LES DOSSIERS TECHNIQUES

Gestion des vulnérabilités informatiques

Vers une meilleure gestion des risques opérationnels – TOME 2

Janvier 2016

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tél. : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

Table des matières

Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Vincent	**MAURY**	*DenyAll*

Les contributeurs :

Christophe	**CHAUBARD WILLM**	*Sogeti HT*
François	**GRATIOLET**	*Qualys*
Eric	**PERRAUDEAU**	*Qualys*
Julien	**ROYERE**	*BearingPoint*
Nicolas	**VIRY**	*Apria R.S.A.*

Les membres actifs du groupe de travail :

Abdellaziz	**TALEB**	*Modis*
Fabien	**TANGUY**	*Qualys*
Arnaud	**TARRAGO**	*EDF*

Le **CLUSIF** remercie également les adhérents ayant participé à la relecture.

I. Introduction

I.1. Objectif du document

Ce document fait suite au dossier technique « Gestion des vulnérabilités informatiques : vers une meilleure gestion des risques opérationnels » publié en Mai 2014 et disponible gratuitement sur le site du CLUSIF[1].

Si le premier tome visait à fournir aux RSSI des éléments d'accompagnement et de sensibilisation à la gestion des vulnérabilités auprès de leur Direction, l'objectif de ce second tome est de permettre aux RSSI/DSI/Risk Managers de formaliser leur programme de gestion des vulnérabilités, de piloter sa mise en œuvre et de mesurer l'efficacité d'un tel programme.

I.2. A qui s'adresse ce document ?

Ce document s'adresse à tout organisme, quels que soient sa taille, son secteur ou son statut (public, privé).

Il vise en particulier les OIV (Opérateur d'Importance Vitale) qui sont soumis à des exigences règlementaires spécifiques (LPM par exemple) et à une évaluation des risques qui doit prendre en compte leur contexte spécifique.

Il s'adresse aussi au Secteur Public (Ministères, Directions décentralisées, Collectivités Territoriales…), dont les exigences règlementaires spécifiques (RGS) imposent la mise en œuvre d'une gestion des vulnérabilités informatiques.

I.3. Description du sujet

La gestion des risques liés au système d'information fait partie intégrante des objectifs de tout organisme. Ceci se justifie d'autant plus si ce dernier est soumis à des lois ou des règlementations sectorielles, typiquement PCI DSS, HDS, ou la loi Mer[2]. En pratique, cette gestion peut dépendre d'une direction qui a la charge de la gestion des risques en général, d'une direction sécurité, d'une direction informatique ou des directions Projets.

Il serait illusoire de penser que le SI (Système d'Information) d'un organisme ne sera jamais la cible d'attaques informatiques. Les conséquences d'un incident de sécurité peuvent largement dépasser le simple coût de la réinstallation du système corrompu. L'identification des systèmes corrompus à elle seule aura un coût non négligeable.

[1] https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2014-Gestion-vulnerabilites-tome-1.pdf

[2] https://fr.wikipedia.org/wiki/Loi_de_sécurité_financière

Les attaques peuvent engendrer ou avoir pour but l'interruption du service, le vol ou la modification non autorisée de données potentiellement confidentielles. Les impacts des risques généralement évalués sont les suivants (sans ordre d'importance particulier) :

- humain : en cas de perturbation de service dans les SI industriels (SII) ou biomédicaux ;
- image : perte de réputation et mauvaise presse suite à incident de sécurité ;
- financier : indisponibilité de service commerçant et coûts élevés d'inventaire des systèmes corrompus et de remise en état, fraude usant des numéros de cartes bancaires volées, accès à des informations sensibles (dont données personnelles engageant la responsabilité de l'organisme), usurpation d'identité, etc. ;
- business : perte de chiffre d'affaires, les clients pouvant être tentés de changer de prestataire ou de renégocier les contrats suite à une perte d'image ;
- patrimoine intellectuel : pertes de connaissances, vol de savoir-faire ou de capacités innovantes ;
- légal : engagement de la responsabilité civile et pénale du directeur de l'organisme et/ou du responsable des traitements, s'il n'a pas pris les mesures techniques et d'organisation appropriées pour protéger son système d'information contre des risques internes ou externes.

Lorsqu'elle est conduite efficacement, la gestion des vulnérabilités permet de réduire le nombre et l'impact des incidents de sécurité, donc leur coût :

- « 99,9% des vulnérabilités exploitées ont été compromises plus d'un an après que leur référence CVE associée fut publiée. »
  Source : Verizon Data Breach Investigations Report, 2015
- « Il convient d'être informé en temps voulu des vulnérabilités techniques… pour traiter le risque associé. »
  Source : ISO/CEI 27002:2013 - Technical Vulnerability Management (A.12.6)
- « Les incidents de sécurité coûtent cher aux entreprises. »
  Source : ITR Manager[3], 2015

I.4. Contexte

L'ouverture et l'interconnexion généralisées des réseaux informatiques permettent de partager facilement les informations internes et entre les clients, fournisseurs et partenaires. Si ces avancées technologiques offrent des gains significatifs d'efficacité et de productivité pour les métiers, ces derniers doivent également considérer les nouveaux risques qu'ils encourent. C'est à l'entité en charge de la gestion des risques que revient le devoir de les avertir et de leur proposer les mesures permettant de les limiter raisonnablement et de leur faire accepter les

[3] http://www.itrmanager.com/articles/158450/incidents-securite-coutent-cher-entreprises.html

risques résiduels (risque subsistant après le traitement du risque)[4&5], tout en les informant et les sensibilisant sur leur responsabilité.

Les menaces actuelles (dénis de service, vers, virus, ou autres outils d'intrusion et de rançonnage) et leurs concepteurs ont su s'adapter à leur environnement pour mener des attaques de plus en plus sophistiquées, efficaces et rapides. Mesurer et gérer les risques informatiques représentent donc de vrais défis pour les services informatiques.

Les mécanismes de défense (pare-feux, anti-virus, contrôle d'accès, détection d'intrusion, etc) sont des éléments nécessaires pour la sécurité mais ne permettent pas de garantir que toutes les vulnérabilités du système d'information sont ou seront détectées et par conséquent traitées. En effet, les attaques actuelles ciblent directement les faiblesses des applications ou des systèmes et peuvent passer outre les couches de protections « classiques ».

De nos jours, la qualité et l'efficacité de la sécurité en place dans l'organisme est mesurable par la rapidité de mise en œuvre de mesures correctives ou palliatives.

Enfin, le contexte juridique relatif aux données personnelles évolue vers l'obligation de déclaration des sinistres informatiques - tel que c'est déjà le cas pour les OIV avec la LPM - et l'application de pénalités si aucune gestion proactive de la sécurité n'était en place.

La gestion des vulnérabilités permet de limiter l'exploitation de failles de sécurité. C'est en cela une activité critique pour le système d'information.

I.5. Définitions et périmètre

Ce document adresse les vulnérabilités informatiques d'un système d'information.

Préambule : veuillez vous référer au chapitre III du tome 1[6] pour avoir la définition d'une vulnérabilité informatique et la description de son cycle de vie.

Afin de bien délimiter le contexte, on distinguera trois grands types de vulnérabilités informatiques :

- Les vulnérabilités matérielles ou logicielles qui nécessitent l'installation d'un correctif ou d'un contournement (en attendant le correctif par exemple).
  Note : Certaines vulnérabilités requièrent un traitement particulier : les « zero day » littéralement « 0 jour », ce qui signifie qu'elles viennent d'être découvertes et n'ont potentiellement pas encore de correctif.
- Les vulnérabilités applicatives qui nécessitent une correction dans le code source de l'application.

[4] ISO/CEI 73: http://www.iso.org/iso/fr/catalogue_detail?csnumber=44651

[5] https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-Gestion-des-risques-2008.pdf

[6] https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2014-Gestion-vulnerabilites-tome-1.pdf

- Les erreurs de configuration qui nécessitent la modification de paramètres, comme les services inutiles qui nécessitent la suppression ou la désactivation de composants inutiles ou obsolètes.

Les vulnérabilités issues par exemple de défauts d'organisation ou de compétence ne sont pas prises en compte dans ce document. Les erreurs de conception ne sont pas non plus abordées dans ce document, malgré leur importance toute particulière dans le cadre des SII.

En termes d'impact sécuritaire, on considèrera généralement les trois critères DIC : Disponibilité, Intégrité et Confidentialité des données. L'exploitation d'une vulnérabilité peut avoir un impact sur un ou plusieurs de ces critères.

II. Cadre organisationnel

II.1. Objectifs et finalités de la gestion des vulnérabilités

La démarche devra clairement définir les finalités de la gestion des vulnérabilités, et particulièrement les objectifs à atteindre, comme par exemple :

- se conformer à la loi ou aux normes qualitatives du secteur ;
- couvrir un risque métier majeur ;
- suivre le budget d'assurance pour couvrir les risques liés à l'absence de correctifs (systèmes difficiles à mettre à jour) ;
- corriger une vulnérabilité dans les n jours suivants la fourniture du palliatif ;
- avoir un taux minimal moyen de vulnérabilités corrigées ;
- etc.

II.2. Alignement stratégie métier / stratégie SSI

Les équipes Métiers, porteurs *in fine* des données et des responsabilités afférentes, sont à même d'apprécier les risques induits par les vulnérabilités, ceux-ci influant sur le processus de gestion des vulnérabilités. Cette analyse de risque comprend la sévérité de la vulnérabilité, l'accessibilité, le service vulnérable, etc.

La stratégie de mise en œuvre d'actions palliatives aux vulnérabilités doit faire l'objet d'un compromis entre les équipes Métiers et la personne en charge de la sécurité. Elle doit considérer particulièrement les éléments suivants :

- planning : la mise en œuvre des correctifs devant prendre en compte les contraintes métier (ex : pas de correctif sur le système de paye en fin de mois) ;
- tests de non régression (TNR) : tests hors production, bilan puis mise en œuvre en production ;
- coût : action la plus adaptée par rapport à la valeur du service présentant la vulnérabilité ;
- le nombre d'actifs (*assets* en anglais) impactés ;
- le type de système impacté.

Les grands principes directeurs de gestion des correctifs doivent figurer dans la Politique de Sécurité (PSSI) qui doit être approuvée et soutenue par la Direction de l'organisme. Cette dernière pourra le cas échéant arbitrer entre les contraintes Métier et sécurité.

