

Une solution possible consisterait à fournir un mécanisme de journalisation manuelle pour les actions effectuées. Il pourrait s'agir d'une interface de connexion permettant aux employés d'indiquer quand une tâche est terminée (sauvegarde d'un serveur ou effacement à distance des données d'une salle de serveurs, par exemple). Il est également possible d'automatiser les feuilles d'émargement utilisées pour gérer l'accès physique aux zones contrôlées, pourquoi pas avec une tablette qui enregistre l'heure de la signature et le nom de la personne, et identifie les comportements inhabituels (accès à des heures tardives, par exemple). La liste des avantages et des inconvénients des solutions automatisées et physiques pourra être complétée par une étude des solutions de surveillance continue actuelles.

COMPARATIF DES SOLUTIONS LOGICIELLES DE SURVEILLANCE CONTINUE

Les directives de l'OMB indiquent que « La phase de surveillance continue doit s'appliquer à l'ensemble des contrôles opérationnels, techniques et de gestion implémentés dans le système d'information et son environnement, y compris les contrôles d'accès physique aux systèmes et à l'information. »[13] À ce titre, l'OMB a créé un tableau répertoriant toutes les applications proposées par le DHS pour les systèmes fédéraux, comme indiqué précédemment.[14] Le logiciel a fait l'objet d'une revue en ligne et ses contrôles ont été triés par type et catégorie, selon la classification du NIST (**Figure 2**).

Une fois les données collectées et examinées, un tableau comparatif a été créé pour répertorier les types de contrôle utilisés et inutilisés. Ces données ont permis de dégager une estimation globale de la couverture totale effective offerte par la solution automatisée actuellement proposée.

ANALYSE DES LOGICIELS DE SURVEILLANCE CONTINUE

Parmi les 21 catégories de contrôles, huit sont couvertes par les offres logicielles du DHS pour la surveillance continue. En outre, de nombreux contrôles spécifiques n'entrent pas dans les différents types de contrôles définis. De manière générale, seulement 38 % des types de contrôles sont pris en charge par l'offre logicielle. Cela laisse la place à des améliorations ultérieures. Il existe des solutions logicielles qui ne figurent pas dans cette liste et qui traitent certaines catégories de contrôles supplémentaires. Pour le moment, aucun système n'est capable d'intégrer l'ensemble des flux de données générés par ces différents outils logiciels.

FRÉQUENCE D'ÉVALUATION DES CONTRÔLES

Pour déterminer la fréquence d'échantillonnage, différents facteurs sont à prendre en compte : le niveau de risque, les modifications de l'élément de contrôle (souvent intermittentes) et le statut en cours ou incomplet du contrôle.[15] Le niveau de risque représente l'impact que pourrait avoir l'exploitation d'une vulnérabilité associée au contrôle. Les seuils et la périodicité doivent être définis par la direction de l'organisation et par l'administration compétente.

Ainsi, un serveur Web public présente un niveau de risque supérieur à un serveur de fichiers situé sur le domaine sécurisé d'une organisation, car la probabilité d'une attaque sur ce dernier est moindre, tout comme l'impact de sa mise hors ligne. C'est pourquoi les échantillonnages sont plus fréquents sur les serveurs publics. Il faut également tenir compte de la sensibilité des données concernées. Si le serveur de fichiers en question contient des numéros de sécurité sociale, la fréquence d'échantillonnage requise sera plus élevée que sur le serveur Web public.

Certains contrôles, tels que la réautorisation annuelle des accès utilisateur, ne nécessitent que deux échantillonnages par an pour un programme donné si le processus associé n'est exécuté qu'une seule fois par an. Effectuer ce contrôle