II.3. Périmètre fonctionnel et technique

Une des premières opérations va consister à déterminer le périmètre à couvrir, et les services offerts aux internes à l'organisme comme aux externes. Chaque service augmente le périmètre à couvrir et donc la surface d'attaque.

On distinguera par la suite l'informatique interne de l'externe et le fait que les services soient accessibles de l'intérieur et/ou de l'extérieur.

L'informatique évoluant en permanence, le périmètre va lui aussi évoluer ; la surface d'attaque doit donc être constamment réévaluée. Il est donc primordial de disposer d'inventaires à jour qui devront inclure la notion de criticité des équipements. Les données de ces inventaires pourront être croisées avec les données relatives aux vulnérabilités.

Informatique interne et externe

Toute ou partie de l'informatique peut être externalisé, il s'agit notamment de services fournis en mode Infrastructure as a Service (IaaS), Platform as a Service (Paas), Software as a Service (SaaS), … Certes les prestataires sont capables de fournir des garanties sur leurs gestion de leurs services cependant, cela n'empêche pas l'organisme de réaliser des contrôles sur l'activité pour s'assurer que la gestion des vulnérabilités est réalisée de manière appropriée par ses prestataires.

Si vous hébergez des données dans un centre de données (Datacenter) qui est certifié ISAE 3404 vous pouvez, voire devez, vous y rendre périodiquement pour vérifier que le service est rendu tel que contractuellement établi. De même, si vous déléguez à un tiers la gestion d'un service, par exemple l'externalisation des feuilles de paye vous pouvez, voire devez, réaliser périodiquement des audits de sécurité.

➔ Veillez bien à ce que des clauses d'audits figurent systématiquement dans les contrats.

Service rendu ou visible aux internes et aux externes

Rendre un service en interne de l'organisme l'expose à des attaques potentielles provenant de l'organisme lui-même. Identifier la raison d'un acte malveillant, volontaire ou non (ex : virus, poste non protégé) sera certainement assez facile à détecter et le « coupable » pourra être assez facilement identifié.

Lorsque le service est rendu à l'extérieur de l'organisme, si détecter un acte malveillant pourra s'avérer assez facile, identifier le « coupable » et faire cesser son action va s'avérer plus ardu. L'impact d'une attaque pourra avoir une influence directe sur l'image de l'organisme.

Du fait de l'exposition du service rendu, qui sur Internet est maximale, il conviendra d'être potentiellement plus réactif quant au plan de gestion des correctifs. Des campagnes de tests régulières doivent être organisées sur l'ensemble des services visibles de l'extérieur.

N'oublions pas que certains services externes se reposent sur des services internes pour pouvoir rendre le service. Le travail de classification des services (plus ou moins critique) devra considérer toute la chaîne pour déterminer les maillons faibles en cas de vulnérabilité exploitée.

Gestion des vulnérabilités : interne ou externe ?

La réponse à cette question est probablement : les deux. Vous pouvez bien évidemment faire gérer les vulnérabilités par une entité externe, mais vous resterez tout de même responsable (Accountable au sens RACI[7]) de cette gestion.

Si vous êtes propriétaire des actifs pouvant être impactés par une vulnérabilité, les constructeurs ou éditeurs de ces actifs vous proposent généralement un abonnement à une lettre d'information pour vous informer des vulnérabilités et de la disponibilité des actions palliatives ou des correctifs. Dans le cas contraire, cette information est généralement disponible sur Internet mais vous demandera d'aller la chercher sur les sites des constructeur/éditeurs.

Vous pouvez également consulter les nombreux sites publics qui tracent les vulnérabilités[8].

En dernier lieu, certains prestataires proposent un service d'abonnement à une lettre d'information soit généraliste (avertissement de toutes les vulnérabilités existantes), soit spécialisée (avertissement des vulnérabilités qui vous concernent) qui permettent d'être informé et donc de réagir au plus vite.

Dans le cas de services rendus à l'extérieur de l'organisme, plusieurs solutions s'offrent à vous :

1. vérifier l'engagement contractuel de maintenance avec vos fournisseurs ;
2. faire réaliser un audit par vos équipes internes ;
3. faire appel à un prestataire qui réalise un audit ponctuel (à considérer si vos audits ne sont réalisés que par vos équipes internes) ;
4. souscrire à un abonnement (SaaS) chez un prestataire qui réalise régulièrement des audits.

Note 1 : certains prestataires proposent des solutions à base de logiciel ou matériel laissé en interne piloté depuis un site externe pour réaliser en interne le même type d'audit que le point 3) ci-dessus.

Note 2 : dans la solution 1) ci-dessus, il faudra éviter d'être juge et partie, les équipes réalisant l'audit ne devraient pas faire partie de la DSI / Informatique. Le responsable sécurité est responsable de la gestion du risque, ce qui n'est idéalement pas la fonction première de la DSI.

[7] RACI : http://fr.wikipedia.org/wiki/RACI

[8] http://www.cvedetails.com/ ; https://nvd.nist.gov/

II.4. Financement : budgets d'investissement et d'exploitation

La gestion des vulnérabilités doit être réalisée en plusieurs phases, partant d'une découverte de vulnérabilité jusqu'à la mise en œuvre du correctif. Cette activité nécessite un budget, qui peut apparaître comme un centre de coût, mais vise surtout à couvrir un risque qui peut coûter bien plus cher qu'assumer le coût d'exploitation d'une vulnérabilité.

Ce budget peut être divisé en deux budgets distincts :

- Un budget d'investissement qui doit couvrir les besoins aussi bien matériels, logiciels ou en service (mode SaaS). Il faudra également considérer les abonnements aux services de veille.
- Un budget d'exploitation lié aux tâches récurrentes en personnel chargé de piloter les matériels, logiciels, SaaS, suivre et mettre en œuvre les recommandations. Selon l'organisme choisi, le contrôle de l'application des correctifs (audit interne et/ou externe) seront également à considérer.

II.5. Acteurs

Rôles et responsabilités

Deux équipes sont en charge du traitement des vulnérabilités : les équipes gestionnaires des actifs et les équipes sécurité. Ceci permet de respecter les principes de séparation des tâches et d'éviter d'être juge et partie. En outre, de nombreuses autres équipes devront être impliquées activement dans le processus, telles que les équipes d'exploitation et les équipes projet typiquement.

Les points suivants sont à considérer afin de permettre une gestion efficace du traitement des vulnérabilités :

- Les équipes gestionnaires d'un actif sont en charge :
    - du suivi des vulnérabilités. Elles sont donc abonnées aux lettres d'information des éditeurs/constructeurs et veille.
    - de l'information de l'équipe sécurité sur le plan de traitement. Les équipes peuvent donc décider de retarder ou ne pas appliquer certains correctifs (contraintes Métier), proposer d'éventuels contournements, produire le plan de déploiement des correctifs retenus.

- Les équipes sécurité sont en charge :
    - Appuyer et soutenir les demandes de mise en œuvre des correctifs auprès du Métier.
    - Faire porter, si nécessaire, le risque sur le Métier qui pourra éventuellement souscrire à une assurance pour couvrir son risque.
    - Produire une analyse critique des correctifs non retenus ou repoussés. Être éventuellement force de proposition.

- Contrôler la bonne mise en œuvre des mesures retenues.
- Eventuellement organiser les discussions Métier et gestionnaire d'actif.

Il est fortement conseillé d'établir un RACI avec des tâches différentes par type d'actif (sensibilité, exposition, …).

Lors de l'établissement du RACI, on veillera donc à ce que ces deux activités y figurent et qu'elles soient exercées par des entités différentes. Ces RACIs pourront ensuite être déclinés en processus.

II.6. Facteurs de mauvaise gestion

Les principaux indicateurs d'une mauvaise gestion des vulnérabilités sont :

- un nombre d'incidents de sécurité trop haut ou trop bas sur une période p par rapport à une période p-1, p-2… p-n,
- l'incapacité d'identifier les vulnérabilités de manière systématique,
- l'incapacité d'évaluer le risque lié aux vulnérabilités,
- l'incapacité de donner des priorités aux tâches correctives,
- laisser des ressources vulnérables sous exposition,
- un manque de relations entre la DSI, le Métier et les équipes sécurité menant à l'incapacité de contrôler et d'effectuer des changements sur les ressources informatiques,
- l'absence d'inventaire (équipements et flux) et criticité des actifs,
- l'absence de classification « sécurité » des incidents,
- l'absence d'un système de gestion du changement s'intégrant avec les processus de gestion des vulnérabilités.

III. Stratégie et gouvernance

Quel que soit le modèle de gestion des vulnérabilités retenu dans votre organisme, la responsabilité de mise en œuvre des mesures incombe à la Direction Générale (ou une autre si elle a délégué la responsabilité). Elle devra s'assurer que le modèle et les responsabilités assignées permettent de rendre un service efficace qui respecte le principe de PDCA (*Plan Do Check Act* ou roue de Deming).

La stratégie et la gouvernance de gestion des vulnérabilités reprennent ce principe. Ainsi, quelle que soit l'organisation retenue pour traiter les vulnérabilités, le modèle global reste le même, à adapter dans ses détails.

III.1. Positionnement dans la gestion IT

Que ce soit au niveau du département ou de l'activité, la gestion des vulnérabilités s'inscrit dans les processus de l'organisme.

III.1.1. Dans le département SSI

La gestion des vulnérabilités est l'un des sujets principaux pour maintenir les actifs en conditions opérationnelles. Le rôle essentiel de la SSI, dans ce cas, est l'identification de vulnérabilités et la vérification de leur remédiation par les équipes opérationnelles. Plusieurs activités de la SSI sont liées à la gestion des vulnérabilités et peuvent être utilisées pour identifier et valider une vulnérabilité. Ces activités doivent être mises en place le plus en amont d'un nouveau projet, avant toute mise en production.

Activités	Détail
La veille sécurité	La veille sécurité permet de s'informer sur les évolutions des normes et protocoles, mais aussi sur les nouvelles vulnérabilités qui ne pourront éventuellement être détectées par des outils automatiques. De plus, les sondes de détection/prévention d'intrusion doivent être régulièrement maintenues à niveau, en fonction des nouvelles attaques développées.
Les audits de conformité	Permettent de vérifier en détail une architecture, et s'assurer que les règles et préconisations pour durcir la sécurité ont bien été suivies.

	Note : Un regard critique du résultat de l'audit sera nécessaire pour vérifier sa pertinence.
Scan et détection de gestion d'incidents informatiques	Les scanners de vulnérabilités et les sondes de détection d'intrusion alertent sur l'exposition des actifs et les failles utilisées. Ils peuvent détecter voire bloquer les tentatives d'intrusion. Les outils de supervision et d'analyse de logs (comme les SIEM) permettent d'analyser et découvrir des événements non identifiés et des intrusions. *Note 1 : Tout comme un antivirus, ces outils demandent d'être actualisés régulièrement.* *Note 2 : Les Systèmes Informatiques Industriels (SII) pouvant avoir des actifs très sensibles, ils pourront être exclus des scans automatiques et requerront un scan manuel ou passif.*
L'exploitation de vulnérabilités	L'exploitation de vulnérabilités valide le risque si une vulnérabilité est exploitable. Exploiter une vulnérabilité peut être très agressif pour un actif. *Note : Ces tests doivent être planifiés avec les équipes métier.*
Les tests d'intrusion	Soulignent une chaîne de points faibles à renforcer, ou une faille dans l'architecture que seuls des experts pourront identifier. *Note : Mener un test d'intrusion avant la mise en place de tout nouveau service ou d'un changement important est généralement une bonne contre-mesure.*

III.1.2. Dans l'IT opérationnelle

La gestion des vulnérabilités s'inscrit dans un programme global initié idéalement par la PSSI (le « Plan » du PDCA). Rappelons que la PSSI matérialise l'engagement de la Direction Générale vis-à-vis de la Sécurité. La norme internationale ISO 27001:2013 exige une politique de gestion des vulnérabilités.

La SSI est propriétaire de la politique de gestion des vulnérabilités qui doit être alignée avec les processus opérationnels de gestion des changements (dont correctifs de sécurité) :

Sujet	Détail

Inventaire des actifs	Un actif est un bien de l'organisme pouvant être un logiciel, un matériel, un système, un sous-système, un flux ou une fonction (liste non exhaustive). L'inventaire peut venir de plusieurs voies : • constitution manuelle d'inventaire ; • constitution automatique d'inventaire (sur demande ou périodique) ; • base des actifs gérés par les opérationnels ; • déclaration auprès de l'équipe SSI. Tout actif doit avoir un propriétaire qui est responsable de la remédiation des vulnérabilités. Il peut en déléguer la gestion à un tiers, la DSI par exemple, qui doit lui rendre des comptes sur ses actions et l'avertir des risques courus par l'actif. *Note : Dans les Systèmes Informatique Industriels (SII), le scan des actifs n'est parfois pas possible car cela peut impacter la production.*
Profils d'actifs	Le type d'analyse est fonction du type d'actif. Afin de simplifier la gestion, on regroupera les actifs par type ou profils : • Quels actifs sont concernés et leur sensibilité (par rapport aux données traitées ou au service rendu) ? • A quelle fréquence sont-ils scannés/audités ? • Quel niveau de scan/vérification : intrusion, agressif, superficiel, etc. ? *Note : Pour des raisons de coût et de ressources, on pratiquera généralement moins de tests d'intrusion sur des systèmes de tests s'ils sont isolés des systèmes de production).*
Résultats de scans / d'audit	Ils sont à communiquer de manière sécurisée : • au propriétaire de l'actif ; • à l'équipe risque. Il est important de protéger l'accès à ces informations sensibles.
Remédiation	Le processus de remédiation doit être formalisé par écrit en accord avec les équipes métiers et doit comporter la durée maximale de résolution d'une vulnérabilité en fonction : • du profil de l'actif ; • du type de vulnérabilité.

	L'escalade en cas de non-remédiation possible par les équipes opérationnelles doit aussi être documentée et mise en place afin de gérer le risque.

Il ne faut pas s'y tromper, la gestion des vulnérabilités constitue un processus à part entière. L'adhérence entre les besoins Métier et les besoins sécurité nécessite la rédaction de la politique de gestion des vulnérabilités validée par les deux parties, à laquelle la PSSI devra faire référence. Cette politique doit bien évidemment aussi faire le lien avec le processus de gestion d'incidents.

III.1.3. Dans l'audit interne

La gestion des vulnérabilités permet ici de valider que les modifications mises en place ont été suivies. La documentation des changements appliqués est obligatoire.

Point important	Détail
Liste des preuves	Etablir des rapports d'audits, résultats de scans, remontées d'information, politique de gestion des vulnérabilités, traces de communication entre équipes.
Recommandations de remédiations	Lister les recommandations de l'audit, et les classer par ordre de priorité, des points majeurs qui doivent être traités au plus vite aux points mineurs qui peuvent être traités comme de l'opérationnel. Ces recommandations sont à aligner avec la politique de sécurité et les lois en vigueur.
Suivi des recommandations de remédiations	Suivre le statut des actions à entreprendre suite aux recommandations, avec les informations sur leur mise en place (date, responsable).
Revue des changements	Vérifier que les processus opérationnels ont été correctement suivis pour la remédiation des vulnérabilités identifiées. Les situations exceptionnelles (telles que les vulnérabilités jugées critiques par les éditeurs, constructeurs…) doivent être suivies au moyen d'outils adaptés à la gestion du changement (tels qu'un outil de gestion de tickets). La rapidité de mise en place des changements dépend aussi de l'état du système (sous maintenance ou fin de vie).

Conformité	S'assurer que les changements nécessaires ont bien été réalisés, en respectant la politique de gestion des vulnérabilités.

III.1.4. Dans la gestion de projet

Gérée en amont, la sécurité au niveau du projet permet d'être totalement intégrée et en accord avec le métier. Cinq grands points sont à mettre en place :

Point important	Détail
Conformité	Le projet doit être conforme aux politiques de sécurité de l'organisme, et en cohésion avec les standards définis par les équipes opérationnelles.
Analyse de risque	Le produit cible du projet doit être analysé en terme de confidentialité, disponibilité, et intégrité face aux menaces qui peuvent peser sur lui.
Veille sécurité	Le circuit d'information et de veille doit être actualisé avec les nouveaux logiciels, produits ou services apportés par le projet.
Maintenance & gestion d'incidents	Processus mis en place par les opérationnels pour la maintenance et pour la gestion des incidents. Ceux-ci doivent inclure les informations utiles pour configurer/appliquer les correctifs sur les actifs présentant des vulnérabilités (sauvegarde préalable, comment récupérer les correctifs authentifiés par les éditeurs et les constructeurs, plages de maintenance, communication aux équipes, etc.).
Développement	Les bonnes pratiques de développement sécurisé doivent être adoptées face aux vulnérabilités les plus connues (top 10 OWASP par exemple), et effectuer un test d'intrusion avant mise en production

III.2. Stratégie de gestion des vulnérabilités

Ce processus doit être mis en place en accord avec les opérationnels, il est :

- Planifié : une fréquence d'identification est définie et respectée.
- Ordonné : les vulnérabilités les plus critiques sont traitées en premier, cela demande la mise en place d'une échelle des vulnérabilités (par exemple : Critique / Haute / Moyen / Faible).
- Adaptatif : capable de gérer et documenter les exceptions, de capitaliser.
- Progressif : fait tourner la roue de Deming et améliore le processus en continu.

III.2.1. Principes directeurs de mise en œuvre

Les principes directeurs de la mise en œuvre de cette stratégie sont essentiellement axés sur une gestion de changement accompagnée et suivie auprès des départements clés de l'organisme :

- adhérence avec les opérationnels ;
- approche raisonnée ;
- approche graduée : l'ensemble du périmètre exposé à l'externe, puis l'interne ;
- gestion et suivi par ticket ;
- amélioration continue (PDCA) ;
- communication.

III.2.2. Instances de gouvernance

La gestion des vulnérabilités est gouvernée par la fonction SSI dont l'organisme dépend, idéalement, de la direction des risques ou mieux : directement de la Direction Générale.

Rappel : les risques incombent in fine à la Direction Générale, et non aux propriétaires des actifs.

III.3. Evaluation et suivi

On préférera les indicateurs présentés sous forme de graphe qui permettent de mettre en évidence rapidement et clairement les avancées ou les dysfonctionnements, surtout chez les personnels moins habitués à la gestion des vulnérabilités tels que la Direction.

Indicateur	Détail (fréquence variable, par défaut à la semaine)
Nombre total de vulnérabilités critiques	Cumul de toutes les vulnérabilités critiques depuis [date]. La qualité d'une vulnérabilité est établie en fonction du produit et/ou du vendeur du produit, c'est au RSSI de déterminer le positionnement du niveau considéré comme « critique ».
Nombre de vulnérabilités critiques non résolues	Nombre de vulnérabilités critiques non résolues depuis [date - 1].
Nombre de vulnérabilités critiques résolues ou remédiées	Nombre de vulnérabilités critiques résolues ou remédiées depuis [date - 1].

Durée de remédiation attendue	Tirée de la politique de gestion des vulnérabilités.
Durée de remédiation effective moyenne	Tirée des tickets de gestion, pour vérifier la performance du processus.
Nombre d'actifs analysés	Nombre total d'actifs, afin de vérifier la variance du nombre total de vulnérabilités critiques.

III.4. Intégration avec les autres processus

III.4.1. Inventaire des actifs

Il est important de partir sur une liste aussi exhaustive que possible des actifs, par couplage avec :

- la gestion « End Of Life » - obsolescence,
- les bases de données internes – par exemple : CMDB ou Active Directory,
- les outils de gestion de parc,
- le monitoring ou scan d'équipement (comme nagios, nmap, scan par exemple, mais difficilement mis en place pour les SII sans impact).

Il s'agit de s'assurer que chaque actif a un propriétaire, quels que soient les événements (un propriétaire quitte l'organisme par exemple), et que ce propriétaire est responsable de la gestion des vulnérabilités qu'il pourra déléguer.

A noter que les « *rogue devices* », c'est-à-dire les équipements connectés de manière légale ou non, dont on ne peut trouver le propriétaire, doivent être identifiés et vérifiés. La remédiation en cas de vulnérabilités étant la plupart du temps un retrait des réseaux. Cela est aussi vrai pour les équipements ramenés par les employés (politique d'accès type « BYOD » ou « COPE »).