Figure 2 : tableau croisé des contrôles de la publication spéciale 800653 du NIST par catégorie et famille			
Catégorie 1	**Famille de contrôles non couverte par les applications du DHS**	**Catégorie 2**	**Famille de contrôle couverte par les applications du DHS**
1	Planification	1	Intégrité du système et de l'information
2	Acquisition de systèmes et de services	2	Appréciation du risque
3	Autorisation d'évaluation de la sécurité	3	Réaction aux incidents
4	Gestion des programmes	4	Gestion des actifs
5	Sécurité individuelle	5	Audits et approbation
6	Sécurité physique et environnementale	6	Gestion de configuration
7	Plan de secours	7	Détection des programmes malveillants
8	Maintenance	8	Accès aux identités
9	Protection des supports		
10	Sensibilisation et formation		
11	Identification et authentification		
12	Audits et approbation		
13	Protection du système et des communications		

chaque minute, jour ou semaine entraînerait un gaspillage de ressources, de puissance de calcul et de stockage. L'éventail des fréquences va d'un contrôle annuel à un contrôle bisannuel. Les organisations ont intérêt à rédiger une feuille de route ou un calendrier standard, pour gagner du temps et de l'énergie. Cela facilitera également l'adhésion de la communauté des utilisateurs. Si ces derniers doivent effectuer des contrôles plus fréquemment que nécessaire, le concept de surveillance continue dans son ensemble pourrait devenir impopulaire au sein de l'organisation.

CONCLUSION

La SCSI joue un rôle positif majeur dans l'amélioration de la gestion des risques et de la conformité dans un grand nombre de secteurs et d'institutions, y compris pour l'administration fédérale des États-Unis, le Département de la Défense et diverses organisations commerciales et financières. Les technologies actuelles contribuent largement à l'amélioration de la sécurité, mais elles ne résolvent pas tous les problèmes, car les solutions proposées à ce jour comportent tout de même quelques failles manifestes. Il serait donc judicieux d'orienter les futures recherches vers des solutions qui comblent ces vides en matière de contrôle, par exemple avec un mécanisme de journalisation physique permettant d'intégrer et d'agréger les activités manuelles associées à un processus dans un système automatisé. En mettant en place de bonnes pratiques de fréquence d'échantillonnage, il est possible de dégager du temps pour la journalisation manuelle. Enfin, il serait souhaitable de modifier le modèle en connectant la solution de surveillance continue à un tableau de bord unique permettant de gérer le risque global. De cette manière, les organisations seraient en mesure d'identifier les domaines qui sont surveillés en continu et ceux qui nécessitent encore un suivi traditionnel. La SCSI est certes grandement prometteuse, mais il reste de nombreux défis à relever pour implémenter ce concept de façon exhaustive. La seule façon de surmonter ces difficultés consiste à mettre en œuvre la SCSI et à partager les leçons tirées de cette expérience avec la communauté des experts en cybersécurité.

NOTES DE BAS DE PAGE

[1] NIST, Publication spéciale 800-53, « *Security and Privacy Controls for Federal Information Systems and Organizations* », États-Unis, 2013, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

[2] C. Bennett : « *With $6 Billion Continuous Monitoring Contract, DHS Takes 'Next Leap' in Cybersecurity* », Fedscoop, 2013, *http://fedscoop.com/with-6-billion-continuous-monitoring-contract-dhs-takes-next-leap-in-cybersecurity/*

[3] J. D. Zients : « *Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management* », OMB, 2012, *www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-20.pdf*

[4] NIST, Publication spéciale 800-137, « *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* », États-Unis, 2011, p. 3, *http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf*

[5] NIST, Publication spéciale 800-37, « *Guide for Applying the Risk Management Framework to Federal Information Systems* », États-Unis, 2010, *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf*

[6] M. Chumer, R. Hiltz, R. Klashner, M. Turoff : « *Assuring Homeland Security: Continuous Monitoring, Control & Assurance of Emergency Preparedness* », *Journal of Information Technology Theory and Application*, 2004, vol. 6(3), p. 1-24, *http://search.proquest.com.library.capella.edu/docview/200008540?accountid=27965*

[7] *Op. cit.*, NIST 2010

[8] S. Schlarman : « *Selecting an IT Control Framework »," Information Systems Security*, 2007, 16(3), p. 147-151

[9] *Op. cit.*, NIST 2010

[10] *Op. cit.*, NIST 2013

[11] *Op. cit.*, NIST 2011

[12] DHS, « *Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS) », Federal Network Security Branch*, 2010, *https://www.dhs.gov/continuous-asset-evaluation-situational-awareness-and-risk-scoring-reference-architecture-report*

[13] *Op. cit.*, Zients, p. 11

[14] DHS, « *BPA Awardees and Tool Suites »," Federal Times*, 2013, *http://apps.federaltimes.com/projects/files/bpa_awardees.pdf*

[15] *Op. cit.*, NIST 2011