III.4.2. Gestion des changements

Lorsque des vulnérabilités sont à corriger, tel un correctif à appliquer ou « bug fix » dans le code, différents processus opérationnels peuvent être suivis et dépendent de votre organisme. Par exemple, si votre organisme s'appuie sur ITIL pour la gestion du changement, il faut se synchroniser avec le CAB (Change Advisory Board) ou avec les responsables de départements (études, production, intégration, etc.). Le CAB devra s'assurer qu'un modèle de changement est prévu pour les vulnérabilités urgentes (ie : changement urgent) et les correctifs purement sécurité n'ayant aucun impact sur le service rendu pour le Métier (changement standard).

III.4.3. Gestion des incidents

La gestion des vulnérabilités doit être intégrée dans la gestion d'incidents, plus précisément pour identifier une vulnérabilité potentielle, qui permet alors de lancer une évaluation de la situation.

Pour plus d'informations sur le sujet, les bonnes pratiques détaillées dans ITIL fournissent une approche générale sur la gestion des incidents. La norme ISO/CEI 27035[9] indique avec plus de précisions les 5 étapes de la gestion d'incidents de sécurité : la préparation, l'identification, l'évaluation, la réponse et les leçons à tirer.

III.4.4. Contrôle et audit

Le contrôle de la performance, du suivi de la politique et des processus documentés est important. Même si la fréquence des contrôles n'est pas quotidienne, ces derniers doivent être planifiés à dates régulières. Ceci doit faire partie intégrante de la PSSI.

La SSI doit gérer les preuves afin de montrer aux auditeurs les raisons de l'initiation d'un processus de changement dû à une vulnérabilité trouvée, et être capable de montrer que la SSI a fait le suivi jusqu'à la résolution et sa vérification.

III.4.5. Gestion de la conformité

Il est important d'inscrire la gestion des vulnérabilités dans la documentation PCI, SOX et toute autre règlementation en vigueur. La politique fait le lien entre les équipes afin que le processus de remédiation de vulnérabilité soit documenté, clair et suivi par toutes les équipes en charge.

[9] Voir l'analyse de la norme ISO 27035 publiée en Décembre 2014 par le CLUSIF.

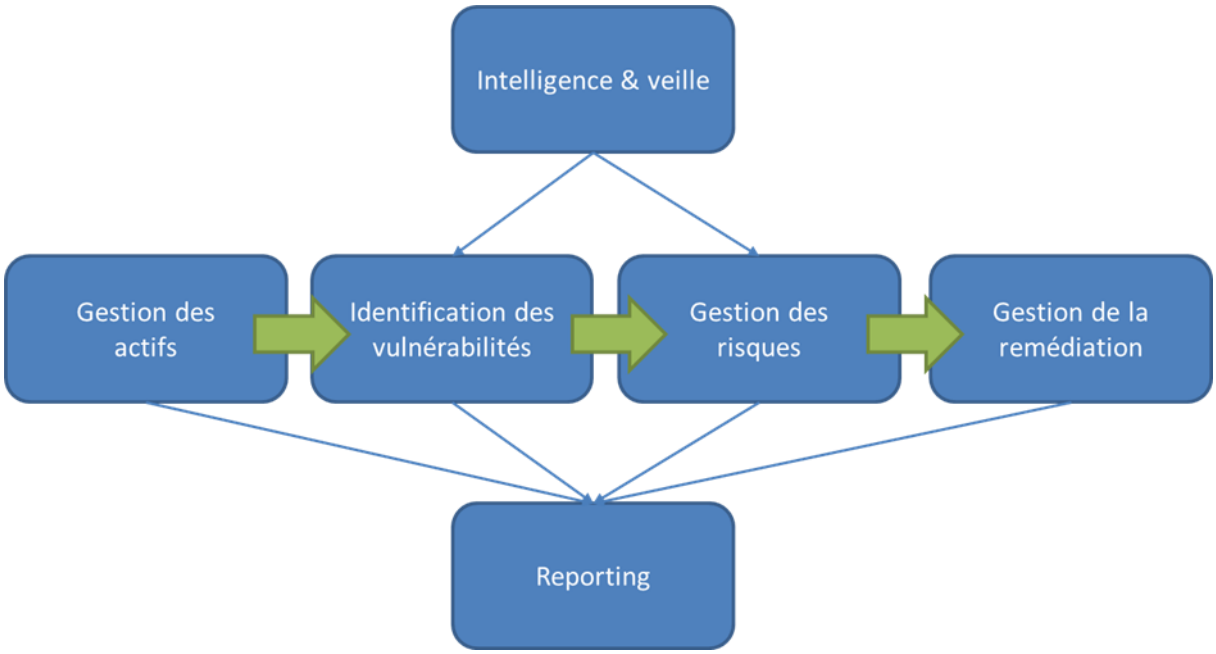
IV. Processus essentiels

Ce chapitre définit plus précisément les étapes et processus essentiels d'une démarche de gestion des vulnérabilités.

IV.1. Introduction

Chaque étape de la démarche est itérative (cyclique voire continue) et alimente les autres étapes. Ainsi, chaque nouvel actif découvert à l'inventaire est passé à l'analyse des vulnérabilités, de la même manière qu'une nouvelle vulnérabilité est ensuite traitée et intégrée au reporting.

L'illustration ci-dessous présente les principales étapes de la gestion des vulnérabilités :



L'intelligence (veille sécuritaire) permet d'alimenter l'identification des vulnérabilités et la gestion des risques. Le cœur de la gestion des vulnérabilités est représenté en 4 étapes (inventaire, identification des vulnérabilités, gestion des risques et de la remédiation). Enfin, toutes ces étapes alimentent le reporting.

Naturellement, la gestion d'actifs est le préambule à toute la stratégie. Ensuite, l'état des lieux (identification des vulnérabilités et des risques relatifs) permettra de constituer un premier niveau de rapport d'audit. Le traitement des risques, puis l'enrichissement de cette gestion par une intelligence et veille sécuritaire en seront la dernière étape de mise en œuvre.

Selon le degré de maturité des processus, l'effort pourra donc être porté sur tel ou tel processus en priorité.

IV.2. Intelligence et veille sécuritaire

Afin de prévenir les attaques ciblées et déclencher potentiellement des recherches exceptionnelles de vulnérabilités précises, les acteurs de la SSI doivent se tenir informés au quotidien des nouvelles vulnérabilités et les comprendre (compréhension globale des risques associés, ainsi que la compréhension propre au SI).

Cette activité de veille se trouve couramment incorporée à l'équipe SOC (*Security Operations Center*) dont la responsabilité couvre la supervision de la sécurité et la détection d'incidents.

Les sources d'information sont nombreuses :

- Les CERTs externes, comme celui de l'ANSSI[10].
- Les éditeurs (Microsoft, Oracle, Cisco, etc.) qui publient des bulletins d'information précisant les vulnérabilités identifiées sur leurs logiciels et les mises à jour à effectuer pour les corriger. Ils documentent également leur politique de support (obsolescence et fin de vie des produits).
- Les réseaux sociaux d'experts (blogs, fils Twitter, groupes LinkedIn, Clusif, etc.) sont autant de relais d'informations utiles.

Par ailleurs, de nombreuses formations existent pour se tenir à niveau sur la sécurité et maintenir ses compétences. La formation ne doit pas être limitée aux seuls initiateurs du processus et responsables SSI, mais doit être répercutée aux collaborateurs, sous forme de e-learning, campagnes de sensibilisation et autres initiatives ludiques et pédagogiques.

Enfin, les conférences – en France ou à l'étranger – sont autant d'occasions d'apprendre et d'échanger avec ses pairs, de se tenir informé des tendances et évolutions dans les menaces, parmi lesquelles nous pouvons citer les conférences du CLUSIF, le SSTIC et la JSSI.

IV.3. Gestion des actifs, Architecture et Déploiement

Le préambule à la gestion des vulnérabilités consiste à cartographier le SI en identifiant les actifs qui le composent et identifier leurs propriétaires. Cette cartographie combine un travail d'inventaire automatisable avec une qualification faisant intervenir les directions Métier.

IV.3.1. Urbanisation et cartographie

L'urbanisation est toujours l'occasion pour l'organisme d'aligner le SI sur sa stratégie. Et surtout, l'urbanisation met en exergues l'importance des actifs.

La cellule d'urbanisme se charge ainsi de maintenir une cartographie décrivant macroscopiquement la classification des actifs selon les métiers, les filiales, les zones réseaux,

[10] http://www.cert.ssi.gouv.fr/

etc. La cartographie fournit également les classifications et regroupements d'actifs (géographique, fonctionnel, technologique, etc.) ainsi que les chaînes de liaison entre actifs.

Cette cartographie s'inscrit au cœur du processus de gestion des vulnérabilités, tant en alimentant l'inventaire et la priorisation des actifs à tester, qu'en retour en s'enrichissant des vulnérabilités découvertes.

IV.3.2. Inventaire

L'inventaire du SI s'appuie sur cette cartographie généralement formalisée.

La découverte automatique repose sur cette cartographie et confronte la théorie avec la réalité des actifs existant dans le SI. Cette découverte vise une exhaustivité d'inventaire, incluant bien entendu les postes et serveurs de l'organisme, mais également les équipements bureautiques (imprimante, vidéoprojecteur, vidéo-conférence, etc.), équipements réseaux (routeur, pare-feu, sonde, etc.) et tout autre équipement connecté sur un réseau (badgeuse, borne de parking, vidéo-surveillance, etc.).

Attention : la découverte automatique utilise généralement une exploration active visant à lister l'exhaustivité des machines et services disponibles dans l'infrastructure. Cette approche, acceptable en SI de gestion, peut se révéler impossible en environnement industriel (SCADA). Dans ce type d'environnement sensible, une approche passive (basée sur l'écoute des flux réseau) sera une solution beaucoup plus longue mais non intrusive.

Afin de simplifier l'administration des équipements, les interfaces propriétaires sont souvent remplacées par un serveur web, comme c'est le cas pour toute imprimante récente qui intègre un serveur web permettant sa configuration à l'aide d'un simple navigateur. Ce serveur web peut avoir des failles (compte d'authentification trivial laissé par défaut, obsolescence du socle technologique, etc.) et permettre ainsi d'accéder à la configuration voire aux travaux d'impression traités par l'imprimante.

Note : certains équipements peuvent bloquer la découverte pour justement empêcher d'accéder à leurs services et donc potentiellement découvrir des failles et les exploiter. Ainsi, la découverte peut nécessiter de déployer des sondes de découverte dans d'autres réseaux comme le réseau d'administration, les DMZ, les réseaux de type SCADA, etc. De plus, certains services ne répondent que lorsqu'ils sont interrogés avec la bonne requête, comme c'est le cas par exemple du SNMP (UDP). Un simple *ping* ICMP peut donc se montrer insuffisant dans de nombreux cas et demande une détection adaptée.

Une fois l'inventaire des machines répondant sur le réseau effectué, l'identification des services fournis par chaque machine apporte un premier lot d'informations sur l'usage de la machine. Ainsi, la lecture des bannières de ces services ou les réponses fournies à certaines requêtes type ajoutent des informations sur les technologies sous-jacentes aux services. Par exemple, le type et la version du serveur web peuvent souvent être identifiés dans les réponses renvoyées. L'obtention d'une technologie et de sa version permet dans de nombreux cas (de technologies couramment utilisées) de déduire toutes les vulnérabilités auxquelles ce service est exposé.

Attention : les bannières ne doivent pas être prises comme une information fiable car elles peuvent masquées voire faussées par l'administrateur à des fins de protection.

L'inventaire des services de chaque équipement permet de lister toutes les instances de bases de données sur un même serveur, ou tous les sites Web hébergés par un même serveur Web. Cette information requiert généralement d'avoir un accès à un service particulier, voire au fichier de configuration local du service. La participation d'un administrateur de base de données à cette étape se révèle donc souvent indispensable.

IV.3.3. Qualification

Un premier enrichissement de cet inventaire consiste à décrire les interdépendances entre les actifs identifiés et les applications métier avec des outils de type CMDB (Configuration Management DataBase). Chaque actif (service applicatif Web, base de données, etc.) doit ainsi avoir son propriétaire, typiquement une fonction Métier en affectant toutes les machines et services inventoriés à des opérationnels, qu'il s'agisse d'actif servant une application métier ou du poste de travail d'un collaborateur de cette fonction Métier.

Note : La DSI portera généralement la responsabilité des actifs de type équipement réseau mutualisé ou applicatifs support IT par exemple, qui ne peuvent pas être affectés à une direction Métier en particulier.

Les actifs portent un risque intrinsèque dépendant de leur usage, qui peut donc être déterminé par leur propriétaire. Ce risque est décrit plus en détail au chapitre IV.5.1.

Enfin, la prise en compte des alertes du processus de veille décrit ci-dessus peut enrichir l'inventaire et apporter une criticité supplémentaire aux actifs ciblés par ces alertes.

IV.3.4. Industrialisation du changement

Naturellement, les actifs mais aussi et surtout leur environnement évoluent sans cesse, les services se créent régulièrement et rarement se suppriment. Le processus d'inventaire et de qualification décrit précédemment nécessite donc une industrialisation s'inscrivant dans la gestion du changement et des configurations (voir les notions d'ITAM, IT *Asset Management*, et d'ITSM, *IT Service Management*).

IV.4. Identification des vulnérabilités

L'objectif est ici d'identifier les vulnérabilités informatiques sur les actifs précédemment cartographiés.

Note : la cartographie du SI peut déjà présenter des failles d'ordre architectural que nous ne détaillerons pas ici.

IV.4.1. Que tester ?

Naturellement, l'identification exhaustive et continue des vulnérabilités dans le contexte d'un SI de taille importante est un travail permanent et primordial. Afin de ne pas être submergé par l'ampleur de la tâche, il convient d'assigner des priorités aux actifs en fonction de leur aspect critique pour les métiers en privilégiant :

- le cœur de réseau avant ses éléments périphériques ;
- les serveurs avant les postes de travail ;
- les applications Métier avant les applications support ;
- les environnements de production et pré-production voire PCA/PRA avant leurs instances de test ou de développement ;
- plus généralement, les éléments les plus menacés avant les éléments les moins menacés.

Note : il est vivement recommandé d'opter pour une standardisation des postes de travail créés à partir d'images uniques et de déploiements systématisés (GPL, outils de patch centralisés). Ainsi les tests par échantillonnage peuvent généralement suffire.

Les tests doivent également couvrir toutes les technologies présentes dans le SI, des couches réseaux jusqu'aux couches applicatives :

- les protocoles réseau type partage de fichiers (SMB, SFTP), accès distant (SSH, RDP), supervision (SNMP), mail (SMTP), etc.,
- les différents OS (Microsoft Windows, Unix, Linux, MacOS, zOS, etc.),
- les bases de données,
- les applicatifs, type sites web bien sûr, mais aussi services web et toute autre technologie utilisée pour supporter une application de l'organisme.

Attention : un actif peu critique peut servir de rebond à un pirate pour accéder à des actifs plus critiques, par le jeu des identifiants partagés par exemple. L'usage des chaînes de liaison décrites dans la cartographie (cf chapitre IV.3.1) prend ici tout son sens.

IV.4.2. Tests manuel ou automatique

La première distinction à apporter dans la méthode de test consiste à réaliser deux types d'audit complémentaires : automatiques et manuels. L'automatisation des tests (à l'aide de logiciels embarquant des bases de milliers de tests) permet une plus grande couverture fonctionnelle mais se trouve aussi très limitée dans l'analyse logique que seul un humain peut apporter, typiquement dans le cas des tests applicatifs.

L'audit manuel réalisé par un expert complètera donc l'approche systématique et automatique par une analyse logique, généralement ciblée, dont l'objectif pourra être de tester l'intrusion dans un système (*penetration testing* - ou *pentest* - en anglais) ou de relire le code d'une application pour en évaluer la qualité.

A un niveau applicatif plus particulièrement, l'objectif optimal consiste donc à obtenir plusieurs analyses complémentaires : la qualité du code applicatif par une revue de code éventuellement outillée (catégorie SAST, *Static Application Security Testing*) et la vue de l'application exécutée pouvant elle aussi être outillée (catégorie DAST, *Dynamic Application Security Testing*).

On voit donc ici l'intérêt de coupler les deux approches, manuelle pour une analyse plus fine et qualifiée, automatique pour une couverture fonctionnelle plus globale et régulière.

IV.4.3. Tests actifs ou passifs

Dans les environnements plus sensibles type SCADA et autres SII de production, l'analyse active de la sécurité est à proscrire, une requête mal interprétée pouvant impacter le service (la fonction).

Il convient alors de réaliser un audit exclusivement manuel et passif, c'est-à-dire sans rien émettre sur le réseau, en se plaçant en écoute uniquement.

Si les tests automatiques actifs sont bannis, l'approche logicielle consiste à déduire les vulnérabilités des équipements inventoriés et des flux transitant sur le réseau, en dédoublant tout le trafic du SII pour les analyser de manière totalement indépendante et passive.

IV.4.4. Tests en boîte noire ou boîte blanche

Dernière distinction à considérer : le niveau de connaissance sur les actifs testés. En effet, si le test à l'aveugle (dit en boîte noire) fournit le point de vue d'une personne malintentionnée étrangère à l'organisme qui cherche une faille sans avoir de compte utilisateur, de schéma de l'architecture réseau ou autre information utile, l'analyse se trouve limitée dans aux vulnérabilités découvrables à distance et manque donc de profondeur.

En conséquence, cette première analyse doit être enrichie par des tests en boîte blanche qui fourniront une vision complémentaire aux premiers, et dont les résultats seront plus riches.

Naturellement, cette approche en boîte blanche nécessite de fournir des comptes privilégiés au test (manuel ou automatique), comptes dont il faudra donc veiller à leur usage, stockage et effacement à l'issue des tests.

Note : un attaquant débute couramment son action par une tentative de récupération d'informations utiles comme le compte utilisateur d'une personne haut placée (disposant d'accès privilégiés), action dite de *social engineering*.

IV.4.5. Quand et à quelle fréquence ?

La fréquence devra s'ajuster à la criticité des actifs et du SI au sens large, certains actifs pouvant justifier des tests hebdomadaires tandis qu'un test annuel peut suffire sur d'autres. Par exemple, les serveurs au cœur du réseau (LDAP, serveurs sous-jacents aux applications critiques de l'entreprise, etc.) justifieront une revue très régulière de leur sécurité, tandis qu'un serveur de

développement sans donnée réelle (jeux de données factices) et sans grand impact en cas d'indisponibilité pourra être testé beaucoup moins régulièrement.

Un test applicatif peut ainsi être lancé systématiquement dans la phase de validation d'un changement, avant mise en production.

Enfin, en cas d'apparition d'une vulnérabilité majeure (selon la norme de notation des risques adoptée dans l'organisme, par exemple si la note CVSS est supérieure à 7) identifiée par le processus de veille, une analyse ponctuelle et spécifique à cette vulnérabilité pourra être lancée. Par exemple, la vulnérabilité heartbleed (openssl)[11] déclenche une analyse de tous les serveurs utilisant le protocole SSL (HTTPS…).

IV.5. Gestion des risques de sécurité

Une fois les vulnérabilités identifiées, leur qualification permettra de décider de leur traitement (action à effectuer). En effet, la quantité de vulnérabilités à traiter ne permet généralement pas de toutes les adresser de front, ni de viser une correction exhaustive à court terme, pour des raisons de délai de correction comme pour des raisons de coût.

L'évaluation des risques de sécurité suit une logique partagée entre les différents documents (ISO 27005:2011, CVSS, MEHARI, etc.) : le calcul du risque intrinsèque à chaque vulnérabilité est mis en regard du risque de l'actif sur lequel la vulnérabilité est identifiée, lui-même rapporté au risque global supporté par l'organisme.

IV.5.1. Risque intrinsèque

Le risque d'une vulnérabilité combine deux facteurs : l'impact potentiel de la vulnérabilité si elle venait à être exploitée, et la probabilité que cette faille soit exploitée (probabilité d'occurrence du risque).

L'impact potentiel peut reprendre simplement les trois dimensions basiques de la sécurité : disponibilité, intégrité et confidentialité. L'exploitation de la faille coupe-t-elle le service ? Combien de temps faudra-t-il pour rétablir le service ? La coupure va-t-elle impacter le niveau de service (SLA) ? L'exploitant pourrait-il modifier des données, altérer des informations ou accéder à des données confidentielles ? Cette réflexion d'impact doit bien sûr s'aligner avec le Métier qui *in fine* supportera les risques.

La probabilité d'occurrence repose essentiellement sur la simplicité d'exploitation de la faille et sa récurrence (expérience). Par exemple, si n'importe qui peut trouver sur Internet un script qui exploite la faille, qui plus est à distance et sans avoir d'information préalable, le risque d'exploitation de ladite faille augmente.

La conjugaison de ces deux éléments (par produit cartésien typiquement) donne donc le risque intrinsèque de la vulnérabilité, comme l'illustre l'exemple ci-dessous :

[11] https://fr.wikipedia.org/wiki/Heartbleed

	Probabilité d'occurrence				
Impact potentiel	1 (faible)	2 (modéré)	3 (moyen)	4 (élevé)	5 (critique)
1 (faible)	1	2	3	4	5
2 (modéré)	2	4	6	8	10
3 (moyen)	3	6	9	12	15
4 (élevé)	4	8	12	16	20
5 (critique)	5	10	15	20	25

Le risque intrinsèque résultant peut être classé en critique (note ≥ 20), élevé (note entre 10 et 20), moyen (note entre 5 et 10) et faible (inférieur à 5) par exemple.

IV.5.2. Risque environnemental et risque final

Où se trouve la vulnérabilité ? Selon l'importance de l'actif (identifiée à l'étape précédente du processus), une même vulnérabilité pourra avoir un risque (et donc une priorité de traitement) tout à fait différent.

De plus, les attaques étant motivées par une volonté politique (hacktivisme), un vol de secret industriel ou une volonté de nuire, les organismes portent dans leur globalité un risque variable d'un organisme à l'autre.

A nouveau, en prenant en compte l'environnement de la vulnérabilité et son risque intrinsèque, on arrive à un risque qui *in fine* doit être calculé séparément pour chaque vulnérabilité.

IV.5.3. Traitement

Une fois le risque de chaque vulnérabilité évalué, la décision de leur arbitrage et le choix des moyens de traitement aboutit au choix de corriger la vulnérabilité, de mitiger (c'est-à-dire atténuer) le risque ou simplement de l'accepter.

Corriger la vulnérabilité apparaît être le choix le plus naturel et trivial. Un système obsolète doit être mis à jour, un mot de passe trivial doit être changé, un code applicatif vulnérable doit être réécrit et remis en production. La remédiation (correction) des vulnérabilités est décrite plus largement dans la suite du document.

Cependant la correction d'une vulnérabilité peut se révéler être une entreprise complexe et coûteuse. Mettre à jour un système peut compromettre l'exécution des applications, voire

nécessiter une maintenance coûteuse ou impossible de par l'obsolescence des couches sous-jacentes, l'indisponibilité des auteurs de l'application, etc.

Deux options s'offrent alors : mitiger le risque ou l'accepter.

Mitiger le risque signifie ajouter un contrôle ou une autre protection permettant de diminuer le risque engendré par la faille, mais sans pour autant éliminer la faille. Par exemple, en ajoutant un niveau d'authentification, en relisant des journaux d'accès, en restreignant l'utilisation du service, en installant des équipements tiers type pare-feu empêchant l'exploitation de la faille. Le risque diminue, mais la faille réside toujours.

Enfin, l'acceptation du risque est parfois envisageable lorsque le coût de correction dépasse largement le risque engendré par la faille, et qu'il n'existe pas de solution simple pour le mitiger. A noter que certaines assurances proposent de couvrir ce risque.

La norme ISO 27005[12] formalise clairement les différents traitements du risque.

Note : là encore, dans les environnements industriels, la remédiation est rarement possible, soit parce que l'éditeur n'a pas fourni de correctif, soit parce que la mise à jour du composant requiert une interruption de service impossible en dehors d'une coupure annuelle pour maintenance. Dans ce cas, le traitement visera à surveiller la potentielle exploitation d'une vulnérabilité identifiée par le même procédé que la détection de la vulnérabilité elle-même : en écoutant passivement le trafic réseau.

IV.6. Gestion de la remédiation

Dans le choix de la correction d'une vulnérabilité, l'approche optimale vise à intégrer cette correction dans un processus maîtrisé de gestion du changement afin de ne pas renouveler des efforts répétitifs et redondants au fil des vulnérabilités à traiter.

IV.6.1. Systématisation des mises à jour (*patch management*)

La SSI et les exploitants doivent convenir d'une politique de mise à jour connue et explicite, consistant par exemple à installer hebdomadairement les mises à jour sur tous les postes et tous les serveurs de pré-production, puis mettre à jour les serveurs de production après deux semaines de test et de validation des correctifs apportés. Cette politique de mise à jour doit être inscrite dans la politique de sécurité. Si l'organisme dispose d'un CAB (*Change Advisory Board*, Comité d'approbation des changements en français), les mises à jour de sécurité peuvent être traitées dans le cadre d'un changement standard.

Dans le cadre des applications, l'implication des études dans la correction des vulnérabilités est indispensable et pourra s'accompagner d'une mise en place de revue de code, d'outillage logiciel (SAST) et autres audits ponctuels afin d'améliorer la sécurité applicative le plus en

[12] https://fr.wikipedia.org/wiki/ISO/CEI_27005

amont possible. Là encore, la gestion de la remédiation a un impact sur la politique de sécurité qui doit donc être mise à jour en conséquence.

IV.6.2. Processus standard de remédiation

La remédiation d'une vulnérabilité s'inscrit naturellement dans le processus standard de changement.

L'usage de tickets de remédiation - tel que préconisé par les bonnes pratiques ITIL - permet d'assigner les tâches de correction aux opérationnels (exploitants, développeurs, etc.). Ces tickets pourront ainsi faire l'objet d'un reporting dédié, voire d'un support d'escalade en cas de crise sur une vulnérabilité majeure à traiter de manière exceptionnelle, qu'il s'agisse d'alerte interne ou de communication vers les opérationnels – la gestion des actifs permettant de savoir à qui s'adresser. Le reporting est décrit plus en détail au chapitre suivant.

IV.6.3. Vérification et validation

Le processus de remédiation doit naturellement intégrer des tâches de contrôle du bon déploiement des remédiations. Le système de tickets de remédiation peut permettre de suivre ces validations en supportant des statuts différenciant la correction effectuée par l'opérationnel et la validation réalisée par la SSI, en s'assurant que la vulnérabilité remédiée ne réapparaît plus.

Idéalement, ce système de suivi est interfacé en retour avec le logiciel de gestion des vulnérabilités, déclenchant un nouvel audit de sécurité pour valider dans le système (automatiquement) que la correction a bien été appliquée.

IV.6.4. Mise à jour de la documentation SSI

Enfin, dernier aspect de la remédiation déjà cité préalablement : la mise à jour des documents SSI comme la politique de sécurité, les guides d'administration, etc. En effet, si certaines vulnérabilités remontées n'ont pas d'exigence déjà formalisée dans la politique de sécurité, celle-ci pourra être rafraichie à l'issue de chaque campagne de test.

Par exemple, si des comptes triviaux créés à l'installation d'une base de données sont toujours actifs (avec leur mot de passe originel), le guide d'administration des bases de données pourra être actualisé en précisant de verrouiller systématiquement les comptes créés par défaut dans une base de données et d'en changer les mots de passe, d'autant plus que la procédure peut être automatisée.

On peut ainsi distinguer à nouveau les efforts à court terme (correction des vulnérabilités ponctuelles) des changements dont l'effet sera visible à plus long terme.

V. Pilotage et reporting

V.1. Introduction

Le reporting vise à fournir des outils de communication entre les parties prenantes du processus de gestion des vulnérabilités :

- reporting managérial au sein de la SSI ;
- reporting technique et opérationnel aux métiers (exploitants, développeurs, etc.) ;
- reporting synthétique pour la Direction.

Le reporting ne doit pas être considéré comme la dernière étape du processus et doit être communiqué tout au long du processus, comme preuve de son efficacité. Il doit faire ressortir l'évolution de la sécurité, les durées de remédiation selon les risques, etc.

Le tableau de bord doit être lisible, visuel, clair et simple à comprendre. Il doit par conséquent regrouper un nombre limité d'indicateurs. Seuls les indicateurs pertinents doivent en faire partie au risque de perturber la compréhension de celui-ci.

Le tableau de bord doit comporter des objectifs quantifiables de sécurité afin d'avoir un ou plusieurs seuils permettant d'agir ou de mettre en place un plan d'action.

V.2. Tableau de bord et indicateurs de performance pour l'expression de besoins

Un reporting ou tableau de bord constitue un élément essentiel permettant de justifier les coûts, ainsi que d'illustrer la couverture des risques (évolution dans le temps de la baisse du nombre d'actifs vulnérables), en montrant par exemple le temps de réaction entre la découverte de vulnérabilité et l'action correctrice.

L'objectif de ce chapitre est de fournir un support et / ou une aide à l'élaboration et la mise en place de tableaux de bord concernant les vulnérabilités des systèmes d'information d'entreprises ou industriels.

V.3. Indicateurs

Ce chapitre propose un découpage en 3 domaines des indicateurs qu'il est possible de mettre en place. Ceci afin de garantir un suivi minimal d'alertes de vulnérabilité.

Note : La liste des indicateurs fournie ici n'est qu'informative et représente les indicateurs conseillés pouvant servir de base de travail Un indicateur est un élément

d'aide à la prise de décision, décision qui portera une mesure d'amélioration à mettre en place.

L'ensemble des indicateurs et des mesures associées constituent d'un tableau de bord de suivi.

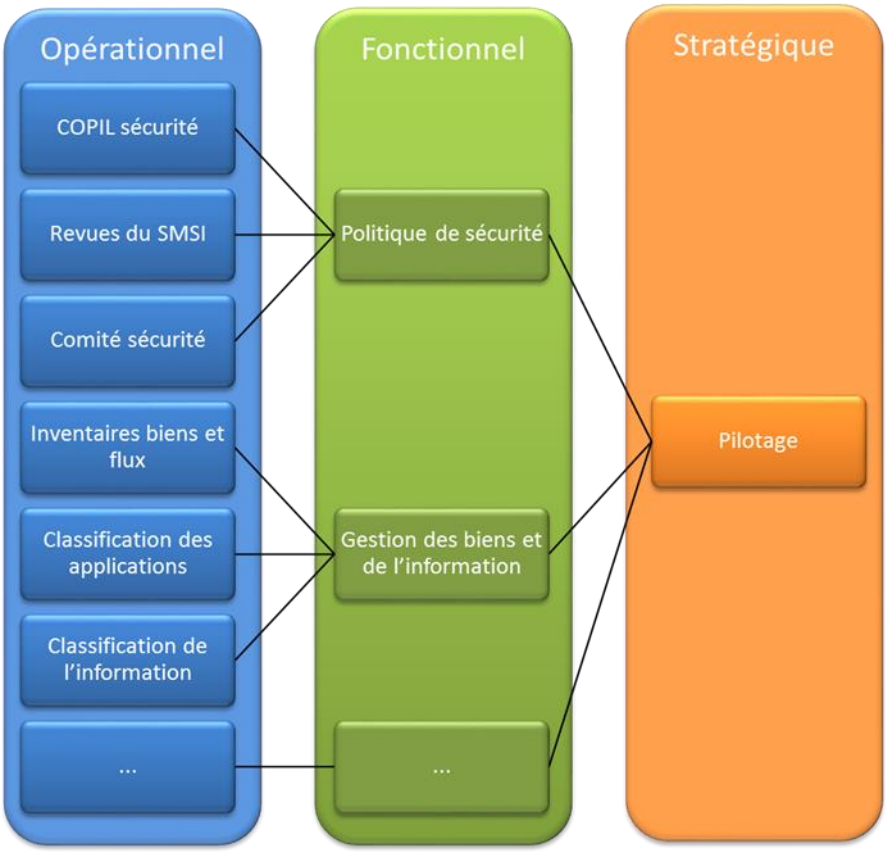
La gestion des indicateurs se fait à l'aide de 3 niveaux :

1. indicateurs de pilotage – de stratégie – pour une prise de décision, atteinte d'un objectif, pour le suivi et/ou la mise en place de la politique de sécurité ;
2. indicateurs de performance ou fonctionnels afin de piloter, suivre et de mesurer l'efficacité de la sécurité au travers de la PSSI, SMSI ;
3. indicateurs opérationnels pour le suivi de la mise en œuvre des mesures de sécurité.

La production et l'utilisation d'un indicateur dépendent de la maturité de l'organisme et du processus de gestion des vulnérabilités :

- faible : organisme sans responsabilité définie ni stratégie ou plan d'action en place ;
- médian : organisme où les responsabilités sont définies mais la gouvernance de la sécurité reste opérationnelle et non stratégique ;
- bien organisée : organisme dont le processus et sa mise en œuvre sont optimaux.

Comme évoqué ci-dessus, il est recommandé de faire un suivi dans le temps de ces indicateurs sous forme graphique.



Remontée des indicateurs - Exemple

V.3.1. Indicateur de pilotage

Voici une liste non exhaustive d'indicateurs de pilotage :

Libellé de l'indicateur	Mesure	Maturité ❶ faible ❷ médian ❸ bien organisé
Avancement du Plan d'actions cyber sécurité défini	Taux	3
Avancement de la sensibilisation à la cyber sécurité	Taux	2
Avancement du suivi de la gestion des actifs (SII, SIE, SIE/SII)[a]	Taux	1
Avancement du suivi de la gestion des inventaires des flux de communication (intra et inter SII, intra et inter SIE, entre SIE et SII)	Taux	2
Nombre d'incidents liés à la cyber sécurité SIE et SII	Nombre	3
Taux de contrats SI ayant une clause cyber sécurité	Taux	3

(nombre de contrats ayant une clause cyber sécurité / nombre de contrats SI géré par la DSI)		
Taux des évaluations cyber sécurité sur les biens numériques (actifs, logiciels, systèmes, sous-systèmes, applications) (nombre de biens ayant fait l'objet d'une étude ou évaluation cyber sécurité / nombre de biens SI gérés par la DSI)	Taux	3
Taux des comptes non utilisés depuis plus de 6 mois (sans justification). (nombre de comptes n'ayant fait l'objet d'aucune connexion au SI / nombre de comptes ayant accès au SI)	Taux	2

[a] SII Système d'Information Industriel ; SIE : Système d'Information d'Entreprise (ou de Gestion)

V.3.2. Indicateurs de performance

Voici une liste non exhaustive d'indicateurs de performance :

Libellé de l'indicateur	Mesure	Maturité ❶ faible ❷ médian ❸ bien organisé
Nombre d'incidents de cyber-sécurité sur la période donnée	Nombre	3
Taux de disponibilité du SIE (temps de fonctionnement / (temps de fonctionnement +temps de remise en fonctionnement)	Taux	2
Taux de disponibilité du SII (temps de fonctionnement / (temps de fonctionnement +temps de remise en fonctionnement))	Taux	1

Autres indicateurs performance à titre d'exemple :

- la politique de sécurité - Organisation de la sécurité de l'information,
- la gestion des biens,
- la sécurité liée aux ressources humaines,
- la sécurité physique et environnementale,
- la gestion des incidents liés à la sécurité de l'information,
- la conformité,
- la gestion Opérationnelle,
- le contrôle d'accès,
- la maintenance des SI,
- la conformité d'activité.

V.3.3. Indicateurs opérationnels

Voici une liste non exhaustive d'indicateurs opérationnels :

Libellé de l'indicateur	Mesure	Maturité ❶ faible ❷ médian ❸ bien organisé
Taux de mise en place des correctifs de vulnérabilités techniques pour un équipement (bien) défini (serveur, station de travail, système, sous-système, routeur,) (nombre de correctifs installés pour un bien ou un ensemble de biens / nombre de correctifs à installer pour un bien ou un ensemble de biens)	Taux	2
Taux de mise en place des correctifs de vulnérabilités techniques pour un système ou sous-système, ou OS, ou applications ou logiciel défini (nombre de correctifs installés pour un système ou pour le SI / nombre de correctifs à installer pour un système ou pour le SI)	Taux	2
Taux de tests de vulnérabilité passés sur les équipements ou biens (nombre de tests passés sur les biens SI / nombre de tests à passer sur les biens SI)	Taux	2
Taux de tests de vulnérabilité passés sur un logiciel ou application ou système ou sous-système (nombre de tests passés sur les systèmes du SI / nombre de tests à passer sur les systèmes du SI)	Taux	2
Taux de projets informatiques ayant fait l'objet de test de vulnérabilité	Taux	2
Taux de projets informatiques ayant fait l'objet d'un audit externe de vulnérabilité	Taux	3
Taux d'applications, dont l'authentification et les autorisations se basent sur l'annuaire d'entreprise	Taux	3

Autres indicateurs opérationnels à titre d'exemple :

- les Revues du SMSI : organisées et réalisées,
- les COPILs Sécurité : organisés et réalisés,
- la gestion des inventaires d'actif,
- la gestion des inventaires de l'ensemble des flux,
- la gestion des configurations,
- les revues de classification des applications : organisées et réalisées,
- les revues de classification des informations : organisées et réalisées,
- la sensibilisation à la sécurité,
- la revue des sites : organisée et réalisée,
- les incidents de sécurité : nombre ou taux,

- les revues de respect du plan d'audit : organisées et réalisées,
- le traitement des écarts : nombre ou taux,
- les revues des non conformités : organisées et réalisées,
- les revues des procédures d'exploitation : organisées et réalisées,
- les environnements de tests,
- les tests de restauration : nombre et taux,
- les revues des droits ou habilitations : organisées et réalisées,
- les revues des procédures de gestion des droits d'accès : organisées et réalisées,
- la revue du plan de reprise et les tests associés : organisées et réalisées,
- la supervision sécurité,
- le durcissement des systèmes,
- les revues de contrats : organisées et réalisées,
- les revues d'assurance : organisées et réalisées.

V.4. Exemples de tableaux de bord

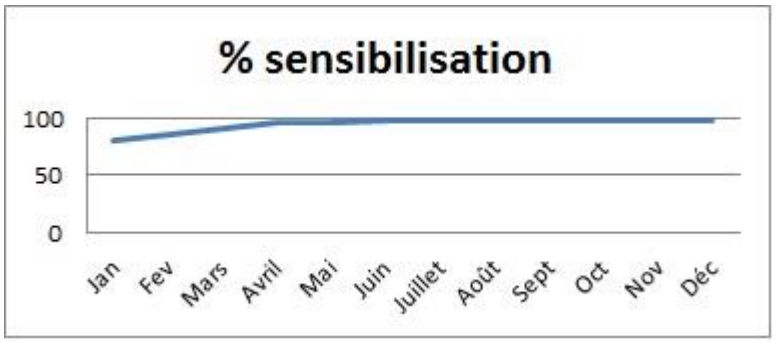
Avant toute chose, un tableau de bord permet de synthétiser et de suivre les événements de cyber sécurité du ou des systèmes d'information de l'organisme. C'est un outil permettant de visualiser le fonctionnement de l'organisation cyber sécurité, et de suivre 'ce qui s'y passe' afin d'engager les actions au travers d'un ou plusieurs plans d'actions afin d'atteindre les objectifs désirés.

Plusieurs tableaux de bord doivent être mis en place afin de satisfaire les différents objectifs des domaines concernés (pilotage (stratégique), performance, opérationnel). Chaque tableau de bord étant établi sur un périmètre donné pour des destinataires spécifiques.

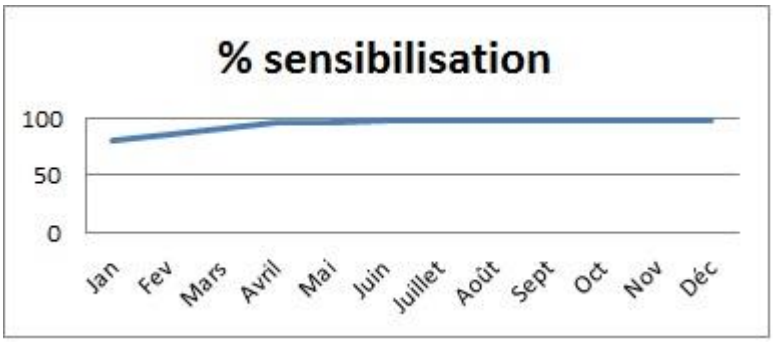
Un tableau de bord regroupe un ou plusieurs indicateurs permettant de suivre et de contrôler le chemin à parcourir pour atteindre les objectifs fixés en matière de cyber sécurité.

V.4.1. Sécurité liée aux ressources humaines

Rappel de l'objectif du paragraphe 7.2 de la norme ISO/CEI 27002:2013 : « S'assurer que les salariés et les contractants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités ».

<table>
<tr><th>Référence</th><th colspan="3">But de l'indicateur</th><th>Périmètre de l'indicateur</th></tr>
<tr><td></td><td colspan="3">Montrer l'efficacité du processus sensibilisation</td><td>L'Entreprise</td></tr>
<tr><th>Fréquence d'évaluation</th><th colspan="4">Moyen d'évaluation</th></tr>
<tr><td>Trimestrielle</td><td colspan="4">Pourcentage du personnel ayant répondu au quiz</td></tr>
<tr><th>Pilote</th><th>Fournisseur</th><th colspan="3">Méthode de calcul</th></tr>
<tr><td>XXX</td><td>XXX</td><td colspan="3">Nb de réponses obtenues au quiz / Nb de collaborateurs</td></tr>
<tr><th colspan="5">Objectifs</th></tr>
<tr><td colspan="2">Cible</td><td colspan="2">Cible court terme</td><td>Alerte</td></tr>
<tr><td>95 % collaborateurs ayant répondu</td><td>  </td><td>80 % collaborateurs ayant répondu</td><td>  </td><td>≤ 50 % collaborateurs ayant répondu</td><td>  </td></tr>
<tr><td colspan="2">Présentation
Graphique glissant sur un an</td><td colspan="4"> 
</td></tr>
</table>

<table>
<tr><th>Référence</th><th colspan="2">But de l'indicateur</th><th>Périmètre de l'indicateur</th></tr>
<tr><td></td><td colspan="2">Montrer l'efficacité du processus de prise en charge des nouveaux arrivants en matière de sécurité</td><td>L'entreprise</td></tr>
<tr><th>Fréquence d'évaluation</th><th colspan="3">Moyen d'évaluation</th></tr>
<tr><td>Trimestrielle</td><td colspan="3">Pourcentage, par site, du personnel entré dans l'organisme sensibilisé à la sécurité dans le mois suivant son arrivée.</td></tr>
<tr><th>Pilote</th><th>Fournisseur</th><th colspan="2">Méthode de calcul</th></tr>
<tr><td></td><td></td><td colspan="2">Pour chaque site du groupe :
❖ Nb de collaborateurs sensibilisés / Nb collaborateurs entrés dans le mois
❖ Fiches de présences signées</td></tr>
<tr><th colspan="4">Objectifs</th></tr>
<tr><td>Cible</td><td colspan="2">Cible court terme</td><td>Alerte</td></tr>
</table>

98%		80%		≤ 50%	
Présentation Graphique glissant sur un an					

V.4.2. Acquisition, développement et maintenance des SI

Rappel de la norme ISO 27002 : « Mettre en place des procédures pour contrôler l'installation de logiciel sur les systèmes d'exploitation ».

Référence	**But de l'indicateur**		**Périmètre de l'indicateur**	
	Vérifier la mise en place des correctifs de vulnérabilités		**Correctifs identifiés comme critiques, à installer sur les outils d'infogérance**	
Fréquence d'évaluation	**Moyen d'évaluation**			
Mensuelle	**Pourcentage des correctifs non installés sur les systèmes**			
Pilote	**Fournisseur**	**Méthode de calcul**		
		Sur la base de l'inventaire des correctifs à installer et de leur qualification en termes de criticité : **Nombre de correctifs non installés / Nombre de correctifs à installer**		
Objectifs				
Cible		Cible court terme	Alerte	
0%		10%		>25%	

V.4.3. Autres propositions de tableau de bord

Enfin, voici quelques autres propositions de tableaux de bord :

- suivi des accès wifi,
- suivi des accès de télémaintenance,
- suivi des incidents de cyber sécurité dans une zone géographique définie,
- suivi des environnements de production,
- suivi des environnements d'un projet défini,

- suivi de la disponibilité du SIE,
- suivi de la disponibilité du SII,
- suivi de la disponibilité d'une application définie ou d'un système et ou d'un sous-système,
- etc.

VI. Conclusion

Le premier guide publié en mai 2014[13] visait à aider les RSSI à sensibiliser leur Direction au besoin de mettre en œuvre un processus de gestion des vulnérabilités au sein de leur organisme.

Ce second livret se veut plus pratique, fournissant un guide complet d'implémentation du processus et son intégration avec les autres processus et parties-prenantes.

Le cœur de ce document (chapitre IV sur les « processus essentiels ») détaille les étapes majeures de la gestion des vulnérabilités, de l'inventaire des valeurs de l'organisme jusqu'au reporting.

L'automatisation de ce processus – par nature cyclique – et la visibilité que vous pourrez apporter à l'état de la sécurité et son évolution garantiront l'adhésion de l'ensemble de l'organisme.

Ce document s'appuie naturellement sur des références en matière de sécurité informatique dont la lecture sera complémentaire et indispensable : la famille ISO/IEC 270xx, les bonnes pratiques ITIL et CVSS entre autres. Ces lectures devront être complétées d'une veille et documentation régulières telles que préconisées au chapitre IV.2.

[13] http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2014-Gestion-vulnerabilites-tome-1.pdf

I. Annexes

I.1. Glossaire

ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CAB	*Change Advisory Board*, Comité d'Approbation des Changements
CERT	*Computer Emergency Response Team*, Centre d'alerte et de réaction face aux attaques informatiques
CLUSIF	Club de la Sécurité de l'Information Français
CMDB	*Configuration Management DataBase*, base de données de la gestion des configurations
COPIL	Comité de Pilotage
CVE	*Common Vulnerabilities and Exposures*, dictionnaire des informations publiques relatives aux vulnérabilités de sécurité
CVSS	*Common Vulnerability Scoring System*, système de notation commune de vulnérabilité
DAST	*Dynamic Application Security Testing*, test de sécurité applicative dynamique
DSI	Direction des Systèmes d'Information
HDS	Hébergement des Données de Santé
IaaS	*Infrastructure as a Service*, infrastructure en tant que service
ITAM	*Information Technology Asset Management*, gestion des actifs informatiques
ITIL	*Information Technology Infrastructure Library*, bibliothèque pour l'infrastructure des technologies de l'information
ITSM	*Information Technology Service Management*, gestion des services informatiques
KPI	*Key Performance Indicator*, indicateur clé de performance
KSI	*Key Security Indicator*, indicateur clé de sécurité
LPM	Loi de Programmation Militaire
MSSP	*Managed Security Service Provider*, fournisseur de service de sécurité
OIV	Opérateur d'importance vitale
OWASP	*Open Web Application Security Project*, communauté travaillant sur la sécurité des applications Web
PaaS	*Platform as a Service*, plateforme en tant que service
PCA	Plan de Continuité d'Activité

PCI DSS	*Payment Card Industry Data Security Standard*, standard de sécurité des données pour les industries de carte de paiement
PDCA	*Plan Do Check Act*, planifier développer/réaliser contrôler ajuster.
PRA	Plan de Reprise d'Activité
PSSI	Politique de Sécurité des Systèmes d'Information
RACI	Matrice de responsabilités (*Responsible, Accountable, Consulted, Informed*)
RFP	*Request For Proposal*, appel d'offres
RGS	Référentiel Général de la Sécurité publié par l'ANSSI
RSSI	Responsable de la Sécurité des Systèmes d'Information
SaaS	*Software as a Service*, logiciel en tant que service
SAST	*Static Application Security Testing*, test de sécurité applicative statique
SCADA	*Supervisory Control And Data Acquisition*, système de contrôle et d'acquisition de données
SIE	Système d'Information d'Entreprise
SIEM	*Security Information and Event Management*, gestion des informations et évènements de sécurité
SII	Système d'Information Industriel
SLA	*Service Level Agreement*, contrat de qualité de service
SMSI	Système de Management de la Sécurité de l'Information
SOC	*Security Operations Center*, centre de surveillance de la sécurité
SSI	Sécurité des Systèmes d'Information
TNR	Tests de Non Régression

I.2. FAQ

Q : Comment trouver mes vulnérabilités ?

R : En combinant un inventaire/scan automatisé (outillé) et un audit manuel périodique, comme précisé dans le chapitre 0.

Q : Pourquoi identifier le propriétaire des machines / des données ?

R : L'identification des propriétaires est cruciale pour l'évaluation des risques. Au-delà des postes de travail, les applications doivent être assignées à leur propriétaire. Reportez-vous au chapitre IV.3.3 pour plus d'informations.

Q : Comment m'assurer que le processus de mise à jour des logiciels fonctionne bien ?

R : Ce processus est généralement outillé et fournit une console centrale de surveillance de l'état du parc et de l'installation des correctifs. Cet outil doit naturellement couvrir tous les actifs de l'entreprise, que ce soit des OS Windows ou Unix/Linux, des logiciels propriétaires type Microsoft aux autres logiciels ou paquets installables sur ces systèmes. Dans tous les cas, la revue des correctifs installés sur les machines permettra de corroborer l'information obtenue par cet outil de gestion de parc.

Q : Comment inventorier toutes les machines de mon environnement ?

R : Le plus simple est d'utiliser un logiciel d'inventaire automatique en le laissant découvrir le plus largement possible toutes les machines, sans le restreindre selon les plages d'adresse présupposées de la cartographie réseau. Attention toutefois aux environnements industriels (SCADA) où les inventaires actifs sont proscrits ! Pour plus d'informations, veuillez vous référer au chapitre IV.3.

Q : Comment communiquer sur l'état de ma sécurité ?

R : La communication se fait essentiellement avec des rapports de sécurité dont la forme variera selon son destinataire, d'un listing détaillé et technique pour les opérationnels, à une vue consolidée macroscopique au top management. Pour plus d'informations, veuillez vous référer au chapitre V (pilotage et reporting).

Q : Quels acteurs impliquer dans la gestion de mes vulnérabilités ?

R : En dehors de la direction de la sécurité, il faut impliquer les opérationnels de la sécurité (exploitants, administrateurs, développeurs, etc.), les parties-prenantes du processus de changement, la direction des risques voire la direction juridique, et le management bien entendu. Pour plus d'informations, veuillez vous référer au chapitre II.5.

Q : Quels sont le coût et la durée de mise en place d'un programme de gestion de vulnérabilités ?

R : Le coût et la durée varient essentiellement selon la taille du parc à gérer et la diversité des technologies employées, ainsi que la criticité des services supervisés (SII *vs* SIE).

Q : Quel est le ROI de la gestion de vulnérabilités ?

R : L'approche basée uniquement sur le ROI n'est pas pertinente car l'investissement n'a pas une vocation opérationnelle directe. Il faut raisonner en gestion de risques, impact de rupture informatique *vs* coût de mise en œuvre.

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
France
✆ +33 1 53 25 08 80
clusif@clusif.fr

Téléchargez toutes les productions du CLUSIF sur
www.clusif.fr